Számmelmélet

Freud, Róbert
Gyarmati, Edit
Tartalom

BEVEZETÉS ........................................................................................................ vii

1. SZÁMELMELETI ALAPFOGALMA ................................................................................. 1
   1.1 Oszthatóság ........................................................................................................... 1
   1.2 Maradéos osztás .................................................................................................... 5
   1.3 Legnagyobb közös osztó ....................................................................................... 9
   1.4 Felbontatlan szám és primszámlak .................................................................... 15
   1.5 A számmelélet alaptétele .................................................................................... 18
   1.6 Kanonikus alak ...................................................................................................... 22

2. KONGRUENCIÁK ........................................................................................................ 32
   2.1 Elemi tulajdonságok ............................................................................................ 32
   2.2 Maradéosztályok és maradékrendszerek ................................................................ 36
   2.3 Az Euler-féle \( \varphi \) -függvény .............................................................................. 42
   2.4 Euler–Fermat-tétel ............................................................................................... 46
   2.5 Lineáris kongruenciák ......................................................................................... 48
   2.6 Szimultán kongruenciarendszerek .................................................................... 54
   2.7 Wilson-tétel ......................................................................................................... 63
   2.8 Műveletek maradéosztályokkal ......................................................................... 65

3. MAGASABB FOKÚ KONGRUENCIÁK ...................................................................... 70
   3.1 Megoldásszám és redukció .................................................................................. 70
   3.2 Rend ..................................................................................................................... 73
   3.3 Primitív gyök ....................................................................................................... 77
   3.4 Diszkrit logaritmus (index) ................................................................................ 84
   3.5 Binom kongruenciák ............................................................................................ 86
   3.6 Chevalley-tétel, König–Rados-tétel ................................................................... 90
   3.7 Prímhatvány modulusú kongruenciák .................................................................. 95

4. LEGENDRE- ÉS JACOBI-SZIMBÓLUM ..................................................................... 100
   4.1 Másodfokú kongruenciák .................................................................................... 100
   4.2 Kvadratikus reciprocitás ..................................................................................... 104
   4.3 Jacobi-szimbólum ............................................................................................... 109

5. PRÍMSZÁMOK .......................................................................................................... 113
   5.1 Klasszikus problémák ......................................................................................... 113
   5.2 Fermat- és Mersemme-prímek .......................................................................... 117
   5.3 Prímzárók számzami sorozatokban ..................................................................... 125
   5.4 Becslések \( \pi(x) \) -re ............................................................................................... 129
   5.5 Hézag a szomszédos prímek között .................................................................... 135
   5.6 A prímek reciprokösszege ............................................................................... 141
   5.7 Prímtesztek ....................................................................................................... 150
   5.8 Titkosírás ......................................................................................................... 161

6. SZÁMELMELETI FÜGGVÉNYEK ......................................................................... 167
   6.1 Multiplikativitás, additivitás .............................................................................. 167
   6.2 Nevezetes függvények ....................................................................................... 172
   6.3 Tökéletes számok ............................................................................................... 179
   6.4 A \( d(n) \) függvény vizsgálata ................................................................................. 181
   6.5 Összegzási és megfordítási függvény ................................................................. 190
   6.6 Konvolúció ....................................................................................................... 194
   6.7 Átlagérték ........................................................................................................ 200
   6.8 Additív függvények karakterizációja ................................................................. 212

7. DIOFANTIKUS EGYENLETEK .............................................................................. 216
   7.1 Lineáris diofantikus egyenlet ........................................................................... 216
   7.2 Pitagoraszi számhármashasok ........................................................................... 220
   7.3 Néhány elemi módszer ...................................................................................... 223
   7.4 Gauss-egészek .................................................................................................. 228
   7.5 Számok előállítása négyzetösszegként ............................................................... 235
   7.6 A Waring-problémakör .................................................................................... 242
## Számelmélet

7.7 A Fermat-sejtés ................................................................. 246
7.8 Pell-egyenlet ........................................................................ 257
7.9 Partíciók ................................................................. 262

8. DIOFANTIUS APPROXIMÁCIÓ .................................................... 269
  8.1 Irracionális szám approximációja ........................................... 269
  8.2 Minkowski-tétel ................................................................. 276
  8.3 Lánctörtek ........................................................................ 281
  8.4 A törtrészek eloszlása .......................................................... 287

9. ALGEBRAI ÉS TRANSCZENDENS SZÁMOK ................................ 292
  9.1 Algebrai szám, transzcendens szám ........................................ 292
  9.2 Minimálpolinom és fokszám ...................................................... 295
  9.3 Műveletek algebrai számokkal .................................................. 298
  9.4 Algebrai számok approximációja ............................................ 302
  9.5 Az $e$ transzcendens szám ...................................................... 308
  9.6 Algebrai egész .................................................................... 313

10. ALGEBRAI SZÁMTESTEK .......................................................... 317
   10.1 Testbővítés .................................................................. 317
   10.2 Egyszerű algebrai bővítés ................................................... 320
   10.3 Másodfokú bővítések .......................................................... 326
   10.4 Norma ................................................................. 339
   10.5 Egész bizis .................................................................. 343

11. IDEÁLOK ................................................................. 350
   11.1 Ideál ................................................................. 350
   11.2 Elemi számelméleti kapcsolatok ........................................... 356
   11.3 Alaptételes gyűrű, főideálgyűrű, euklideszi gyűrű ................. 359
   11.4 Ideálok oszthatósága .......................................................... 366
   11.5 Dedekind-gyűrű ................................................................. 373
   11.6 Osztályzsám ................................................................. 383

12. KOMBINATORIKUS SZÁMÉLMÉLET ....................................... 388
   12.1 Csupa különböző összeg ...................................................... 388
   12.2 Sidon-sorozatok ................................................................. 396
   12.3 Összeghalmazok ................................................................. 405
   12.4 Schur tétele ................................................................. 415
   12.5 Fedőrendszerék ................................................................. 420
   12.6 Additív komplementumok .................................................... 423

13. EREDMÉNYEK ÉS ÚTMUTATÁSOK ........................................ 431
   13.1 Számelméleti alapfogalmak .................................................. 431
      13.1.1 ................................................................. 431
      13.1.2 ................................................................. 433
      13.1.3 ................................................................. 435
      13.1.4 ................................................................. 437
      13.1.5 ................................................................. 438
      13.1.6 ................................................................. 438
   13.2 Kongruenciák ................................................................. 442
      13.2.1 ................................................................. 442
      13.2.2 ................................................................. 443
      13.2.3 ................................................................. 445
      13.2.4 ................................................................. 447
      13.2.5 ................................................................. 449
      13.2.6 ................................................................. 449
      13.2.7 ................................................................. 451
      13.2.8 ................................................................. 453
   13.3 Magasabb fokú kongruenciák ............................................ 455
      13.3.1 ................................................................. 455
      13.3.2 ................................................................. 456
      13.3.3 ................................................................. 459
      13.3.4 ................................................................. 461
      13.3.5 ................................................................. 462
BEVEZETÉS

A könyv szándékaink szerint a következő funkciók betöltésére készült:

(A) Elméleti tankönyv a magyarországi egyetemeken és főiskolákon folyó számelmélet-oktatáshoz, elsősorban az egyetemek matematikus, alkalmazott matematikus, matematika tanári és informatika szakos hallgatói, valamint a tanárképző főiskolák matematika tanári szakos hallgatói részére.

(B) Számelmélet feladatgyűjtemény, szintén elsősorban a fenti hallgatói rétegek számára.

(C) A kötelező és fakultatív anyagon túlmenően a számelmélet egyes fejezetet, problémaköreit részletesen tárgyaló „szakkönyv”, az ilyen témából szakadolgozatot készítők és más, a terület iránt mélyebben érdeklődők számára.

(D) A(z elemi) számelmélet legfontosabb területeit áttekintő „közikönyv” matematikusok és matematikatanároknak részére.

A könyv felépítése

A fenti célok minél jobb megvalósítása érdekében a tárgyalást teljesen az alapoknál kezdjük és az első két fejezetben csak a középiskolás anyagra támaszkodunk. Ennél a résznél elemi és kevésbé absztrakt segédeszközöket használunk, és a túlzottan tömör indoklások helyett inkább részletes magyarázatokat adunk, hogy a megértést a „kezdő” Olvasók számára is maximálisan megkönnyítsük. Úgyanakkor már itt is nagy súlyt helyezünk az anyag mélyebb összefüggéseit feltáró tételek, a „szép” és nehéz gondolatokat tartalmazó bizonyítások bemutatására.

A későbbi fejezetekben egyre mélyebbre hatolunk a különféle számelméleti témakörök tárgyalásában. Arra törekszünk, hogy a számelmélet rendkívül sokszínű problémavilágából (beleértve a rengeter regi, de még mindig megoldatlan problémát is) és az ezek kezelésére az évszázadok (sőt évezredek) alatt kidolgozott változatos módszerekből minél több, ne tudunk betekintést. Ahol lehet, bemutatjuk a számelmélet legújabb eredményeit és alkalmazásaikat is. Egyes részeknél felhasználjuk a matematika más területeinek tetejeit és módszereit is, elsősorban (klasszikus, lineáris és absztrakt) algebrát, analízist és kombinatorikát.

A könyv szerkezetét úgy alakítjuk ki, hogy az az egyes fejezetek egymásra épülését és az anyag rendszerezését minél jobban biztosítsa.

A könyv egészére jellemző, hogy a fogalmakat, állításokat stb. a formális megfogalmazáson túlmenően is alaposan „körbejárjuk”, mindig példákkal illusztráljuk, megpróbáljuk a „lényegi” vonásait megragadni, bemutatjuk a korábbi anyaghoz való kapcsolódást, felhívjuk a figyelmet az esetleges baktatókrá, elemezzük, mi indokolja az adott fogalom bevezetését stb. Nagy súlyt helyezünk arra, hogy lehetőleg a konkrétből kiindulva haladjunk az általános felé. Igyekszünk a számelméletnek a matematika más területeivel való szoros és sokszínű kapcsolatának minél átfogóbben érzelkeltetni.

Feladatok

A fejezeteket alkotó minden egyes pont után feladatok következnek. A feladatok részben az aktuális fogalmak, tételek, módszerek stb. megértését ellenőrizik és ezek elmélyítését segítik elő, részben újabb példákat, összefüggéseket és alkalmazásokat mutatnak be, részben pedig az adott témakörhöz kapcsolódó egyéb problémákat vizsgálnak. Gyakran szerepelnek feladatnak „álcazott” tételek is, amelyek az anyag részletesen nem tárgyalt további érdekes vonatkozásaira, távolabbi összefüggéseire hivják fel a figyelmet.

Ennek megfelelően a feladatok mennyisége és nehézsége igen tág határoko között mozog, az éppen sorra kerülő anyag témájától, terjedelmétől és mélységétől függően. A(z általunk) nehezebben ítélt
feladatokat csillaggal, a kiemelkedően nehéznek tartott feladatokat pedig két csillaggal jelezzük. (Természetesen egy feladat nehézsége mindig relativ; a megoldó képességeitől, érdeklődésétől és általános előismeretétől eltekintve jelentősen függhet — többek között — a korábban megoldott feladatoktól is.)

A feladatok eredményét és/vagy a megoldáshoz vezető (egyik lehetséges) útmutatást — minimális számú kivételtől eltekintve — az „Eredmények és útmutatások” c. fejezetben közzéjük. Néhány (elsősorban nehezebb) feladathoz részletes megoldást is adunk a „Megoldások” c. fejezetben, ezeket a feladatokat a kitűzésnél M betűvel jelöltük meg.

Az Olvasónak azt tanácsoljuk, hogy lehetőleg csak akkor nézze meg a feladatokhoz adott útmutatást vagy megoldást, ha semmiképpen sem boldogul a feladattal. Térjen inkább vissza többször is ugyanarra a problémára, esetleg oldja meg előbb valamelyik speciális esetet.

Fontos, hogy próbálja meg felderíteni a feladat „mondanivalóját”, hátterét, a matematikai környezetben elfoglalt helyét és szerepét. Nagyon hasznos az általánosítás vagy újabb problémák önálló felvetése (még akkor is, ha ezeket nem sikerül megoldani).

Az egyes fejezetek rövid ismertetése

Az első két fejezet bevezető jellegű, ezekben az egész számok oszthatóságával, a legnagyobb közös osztóval, a számmá admélet alapfeltételével (azaz az egyértelmű prímfelbontással), illetve a kongruenciákkal kapcsolatos elemi ismereteket tárgyaljuk. Ezek biztos elsajátítása elengedhetetlen a további fejezetek tanulmányozásához.

A 3. és 4. fejezetben a kongruenciák elméletét építjük tovább.

Az 5. fejezet témája a prímszámok, amelyek a matematika egyik legegyszerűbbően definiált, ugyanakkor talán legtitkosabb halmazát jelentik. Ebben a fejezetben Euklidész több mint 2000 éves tételei, valamint azóta is megoldatlan problémái és az utóbbi évtizedek egyik matematikai szenzációját jelentő, a gyors primestesztelésen és az ehhez képest összemérhetetlenül lassú primfaktorizáción alapuló nyílvános jelkulcsú titkosítások egyaránt helyet kapnak. Ebben a fejezetben a korábbi számmáadméleti ismeretek felhasználásán túl számos helyen intenzíven támaszkodunk az elemi analízis eredményeire és módszereire is.

A 6. fejezet a számmáadméleti függvényekkel foglalkozik. Az egyes fontos függvények bemutatása mellett számos általános konstruktión és alkalmazást tárgyalunk.


A 8. fejezet az alkalmazások szempontjából fontos diofantikus approximációval foglalkozik. Röviden bemutatjuk az approximációknak a geometriai számmáadmélettel, illetve a lánctörtekkel való kapcsolatát is.

A(z első kiadáshoz képest teljesen új) 12. fejezet néhány érdekes kombinatorikus számmelméleti problémát mutat be. Ezek nemelyike akár középiskolai szakkörön is tárgyalható, más esetben viszont a megoldáshoz a matematika más ágaihoz is mélyebb módszereit is igénybe kell venni. Reméljük, hogy a válókatásunkkal azt is sikerül érzékeltenünk, milyen nagy szerepet játszottak a témakör fejlődésében Erdős Pál igalmazás problémafeleltetései és szellemes bizonyításai.

A könyvben sok helyen kitérünk érdekes matematikatörténeti vonatkozásokra is, és ilyen célt szolgál a könyv végén található „Történeti névtár” is.

Amint a fenti leírásból is kiderül, a számmelmélet egyes területei ezer szállal kötődnek egymáshoz és más matematikai ágakhoz egyaránt. Ezért komoly és nem is teljesen áthidalható nehézséget jelent az a kettősség, hogy egyrészt az egyes témakörök tárgyalásánál jól érzékelhető legyen ez a szoros kapcsolat, másrészt az adott témakört bemutató fejezet minél inkább önmagában is érthető és teljes legyen. Igyekezünk olyan egysélyt kialakítani, hogy annak, aki a könyvet folyamatosan dolgozza fel, fokozatosan, összefüggéseiben és minél teljesebben találjon fel egy probléma- és gondolatgazdag matematikai diszciplína, ugyanakkor a csak néhány fejezetből „csipegegő” olvasónak is lehetősége nyiljék érdekes, tartalmas és hasznos ismeretek elsajátítására.

Technikai tudnivalók

Az egyes fejezetek új. pontokra tagolódnak. A definíciókat, a tételeket és a feladatokat $k_{11}$ típusú módon számoztuk, ahol $k$ a fejezetet, $n$ ezen belül a pontot és $n$ a ponton belüli sorszámot jelenti. A definíciók és a tételek „közös listá” futnak, tehát pl. a D 6.2.1 Definíció után a T 6.2.2 Tétel következik. Az illusztrációs példák, képletek stb. (simma, egy számnál történő) számozása pontonként újrakezdődik. A definíciók, illetve a tételek megfogalmazásának a végén $\bullet$ áll, a bizonyítások befejezését pedig $\blacksquare$ jelzi.

A jelölések, fogalmak, tételek visszakeresését megkönnyítheti a könyv végén található „Tárgymutató”, amelyet igyekeztünk nagyon részletesen összeállítani.

Néhány általános jelölés: Megkülönböztetjük a (valós) számok alsó és felső egészrészét, és ezeket $\lfloor \cdot \rfloor$, illetve $\lceil \cdot \rceil$ jelölő, így pl. $\lfloor \pi \rfloor = 3$, $\lceil \pi \rceil = 4$, a $\lfloor \cdot \rfloor$ jelölést nem használjuk. A számok tört részét $\{ \cdot \}$ jelöli, tehát $\{c\} = c - \lfloor c \rfloor$. Az oszthatóságra, a legnagyobb közös osztóra és a legkisebb közös többszörössére a szokásos jelöléseket használjuk, tehát pl. $7 | 42, \ (9,13) = 3, \ [9, 15] = 45$. Á $\lfloor \cdot \rfloor$ szöglletes zárójel legkisebb közös többszörössz, zárt intervallumot vagy egyszerűen zárójelet jelöl (ez utóbbi különösen a 11. fejezetben jellemző, ahol a $\langle \cdot \rangle$ kerek zárójel ideális jelent; a megkülönböztetés érdekében itt a legnagyobb közös osztóra is az $\lfloor \cdot \rfloor$ jelölést használjuk).

A polinomok és függvények jelölésére többnyire az (argumentum nélküli) $f, \ g$ stb. jelölés szerepel, de helyenként az $f(x), \ g(x)$ stb. írásmód is előfordul. A polinomok fokszámát (az angol degree szó megfelelően) „deg”-gel jelöljük, tehát pl. $\deg(x^3 + x) = 3$. A szokásos módon $\mathbb{Q}, \mathbb{R}$, illetve $\mathbb{C}$ rendre a racionális, a valós, illetve a komplex számok testét, $\mathbb{Z}, \mathbb{Z}_m$ , illetve $\mathbb{T}[x]$ pedig az egész számok, a modulo $\mod m$ maradékosztályok, illetve a $\mathbb{T}$ feletti polinomok gyűrűjét jelenti.

A testbővítéseknek $\mathbb{Q}(d), \mathbb{E}(d)$ a racionális test $d$ -val való egyszerű bővítését, illetve (algebrai $d$ esetén) az ebben található algebrai egészek gyűrűjét jelenti, $\mathbb{E}$ -vel pedig az összes algebrai egész gyűrűjét jelöljük. A $\mathbb{P}$ betűt szinte kizárólag a (povitív) primszámok jelölésére tartjuk fenn. A sima (index nélküli) log jelölés a természetes ($\mathbb{N}$ alapú) logaritmust jelenti. A (véges vagy végtelen) szorzatok és összegek jelölésére gyakran használjuk a $\prod$ és $\sum$ jeleket, például

$$\prod_{i=-1}^{r} p_i^{\alpha_i}, \ \ \ \prod_{p \leq \alpha} p, \ \ \ \sum_{p} \frac{1}{p^2}$$
rendre a \(p_1^{e_1} \cdots p_k^{e_k}\) szorzatot, az \(n\) -nél nem nagyobb (pozitív) primszámok szorzatát, illetve a (pozitív) primszámok négyzetének reciprokösszegét jelenti.

Megemlékezés

A könyvet Turán Pál, Erdős Pál és Gallai Tibor akadémikusok emlékének ajánljuk (akik egyébként egymás jó barátaik és közeli munkatársai voltak).

Mindketten abban a szerencsés helyzetben voltunk, hogy szoros kapcsolatban állhattunk a huszadik századi számelmélet két kiemelkedő egyéniségeivel, Turán Pállal és Erdős Pállal.

Mindketten Turán Pál legendás számelmélet szemináriumain nevelkedtünk, ott köstoltunk bele először igazán abba, hogy hogyan kell egy-egy probléma lényeges elemeit kibontani, feldolgozni és mindezt mások számára megvilágítani. Turán Páltól tanultuk, hogy a látszólag távoli területek összekapcsolása gyakran új, hatékony megközelítési módot eredményez.

Könyvünk előzményeihez tartozik az a (feladatokat nem tartalmazó) országos Számelmélet jegyzet, amelyet 35 évvel ezelőtt Gyarmati Edit több más forrásunka mellett Turán Pál előadásainak felhasználásával írt. Az azóta eltelt idő alatt tartott előadásaink tapasztalatai, a hallgatók előismeretének gyarapodása (pl. lineáris algebra) és az időközben született új eredmények azt indokolták, hogy a már régóta aktuális felfrissítés és átdolgozás helyett egy új könyvet írjunk. Könyvünk szelleme és felépítése természetesen több rokon vonást mutat az említett jegyzettel.

Mindkettőnkre nagy hatással volt Erdős Pál matematikai és emberi nagysága, ahogyan a „szép” matematikai problémák és bizonyítások iránti szenvedélyes szeretetét másokkal megosztotta, ugyanolyan természetes közvetlenséggel beszélve ezekről (és sok minden másról is) komoly tudósok és kezdő érdeklődők előtt egyaránt. Freud Róbert sok közös matematikázás élményét és szakmai fejlődésének jelentős részét is Erdős Pálnak köszönheti.

Gyarmati Edit pályaválasztásában meghatározó szerepet játszott felépítettlen középiskolai tanára, Gallai Tibor, a gráfelmélet világhírű kutatója. Gallai Tibor zseniális tanáregyéniség volt, akinek csodálatos gimnáziumi órai és egyetemi előadásai a legjobb hallgatókat sikerrel indították el a matematikai kutatás útján, miközben a gyengébb diákok számára is a megértés és az alkotás élményét nyújtották.

Köszönetnyilvánítás

Nagy köszönettel tartozunk azért a munkáért, amelyet a lektorok, Ruzsa Imre (12. fejezet), Sárközy András (1–12. fejezet) és Szalay Mihály (1–11. fejezet) végeztek. Mindhárman rendkívüli alapossággal nézték át a kéziratot, és igen sok általános, konkrét és stilisztikus észrevételt tettek, amelyeket szinte kivétel nélkül figyelmelembe vettünk. Sárközy András koncepcionális megjegyzéseinek nyomán több helyen egységesebb fogalomalkotást, jobban harmonizáló felépítést és további eredményekre történő utalásokat tudtunk megvalósítani. Szalay Mihály a legarább részletekbe menően ellenőrizte a kéziratot, és igen gondosan végigszóolta azokat a feladatokat is, amelyek részletes megoldását nem adtuk meg; figyelmét nem kerülete el a legarább pontatlanság sem, és konkrétan megfogalmazott módosítási javaslatait sok kisebb-nagyobb hiba, egyenletenség kijavítását tettek lehetővé. Ruzsa Imre az általa átnézett 12. fejezethez írt hibákat és eredményeket.

Nagyon köszönjük a Nemzeti Tankönyvkiadó munkatársainak, Palojtay Mária fölszerkesztőnek és Balassa Zsófianának, az első kiadás szerkesztőjének kiváló munkáját és segítő együttműködését.

A könyvben a szerzők (és a lektorok) minden igyekezette ellenére bizonyára akadhatnak hibák és hiányosságok. Bárkitől köszönettel fogadjuk az ezzel kapcsolatos észrevételeket.

Budapest, 2006. február
Freud Róbert (freud@cs.elte.hu [mailto:freud@cs.elte.hu]), Gyarmati Edit (gyedit@cs.elte.hu [mailto:gyedit@cs.elte.hu])

ELTE TTK Matematikai Intézet, Algebra és Szármelmélet Tanszék

1117 Budapest, Pázmány Péter sétány 1c
1. fejezet - SZÁMELMÉLETI ALAPFOGALMAK

Ebben a fejezetben az egész számok oszthatóságával kapcsolatos néhány alapvető fogalmat, tételeket és módszert tekintünk át. A fogalmak bevezetésénél legtöbbször csak általános oszthatósági vonatkozásokra építünk, és minél kevesebbet támaszkodunk az egész számok speciális tulajdonságaira. A páros számok és más példák segítségével igyekszünk rámutatni arra is, hogy az egész számoknál „megszokott” tételek egy része, köztük az egyértelmű prímfelbontás (más néven a számmelmélet alaptétele) egyáltalán nem magától értetődő.

A felépítés során úgy jutunk el a számmelmélet alaptételéhez, hogy a maradékos osztásból kiindulva az euklideszi algoritmus segítségével megmutatjuk a legnagyobb közös osztó „kitüntetett” tulajdonságát, majd ennek alapján igazoljuk, hogy az egész számok körében a felbontatlan számok és a prímszámok egybeesnek. Az alaptételre egy, a maradékos osztástól független, közvetlen indukciós bizonyítást is adunk, majd az alaptétel néhány fontos következményét tárgyaljuk.

1.1 Oszthatóság

Ha \( a \) és \( b \) racionális számok és \( b \neq 0 \), akkor \( a \) -t \( b \)-vel elosztva ismét racionális számot kapunk. Hasonló állítás az egész számok körében nem érvényes. Ezért érdemes bevezetni a következő definíciót:

1.1.1 Definíció. \( D \, 1.1.1 \)

A \( b \) egész számot az \( a \) egész szám osztójának nevezzük, ha létezik olyan \( q \) egész szám, amelyre \( a = bq \). ♦

Jelölés: \( b \mid a \). Ugyanez a kapcsolatot fejezi ki más szavakkal, hogy az \( a \) osztható \( b \)-vel, illetve az \( a \) többszöröse a \( b \)-nek. Ha nem létezik olyan \( q \) egész, amelyre \( a = bq \), akkor a \( b \) nem osztója \( a \)-nak, ennek jelölése: \( b \nmid a \).

A továbbiakban, ha egyéb kikötést nem teszünk, akkor számon mindig egész számot értünk.

A 0 minden számmal osztható (a 0-val is!), hiszen bármely \( b \)-re \( 0 = b \cdot 0 \). A másik „végletet” azok a számok alkotják, amelyek minden számnak osztói:

1.1.2 Definíció. \( D \, 1.1.2 \)

Ha egy szám minden számnak osztója, akkor egységnek nevezzük. ♦

1.1.3 Tétel. \( T \, 1.1.3 \)

Az egész számok körében két egység van, az \( 1 \) és \( a - 1 \). ♦

Bizonyítás: Az \( 1 \) és \( a - 1 \) valóban egységek: bármely \( e \) -ra \( \pm 1 \mid e \), hiszen \( a = (\pm 1)\cdot(e) \).

Megfordítva, ha \( e \) egység, akkor az \( e \) az 1-nek is osztója, azaz alkalmas \( q \)-val \( 1 = ez \). Mivel \( |e| \geq 1 \) és \( |q| \geq 1 \), így csak \( |e| = 1 \), azaz \( e = \pm 1 \) lehetséges. ♦

Megjegyzés: Az oszthatóságot az egészektől különböző számkörökben (sőt általánosabban bármely integritási tartományban, lásd az 1.1.23 feladatot [5]) be lehet vezetni. Tekintsük példaként a
páros számokat. Itt $b \mid a$ azt jelenti, hogy létezik olyan $q$ páros szám, amelyre $a = bq$. Ennek megfelelően ít $2 \div 20$, de $2 \div 10$, sőt a 10-nek egyáltalán nincs is osztója. Ebből az is következik, hogy a páros számok körében egyáltalán nincsenek egységek. Ugyanakkor a $c \div \sqrt{2}$ alakú (speciális valós) számok körében, ahol $c$ és $d$ tetszőleges egészek, végigten sok egység található (lásd az 1.1.22 feladatot [4]). Mindez azt jelenti, hogy az egységek változatos képet mutathatnak, és általában nem (csak) az előjelbeli eltéréssel hozhatók kapcsolatba, mint ahogy azt az T 1.1.3 Tétel esetleg tévesen sugallhatná.

**1.1.4 Tétel.**  

Ha $\varepsilon$ és $\delta$ egységek és $b \mid a$, akkor $\varepsilon b \mid \delta a$ is teljesül. ♦

*Bizonyítás:* Az $\varepsilon$ az 1-nek is osztója, azaz alcalkas $\tau$-rel $1 = \varepsilon \tau$. Ha $a = b\alpha$, akkor $\delta a = (\varepsilon b)(\delta \alpha)$, tehát valóban $\varepsilon b \mid \delta a$. ■

Az T 1.1.4 Tétel azt fejezi ki, hogy egy szám és az egységszerű oszthatósági szempontból teljesen azonosan viselkednek; az egységek az oszthatóság szempontjából „nem számítanak”. Ennek alapján nem jelent (majd) megszorítást, ha az egész számok oszthatósági vizsgálatát leküszköztjük a nemnegatív egészekre, sőt (a 0 speciális szerepének tisztázása után) csak a pozitív egészekkel foglalkozunk.

A következő tételben az egész számok oszthatóságának néhány egyszerű, de fontos tulajdonságát foglaljuk össze.

**1.1.5 Tétel.**  

(i) Minden $a$-ra $a \mid a$.

(ii) Ha $c \mid b$ és $b \mid e$, akkor $c \mid a$.

(iii) Az $a \mid b$ és $b \mid a$ oszthatóságok egyszerre akkor és csak akkor teljesülnek, ha az $a$ a $b$-nek egységszerese.

(iv) Ha $c \mid a$ és $c \mid b$, akkor $c \mid a + b$, $c \mid a - b$, tetszőleges (egész) $k$-ra $c \mid ka$, és tetszőleges (egész) $s$-re $c \mid s a + s b$. ♦

Az (i)-(iii) tulajdonságok rendre azt fejezik ki, hogy az egész számok oszthatósága reflexív és tranzitív, de nem szimmetrikus reláció. A (iv)-beli állítások közül a legtöbbször az első hármat alkalmazzuk, ezek egyébként valamennyi az utolsónak speciális esetek ( $\tau = 1$ ; $\tau = 1$ , $s = -1$ ; illetve $\tau = k$ , $s = 0$ ).

*Bizonyítás:* Csak (iii)-at igazoljuk, a többi könnyen bizonyítható az oszthatóság definíciójából.

Ha $a = \varepsilon b$, ahol $\varepsilon$ egység, akkor $b \mid a$ azonnal adódik. Továbbá $1 = \varepsilon$ miatt $\tau a = \tau b$, tehát $a \mid b$ is teljesül.

Megfordítva, ha $a \mid b$ és $b \mid a$, azaz alcalkas $q$ és $s$ egészekkel $b = aq \mid a = bs$, akkor innen $b = b(qs)$. Ha $b = 0$, akkor szükségképpen $a = 0$, tehát $a = \varepsilon b$. Ha $b \neq 0$, akkor $qs = 1$, azaz $s$ (és $q$ is) egység, tehát ekkor is $a = \varepsilon b$. ■

**Feladatok**

(Ha más kikötést nem teszünk, a feladatokban értelemszerűen egész számok szerepelnek, a hatványkitevők pedig nemnegatív egészek.)
1.1.1 Írjunk le egy háromjegyű számot kétszer egymás mellé. Mutassuk meg, hogy az így kapott hatjegyű szám osztható 91-gyel.

1.1.2 Lássuk be, hogy két páratlan szám négyzetétének a különbsége mindig osztható 8-cal.

1.1.3 Tegyük fel, hogy az \( (a,b,c) \) számjegyekből álló \( abc \) háromjegyű szám osztható 37-tel. Igazoljuk, hogy ekkor a \( bca \) szám is osztható 37-tel.

1.1.4 Bizonyítsuk be, hogy ha \( 5a + 9b \) osztható 23-mal, akkor \( 3a + 10b \) is osztható 23-mal.

1.1.5 Melyek igazak az alábbi állítások közül?

(a) \( c \mid a + b \longrightarrow c \mid a, c \mid b \).

(b) \( c \mid a + b, c \mid a \longrightarrow c \mid b \).

(c) \( c \mid a + b, c \mid a - b \longrightarrow c \mid a, c \mid b \).

(d) \( c \mid 2a + 5b, c \mid 3a + 7b \longrightarrow c \mid a, c \mid b \).

(e) \( c \mid ab \longrightarrow c \mid a \) vagy \( c \mid b \).

(f) \( c \mid a, d \mid b \longrightarrow cd \mid ab \).

(g) \( c \mid a, d \mid a \longrightarrow cd \mid c \).

1.1.6 Igazoljuk az alábbi oszthatóságokat:

(i) \( a - b \mid a^n - b^n \);

(ii) \( a + b \mid a^{2k+1} + b^{2k+1} \);

(iii) \( a - b \mid a^{2k} - b^{2k} \).

1.1.7 Mely \( c \) egészekre lesz \( (c^3 - 3)/c(c^2 + 2) \) is egész szám?

1.1.8 Igazoljuk, hogy minden \( n \) természetes számról \( 133 \mid 11^{n+2} - 12^{2n+1} \).

1.1.9 Adjunk meg végteken sok olyan \( n \)-et, amelyre \( 2^3 \mid 2^n + 5^k \).

1.1.10 Mutassuk meg, hogy \( (b - 1)^2 \mid b^8 - 1 \) akkor és csak akkor teljesül, ha \( b - 1 \mid b \).

1.1.11 (*) Tegyük fel, hogy \( p^b - 1 \mid p^a + 1 \). Lássuk be, hogy \( b = 1 \) vagy 2.

1.1.12 Bizonyítsuk be az alábbi állításokat.

(a) Ha \( b \mid a \) és \( a \neq 0 \), akkor \( |b| \leq |a| \).

(b) Minden nemnulla egész számnak csak véges sok osztója van.

1.1.13 Melyek azok a számok, amelyek felírhatók (a) két; (b) három (nem feltétlenül különböző) pozitív osztójuk összegeként?

1.1.14 Igazoljuk, hogy egy (tízes számrendszerben felírt természetes) szám akkor és csak akkor osztható
(a) 3-mal, illetve 9-cel, ha a számjegyeinek az összege osztható 3-mal, illetve 9-cel;
(b) 4-gyel, illetve 25-tel, ha az utolsó két számjegyéből álló szám osztható 4-gyel, illetve 25-tel;
(c) 8-cal, illetve 125-tel, ha az utolsó három számjegyéből álló szám osztható 8-cal, illetve 125-tel;
(d) 11-gyel, ha a számjegyeinek váltakozó előjellel vett összege osztható 11-gyel.

1.1.15 Létezik-e 2-nek olyan pozitív egész kitevős hatványa, amelyben mind a tíz számjegy ugyananniszor fordul elő?

1.1.16 (*) Létezik-e olyan szám, amelyben csak az 1 és 2 számjegyek fordulnak elő, és amely osztható $2^{10001}$-tel?

1.1.17 Mutassuk meg, hogy
(a) három szomszédos egész szám szorzata osztható 6-tal;
(b) $k$ szomszédos egész szám szorzata osztható $k!$-sal.

1.1.18 (M [550]) Legyen $n > 1$ tetszőleges egész. Csongor meglevő $n$-nek egy tetszőleges pozitív osztóját, legyen ez $d_1$. Ezután Tünde választ egy $d_2$ pozitív osztót, amely nem lehet osztója $d_1$-nek. Ismét Csongor választ egy $d_3$-at, amely nem osztója sem $d_1$-nek, sem $d_2$-nek stb. Az veszít, aki magát az $n$-et kénytelen választani. Kinek van nyerő stratégiája, ha $n$ értéke

(a) 16;
(b) $3^{1111}$;
(c) 10;
(d) 50;
(e) $2^{123456789101112131415}$?

1.1.19 (*) Válasszunk ki az $1, 2, \ldots, 2^n$ számok közül tetszőlegesen $n + 1$ darabot. Igazoljuk, hogy a kiválasztott számok között biztosan lesz két olyan, hogy az egyik a másiknak osztója.

1.1.20 Mi az oka annak, hogy noha a $0 \mid 0$ oszthatóság igaz, a $0 \nmid 0$ osztásnak még sincs értelme?

1.1.21 A páros számok körében melyek azok az elemek, amelyeknek
(a) egyáltalán nincs osztója;
(b) pontosan két (pozitív vagy negatív) osztója van?

1.1.22 Tekintsük oszthatósági szempontból a $c : d \sqrt{2}$ alakú (speciális valós) számokat, ahol $c$ és $d$ tetszőleges egészek.

(a) Döntsük el, hogy $12 - 7 \sqrt{2}$ osztható-e $3 + 4 \sqrt{2}$-vel.
(b) Igazoljuk, hogy az $1 + \sqrt{2}$ egység.
(c) Mutassuk meg, hogy végéntelen sok egység van.
(d) Hány osztója van egy tetszőleges elemnek?
(e) Lássuk be, hogy $c + d \sqrt{2}$ akkor és csak akkor egység, ha $|c^2 - 2d^2| = 1$. 
(f) M\textsuperscript{*} Bizonyítsuk be, hogy az egységek éppen a \( \pm (1 + \sqrt{2})^k \) alakú elemek, ahol \( k \) tetszőleges egész.

(g) Hányoszor fordul elő az egész számok körében, hogy egy négyzetszám kétszerese egygyel nagyobb, illetve eggyel kisebb egy (másik) négyzetszámnál?

1.1.23 Integrációs tartománynak a (legalább kételemű) kommutatív, nullosztómentes gyűrűket nevezzük, azaz amelyekben az összeadás és a szorzás kommutatív és asszociatív, van nullelem, minden elemnek van ellentettje, érvényes a disztributivitás, és két nemnulla elem szorozata sem lehet nulla. (Ez pongyolán fogalmazva azt jelenti, hogy az összeadás, kivonás és szorzás tekintetében az egész számoknál megszokott „szép” tulajdonságok teljesülnek.) Vezessük be az oszthatóságot és az egység fogalmát az D 1.1.1 és D 1.1.2 Definíciók szerint, és lássuk be az alábbiakat.

(a) M Akkor és csak akkor létezik egység, ha a szorzásnak létezik egységeleme (azaz olyan \( e \)-val, amelyre \( e a = a \) teljesül).

(b) Az egységek éppen az egységelem osztói, illetve más megfogalmazásban azok az elemek, amelyeknek (a szorzásra nézve) létezik inverze.

(c) Egy egység minden osztója és két egység szorzata is egység.

(d) Vizsgáljuk meg az T 1.1.5 Tétel állításait.

1.2 Maradékos osztás

1.2.1 Tétel. T 1.2.1

Tetszőleges \( a \) és \( b \neq 0 \) egész számokhoz léteznek olyan egyértelműen meghatározott \( q \) és \( r \) egész számok, melyekre

\[ a = bq + r \quad \text{és} \quad 0 \leq r < |b|. \]

Bizonyítás: Legyen először \( b > 0 \). A

\[ 0 \leq r = a - bq < b \]

feltétel pontosan akkor teljesül, ha

\[ bq \leq a < b(q + 1), \]

azaz

\[ q \leq a/b < q + 1. \]

Ilyen \( q \) egész szám pedig nyilván pontosan egy létezik; \( q \) az \( a/b \) (alsó) egérszám, \( q = \lfloor a/b \rfloor \), azaz a legnagyobb olyan egész szám, amely még kisebb vagy egyenlő, mint \( a/b \).

Ha \( b < 0 \), akkor a

\[ 0 \leq r = a - bq < -b \]

feltétel

\[ q \geq a/b > a - 1 \]
teljesülésével ekvivalens, ami ismét pontosan egy \( q \) egészre áll fenn (ekkor \( q \) az \( a/b \) felső egészrészéhez, \( q = \left[ a/b \right] \), azaz a legkisebb olyan egész, amely még nagyobb vagy egyenlő, mint \( a/b \).

A maradékos osztásnál kapott \( q \) számot hányadosnak, az \( r \)-et pedig (legkisebb nemnegatív) maradéknak nevezzük. \( \overline{a/b} \) oszthatóság (\( b \neq 0 \) esetén) pontosan akkor teljesül, ha a maradék 0.

Gyakran kényelmesebb, ha negatív maradékokat is megengedünk. Erre vonatkozik az T 1.2.1 Tétel alábbi variánsa, amely hasonlóan bizonyítható:

**1.2.1A Tétel.** T 1.2.1A

Tetszőleges \( a \) és \( b \neq 0 \) egész számokhoz létezik olyan egyértelműen meghatározott \( q \) és \( r \) egész számok, melyekre

\[
a = bq + r \quad \text{és} \quad -\frac{|b|}{2} < r \leq \frac{|b|}{2}. \]

Ebben az esetben az \( r \)-et legkisebb abszolút értékű maradéknak nevezzük.

**Példa:** Legyen \( a = 30 \), \( b = -8 \), ekkor

\[
30 = (-8)(-3) + 6 = (-8)(-4) - 2;
\]

tehát a legkisebb nemnegatív maradék a 6, a legkisebb abszolút értékű maradék pedig a \(-2\).

Az alábbi tétel bizonyításából látni fogjuk, hogy a maradékos osztás felhasználható a pozitív egész számok ún. számrendszeres felírásához is.

**1.2.2 Tétel.** T 1.2.2

Legyen \( t > 1 \) rögzített egész. Ekkor bármely \( A \) pozitív egész egyértelműen felírható az alábbi alakban:

\[
A = a_0 t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0, \quad \text{ahol} \quad 0 \leq a_i < t \quad \text{és} \quad a_n \neq 0.
\]

**Bizonyítás:** \( A \neq 0 \leq a_0 < t \) és \( i \mid A - a_0 \) feltétel miatt \( a_0 \) éppen az \( A \)-nak a \( t \)-vel történő maradékos osztásakor keletkező legkisebb nemnegatív maradék, tehát pontosan egy megfelelő \( 0 \)-létezik. Jelöljük a hányadost \( 0 \)-lal, ekkor a

\[
q_0 = \frac{A - a_0}{t} = a_n t^{n-1} + a_{n-1} t^{n-2} + \cdots + a_1 t + a_0
\]

felírásból az előzőhöz hasonlóan adódtik, hogy \( a_1 \) éppen a \( q_0 \)-nak a \( t \)-vel történő maradékos osztásakor keletkező legkisebb nemnegatív maradék. Az eljárást folytatva kapjuk a megfelelő \( A \)-k létezését és egyértelműségét.

Az \( A \) szám fenti

\[
A = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0
\]

előállításában az \( a_i \) számok az \( A \) számjegyei \( t \) alapú számrendszerben (ha \( t > 1 \), akkor a \( 0, 1, \ldots, 9 \) mellett újabb számjegyeleket is be kell vezetni). A fenti előállítást

\[
A = \overline{a_0 a_{n-1} \ldots a_1 a_0} \quad \text{vagy} \quad A = \overline{a_n a_{n-1} \ldots a_1 a_0}
\]
alakban jelöljük (a felülvonással szükség esetén azt jelezzük, hogy egymás mellé írt számjegyekről és nem például szorzásról van szó). Ha $t = 10^t$, akkor a számrendszer alapszámára utaló jelölést legtöbbször elhagyjuk.

Példa: $38 = 38;10 = 123[10]$, hiszen $38 = 1 \cdot 5^2 + 2 \cdot 5 + 3 \cdot 1$.

A mindennapi életben általában a tízes számrendszerrel dolgozunk, de gyakran hasznosabb pl. a kettes számrendszer, többek között a számítógépeknél. Ez utóbbiban csak kétféle számjegy szerepel, a 0 és az 1, az összeadás és a szorzás elvégzéséhez pedig csak az alábbi egyszerű egymegegy, illetve egyszerû táblát kell tudni (igaz, hogy mindezért cserébe egy szám felírásához jóval több számjegyre van szükség, mint pl. tízes számrendszerben):

<table>
<thead>
<tr>
<th>$+$</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$\odot$</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

A maradékos osztás — egyszerûsége ellenére — mind gyakorlati, mind pedig elméleti szempontból igen jelentôs (akár a legkisebb nemnegatív, akár a legkisebb abszolút értékû maradék szerint végezzük). Többek között jól használható oszthatósági kérdések vizsgálatánál, hiszen gyakran „csak a maradék számíti”. Legfontosabb alkalmazása talán a maradékos osztások sorozatából álló euclidesi algoritmus, amelyet a következő pontban tárgyalunk.

Feladatok

1.2.1 Ha 10849-et és 11873-at ugyanazzal a háromjegyû (tízes számrendszerbeli pozitív egész) számmal maradékosan elosztjuk, mind a kétszer ugyanazt a (nemnegatív) maradékot kapjuk. Mennyi ez a maradék?

1.2.2 Lássuk be, hogy minden $n$-hez végtelen sok olyan kettôhatvány létezik, amelyek közül bármely kettônek a különbsége osztható $n$-mel.

1.2.3 Mutassuk meg, hogy $n$ egész számból mindig kiválasztható néhány (esetleg egy, esetleg az összes), amelyek összege osztható $n$-nel.

1.2.4 Bizonyítsuk be, hogy minden pozitív egész számnak létezik olyan nemnulla többszöröse, amelyen csak a 0 és 1 számjegyek fordulnak elő (tízes számrendszerben).

1.2.5 (*) A Fibonacci-számok sorozatát a

$$\varphi_0 = 0, \quad \varphi_1 = 1, \quad \varphi_{j+1} = \varphi_j + \varphi_{j-1}, \quad j = 1, 2, \ldots$$

rekurzióval definiáljuk. A sorozat elsô néhány eleme:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$$

Bizonyítsuk be, hogy minden $n$-hez végtelen sok $m$-mel osztható Fibonacci-szám létezik.

(Megjegyzés: A szakirodalom egy részében a 0-t nem tekintik Fibonacci-számnak, tehát a sorozatot a $\varphi_1 = \varphi_2 = 1$ értékektől kiindulva definiálják a fenti rekurzióval. Ez a kétfeleség nem okozhat zavart, ha megegyezünk abban a szóhasználatban, hogy az „$n$-edik Fibonacci-számm” mindig $\varphi_n$-et jelentse.)

1.2.6 Milyen maradéket adhat egy négyzetszám (a) 3-mal; (b) 4-gyel; (c) 5-tel; illetve (d) 8-cal osztva?

1.2.7 Mutassuk meg, hogy 12 egymást követô egész szám négyzetének az összege sohasem lehet négyzetszám.
1.2.8 (A feladat tízes számrendszerre vonatkozik.)

(a) Van-e olyan (9-nél nagyobb) négyzetszám, amely csupa azonos számjegyből áll?

(b) * Adjuk meg a 81-nél nagyobb összes olyan négyzetszámot, amely páros sok jegyű, és az „első fele” is csupa azonos számjegyből áll, valamint a „második fele” is csupa azonos számjegyből áll.

1.2.9 Mutassuk meg, hogy egy egész szám három páratlan kiveőjtő hatványának az összege mindig osztható 3-mal.

1.2.10 (*) Vegyük nyolc tetszőleges (különböző) természetes számot, és képezzük a páronkénti különbségeik sorozatát. A 2-nek legalább hányadik hatványával osztható ez a sorozat?

1.2.11 Hány olyan legfeljebb 10-jegyű pozitív egész szám van, amely osztható négyzetgyökének (alsó) egészrészével? (Pl. a 12 ilyen, mert \( \sqrt[2]{12} = 3 \) osztója a 12-nek, de a 22 nem ilyen, mert \( \sqrt[2]{22} = 4 \) nem osztója a 22-nek.)

1.2.12 Milyen kapcsolatban áll \(|a + b|\) és \(|a| + |b|\) ?

1.2.13 Elvégezhető-e a maradékos osztás a páros számok körében (azaz érvényes-e az T 1.2.1–T 1.2.1A Tételek megfelelője)?

1.2.14 Mutassuk meg, hogy az 1.1.14 feladatban [3] megismert szabályok értelmezésben adott festmény nemcsak az oszthatóság elfogadására, hanem az osztási maradék megállapítására is alkalmazható. Hogyan általánosítható ezen a más alapú számrendszelekre?

1.2.15 Érdekes módon \( 28 \div 46 \div 12 + 18 = 99 \) és 99 osztója a számok egymás mellé irásával keletkező 23461218-nak. Tényleg a véletlen játékával állunk szemben?

1.2.16 Képezzük az \( \sqrt[2]{12231601} \) szám (tízes számrendszerbeli) számjegyeinek az összegét, majd az így kapott szám számjegyeinek az összegét stb., amíg egyjegyű számhoz nem jutunk. Mi lesz a végeredmény?

1.2.17 Hogyan lehet gyorsan megkapni egy szám 9-es számrendszerbeli felirásából a 3-as számrendszerbeli alakját és viszont? Milyen számrendszer kőzötti átváltásánál alkalmazható hasonló gyors eljárás?

1.2.18 Egy \( n \) pozitív egész valamely számrendszerben négyjegyű, az eggyel nagyobb alapú számrendszerben pedig kétjegyű. Határozzuk meg \( n \) -et.

1.2.19 Az alábbi sorozában nem a számrendszer alapjának, sem a \( \times \)-gal jelölt (nem feltétlenül egyforma) számjegyeket nem ismerjük. Határozzuk meg ezeket. (Egyik szám első jegye sem lehet 0.)

\[
\begin{array}{cccc}
2 & \times & \times & \times \\
\times & 1 & \times & \times \\
\times & \times & 2 & \times & \times \\
\times & \times & \times & \times & \times \\
\end{array}
\]

1.2.20 A 740-et a \( \hat{t} \) alapú számrendszerbe átszámolva olyan négyjegyű számot kapunk, amelynek utolsó jegye \( 5 \). Határozzuk meg \( \hat{t} \) értékét.

1.2.21 Egy kétkarú mérleghez tíz darab súlyból álló súlykészletet szeretnénk gyártani, amelyel egy minél nagyobb határig bezárólag minden egész grammmnyi súlyt le lehet mérni. Milyen súlyokat válasszunk, ha mérsékkel

(a) csak a mérleg egyik serpenyőjébe tehetünk súlyt;

(b) * mindkét serpenyőbe tehetünk súlyt?
1.2.22 Vizsgáljuk meg, hogy körülbélül hányszor annyi számjegy kell egy nagy szám kettes számrendszerbeli felírásához, mint a tízes számrendszerbeli felírásához. Ez pontos megfogalmazásban a következőt jelenti. Jelöljük az \( n \) szám számjegyeinek a számát kettes számrendszerben \( K(n) \) -nel, tízes számrendszerben pedig \( T(n) \) -nel. Mutassuk meg, hogy a \( K(n)/T(n) \) sorozatnak létezik határértéke, és számítsuk ki ezt a határértéket.

1.2.23 Változó alapú számrendszer. Legyenek \( t_1, t_2, \ldots \) tetszőleges egynél nagyobb egész számok. Mutassuk meg, hogy bármely \( A \) pozitív egész egyértelműen felírható

\[
A = a_n t_n b_n - 1 \ldots t_1 + a_{n-1} t_{n-1} \ldots t_1 + \cdots + a_1 t_1 + a_0
\]

alakban, ahol \( 0 \leq a_i < t_{i+1} \) és \( a_n \neq 0 \).

1.3 Legnagyobb közös osztó

1.3.1 Definíció . D 1.3.1

Az \( a \) és \( b \) számok legnagyobb közös osztója \( d \), ha

(i) \( d \mid a \), \( d \mid b \); és

(ii) ha egy \( c \) -re \( c \mid a \), \( c \mid b \) teljesül, akkor \( |c| \leq |d| \).

Jelölés: \( d = (a, b) \) vagy \( d = \text{lcm}(a, b) \) vagy \( d = \text{lcm}\{a, b\} \).

Ha \( a = b = 0 \), akkor nem létezik legnagyobb közös osztójuk, hiszen minden egész szám közös osztó, és ezek között nincs legnagyobb abszolút értékú.

Minden más esetben viszont (adott \( a \) és \( b \) mellett) az D 1.3.1 Definíciót pontosan két \( d \) szám elégti ki, amelyek egymás ellentettjei. Mivel egy szám és a negatívja oszthatósági szempontból teljesen egyenértékű, ezért \( a \) és \( b \) összes közös osztóját úgy kapjuk meg, hogy a pozitív közös osztók mellé vesszük azok negatívjait. A pozitív közös osztók \( P \) halmaza nem az üres halmaz, hiszen az 1 biztosan közös osztó, továbbá \( P \)-nek csak véges sok eleme lehet, mert egy nemnulla számnak csak véges sok osztója van (lásd az 1.1.12b feladatot [3]). Ennél fogva \( P \) elemei között létezik egy legnagyobb, jelöljük \( h \) -val. Ekkor nyilván \( d = l \) és \( d = -h \) kielégítik az D 1.3.1 Definíciót, más szám viszont nem.

1.3.2 Definíció . D 1.3.2

Az \( a \) és \( b \) számok kitüntetett közös osztója \( \delta \), ha

(i) \( \delta \mid c \), \( \delta \mid b \); és

(ii') ha egy \( c \) -re \( c \mid a \), \( c \mid b \) teljesül, akkor \( c \mid \delta \).

A kitüntetett közös osztó tehát olyan közös osztó, amely minden közös osztónak többszöröse.

A definícióból következik, hogy ha két számnak létezik kitüntetett közös osztója, akkor az egységszerestől eltérülnie egyértelmű. Ez részletesen kifejtve azt jelenti, hogy egyrészt egy kitüntetett közös osztó bármely egységszerese is az, másrészt két kitüntetett közös osztó szükségképpen egymás egységszerese. Ennek igazolását az 1.3.10 feladatban [14] tüzünk ki.

Ha \( a = b = 0 \), akkor a kitüntetett közös osztójuk a definíció szerint 0.
A továbbiakban ezzel az esettel egyáltalán nem foglalkozunk, azaz mindig eleve felteszük, hogy $a$ és $b$ közül legalább az egyik nem nulla.

Megmutatjuk, hogy ha egyáltalán létezik a $\delta$ kitüntetett közös osztó, akkor $\delta$ csak a legnagyobb közös osztó (valamelyik értéke) lehet. Jelöljük $d$-vel a $\delta$-val azonos előjelű legnagyobb közös osztót. Ekkor egyrészt (ii) miatt

$$|\delta| \leq |d|,$$

másrészt (ii') alapján $d \mid \delta$, amiből

$$|d| \leq |\delta|$$

következik. A két egyenlőtlenségből kapjuk, hogy $|d| = |\delta|$, és így az azonos előjel miatt $\delta = d$.

Egyáltalán nem magától értetődő azonban, hogy a legnagyobb közös osztó valóban rendelkezik a (ii') kitüntetett tulajdonsággal is, vagyis hogy bármely két egész számnak létezik kitüntetett közös osztója.

1.3.3 Tétel. T 1.3.3

Bármely két egész számnak létezik kitüntetett közös osztója.

Bizonyítás: A kitüntetett közös osztó létezését a matematika egyik legősibb eljárásával, az euklideszi algoritmus felhasználásával igazoljuk. Az egyik számot maradékosan elosztjuk a másikkal. Majd a másik számtól a maradékkal stb. mindig az osztót a maradékkal, amíg 0 maradékhoz nem jutunk. Megmutatjuk, hogy az eljárás véges, és az utolsó nemnulla maradék lesz a két szám (egyik) kitüntetett közös osztója.

Nézzük mindezt részletesen. Tegyük fel, hogy (pl.) $\hat{b} \neq \emptyset$. Ha $b \mid c$, akkor $\delta = b$ megfelel.

Ha $\hat{b} \nmid c$, akkor alkalmazsuk a $T_i$, $R_i$ egészekkel

$$c = bq_1 + r_1, \quad a \mid d, \quad 0 < r_1 < |b|,$$

$$\hat{b} = r_1q_2 + r_2, \quad a \mid d, \quad 0 < r_2 < r_1,$$

$$\vdots$$

$$r_{n-2} = r_{n-1}q_n + r_n, \quad a \mid d, \quad 0 < r_n < r_{n-1},$$

$$(r_{n+1} = 0).$$

Az eljárás biztosan befejeződik véges sok lépésben, ugyanis a maradékok nemnegatív egészekből álló szigorúan csökkenő sorozatot alkotnak:

$$|b| > r_1 > r_2 > \ldots$$

Most belátjuk, hogy $R_n$ valóban az $a$ és $\hat{b}$ számok (egyik) kitüntetett közös osztója.

Az algoritmus egyenlőségein alulról felfelé haladva először azt igazoljuk, hogy $R_n$ közös osztója $a$-nak és $\hat{b}$-nak. Az utolsó egyenlőségből $r_{n-1} \mid r_n - 1$. Az utolsó előtti egyenlőségre rátérve

$$r_n \mid r_{n-1}, r_n \mid r_n \rightarrow r_n \mid r_{n-1}q_n + r_n = r_{n-2}.$$

Ugyanígy folytatva végül $r_1 \mid b$, majd (az első egyenlőségből) $r_1 \mid a$ adódik.

A kitüntetett tulajdonság igazolásához felülről lefelé haladunk. Legyen $c \mid a, c \mid b$, ekkor az első egyenlőségből $c \mid c - bq = r_1$. A második egyenlőségre rátérve
SZÁMELMÉLETI
ALAPFOGALMAK

\[ \frac{b}{c} \mid r_1 \implies \frac{b}{c} \mid r_1 - r_2 = r_2. \]

Ugyanígy folytatva végül az utolsó előtti egyenlőségből kapjuk, hogy \[ \frac{c}{r_n}. \]

Megjegyzések: 1. Az euklideszi algoritmust a legkisebb nemnegatív maradékok helyett a legkisebb abszolút értékű maradékokkal is végezhetjük; ebben az esetben a maradékok abszolút értékű értékei alkotnak nemnegatív egészegyütteseit álló szigorúan csökkenő sorozatot, és így az eljárás ekkor is véges sok lépésben biztosan befejeződik.

2. Szokás a legnagyobb közösen osztót eleve pozitívnak definiálni. Mivel azonban egy szám és a negatívja egymás egységképe, azaz bármely oszthatósági kérdésnél teljesen azonosan viselkednek, ezért semmi ok sincs arra, hogy a legnagyobb közösen osztó fogalmából a negatív számokat eleve kirekesszük. Ezért adtuk meg a legnagyobb közösen osztó definícióját úgy, hogy abba a két legnagyobb abszolút értékű közösen osztó egyenrangúan belefőjejen.

3. Az előrebocsátott megjegyzések alapján nem jelent megszorítást, ha a továbbiakban kényelmi okokból a legnagyobb közösen osztó, illetve az (vele már bizonyítottan megegyező) alakított közösen osztó két értéke közül mindig a pozitívát tekintjük. Ezért úgy is megadottuk a legnagyobb közösen osztó definícióját úgy, hogy abba a két legnagyobb abszolút értékű közösen osztó egyenrangúan belefőjejen.

4. A legnagyobb közösen osztó gyakorlati kiszámításánál az egyszerűen adódó \( (a, \hat{b}) = \left( \hat{b}, a - \frac{a}{\hat{b}} \hat{b} \right) \) összefüggés alapján gyakran kényelmesebb az euklideszi algoritmusnak az \( (a, \hat{b}) = \left( \hat{b}, r_1 \right) = \left( r_1, r_2 \right) = \cdots = \left( r_{n-1}, r_n \right) = \left( r_n, \hat{b} \right) = r_n \) alakját használni.

5. Az D 1.3.2 Definíciót, az ottani (ii') kitüntetett tulajdonság bevezetését az indokolja, hogy csak oszthatósági relációt használ fel, azaz az egész számok számelméleti vizsgálatával szemben az D 1.3.1 Definícióval amelyben rendezési reláció (nagyobb-kisebb) is szerepel. Ennél fogva nem meglepő, hogy az euklideszi algoritmusnak az azt hámorosan látni fogjuk — mind elmeleti, mind pedig gyakorlati szempontból elsősorban a (ii') kitüntetett tulajdonságra tudunk majd támaszkodni. A csak az oszthatóságra épülő fogalmalkotás további előnye, hogy bizonyos számkörökben (illetve általánosabban integrált tartományokban) az D 1.3.1 Definíció nem is értelmes. Ennek egyik nyilvánvaló oka az, hogy nem definiálható a számkörben (a szokásos „jó” tulajdonságokkal bíró) rendezés, így a komplex számok bizonyos részhalmazai. Az D 1.3.1 Definícióval azonban olyan számkörökben is adódhat probléma, amelyekben van rendezés, például a \( c + \sqrt{2} \) egészek számkörében is ez a helyzet. Itt ugyanis a végtelen sok egység miatt bármely két elemnek végtelen sok közösen osztója van, és ezek között nincs legnagyobb abszolút értékű. (Ha csak páronként nem egységképes közös osztókat tekintünk, akkor sincs értelme az D 1.3.1 Definíciókban, mert bármely két közös osztó esetén létezik az elsőnek olyan egységképessége, amely nagyobb a második osztónál.) Ezért a számelmélet további fejezetekben egyenesen az D 1.3.2 Definíció szerint értelmezjük majd a legnagyobb közösen osztót.

Most (az egész számok körében) a legnagyobb közösen osztó néhány fontos tulajdonságát tárgyaljuk.

1.3.4 Tétel . T 1.3.4

Ha \( c > 0 \), akkor \( (\alpha c, \beta b) = c (\alpha, \beta) \).

Bizonyítás: Tekintsük az \( (\alpha c, \beta b) \) előállítására szolgáló euklideszi algoritmust, legyen az utolsó nemnulla maradék \( r_u = (\alpha c, \beta b) \). Szorozzunk meg minden egyenlőséget \( c \) -vel, ekkor éppen a \( (\alpha c, \beta b) \) -t előállító euklideszi algoritmushoz jutunk. Ebben az utolsó nemnulla maradék \( (\alpha c, \beta b) = c r_u = c (\alpha, \beta) \).

Az T 1.3.4 Tétel egy másik lehetséges bizonyítására vonatkozóan lásd az 1.3.11 feladatot [14].
1.3.5 Tétel . T 1.3.5

Az $a$ és $b$ számok legnagyobb közös osztója alkalmas $\mathfrak{u}$ és $\mathfrak{v}$ egészekkel kifejezhető
\[(a, b) = a\mathfrak{u} + b\mathfrak{v}\]
alakban. ♦

Bizonyítás: Az euklideszi algoritmus első egyenlőségétől $\mathfrak{r}_1$-et kifejezve
\[\mathfrak{r}_1 = a - b\mathfrak{q}_1\]
adódik. Ennek felhasználásával a második egyenlőségből az
\[\mathfrak{r}_2 = b - \mathfrak{r}_1\mathfrak{q}_2 = b - (a - b\mathfrak{q}_1)\mathfrak{q}_2 = a(-\mathfrak{q}_2) + b(1 - \mathfrak{q}_1\mathfrak{q}_2)\]
előállításhoz jutunk, azaz $\mathfrak{r}_2$ felírható $a\mathfrak{u}_2 + b\mathfrak{v}_2$ alakban. Hasonlóan továbbhaladva az utolsó előtti egyenlőségből azt kapjuk, hogy $(a, b) = \mathfrak{r}_n$ is kifejezhető $a\mathfrak{u} + b\mathfrak{v}$ alakban. ■

Az T 1.3.5 Tétel fontos következménye az $ax + by = c$ kétszeretetlenes lineáris diofantikus egyenlet megoldhatóságára vonatkozó alábbi tétel. Diofantikus egyenletnek általában olyan egész együthathatós algebrai egyenletet nevezünk, melynek a megoldásait az egész számok körében keresünk, ezekkel részletesen a 7. fejezetben foglalkozunk. A fenti $ax + by = c$ egyenletben tehát $a, b, c$ rögzített egész számok, és megoldáson egy $x, y$ egész számpár értünk.

1.3.6 Tétel . T 1.3.6

Legyenek $a, b, c$ rögzített egész számok. Az $ax + by = c$ diofantikus egyenletnek akkor és csak akkor létezik megoldása, ha $(a, b) \mid c$, ♦

Bizonyítás: Először tegyük fel, hogy létezik $x_0, y_0$ megoldás. Ekkor $(a, b) \mid a\mathfrak{x}_0 + b\mathfrak{y}_0 = c$ alapján szükségképpen
\[(a, b) \mid a\mathfrak{x}_0 + b\mathfrak{y}_0 = c\]
Megfordítva, tegyük fel, hogy $(a, b) \mid c$, vagyis van olyan $t$ egész, amelyre $(a, b)t = c$. Az T 1.3.5 Tétel alapján
\[(a, b) = a\mathfrak{u} + b\mathfrak{v}\]
teljesül alkalmas $\mathfrak{u}, \mathfrak{v}$ egészekkel. Ezt az egyenlőséget $t$-vel beszorozva kapjuk, hogy
\[c = a(t\mathfrak{u}) + b(t\mathfrak{v})\]
azaz $x = a\mathfrak{u}_t, y = v\mathfrak{v}_t$ megoldása az $ax + by = c$ diofantikus egyenletnek. ■

Az T 1.3.6 Tételt kiegészíthetjük azzal, hogy megoldhatóság esetén az euklideszi algoritmus egyúttal eljárást is szolgáltat a lineáris diofantikus egyenlet (egyik) megoldásának a megkereséséhez.

A lineáris diofantikus egyenlet további vonatkozásai (megoldásszám, összes megoldás előállítása, más megoldási módszer) részletesen a 7.1 pontban foglalkozunk, a lineáris kongruenciákkal való kapcsolatát pedig a 2.5 pontban tárgyaljuk.

Több szám legnagyobb közös osztóját rögtön a „kitüntetett” tulajdonsággal definiáljuk; olyan közös osztó, amely minden közös osztónak többszöröse. Az $a_1, a_2, \ldots, a_t$ (nem cusa 0) számok pozitív legnagyobb közös osztóját $(a_1, a_2, \ldots, a_t)$-val jelöljük. Ennek létezését a legegyszerűbben annak
alapján igazolhatjuk, hogy két szám közös osztóiak a halmaza megegyezik a két szám legnagyobb közös osztója osztóiak a halmával. Ebből kapjuk, hogy

\[(a_1, a_2, \ldots, a_k) = (\ldots (a_1, a_2), a_3), \ldots, a_{k-1}), a_k)\]  

1.3.7 Definíció. D 1.3.7

Az \(a_1, a_2, \ldots, a_k\) számok relatív prímek, ha nincs egységtől különböző közös osztójuk, azaz \((a_1, a_2, \ldots, a_k) = 1\).

1.3.8 Definíció. D 1.3.8

Az \(a_1, a_2, \ldots, a_k\) számok páronként relatív prímek, ha közülük semelyik kettőnek sincs egységtől különböző közös osztója, azaz minden \(1 \leq i \neq j \leq k\) esetén \((a_i, a_j) = 1\).

Nyilvánvaló, hogy a páronként relatív prim számok együttal relatív prímek is, de ez \((k > 2\) esetén) megfordítva nem igaz (lásd az 1.3.5 feladatot [14]).

Már az 1.1.5e feladatban [3] is láttuk, hogy ha egy szám osztója egy szorzatnak és az egyik tényezőnek nem osztója, akkor ebből nem következik, hogy a másik tényezőnek osztója legyen. A helyes feltételt az alábbi tétel adja, amely már Euklidésznél is szerepel, és amely az oszthatósági feladatokban való felhasználhatósága mellett kulcsszerepet játszik a származélet alaptételének bizonyításánál is.

1.3.9 Tétel. T 1.3.9

Ha \(c \mid ab\) és \((c, a) = 1\), akkor \(c \mid b\).

Bizonyítás: Nyilván elég arra az esetre szoritkoznunk, ha \(a, b\) és \(c\) pozitív. Ekkor a \(c \mid ab\) és \(c \mid cb\) oszthatóságokból a legnagyobb közös osztó kitüntetett tulajdonsága, valamint az T 1.3.4 Tétel alapján következik, hogy

\[c \mid (ab, cb) = (a, c)b = b\]

Feladatok

(Ha egy feladatban előfordul valamilyen \(u\), \(v\) számpátra az \(\langle u, v \rangle\) jelölés, akkor automatikusan feltehetjük, hogy az \(u\) és \(v\) közül legalább az egyik nem nulla.)

1.3.1 Számítsuk ki \((3794, 2226)\) értékét, és írjuk fel \(3794u + 2226v\) alakban.

1.3.2 Mutassuk meg, hogy az alábbi törtek semmilyen \(n\) pozitív egész esetén sem egyszerűsíthetők:

\[
\frac{5n + 1.5}{7n - 12};
\]

\[
\frac{3n^2 - 1}{4n^2};
\]

\[
\frac{n^2 - 1}{7n + 10};
\]

\[
\frac{2n^2 - 2}{3n^2 - 3}.
\]

1.3.3 Adjuk meg \((n^2 + 2, n^4 + 4)\) lehetséges értékeit, ha \(n\) végigfut a természetes számokon.
1.3.4 Tegyük fel, hogy \((a, b) = 5\). Számítsuk ki
(a) \((a + b, a - b)\);
(b) \((a + 2b, a_4 - b)\)
lehetséges értékeit.

1.3.5 Adjunk meg három olyan számot, amelyek relatív prímek, de közülük semelyik kettő sem relatív prím.

1.3.6 Melyek igazak az alábbi állítások közül?
(a) Ha \((a, b) = d\), akkor \((\frac{a}{d}, \frac{b}{d}) = 1\).
(b) Ha \((a, b) = d\), akkor \((\frac{a}{d}, b) = 1\) és \((a, \frac{b}{d}) = 1\) közül legalább az egyik teljesül.
(c) \(c | ab \iff (c, a) | b\).
(d) \(c | ab, (a, b) = 1 \implies c | a\) vagy \(c | b\).

1.3.7 Legyenek \(a\) és \(b\) pozitív egészek. Hány \(b\)-vel osztható szám van az \(a, 2a, 3a, \ldots, 5a\) számok között?

1.3.8 Legyenek \(a\) és \(b\) különböző pozitív egészek. Melyek igazak az alábbi állítások közül?
(a) Végtelen sok \(n\) egészre \((a + r, b + r) = 1\).
(b) Végtelen sok \(n\) egészre \((a + r, b + r) = (b + r, bn) = 1\).
(c) Végtelen sok \(n\) egészre \((a + r, bn) = (b + u, ba) = 1\).

1.3.9 (a) Hány olyan \(u, v\) egész számpár található, amelyre \((u, v) = \omega u + bv\)?
(b) Az \((a, b) = au + bv\) előállításban mennyi \(n\) és \(v\) legnagyobb közös osztója?
(c) Legyen \(\overline{H}\) az \(au - bv\) alakú számok halmaza, ahol \(a\) és \(v\) végigfut az egész számokon. Mi lesz \(\overline{H}\) legkisebb pozitív eleme?

1.3.10 A kitüntetett közös osztó egyértelműsége. Legyen \(\delta\) az \(a, b\) egész számok (egyik) kitüntetett közös osztója. A kitüntetett közös osztó definíciója alapján bizonyítsuk be az alábbiakat.
(a) Tetszőleges \(\varepsilon\) egységre \(\varepsilon \delta\) is kitüntetett közös osztója \(a, b\)-nek.
(b) Ha \(\delta \delta\) is kitüntetett közös osztója \(a, b\)-nek, akkor \(\delta = \varepsilon \delta\), ahol \(\varepsilon\) alkalmas egység.

1.3.11 (M [550]) Adjunk az T 1.3.4 Tételre új bizonyítást, amely csak a kitüntetett közös osztó fogalmára és létezésére támaszkodik, és nem használja fel (közvetlenül) magát az euklideszi algoritmust.

1.3.12 Nevezzük csupaegynek azokat a pozitív egészeket, amelyeknek (tízes számrendszerben) minden számjegye 1-és.
(a) Mely számoknak létezik csupaegy többszöröse?
(b) A $3^{1000}$-nek melyik a legkisebb csupaegy többszöröse?

1.3.13 (M [550]*) Mutassuk meg, hogy bármely $a > 0$, $k > 0$ és $a > 1$ egészekre

$$\left(a^k - 1, a^k - 1\right) = a^{\left\lfloor \log_a k \right\rfloor} - 1.$$

1.3.14 Legyen $a$ pozitív egész.

(a) Igazoljuk, hogy ha $n$ és $k$ különböző kettőhatványok és $a$ páros szám, akkor $\left(a^n + 1, a^k + 1\right) = 1$.

(b) Határozzuk meg általában $\left(a^n + 1, a^k + 1\right)$ értékét.

1.3.15 Bizonyítsuk be, hogy a szomszédos Fibonacci-számok (lásd az 1.2.5 feladatot [7]) relatív primek. Mi a helyzet a másodszomszédokkal? És a harmadszomszédokkal?

1.3.16 (**) Legyen $\varphi_n$ az $n$-edik Fibonacci-szám. Igazoljuk, hogy

$$k \mid n \iff \varphi_k \mid \varphi_n, \text{ a ből } \varphi_{(k,n)} = \left(\varphi_k, \varphi_n\right).$$

1.3.17 Szakaszok összemérhetősége. Euklidész „Elemek” e. könyvében egész számok közös osztói mellett foglalkozik szakaszok közös mértékével is. Két szakasz közös mértékén egy olyan szakaszt érünk, amely egész számszor felmérhető (maradék nélkül) mind a két szakasza. Két szakaszt összemérhetőnek nevezzünk, ha létezik közös mértékük.

(a) Bizonyítsuk be, hogy két szakasz akkor és csak akkor összemérhető, ha a hosszaik aránya racionális szám.

(b) Két adott összemérhető szakasznak hány közös mértéke létezik?

(c) Fogalmazzuk meg a maradékos osztás szakaszokra vonatkozó értelmszerű megfelelőjét, és mutassuk meg, hogy az erre épülő euklideszi algoritmus akkor és csak akkor fejeződik be véges sok lépésben, ha a két kiindulási szakasz összemérhető.

(d) Igazoljuk, hogy összemérhető szakaszok esetén létezik a közös mértékeik között legnagyobb, és erre az összes közös mérték egész számszor felmérhető (maradék nélkül).

(e) Lássuk be, hogy egy négyzet oldala és átlója esetén az euklideszi algoritmus nem ér véget. (Ezzel a $\sqrt{2}$ irracionalitását geometriai úton igazoltuk.)

### 1.4 Felbonthatatlan szám és prímszám

Láttuk, hogy oszthatósági szempontból a 0, illetve az egységek különleges szerepet játszanak: a 0- nak minden szám osztója, az egységek pedig minden számot osztanak. Legyen a továbbiakban $a$ tetszőleges, 0-tól és egységtől különböző szám. Az egység definíciója alapján bármely $\varepsilon$ egység esetén $\varepsilon \mid a$ és $\varepsilon \mid a$. Ezeket az $e$ triviális osztóinak nevezzük. A továbbiakban fontos szerepet játszanak azok a számok, amelyeknek csak triviális osztóik vannak:

1.4.1 Definíció. D 1.4.1

A $\mathcal{P}$ egységtől (és nullától) különböző számot felbonthatatlan szánnak nevezzük, ha csak úgy bontható fel két egész szám szorzatára, hogy valamelyik tényező egység. Azaz

$$\varphi = ab \implies a \text{ vagy } b \text{ egység.}$$
Itt \( \mathbb{P} \neq \{0\} \)-t azért nem szükséges külön kikötni, mert a \( \emptyset \) nemtriviálisan is szorzattá bontható, pl. \( \emptyset = 5 \cdot \emptyset \). Megjegyezzük még, hogy a \( \mathbb{P} = ab \) szorzatban nem lehet mindkét tényező egység, hiszen akkor a szorzatuk, azaz \( \mathbb{P} \) is egység lenne. (Így az D 1.4.1 Definíció végén tulajdonképpen „kizáró vagy” szerepel.)

A felbonthatatlan számok tehát azok az egységtől különböző egészek, amelyek csak triviálisan bonthatók két egész szám szorzatára, vagy más szóval, amelyek csak az egységekkel és saját maguk egységszereseivel oszthatók. Ilyenek például a 2, 3, \(-17\) stb. Ha egy nemnulla számnak triviálistól különböző osztója is van, akkor \( \text{összetett számnak} \) nevezzük.

A következő fogalom bevezetéséhez emlékeztetünk arra, hogy ha egy \( c \) szám osztója egy szorzat valamelyik tényezőjének, akkor \( c \) osztója a szorzatnak is, de ennek a megfordítása nem igaz: pl. \( c = 6 \) -ra \( 6 \cdot 3 \cdot 4 \), de \( 6 \mid 3 \), \( 6 \mid 4 \). Fontos szerepet játszanak azok a \( c \) számok, amelyekre a megfordítás is érvényes:

1.4.2 Definíció . \( \text{D 1.4.2} \)

A \( \mathbb{P} \) egységtől és nullától különböző számot \textit{prímszám}nak (vagy röviden \textit{prím}nek) nevezzük, ha \textbf{csak} úgy lehet osztója két egész szám szorzatának, ha legalább az egyik tényezőnek osztója. Azaz

\[
\mathbb{P} \mid ab \implies \mathbb{P} \mid c \text{ vagy } \mathbb{P} \mid b. \]

Az D 1.4.2 Definíció végén „megengedő vagy” szerepel, hiszen előfordulhat, hogy \( \mathbb{P} \) a szorzat mindkét tényezőjét osztja. Megjegyezzük még, hogy most \( \mathbb{P} \neq \emptyset \) -t mindenképpen külön ki kellett kőtni, hiszen a 0-ra teljesül az D 1.4.2 Definíció további részében megfogalmazott tulajdonság:

\[
0 \mid ab \implies a = 0 \text{ vagy } b = 0 \implies 0 \mid a \text{ vagy } 0 \mid b. \]

Az D 1.4.2 Definícióból rögtön következik, hogy egy prímszám egy (kettőnél) több tényezős szorzatnak is csak úgy lehet osztója, ha legalább az egyik tényezőnek osztója.

1.4.3 Tétel . \( \text{T 1.4.3} \)

Az egész számok körében \( \mathbb{P} \) akkor és csak akkor prím, ha felbonthatatlan. \( \blacklozenge \)

Bizonyítás: Nyilván feltehető, hogy \( \mathbb{P} \) nem nulla és nem egység.

I. Először tegyük fel, hogy \( \mathbb{P} \) prím, és lássuk be, hogy felbonthatatlan is. Induljunk ki egy \( \mathbb{P} = ab \) szorzat-elállításból; azt kell igazolnunk, hogy \( a \) és \( b \) valamelyike egység.

Mivel \( \mathbb{P} = ab \), így \( \mathbb{P} \mid ab \) is igaz. Mivel \( \mathbb{P} \) prím, ezért ebből \( \mathbb{P} \mid a \) vagy \( \mathbb{P} \mid b \) következik. Az első esetben \( ab \mid a \), tehát \( a \neq 0 \) (miatt) \( b \mid 1 \), vagyis \( b \) egység, a második esetben pedig ugyanig kapjuk, hogy \( a \) egység.

II. Most tegyük fel, hogy \( \mathbb{P} \) felbonthatatlan, és lássuk be, hogy prím is. Induljunk ki egy \( \mathbb{P} \mid ab \) oszthatóságból; azt kell igazolnunk, hogy \( \mathbb{P} \mid a \) é és \( \mathbb{P} \mid b \) közül legalább az egyik teljesül.

Ha \( \mathbb{P} \mid c \), akkor készen vagyunk. Ha \( \mathbb{P} \mid a \), akkor \( \mathbb{P} \) felbonthatatlansága és \( (\mathbb{P}, a) \mid p \) miatt \( (a,c) = 1 \). A \( \mathbb{P} \mid ab \) és \( (\mathbb{P}, a) = 1 \) feltételekből az T 1.3.9 Tétel alapján \( \mathbb{P} \mid b \) következik. \( \blacksquare \)

Ezzel megmutattuk, hogy az egészek körében a felbonthatatlan számok és a prímszámok egybeesnek. Ezért jogosult a felbonthatatlan vagy prím elnevezéseket bármelyikének a használata, és az is, hogy a középsíkolkákban az egészre a felbonthatatlan számok megfelelő tulajdonságai értelmezik a prímszámot. A továbbiakban a rövidség kedvérért a prím(szám) szót fogjuk általában használni, kivéve, ha hangsúlyozni akarjuk a szám felbonthatatlan tulajdonságát.
A két fogalom azonban sok más számkörben nem ekvivalens. Például a páros számok körében a 6 felbonthatatlan, hiszen egyáltalán nem bontható két páros szám szorzatára, azonban nem prim, mert osztója a 1 és 2 szorzatnak, de nem osztja egyik tényezőt sem. Továbbá példákat látunk majd a 10. fejezetben.

Az egészek körében a prímszámok vizsgálata a számemlélet egyik legfontosabb területe. Már Euklidész bebizonyította, hogy végont sok prímszám létezik (T 5.1.1 Tétel), ugyanakkor a prímszámokkal kapcsolatban rengeteg az olyan egyszerűen megfogalmazható probléma, amely még ma is megoldatlan. Mindezekkel bővebben az 5. fejezetben foglalkozunk.

Feladatok

A szokásos szóhasználatnak megfelelően az egész számok körében már az alábbiakban is a prím vagy prímszám szót fogjuk használni a felbonthatatlan számra is. Megjegyzzük azonban, hogy az 1.4.1 [17]–1.4.7 feladatok [18] mindegyike tulajdonképpen felbonthatatlan számokra vonatkozik.

1.4.1 Adjuk meg az összes olyan pozitív egészt, amelyre az alábbiakban is prímszám:
(a) $n$, $n + 2$ és $n + 4$;
(b) $n$ és $n^2 + 8$;
(c) $n$, $n + 6$, $n + 12$, $n + 18$ és $n + 24$;
(d) $n$, $n^3 - 6$ és $n^5 + 6$.

1.4.2 Létezik-e végtelen hosszú, nemnulla differenciájú számtani sorozat csupa prímszámból?

1.4.3 Halhatatlan kapitálynak három halhatatlan unokája van, akiknek az életkora három különböző prímszám és ezek négyzetének az összege is prímszám. Hány éves a kapitány legkisebb unokája? (Ne felejsük el, hogy az unokák halhatatlanok, tehát akár több millió évesek is lehetnek!)

1.4.4 Legyenek $a$ és $k$ egynél nagyob, egészegy, bizonyítsuk be az alábbi állításokat.
(a) Ha $a^k - 1$ prim, akkor $a = 2$ és $k$ prim.
(b) Ha $a^k + 1$ prim, akkor $k$ kettőhatvány.

Megjegyzés: A $2^k - 1$ alakú primeket Mersenne-prímeknek, a $2^k + 1$ alakú primeket pedig Fermat-prímeknek nevezzük, ezekkel részletesen az 5.2 pontban foglalkozunk majd.

1.4.5 (M [551]) Adjuk meg az összes olyan $i > 1$ egész és $k > 0$ páratlan számot, amelyre $1^k + 2^k + 3^k + \cdots + i^k$ prímszám.

1.4.6 Mely $n$ pozitív egészre lesz prímszám
(a) $n^5 - n + 3$;
(b) $n^5 - 27$;
(c) $n^8 + n^7 + n^6 + n^5 + n^4 + n^3 + n^2 + n + 1$;
(d) $n^4 + 4$;
(e) $n^8 + n^6 + n^4 + n^2 + 1$?
1.4.7 Legyen \( u > 1 \) egész szám. Bizonyítsuk be az alábbi állításokat.

(a) Ha \( u \) -nek nem létezik olyan \( t \) osztója, amelyre \( 1 < t \leq \sqrt{u} \), akkor \( u \) prím szám.

(b) Az \( u \) szám 1-nél nagyobb osztói közül a legkisebb szükségképpen prim.

(c) Ha \( u \) összetett, de nem létezik olyan \( t \) osztója, amelyre \( 1 < t \leq \sqrt[3]{u} \), akkor \( u \) két prím szám szorzata.

1.4.8 Bizonyítsuk be, hogy \( (n-5)(n+12) + 51 \) semmilyen \( n \) egész esetén sem osztható 289-cel.

1.4.9 Mik lesznek a páros számok körében a felbontathatlanok, illetve a prímek?

1.4.10 A felbontathatlan és prim fogalma tetszőleges \( I \) integratúra tartományban (lásd az 1.1.23 feladatot [5]) értelmezhető. Bizonyítsuk be az alábbi állításokat.

(a) Ha \( I \) -ben a szorzásnak nincs egységeleme, akkor \( I \) -ben nincs prim.

(b) Ha \( I \) -ben a szorzásnak van egységeleme, akkor \( I \) -ben minden prim szükségképpen felbontathatlan is.

1.5 A számelmélet alaptétele

1.5.1 Tétel (A számelmélet alaptétele) . T 1.5.1

Minden, a 0-tól és egységektől különböző egész szám felbontható véges sok felbontathatlan szám szorzatára, és ez a felbontás a tényezők sorrendjétől és egységszeresektől eltekintve egyértelmű. (Az egyértelműség azt jelenti, hogy ha

\[ a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s, \]

ahol a \( p_i \) és \( q_j \) számok valamennyien felbontathatlanok, akkor \( r = s \) , és a \( p_i \) és \( q_j \) számok párba állíthatók úgy, hogy mindegyik \( p_i \) a hozzá tartozó \( q_j \) -nek egységszerese.)

Megjegyzések:

1. A 0-t és az egységeket azért kellett kizárni, mert azok egyáltalán nem bonthatók fel felbontathatlan számok szorzatára, és ez a felbontás a tényezők sorrendjétől és egységszeresektől eltekintve egyértelmű. (Az egyértelműség azt jelenti, hogy ha

\[ a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s, \]

ahol a \( p_i \) és \( q_j \) számok valamennyien felbontathatlanok, akkor \( r = s \) , és \( p_i \) és \( q_j \) számok párba állíthatók úgy, hogy mindegyik \( p_i \) a hozzá tartozó \( q_j \) -nek egységszerese.)

Megjegyzések:

1. A 0-t és az egységeket azért kellett kizárni, mert azok egyáltalán nem bonthatók fel felbontathatlan számok szorzatára: az egységek csak úgy írhatók fel szorzatként, hogy minden tényező egység, a 0 pedig csak úgy, hogy legalább az egyik tényező 0 (és akkor ez a tényező nem felbontathatlan).

2. Magukra a felbontathatlan számokra a tétel olyan formában érvényes, hogy ezeket egytényezős szorzatoknak tekintjük.

3. Néhány észrevétel az egyértelműséghez. Tegyük fel, hogy az \( a \) szám \( a = p_1 p_2 \cdots p_r \) alakban előáll felbontathatlanok szorzataként. Ekkor nyilván a tényezőket tetszőleges más sorrendben összeszorozva ugyancsak \( a \) -t kapunk. Emellett legyenek \( \epsilon_1, \cdots, \epsilon_r \) tetszőleges olyan egységek, amelyek szorzata 1, ekkor \( \epsilon_1 p_1, \cdots, \epsilon_r p_r \) is felbontathatlanok, és ezek szorzata is \( a \) -val egyenlő. Az alaptétel egyértelműségi része éppen azt fejezi ki, hogy ezektől a variálási lehetőségektől eltekintve az \( a \) másképpen már nem írható fel felbontathatlanok szorzataként. Például a 12 esetében néhány ilyen felírás

\[ 12 = 2 \cdot 2 \cdot 3 = 2 \cdot (-3) \cdot (-2) = 3 \cdot (-2) \cdot (-2). \]

4. A tétel kimondásánál mindenképpen a felbontathatlan szám fogalmát érdemes használni, hiszen a tétel éppen azt fejezi ki, hogy ilyen „építőkövekből” lényegében minden szám lényegében egyértelműen „összerakható”. A bizonyítás során is meg fogjuk különböztetni a felbontathatlan és a
SZÁMELMÉLETI
ALAPFOGALMAK

prim fogalmát. Ezek ekvivalenciajája — amint látni fogjuk — szorzó összefüggésben áll a számelmélet alaptételének az érvényességeivel.

5. Sok számkörben (illetve integrációs tartományban) nem érvényes a számelmélet alaptétele. Például a páros számok körében a 100-nak két lényegesen különböző felbontása létezik felbonthatatlanok szorzatára: \(100 = 2 \cdot 50 = 10 \cdot 10\). További példákat látunk majd a 10. fejezetben.

Most rátérünk az alaptétel igazolására. Az egyértelműségi részre két bizonyítást is adunk.

A felbonthatóság bizonyítása: Tekintsünk egy nullától és egységektől különböző tetszőleges \(a\) számot. Ha \(a\) felbonthatatlan, akkor készen vagyunk.

Ha \(a\) nem felbonthatatlan, akkor létezik nemtriviális felbonthatatlan osztója, mert a legkisebb pozitív nemtriviális osztója szükségképpen felbonthatatlan (lásd az 1.4.7b feladatot \[18\]). Ekkor \(a = p_1 q_1\), ahol \(P_1\) felbonthatatlan és \(q_1\) nem egység.

Ha \(q_1\) felbonthatatlan, akkor készen vagyunk; ha nem, akkor van olyan \(P_2\) felbonthatatlan szám, amellyel \(q_1 = p_2 q_2\), ahol \(q_2\) nem egység.

Hasonlóan járunk el \(q_2\) -vel stb. Eljárásunk véges sok lépésekben be kell hogy fejeződjön, ugyanis az \(|q_2|\) számok pozitív egészek, és szigorúan esőkően sorozatot alkotnak:

\[|a| > |q_1| > |q_2| > \ldots,\]

tehát eljutunk egy olyan \(a_k\) -hoz, amely már felbonthatatlan, \(a_k = p_k\).

Ekkor az \(a = p_1 p_2 \ldots p_k\) előállítást nyerjük. □

Az egyértelműség első bizonyítása: Ebben a bizonyításban a fő segédeszközünk az lesz, hogy minden felbonthatatlan egyben prím is (T 1.4.3 Tétel).

Tegyük fel indirekt, hogy valamely \(a\) -nak létezik (legalább) két lényegesen különböző felbontása felbonthatatlanok szorzatára:

\[a = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s.\]

Ha itt valamelyik \(p_i\) egységszerese valamelyik \(q_j\) -nek, például \(p_1 = \bar{q}_1\), akkor \(p_1\) -gyel egyszerűsítve

\[a' = \frac{a}{q_1} = (\bar{z}q_2)p_3 \ldots p_r = q_2 q_3 \ldots q_s,\]

adódik, vagyis az \(a'\) számnak kapjuk két lényegesen különböző felbontását felbonthatatlanok szorzatára.

Az eljárást folytatva így végül egy olyan számhoz jutunk, amelynek a kétféle felbontásában már nincsenek egységszeres tényezők. Az általánosság megszorítása nélkül feltéthetjük, hogy az (1)-beli előállítás ilyen, azaz \(p_k \nmid \bar{z}q_i\).

(1)-ből kapjuk, hogy \(P_1 | q_1 q_2 \ldots q_s\). Mivel \(P_1\) felbonthatatlan, így az T 1.4.3 Tétel alapján prim is, ezért \(P_1\) szükségképpen osztója legalább az egyik \(q_j\) tényezőnek.

Azonban ha \(P_1 | q_j\), akkor \(q_j\) felbonthatatlansága miatt \(P_1\) vagy egység, vagy pedig a \(q_j\) egységszerese, és mindkettő ellentmondás. □

Az egyértelműség második bizonyítása: Ebben a bizonyításban \(|a|\) -ra vonatkozó teljes indukciót használunk.
Mivel egy szám és az egységszerei minden oszthatósági szempontból egyenértékűek, ezért nem jelent megszorítást, ha pozitív egésznek pozitív felbonthatlanok szorzatára való felbontásaival foglalkozunk.

Ha \( a = 2 \), akkor az egyértelműség (a 2 felbonthatlan volta miatt) igaz.

Tegyük most fel, hogy minden \( 1 < a < n \) szám egyértelműen bomlik fel felbonthatlanok szorzatára, és megmutatjuk, hogy ekkor \( a = n \) felbontása is egyértelmű. Tegyük fel indirekt, hogy \( n \)-nek létezik (legalább) két különböző felbontása felbonthatlanok szorzatára:

\[
\begin{align*}
\nu &= p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s. 
\end{align*}
\]

Itt nyilván \( r \geq 2, \quad s \geq 2 \), továbbá \( p_i \neq q_1 \), mert ha például \( \nu = q_1 \), akkor az \( 1 < n/p_1 < n \) számok két különböző felbontása lenne, ami ellentmond az indukciós feltevésnek.

Tegyük fel, hogy \( \nu_1 < q_1 \) és legyen \( \nu_1 = \nu - \nu_1 q_2 \cdots q_s \). Megmutatjuk, hogy

\[
1 < \nu_1 < \nu, 
\]

és

\[
\nu_1 \text{-nek is van két különböző felbontása,} 
\]

ami ellentmondás.

Az \( \nu_1 = \nu - \nu_1 q_2 \cdots q_s \) kifejezésbe \( n \) helyére a (2)-beli felbontásokat beírva kapjuk, hogy

\[
\nu_1 = \nu q_2 \cdots q_s (q_1 - 1) = q_2 \cdots q_s (q_1 - 1). 
\]

Nyilván \( \nu_1 < \nu \), továbbá \( \nu_1 < q_1 \) miatt

\[
\nu_1 = q_2 \cdots q_s (q_1 - 1) \geq q_2 \cdot 1 = q_2 > 1, 
\]

ami ellentmondás.

Bontsuk fel az \( \nu_1 \) mindkét (5)-beli szorzat-előállításának utolsó tényezőjét felbonthatlanok szorzatára:

\[
q_2 \cdots q_s (q_1 - 1) = q_1 \cdots q_k. 
\]

Ennek alapján az \( \nu_1 \) az alábbi módon áll elő felbonthatlanok szorzataként:

\[
\nu_1 = q_2 \nu_1 \cdots q_k = q_2 \cdots q_k. 
\]

(Ha esetleg \( q_1 - 1 = 1 \), akkor (6) úgy értendő, hogy a \( q_i \)-k hiányoznak, a további gondolatmenet ekkor „még inkább” érvényben marad.)

Megmutatjuk, hogy (6) az \( \nu_1 \) két különböző felbontását adja. Az első felbontásban szerepel a \( \phi_1 \). A másodikban viszont nem, ugyanis egyképpen \( \phi_1 \neq q_j \), másrészt, ha valamelyik \( i \)-re \( \phi_1 = q_i \), akkor

\[
\phi_1 | \nu_1 \cdots \nu_{k_1} = q_1 - p_1 \implies \phi_1 | q_1 
\]

következne, ami lehetetlen. Ezzel (4)-et is beláttuk. ∎

Megjegyzések: 1. Az egyértelműség első bizonyítását elemezve megállapíthatjuk, hogy az tulajdonképpen a maradékos osztáson múlt. Ugyanis a maradékos osztásra támogató euklideszi algoritmus is igazoltuk a kitüntetett közös osztó létezését, majd ennek felhasználásával mutattuk meg
(az T 1.3.9 Tétel segítségével), hogy egy felbonthatatlan szám szükségképpen prim is, és ez volt a bizonyítás kulcslépése.

Általában is igaz, hogy ha egy számkörben (illetve integratív tartományban) létezik a maradékos osztás megfelelője, akkor ott érvényes a szármelélet alaptétele is. Az egyértelműségi részre az egész számnoknál adott gondolatmenetünk az általános esetre is szó szerint átiható, a felbonthatóságnál esetenként finomabb meggondolásokra is szükség lehet. Ennek megfelelően a példák szerepelnek majd a 7. és 10. fejezetben. A 11.3 pontban az ideálok segítségével az általános esetben is egységes bizonyítást adunk arra, hogy a maradékos osztásból következik a szármelélet alaptétele (felbonthatóság és egyértelműség egyaránt).

Megjegyezzük még, hogy a maradékos osztás és az alaptétel kapcsolata nem szimmetrikus; vannak olyan számkörök, amelyekben érvényes a szármelélet alaptétele, noha semmilyen értelmenben sem létezik bennük maradékos osztás. Ilyen példát láthatunk majd a 10. fejezetben.

2. Az egyértelműség második bizonyítása nem támaszkodott az 1.3 és 1.4 pontok tételeire. Ez lehetőséget ad arra, hogy ezeknek a tételeknek egy részére az alaptétel segítségével új bizonyítást adjunk. Ezek közül két fontos téttel különböző létekéssel az egész számoknál, az új bizonyítás értékeletünk az alaptételből. Ez az utóbbiakban feltételezésének lényegében az T 1.6.4 Tétel bizonyításánál láthatjuk meg, az útjuk hátságának 1.5.8 feladatot [21].

Feladatok

1.5.1 Igazoljuk, hogy egy $a$ szám felbonthatatlan számok szorzataként történő előállításában a tényezők száma legfeljebb $\lfloor \log_2 |a| \rfloor$.

1.5.2 Tekintsük a páros számok körét.

(a) Mely elemek írhatók fel lényegében egyértelműen felbonthatatlanok szorzataként?

(b) Adjunk meg olyan elemet, amelynek pontosan 1000 lényegesen különböző felbontása van.

1.5.3 Vizsgáljuk meg, hogy az egyértelműségre adott bizonyításaink hol buknak meg a páros számok körében?

1.5.4 Mutassuk meg, hogy a 10-zel osztható egész számok körében nem érvényes a szármelélet alaptétele, sőt itt van olyan elem is, amelynek két különböző felbontásában még a felbonthatatlan tényezők darabszámára sem azonos.

1.5.5 Tekintsük a véges tizedes törtek $V$ halmazát.

(a) Határozzuk meg az egységeket és a felbonthatatlanokat.

(b) Bizonyítsuk be, hogy $V$ -ben érvényes a szármelélet alaptétele.

(c) Lássuk be, hogy $V$ -ben létezik a maradékos osztás megfelelője, azaz minden $c \in V$ elemhez hozzá tudunk rendelni egy $f(c)$ nemnegatív egész számot úgy, hogy $f(c) = 0 \iff c = 0$, továbbá minden $a, b \in V$, $b \neq 0$ esetén létezik olyan $q, r \in V$, hogy $a = bq + r$ és $f(r) < f(q)$.

1.5.6 Az egyértelműségre adott második bizonyításnak sok más változata is elkészíthető. Hol kell módosítani a gondolatmenetet, ha $v_1 - v_2 = \mathbb{P} \mathbb{Z}$ -nek vásároljuk?

1.5.7 Hányféleképpen írható fel egy egész szám felbonthatatlanok szorzataként, ha most a csak a sorrendben és/vagy egységészeresekben való eltérést is különböző felbontásnak tekintjük?

1.5.8 (M [551]) Vezzessük le a szármelélet alaptételéből, hogy minden felbonthatatlan egyben prim is.
1.5.9 Keressük meg (az egészek körében) az összes olyan \( p_1 \cdot p_2 \cdot p_3 \) (nem feltétlenül pozitív és nem feltétlenül különböző) prímszámokat, amelyekre

\[
\frac{1}{p_1 - p_2 - p_3} = \frac{1}{p_2} + \frac{1}{p_3}.
\]

1.5.10 (M [552]*) Adjuk meg (az egészek körében) az összes olyan pozitív prímszámot, amelynek alkalmas (pozitív egész kitevős) hatványa felírható két pozitív egész szám köbének az összegeként.

1.6 Kanonikus alak

A továbbiakban csak pozitív számok pozitív osztóival foglalkozunk, és prímszámon is pozitív felbontatlan számot fogunk érteni. Ebben az esetben a számelmélet alaptétele úgy fogalmazható, hogy minden \( n > 1 \) egész szám felbontatható véges sok (pozitív) prímszám szorzatára, és ez a felbontás a tényezők sorrendjétől eltekintve egyértelmű. (Az egységek a pozitivitás miatt most nem játszanak szerepet.)

Az ilyen primitív alakos előállításban az azonos prímek szorzatát általában hatványcént jellejük, vagyis a számot különböző prímek hatványainak a szorzataként írjuk fel. Ekkor a számelmélet alaptételenek az alábbi alakját kapjuk:

1.6.1 Tétel. \( \text{T 1.6.1} \)

Minden \( n > 1 \) egész szám felírható

\[
\alpha = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i}
\]

alakban, ahol \( p_1, \ldots, p_r, \) különböző (pozitív) prímek és \( \alpha_i > 0 \) egész. Ez a felírás a \( p_i^{\alpha_i} \) prímkonyvtényezők sorrendjétől eltekintve egyértelmű.

Ezt az előállítást az \( n \) szám kanonikus alakjának nevezzük.

Látjuk, hogy bizonyos esetekben (például több szám egyidejű vizsgálatánál) kényelmesebb, ha megengedjük, hogy a kanonikus alakban egyes prímek kitevője 0 is lehessen, ekkor az egyértelműség természetesen ezekből (ez esetleges fiktív) tényezőkből eltekintve értendő. Ily módon az 1 számnak is beszélhetünk kanonikus alakjáról (ebben csak 0 kitevővel szerepelnek prímek). Külön fognak jelzébe lépni, mikor érdemes a 0 kitevőt is megengedni a kanonikus alakban, a többi esetben automatikusan feltesszük, hogy minden kitevő pozitív (egész).

Először azt mutatjuk meg, hogyan tekinthetők át a kanonikus alak segítségével egy szám osztói, a szám legnagyobb közös osztója és legkisebb közös többszöröse.

1.6.2 Tétel. \( \text{T 1.6.2} \)

Az

\[
\alpha = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}
\]

kanonikus alakú \( \alpha \) számnak egy \( d \) pozitív egész akkor és csak akkor osztója, ha \( d \) kanonikus alakja

\[
d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_r^{\beta_r}, \quad \text{ahol} \quad 0 \leq \beta_i \leq \alpha_i, \quad i = 1, 2, \ldots, r.
\]

Az osztók esetében a 0 kitevőt is megengedő módosított kanonikus alakot használtuk.
Az 1, illetve \( \mathfrak{n} \) triviális osztókat abban a két speciális esetben kapjuk meg, amikor (minden \( \mathfrak{i} \)-re)
\( \beta_{\mathfrak{i}} = 0 \), illetve \( \beta_{\mathfrak{i}} = \alpha_{\mathfrak{i}} \).

**Bizonyítás:** Az elégségesség igazolásához tegyük fel, hogy \( d \) a fenti alakú. Ekkor a
\[
q = p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2 - \beta_2} \cdots p_r^{\alpha_r - \beta_r},
\]
szám \( \alpha_i \geq \beta_i \) miatt egész, és \( \mathfrak{n} = d \cdot q \), vagyis \( d \mid \mathfrak{n} \). (Ennél a résznél nem használtuk ki a kanonikus alak egyértelműségét, sőt azt sem, hogy a \( \mathfrak{p}_i \)-k prímek.)

A szükségességhoz tegyük fel, hogy \( d \mid \mathfrak{n} \), azaz van olyan \( q \) ( pozitív) egész, amelyel \( \mathfrak{n} = d \cdot q \). Ekkor \( \mathfrak{n} \) kanonikus alakját a \( d \) és a \( q \) kanonikus alakjának az összeszorzásából kapjuk meg. Ez azt jelenti, hogy \( \mathfrak{n} \) kanonikus alakjában \( d \) minden prímosztója szerepel, éspedig legalább akkora hatványon, mint \( d \)-ben, vagyis \( \alpha_i \geq \beta_i \). ■

Egy \( \mathfrak{n} > 0 \) egész pozitív osztóinak a számát \( \mathcal{d}(\mathfrak{n}) \)-nel jelöljük.

**Példa:** \( \mathcal{d}(1) = 1 \), \( \mathcal{d}(10) = 4 \), \( \mathcal{d}(11) = 2 \iff \mathfrak{n} \) prim.

### 1.6.3 Tétel.

**T 1.6.3**

Az
\[
\mathfrak{n} = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}
\]
kanonikus alakú \( \mathfrak{n} \) szám pozitív osztóinak a száma
\[
\mathcal{d}(\mathfrak{n}) = (\alpha_1 + 1)(\alpha_2 + 1)\cdots(\alpha_r + 1).
\]

**Bizonyítás:** Az T 1.6.2 Tétel szerint az \( \mathfrak{n} \) összes pozitív osztóját úgy kapjuk meg, ha a
\[
d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r},
\]
kifejezésben a \( \beta_1, \beta_2, \ldots, \beta_r \) kitevők egymástól függetlenül végigfutnak a
\[
\beta_1 = 0, 1, \ldots, \alpha_1, \quad \beta_2 = 0, 1, \ldots, \alpha_2, \quad \ldots, \quad \beta_r = 0, 1, \ldots, \alpha_r,
\]
értékeken. A \( \beta \) kitevő tehát \( \alpha_i + 1 \)-féléképpen választható, és így a \( \beta \)-kitevők egymástól független megválasztására összesen
\[
(\alpha_1 + 1)(\alpha_2 + 1)\cdots(\alpha_r + 1)
\]
lehetőség van. Mivel az \( \mathfrak{n} \) minden pozitív osztójá csak egyféleképpen áll elő a fenti alakban (hiszen ennek az osztóknak is egyértelmű a prímtevékenység felbontása), ezért az (1) képlet valóban az \( \mathfrak{n} \) pozitív osztóinak a számát adjá. ■

Most rátérünk két szám legnagyobb közös osztójának a kanonikus alakjára. Itt ismét a módosított kanonikus alakkal dolgozunk: mindkét számnál küljük azokat a primszámokat is, amelyek csupán az egyik számnak osztói (a másik szám kanonikus alakjában ezek természetesen 0 kitevővel szerepelnek).

### 1.6.4 Tétel.

**T 1.6.4**

Legyen az \( a \) és \( b \) pozitív egészken kanonikus alakja
\[ a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r} \quad \text{és} \quad b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_r^{\beta_r}, \quad \text{ahol} \quad \alpha_i \geq 0, \beta_j \geq 0. \]

Ekkor

\[ (a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdot p_2^{\min(\alpha_2, \beta_2)} \cdots p_r^{\min(\alpha_r, \beta_r)} \]

(ahol \( \min(\alpha_i, \beta_i) \) az \( \alpha_i \) és \( \beta_i \) számok közül a kisebbiket jelenti, ha \( \alpha_i \neq \beta_i \), illetve a közös értéküket, ha \( \alpha_i = \beta_i \).)

Bizonyítás: Legyen

\[ d = \prod_{i=1}^{r} p_i^{\gamma_i}, \quad \text{ahol} \quad \gamma_i \leq \alpha_i, \gamma_i \leq \beta_i. \]

Azt fogjuk megmutatni, hogy \( d \) egyrészt közös osztója \( a \) -nak és \( b \) -nek, másrészt pedig minden közös osztónak többszöröse. A bizonyításban az T 1.6.2 Tételre fogunk támaszkodni.

Mivel \( \min(\alpha_i, \beta_i) \leq \alpha_i \) és \( \min(\alpha_i, \beta_i) \leq \beta_i \), ezért \( d \) \( a \) és \( d \) \( b \), azaz \( d \) közös osztó.

Legyen most \( c \) az \( a \) és \( b \) tetszőleges pozitív közös osztója. Ekkor

\[ c = \prod_{i=1}^{r} p_i^{\gamma_i}, \quad \text{ahol} \quad \gamma_i \leq \alpha_i, \gamma_i \leq \beta_i. \]

Ez azt jelenti, hogy \( \gamma_i \leq \min(\alpha_i, \beta_i) \), és így \( c \mid d \). □

példa: Számítsuk ki 4840 és 2156 legnagyobb közös osztóját.

A számok kanonikus alakja: \( 4840 = 2^3 \cdot 5 \cdot 11^2 \) és \( 2156 = 2^2 \cdot 7^2 \cdot 11 \). Tehát \( (4840, 2156) = 2^1 \cdot 5^0 \cdot 7^0 \cdot 11 = 44 \).

Megjegyzés: A legnagyobb közös osztó fenti kiszámítási módja nagyon kényelmesnek tűnik, sajnos azonban nagy számokra általában nem alkalmazható, ugyanis nem ismerünk gyors eljárást nagy számok esetén a kanonikus alak meghatározására. Az euklideszi algoritmus ugyanakkor nagy számok esetén is gyorsan megadja a két szám legnagyobb közös osztóját. Mindezekről (alkalmazásokkal együtt) részletesen az 5.7 és 5.8 pontban lesz szó.

Rátérve a legkisebb többszörössére, ez nevének megfelelően a pozitív közös többszörösök közül a legkisebbet jelenti:

1.6.5 Definíció . D 1.6.5

Az \( a \) és \( b \) pozitív egészek legkisebb közös többszörése a \( k \) pozitív egész, ha

(i) \( a \mid k \), \( b \mid k \); és

(ii) ha egy \( c > 0 \)-ra \( a \mid c \), \( b \mid c \) teljesül, akkor \( c \geq k \). □

Az \( a \) és \( b \) legkisebb közös többszörését \([c, b]\) -vel (vagy \( \text{lkt}(a, b) \)-vel) jelöljük.

Mivel a két szám szorza, \( ab \) nyilvánvalóan közös többszöröse \( a \)-nak és \( b \)-nek, így \([a, b]\) meghatározásához elég az \( cb \)-nél nem nagyobb véges sok pozitív egész között megkeresni az \( a \) és \( b \) közös többszörösei közül a legkisebbet. A legkisebb közös többszörös létezése és egyértelműsége tehát nyilvánvaló.
A legnagyobb közös osztónál látottakhoz hasonlóan azonban a legkisebb közös többszörösnél is — a definícióban szereplő „legkisebbég” helyett — inkább egy speciális oszthatósági tulajdonságot játszik fontos szerepet: a legkisebb közös többszörös minden közös többszörősnek osztója (szokás a legkisebb közös többszöröst egyenesen ezzel a tulajdonsággal definiálni). Ezt és a legkisebb közös többszörösre vonatkozó további alapvető eredményeket a következő tételben foglaljuk össze:

1.6.6 Tétel. T 1.6.6

I. Ha az \(a\) és \(b\) pozitív egészek kanonikus alakja

\[
a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} \quad \text{és} \quad b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}, \quad \text{ahol} \quad \alpha_i \geq 0, \beta_j \geq 0,
\]

akkor

\[
[a, b] = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \ldots p_r^{\max(\alpha_r, \beta_r)}
\]

(ahol \(\max\{\alpha_i, \beta_i\}\) az \(\alpha_i\) és \(\beta_i\) számok közül a nagyobbikat jelenti, ha \(\alpha_i < \beta_i\), illetve a közös értékeket, ha \(\alpha_i = \beta_i\)).

II. \(a \mid c, b \mid e \iff [a, b] \mid c\).

III. \([a, b][c, d] = [a, c][b, d]\).

Bizonyítás: I. és II. Egy \(c\) pozitív egész akkor és csak akkor közös többszöröse \(a\) -nak és \(b\) -nek, ha \(c \mid a\) és \(c \mid b\) egyszerre érvényes. Ez azt jelenti, hogy \(c\) kanonikus alakjában mindegyik \(p_i\) prim kitevőjére \(\gamma_i \geq \alpha_i\) és \(\gamma_i \geq \beta_i\) teljesül, ez pedig azzal ekvivalens, hogy \(\gamma_i \geq \max(\alpha_i, \beta_i)\).

Az ilyen \(c\) számok közül az a legkisebb, amikor egyrészット \(\gamma_i = \max(\alpha_i, \beta_i)\) (\(i = 1, 2, \ldots, r\)), másrészt \(c\) a \(p_i\)-ken kívül más primékekkel egyáltalán nem osztható. Ezzel beláttuk, hogy \([a, b]\) kanonikus alakja valóban az I-beli.

Azt is kaptuk, hogy az összes \(c\) közös többszörös kanonikus alakjában a \(p_i\)-k kitevője legalább akkora, mint \([c, d]\)-ben, és emellett ezekben más primek is előfordulhatnak, vagyis a \(c\) közös többszöröseök éppen az \([a, b]\) többszöröseivel egyeznek meg. Ezzel II-t is igazoltuk.

III. Megmutatjuk, hogy \([a, b][c, d]\) és \(a\) \(b\) kanonikus alakjában mindegyik \(p_i\) prim ugyanakkora kitevővel szerepel, vagyis

\[
\min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i) = \alpha_i + \beta_i, \quad i = 1, 2, \ldots, r.
\]

Ha például \(\alpha_i \leq \beta_i\), akkor itt a bal oldalon \(\alpha_i + \beta_i\) áll, ami valóban ugyanaz, mint a jobb oldal.

Megjegyzések: 1. A III. összefüggés fontos speciális eseteként kapjuk, hogy

\[
a \mid [c, d] \iff \min(\gamma_c, \gamma_d) = 1.
\]

2. Ne felejtjük el, hogy \(a \mid c\) és \(b \mid c\) fennállásából nem következik \(ab \mid c\), például \(4 \mid 36, 5 \mid 36\), azonban \(24 \mid 36\). A helyes következtetést éppen II-ből kapjuk:

\[
a \mid c, b \mid e \iff [a, b] \mid c.
\]

Ha \(a\) és \(b\) relatív primek, akkor az előző megjegyzés szerint \([a, b] = ab\), és ekkor az alábbi fontos speciális esetet nyerjük:
Például 72 | c igazolásához elegendő azt belátni, hogy a c: 8-cal és 9-cel is osztható. Általában is, bármely osztathatósági kérdés visszavezethető primhatványokkal való osztathatóságokra: ha \( m = \prod_{i=1}^{r} p_i^{\alpha_i} \) (\( \alpha_i > 0 \)), akkor
\[ m \mid c \iff p_i^{\alpha_i} \mid c, \quad i = 1, 2, \ldots, r. \]

3. A legkisebb közös többszörös fogalma és fő tulajdonságai kettőnél több számra is átvihetők. Kiemeljük, hogy véges sok pozitív egész legkisebb közös többszöröse akkor és csak akkor egyenlő a szorzatukkal, ha páronként relatív prímek. Megjegyezzük még, hogy a III. egyenlőségnek nincs közvetlen egyszerű általánosítása több szám esetére (lásd az 1.6.15 feladatot [29]).

A számelmélet alaptételéből (is) következik, hogy két szám akkor és csak akkor relatív prím, ha nincs közös prímosztójuk. Ebből azonnal adódik az alábbi tétel:

1.6.7 Tétel. T 1.6.7

Ha két pozitív egész relatív prím, akkor általában az alábbi formában célszerű a kanonikus alakjukat megadni:
\[ a = \prod_{i=1}^{\varphi} p_i^{\alpha_i}, \quad b = \prod_{i=1}^{\lambda} q_i^{\beta_i}, \quad p_i \neq q_j. \]

Végül az \( n! \) kanonikus alakját tárgyaljuk:

1.6.8 Tétel. T 1.6.8

Az \( n! \) kanonikus alakja
\[ n! = \prod_{p \leq n} p^{\epsilon_p}, \quad \text{ahol} \quad \epsilon_p = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor. \]

A fenti képletben \( \lfloor x \rfloor \) az \( x \) szám (alsó) egészrész, és a produktum jel alatti \( p \) (pozitív) prímet jelent, azaz a sorozatot az összes olyan \( p \) prim szerint kell képezni, amelyre \( p \leq n \). Ilyen típusú jelölésekkel később is gyakran találkozunk majd, például
\[ \sum_{p \leq n} 1, \quad \prod_{p \leq n} p, \quad \sum_{p | n} 1. \]

rendre az \( n \) -nél nem nagyobb prímek reciprokosszegét, az \( n \) -nél nem nagyobb prímek sorzatát, illetve az \( n \) különböző prímosztóinak a számát jelenti.

Megjegyezzük még, hogy az T 1.6.8 Tételnél az \( a_p \) kitévőt előállító összegben elég csak véges sok tagot tekinteni, mert ha \( p^{k} > n \), akkor \( [n/p^k] = 0 \) (a nemnulla tagok száma tehát \( \lfloor \log_p n \rfloor \)).

Bizonyítás: Mivel az \( \frac{1}{1} \cdot \frac{1}{2} \cdot \cdots \cdot \frac{1}{n} \) szorzat mindegyik tényezője legfeljebb \( n \), ezért \( n \) -nél nagyobb prímszám nem fordul elő \( n! \) kanonikus alakjában.

Legyen \( \forall \leq n \) tetszőleges rögzített prim, és jelölje \( \epsilon_p \) a \( p \) kitévőjét az \( n! \) kanonikus alakjában. Azt kell igazolnunk, hogy
Az \( \alpha_\nu \) meghatározásához bontsuk az \( 1, 2, \ldots, \nu \) számok mindegyikét prímek szorzatára, és számoljuk össze, hogy összesen hányszor fordul elő ezek között a \( P^t \).

Minden \( P \)-vel osztható számban szerepel legalább egy darab \( P \), először ezeket vesszük számítsásba. A \( P \)-vel osztható számok a következők:

\[
p, 2p, \ldots, tp, \quad \text{ahol} \quad tp \leq \nu < (t + 1)p.
\]

Innen

\[
t \leq \frac{\nu}{p} < t + 1, \quad \text{vagyis} \quad t = \left\lfloor \frac{\nu}{p} \right\rfloor.
\]

Ez azt jelenti, hogy az \( 1, 2, \ldots, \nu \) egészek között a \( P \)-vel oszthatók száma \( \lfloor \nu/p \rfloor \).

A \( P^2 \) többszörösei legyen két darab \( P \)-szerep, ezekből azonban eddig csak egyet vettünk figyelembe. Így a \( P^2 \) minden többszöröse egy-egy „újabb” \( P \)-t jelent. Ezek száma az előzők között teljesen hasonlóan \( \lfloor \nu/p^2 \rfloor \).

Ugyanígy haladunk tovább. A \( P^3 \) többszörösei egy-egy újabb \( P \)-t adnak, hiszen az ezekben előforduló legalább három darab \( P \)-ból az első két lépésben még csak kettőt vettünk figyelembe. Ez további \( \lfloor \nu/p^3 \rfloor \) darab \( P \)-t jelent stb.

Az eljárás véges sok lépésben befejeződik, hiszen ha \( p^k > \nu \), akkor az \( 1, 2, \ldots, \nu \) számok egyike sem osztható \( p^k \)-nal.

A fenti módon az \( \nu \)-ban szereplő összes \( P \)-t pontosan egyszer vettük figyelembe, vagyis \( \alpha_\nu \) valóban a (2)-ben megadott összeggel egyenlő.

## Feladatok

(A feladatokban számon, osztón, prímszámon stb. mindig pozitív számot értünk.)

### 1.6.1
Hogyan olvasható le egy szám kanonikus alakjából, hogy négyzetszám, köbszám, illetve általában \( k \)-adik hatvány (azaz egy pozitív egész \( k \)-adik hatványa)?

### 1.6.2
(a) Mutassuk meg, hogy ha két relatív prim szám szorzata \( k \)-adik hatvány, akkor külön-külön is \( k \)-adik hatványok.

(b) Hogyan kell módosítani ezt az állítást, ha (a pozitív egészek helyett) az összes egész számot tekintjük?

(c) Hogyan általánosítható az állítás (kettőnél) több tényezős szorzat esetére?

### 1.6.3
(M [552]) Bizonyítsuk be, hogy

(a) 2;

(b) 3;
(c) 4 egymást követő ( pozitív egész) szám szorzata nem lehet teljes hatvány (azaz egy egész szám egyenlő nagyobb egész kiterjesztve hatvánýa).

Megjegyzés: Általában is igaz, hogy egymást követő pozitív egészek szorzata sohasem lehet teljes hatvány. Ezt a Catalantól származó és hosszú ideig megoldatlan sejtést Erdős Pál és John Selfridge bizonyították be 1975-ben.

1.6.4 (M [553]) Mely \( p \) primszámok esetén lesz \( \left( 2^{p-1} - 1 \right)/p \) négyzetszámmal?

1.6.5 (a) Bizonyítsuk be, hogy \( c \mid ab \iff c = a_1b_1 \), ahol \( a_1 \mid c \) és \( b_1 \mid b \).

(b) Mutassuk meg, hogy ha \( \langle a, b \rangle = 1 \), akkor (adott \( c \mid ab \)-hez) a fénti \( a_1 \) és \( b_1 \) egyértelmű.

(c) Lássuk be, hogy ha \( \langle a, b \rangle \neq 1 \), akkor van olyan \( c \mid ab \), amely többféleképpen is előáll \( c = a_1b_1 \) alakban.

(d) Bizonyítsuk be, hogy bármely \( c \mid ab \) legfeljebb \( d(\langle c, b \rangle) \)-féleképpen áll elő \( c = a_1b_1 \) alakban.

(e) Mely \( c \mid ab \) osztóknak létezik \( d(\langle c, b \rangle) \)-féle \( c = a_1b_1 \) típusú előállítása?

1.6.6 Tegyük fel, hogy minden \( k \)-ra \( a^k \mid b^{k+100} \). Bizonyítsuk be, hogy \( a \mid b \).

1.6.7 Melyik az a legkisebb pozitív egész, amelynek pontosan

(a) 31;

(b) 33;

(c) 32

( pozitív) osztója van?

1.6.8 Mely \( n \)-ekre lesz \( d(n) \) páratlan?

1.6.9 Egy kegyetlen várú röntönlének 400 szűk cellájában egy-egy rab sínlylódik. A cellák ajtaján levő zár úgy működik, hogy egy elfordítás esetén nyílik, még egy elfordítás esetén ismét bezárul stb. Jelenleg természetesen minden ajtó zárva van. A várú a születésnapján elhatározza, hogy nagylelkű lesz, és megpróbálja megnyitni mindet. Az azonban azonban megmondja magát, és utánaküld egy másik őrt, akit azzal bíz meg, hogy minden második záron fordítson egyet. Ezt követi a harmadik őr, aki a harmadik záron változtat stb., végül a negyedik őr a negyedik cella zárjának az állását módosítja. Azok a rabok szabadulnak ki, akiknek most nyitva áll az ajtaja. Hány rabot bocsátott szabadon a várúr?

1.6.10 (M [554]) Egy természetes számon \( n \) egész nevezünk, ha nem osztható semmilyen egynél nagyobb egész szám négyzetével. Például az 1 vagy a 30 négyzetmentes, a 12 viszont nem. Egy \( n \) szám (pozitív) négyzetmentes osztóinak a számát jelöljük \( A(n) \)-nel, a négyzetszámok számát pedig \( D(n) \)-nel.

(a) Bizonyítsuk be, hogy bármely \( n \)-re \( A(n)D(n) \geq d(n) \).

(b) Mely \( n \)-kre áll egyenlőség?

1.6.11 Mutassuk meg, hogy

(a) \( d(n) \leq n/2 + 1 \);

(b) \( d(n) \leq n/3 + 2 \).
1.6.12 Mivel egyenlő egy \( n \) szám (pozitív) osztóinak a szorzata?

1.6.13 A \( 10^p \) osztóból maximálisan hányat lehet kiválasztani úgy, hogy ezek közül egyik se legyen osztója valamelyik másiknak?

1.6.14 (a) Mely \( a, b \) számpárokhoz találhatók olyan pozitív egészek, amelyek legnagyobb közös osztója \( a \) és legkisebb közös többszöröse \( b \)?
(b) Hány ilyen számpár létezik, ha \( a = 5 \) és \( b = 35030 \)?
(c) Általában is határozzuk meg az ilyen számpárok számát (tetszőleges \( a, b \) esetén).

1.6.15 Bizonyítsuk be az alábbi állításokat.
(a) \( \{(a, b, c) \mid a, b, c \} | abc \), de általában nem áll fenn egyenlőség.
(b) \( \{a, b, c\} | abc \) \( \iff \) \( a, b, c \) páronként relatív prímek.
(c) \( \{ab, bc, ac\} | abc \).

1.6.16 Melyek igazak az alábbi állítások közül?
(a) \( (a, b) = (a + b, ab) \).
(b) \( (a, b) = 1 \iff (a + b, ab) = 1 \).
(c) \( (a, b) = (a, b)(a, c) \).
(d) \( (a^3, b^3) = (a, b)^3 \).

1.6.17 Bizonyítsuk be az alábbi állításokat.
(a) \( a, b \mid a + b \iff a = b \).
(b) \( a + b \mid [a, b] \) sohasem teljesül.
(c) Van végтelen sok olyan \( a \neq b \), amelyre \( a + b \mid ab \).
(d) \( a + b \mid ab \iff a + b \mid (a, b)^2 \).

1.6.18 Lássuk be, hogy ha \( (a, b^2) = (a^2, b) \), akkor \( (a^7, b^{1000}) = (a^{1000}, b^7) \).

1.6.19 Igazoljuk az alábbi „disztributivitási” azonosságokat.
(a) \( [a, (b, c)] = ([a, b], [a, c]) \).
(b) \( (a, [b, c]) = ([a, b], [a, c]) \).

1.6.20 (a) Bizonyítsuk be, hogy az \( a, b \) és \( c \) pozitív egészekhez akkor és csak akkor létezik olyan \( x, y \) és \( z \), amelyekkel
\[
(x, y) = a, \quad (y, z) = b \quad \& \quad (z, x) = c.
\]
ha \((u, b) = (b, r) = (c, a)\). 

(b) Hány ilyen \(x, y, z\) számhármas létezik (adott \(a, b, c\) esetén)?

(c) Vizsgáljuk meg a „duális” problémát legnagyobb közös osztók helyett legkisebb közös többszörösekre.

1.6.21 Igazoljuk, hogy ha \(P\) egy 5-nél nagyobb prim, akkor \(2 \cdot 10 \mid p^4 - 1\).

1.6.22 Lássuk be, hogy ha \(\langle a, b, 42 \rangle = 1\), akkor \(504 \mid a^6 - b^6\).

1.6.23 Mutassuk meg, hogy \(a^3 + 85c^4 + 294c^2\) bármely \(a\) esetén osztható 360-tal.

1.6.24 Bizonyítsuk be, hogy \(20^{101} - 33^{101} + 7^{101}\) osztható \(6!\)-tal.

1.6.25 Hány 0-ra végződik (a) \(1111!\); (b) \((1225)!\)?

1.6.26 (a) Bizonyítsuk be, hogy ha \(c > 1\), akkor \(c^2 \mid c!\).

(b) Adjuk meg azokat az \(u, v\) és \(c > 1\) számokat, amelyekre \(c^{c+1} \mid c!\).

1.6.27 Legyen \(n \geq 2\) és \(1 \leq k \leq n - 1\).

(a) Mutassuk meg, hogy ha \(k\) és \(n\) relatív prímek, akkor \(n \mid \binom{n}{k}\).

(b) Igaz-e az (a)-beli állítás megfordítása?

(c) Melyek azok az \(u\) -ek, amelyekre minden \(1 \leq k \leq n - 1\) esetén

\(\begin{align*}
& (c1) \ n \mid \binom{n}{k} \\
& (c2) \ (\frac{n}{k}) \ páros; \\
& (c3) \ (\frac{n}{k}) \ páratlan?
\end{align*}\)

(d) Van-e olyan \(n\) és \(1 \leq k \leq n - 1\), amelyre \(n\) és \(\binom{n}{k}\) relatív prímek?

1.6.28 (M [554]) Egy kerek asztal körül véges sok rozmár ül, és a következő játékot játszak. Mindegyikük előtt egy tízforintos fekszik az asztalon. Vezérszóra mindegyik rozmár megnézi a jobb oldali szomszédja előtti tízforintost: ha fejet lát, akkor megfordítja a saját tízforintosát; ha írást lát, akkor nem csinál semmit. Ezt addig ismételgetik, amíg mindegyik tízforintos írást nem mutat. Mekkora lehet a rozmárok száma, ha a tízforintosok tetszőleges kiinduló helyzete esetén a játék előbb-utóbb véget ér?

1.6.29 (M [555]) Mutassuk meg, hogy az \(n! + 1, \ldots, n! + n\) számok mindegyikének van olyan prímosztója, amely a többi \(n - 1\) szám egyikének sem osztója.

1.6.30 (M [555]) Tekintsünk 5000 különböző pozitív egész, amelyek közül bármely tíznek ugyanaz a legkisebb közös többszöröse. Maximálisan hány szám lehet közöttük, amelyek páronként relatív prímek?

1.6.31 Mely \(n\) pozitív egészek rendelkeznek az alábbi tulajdonsággal: \(n \mid k^2 \longrightarrow n \mid k\) (azaz \(n\) egy szám négyzetének csak úgy lehet osztója, ha magának a számnak is osztója)?
1.6.32 Mutassuk meg, hogy (\(k > 1\) esetén) két \(k\)-adik hatvány különbsége sohasem lehet osztója az összegüknek.

1.6.33 Bizonyítsuk be, hogy (a) \(\sqrt[3]{100}\); (b) \(\log_5 18\) irracionalis számok.

1.6.34 (M [556]*) Egy tetszőleges \(mn\) pozitív egészhez vegyünk minden lehetséges módon olyan \(a_1 < a_2 < \cdots < a_t\) egészeket, amelyekre \(a_1 = m\) és az \(a_1a_2\cdots a_i\) szorzat négyzetszám (\(i = 1\) is megengedett). Jelöljük \(S(m)\) -mel \(a_t\) lehető legkisebb értékét. Például \(S(1) = 1, S(2) = 6\), mert \(m = 2\) esetén a \(2 \times 3 \times 6\) szorzat a legjobb választás, \(S(3) = 8, S(4) = 4\) stb.

Bizonyítsuk be, hogy az \(S(2), S(3), S(4), \ldots\) sorozatban éppen a pozitív összetett számok szerepelnek, éspedig mindegyik pontosan egyszer fordul elő.

1.6.35 (M [556]*) (a) Létezik-e (nem csupa azonos tagból álló) végtelen hosszú számtani sorozat csupa teljes hatványból?

(b) Létezik-e (nem csupa azonos tagból álló) akármilyen hosszú (véges) számtani sorozat csupa teljes hatványból?
2. fejezet - KONGRUENCIÁK

Ebben a fejezetben a kongruenciákkal kapcsolatos alapvető ismereteket tárgyaljuk. A kongruenciához kapcsolódó fogalaim, valamint az Euler-féle \( \varphi \) -függvényekkel foglalkozunk. Bebizonyítjuk az Euler–Fermat-tételt és a Wilson-tételt, ez utóbbihoz a lineáris kongruenciákat is felhasználjuk. A lineáris kongruenciához kapcsolódóan áttekintjük a szimultán kongruenciarendszereket is. Az ismeretlenes kongruenciák általánosabb vizsgálatára a 3. és 4. fejezetben kerül majd sor.

2.1 Elemi tulajdonságok

Oszthatósági kérdések vizsgálatánál gyakran tapasztaljuk, hogy tulajdonképpen csak egy adott számmal való osztási maradék számít, vagyis teljesen egyformán viselkednek azok az egészek, amelyeknek az adott számmal osztva azonos a maradéka. Ez (is) indokolja a következő fogalom bevezetését:

2.1.1 Definíció .  
Legyenek \( a \) és \( b \) egész számok és \( m \) pozitív egész. Azt mondjuk, hogy \( a \) kongruens \( b \)-vel modulo \( m \), ha \( m \mid a - b \). Jelölés: \( a \equiv b \pmod{m} \) vagy röviden \( a \equiv b \). Az (általánosan rögzített) \( m \) számot modulusnak nevezzük.

Mivel \( m \mid a - b \iff m \mid b - a \), ezért

\[ a \equiv b \pmod{m} \iff b \equiv a \pmod{m}, \]

és így helyes az „\( a \) és \( b \) kongruensek modulo \( m \)” szóhasználat is. (A „modulo \( m \)” helyett a „mod \( m \)” vagy „az \( m \) modulusra nézve” vagy „az \( m \) modulus szerint” kifejezéseket is szokás mondani.)

Az is világos, hogy \( a \) és \( b \) akkor és csak akkor kongruensek modulo \( m \), ha \( a \) és \( b \) az \( m \)-mel osztva ugyanazt a maradékat adják. (Itt maradékon a szokásos legkisebb nemnegatív maradékot értjük, de ugyanez érvényes akkor is, ha — mindkét számnál — a legkisebb abszolút értékű maradékról van szó.)

Ha \( a \) és \( b \) nem kongruensek modulo \( m \), akkor ezt \( a \not\equiv b \pmod{m} \) jelöli, és azt mondjuk, hogy \( a \) és \( b \) inkongruensek modulo \( m \) (vagy \( a \) inkongruens \( b \)-vel modulo \( m \)).

Példa: \( 11 \equiv 5 \pmod{3} \); \( 32 \equiv -1 \pmod{11} \); \( 21 \not\equiv 6 \pmod{10} \).

Nyilván bármely két egész szám kongruens az \( m = 1 \) modulus szerint.

A kongruencia definíciója minden változtatás nélkül kiterjeszthető lenne az \( m \leq 0 \) esetére is. Ezzel azonban nem érdemes külön foglalkozni, ugyanis \( m \mid a - b \iff -m \mid a - b \).

2.1.2 Tétel .  
(i) Minden \( a \)-ra \( a \equiv a \pmod{m} \).

(ii) \( a \equiv b \pmod{m} \implies b \equiv a \pmod{m} \).

(iii) \( a \equiv b \pmod{m} , b \equiv c \pmod{m} \implies a \equiv c \pmod{m} \).

(iv) \( a \equiv b \pmod{m} , c \equiv d \pmod{m} \implies a + c \equiv b + d \pmod{m} \) és \( a - c \equiv b - d \pmod{m} \).

32
KONGRUENCIÁK

(v) \( a \equiv b \mod{m}, \; c \equiv d \mod{m} \implies ac \equiv bd \mod{m} \).

Bizonyítás: Valamennyi állítás könnyen adódik a kongruencia definíciójából és az oszthatóság elemei tulajdonságaitól, ezért mintaként csak az (v) tulajdonságot igazoljuk.

A feltétel szerint \( m \mid a - b \) és \( m \mid c - d \), amiből

\[ m \mid c(a - b) + b(c - d) = ac - bd, \quad \text{azaz} \quad ac \equiv bd \mod{m} \]

következik. ■

Az (i), (ii) és (iii) tulajdonságok azt fejezik ki, hogy a kongruencia reflexív, szimmetrikus és transzitív reláció, azaz ekvivalenciareláció. Ennek alapján az egész számokat (páronként) diszjunkt halmazok egyesítésére lehet bontani: egy halmazba kerülnek az „egymással kongruens” számok, vagyis azok, amelyek ugyanolyan maradékokat adnak \( m \)-mel osztva (az idézőjeles kijelentésnek éppen az (i)–(iii) tulajdonságok alapján van egyáltalán értelme). Ezek a halmazok lesznek a modulo \( m \) maradékosztályok, amelyekkel részletesen a 2.2 pontban foglalkozunk.

A (iv) és (v) tulajdonságok alapján (az ugyanazon modulus szerinti) kongruenciák „összeadhatók, kivonhatók és összeszorozhatók.” Ezekből azonnal következik, hogy egy kongruencia mindkét oldalához hozzáadhatjuk ugyanaz a számot, és ugyanez vonatkozik a kivonásra és a szorzásra is, továbbá egy kongruenciát önmagával is akárhányhnyez összeszorozhatunk, vagyis egy kongruenciát szabad (pozitív egész kitevős) hatványra emelni:

(vi) \( a \equiv b \mod{m} \implies a + c \equiv b + c \mod{m} \).

(vii) \( a \equiv b \mod{m} \implies ac \equiv bc \mod{m} \).

(viii) \( a \equiv b \mod{m} \implies a^c \equiv b^c \mod{m} \).

Mindezek ismételt alkalmazásától az alábbi jól használható összefüggést nyerjük:

(ix) Legyen \( f \) egy egész együtthatós polinom. Ekkor

\[ a \equiv b \mod{m} \implies f(a) \equiv f(b) \mod{m} \]

A fentiek alkalmazására néhány egyszerű példát mutatunk.

Példák:

P1 Bizonyítsuk be, hogy bármely \( n \) természetes számra

\[ 17 \mid 3^{3n+1}5^{2n+1} + 2^{5n+1}11^n. \]

Megoldás: Azt kell belátni, hogy

\[ 3^{3n+1}5^{2n+1} + 2^{5n+1}11^n \equiv 0 \mod{17}. \]

A bal oldalt a fenti tulajdonságok felhasználásával vele kongruensiaké a kongruensiaké alakítjuk, amíg 0-t nem kapunk:

\[ 3^{3n+1}5^{2n+1} + 2^{5n+1}11^n \equiv 3 \cdot 3^n \cdot 5 \cdot 5^n + 2 \cdot 2^n \cdot 11^n \equiv \]

\[ = 15(-7)^n 8^n + (2(2)^n (6)^n = \]

\[ = 15(-56)^n + 12(12)^n = 15(5)^n + 2(5)^n = \]

\[ = 17(5)^n \equiv 0 \mod{17}. \]

P2 Igazoljuk (újra) az \( a \equiv b \mod{m} \) oszthatóságot.
Megoldás: Nyilván elég az $a - b > 0$ esetre szoritkozni. Alkalmazzuk (viii)-at:

$$a = b \pmod{e - b} \Rightarrow a^k = b^k \pmod{e - b}.$$  

P3 Mutassuk meg, hogy $2^{32} + 1$ összetett szám. (Vesd össze az 1.4.4 feladattal [17] és az 5.2 ponttal.)

Megoldás: Azt látjuk be, hogy $641 \mid 2^{32} + 1$. Ehhez felhasználjuk, hogy

$$641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1.$$  

Ezekből

$$-1 = 5 \cdot 2^7 \pmod{641} \quad \text{és} \quad 5^4 = -2^4 \pmod{641}.$$  

Az első kongruenciát negyedik hatványra emelve, majd behelyettesítve a másodikat, azt kapjuk, hogy

$$1 = (-1)^4 \equiv 5^4 \cdot 2^{32} \equiv -2^4 \cdot 2^{32} = -2^{32} \pmod{641},$$  

azaz $641 \mid 2^{32} + 1$.

Láttuk, hogy az összeadás, kivonás és szorzás műveletére vonatkozóan a kongruenciák ugyanúgy viselkednek, mint az egyenlőségek. Az osztás műveleténél azonban jelentős eltérés van, két kongruenciát nem szabad egymással elosztani. Először is, osztáskor nem feltétlenül kapunk egész számokat, és ekkor a hányadosok közötti kongruenciának eleve nem is lehet értelme, hiszen a kongruenciákban egész számoknak kell szerepelniük. Azonban még abban az esetben sem lesz általában igaz az osztáskor kapott kongruencia, ha az osztás után mindkét oldalon egész számok maradnak. Például

$$28 = 46 \pmod{6} \quad \text{és} \quad 2 = 2 \pmod{6}, \quad \text{azonban} \quad 14 \neq 23 \pmod{6}.$$  

A kongruenciák osztására vonatkozó tilalommal kapcsolatban azt se felejtsük el, hogy a tört is tulajdonképpen osztást jelent. Ezért egy egész értékű tört számlálójába és/vagy nevezőjébe akkor sem szabad vele kongruens számot írni, ha a hányados továbbra is egész marad. Például:

$$45 = 35 \pmod{10} \quad \text{és} \quad 15 = 5 \pmod{10}, \quad \text{de} \quad 3 = \frac{45}{15} \neq \frac{35}{7} = 7 \pmod{10}.$$  

A tiltások után térjünk rá arra, hogy ebben a kérdéskörben mi az, ami megengedett. Csak az osztás speciális esetével, az egyszerűsítéssel foglalkozunk. Az alábbi tétel azt mondja ki, hogy az egyszerűsítést csak úgy lehet elvégezni, hogy közben a modulust is meg kell változtatni:

2.1.3 Tétel.  T 2.1.3

Legyen $d = (c, m)$. Ekkor

$$ac = bc \pmod{mn} \iff a = b \pmod{\frac{mn}{d}}.$$  

Bizonyítás: A kongruencia definícija alapján

$$ac = bc \pmod{mn} \iff mn \mid (a - b)c,$$

ami tovább ekvivalens az

$$\frac{mn}{d} \mid \frac{(a - b)c}{d} \quad (1)$$

oszthatósággal. Mivel $(mn/d, c/d) = 1$, ezért (1) pontosan akkor teljesül, ha
A $T_{2.1.3}$ Tétel fontos speciális eseteként kapjuk, hogy ha $a$ és a modulus relatív prímek, akkor a $c$-vel történő egyszerűsítés után a kongruencia változatlan modulus mellett érvényben marad:

2.1.3A Tétel. \[ T_{2.1.3A} \]

\[ ac \equiv bc \pmod{m}, (c, m) = 1 \implies a \equiv b \pmod{m}. \]

**Feladatok**

2.1.1 Bizonyítsuk be, hogy $23 \mid 61^{k+1} + 11^k 7^k 3^k 2^k + 3$.

2.1.2 Adjuk meg $999^{999^{999}}$ utolsó három számjegyét (tízes számrendszerben).

2.1.3 Bizonyítsuk be (újra) a 9-cel és a 11-gyel való oszthatósági szabályokat (1.1.14 feladat [3]) és ezek más alapú számrendszerre történő általánosításait (1.2.14 feladat [8]) a kongruenciák segítségével.

2.1.4 Melyek igazak az alábbi állítások közül?

(a) $k \mid n, a \equiv b \pmod{n} \implies a \equiv b \pmod{k}$.

(b) $k \mid n, a \equiv b \pmod{k} \implies a \equiv b \pmod{n}$.

(c) $a \equiv b \pmod{n}, a \equiv b \pmod{k} \iff a \equiv b \pmod{kn}$.

(d) $a \equiv b \pmod{n}, a \equiv b \pmod{k} \implies a \equiv b \pmod{|k,n|}$.

(e) $a \equiv b \pmod{n} \implies ka \equiv kb \pmod{kn}$.

(f) $a \equiv b \pmod{n}, c \equiv d \pmod{k} \implies ac \equiv bd \pmod{kn}$.

(g) $a^2 \equiv b^2 \pmod{n} \implies a \equiv \pm b \pmod{n}$.

(h) $a^2 \equiv b^2 \pmod{101} \implies a \equiv \pm b \pmod{101}$.

2.1.5 A tízes számrendszerben több olyan számjegy is van, amelyre nem végződhet négyzeteszám. Hány ilyen számjegy van a 101 alapú számrendszerben?

2.1.6 Kommentáljuk Butus Maximus professzor alábbi „tételét” és „bizonyítását”:

„Tétel: Bármely $n > 3$ egészre \( C_4^{(n)} = \binom{(n+1)}{4} \pmod{4} \).

Bizonyítás: Mivel bármely $n$ egészre $n+1 \equiv n-3 \pmod{4}$, ezért

\[ \binom{n}{4} = \frac{n(n-1)(n-2)(n-3)}{1 \cdot 2 \cdot 3 \cdot 4} = \frac{n(n-1)(n-2)(n+1)}{1 \cdot 2 \cdot 3 \cdot 4} = \binom{n+1}{4} \pmod{4}. \]

2.1.7 Bizonyítsuk be: $m \mid a - b \implies m^2 \mid a^m - b^m$.

2.1.8 Tegyük fel, hogy $3 \mid a$, $(6, n) = 1$ és $a^k \equiv b^k \pmod{3^n}$. Mutassuk meg, hogy ekkor $a \equiv b \pmod{3^n}$.
2.1.9 Legyen \( p > 2 \) prim, \( 1 \leq k \leq p - 1 \). Igazoljuk az alábbi modulo \( p \) kongruenciákat:

(a) \( \left( \frac{1}{k} \right) = 0 \);

(b) \( \left( \frac{p-1}{k} \right) = (-1)^k \);

(c) \( \left( \frac{p-2}{k} \right) \equiv (-1)^k (k+1) \).

2.1.10 Határozzuk meg az(oka)t a \( P \) prim(ek)et, amelyekre \( \left( \frac{a}{p} \right) \) a \( P \)-vel osztva \( p - 2 \) maradékot ad.

2.1.11 (*) Legyen \( p \) prim. Bizonyítsuk be a következő modulo \( P \) kongruenciákat:

(a) \( \left( \frac{c}{m} \right) \equiv \left( \frac{a}{m} \right) \);

(b) \( \left( \frac{a}{m} \right) \equiv \left( \frac{1}{m} \right) \);

(c) \( \left( \frac{a}{m} \right) \equiv \left( \frac{1}{m} \right) \).

2.2 Maradékosztályok és maradékrendszernek

A modulo \( n \) maradékosztály fogalmát már a T 2.1.2 Tétel után megemlítettük: azok az egész számok tartoznak egy maradékosztályba, amelyek \( n \)-mel osztva azonos maradékot adnak.

2.2.1 Definíció .

Rögzített \( n \) modulus mellett az \( a \)-val kongruens elemek halmazát az \( a \) által reprezentált maradékosztálynak nevezzük. ♦

Jelölés: \( \langle a \rangle_n \). Ha nem okoz felhőértést, akkor a modulusra utaló \( n \) indexet elhagyjuk.

Az \( \langle a \rangle_n \) maradékosztály tehát egy „mindkét irányban végtesen számtani sorozat”, amelynek egyik eleme \( a \) és a differenciája \( n \). A modulo \( n \) maradékosztályok száma \( n \), és minden maradékosztálynak végtesen sok eleme van. A definíció alapján \( \langle a \rangle_n = \langle c \rangle_m \iff a \equiv c \ (\text{mod } n) \).

Példa: \( \langle 23 \rangle_7 = \{ \ldots, -5, 2, 9, 16, 23, 30, \ldots \} = \langle 10 \rangle_7 \).

2.2.2 Definíció .

Ha rögzített \( n \) modulus mellett minden maradékosztályból egy és csak egy elemet kiveszünk, az így kapott számokat modulo \( n \) teljes maradékrendszernek nevezzük. ♦

Példa: \( \{ 33, -5, 11, -11, -8 \} \) teljes maradékrendszer modulo 5.

A leggyakrabban a következő teljes maradékrendszerket használjuk:

(A) Legkisebb nemnegatív maradékok: \( 0, 1, \ldots, n - 1 \).

(B) Legkisebb abszolút értékű maradékok:

\( 0, \pm 1, \pm 2, \ldots, \pm \frac{m-1}{2} \), ha \( m \) páratlan,
illetve
\[0, \pm 1, \pm 2, \ldots, \pm \frac{m-2}{2}, \frac{m}{2} \quad \text{ha } m \text{ páros}\]

(nyilván ez utóbbi esetben \(m/2\) helyett \(-m/2\) is vehető).

Azt, hogy adott számok teljes maradékrendszer alkotnak-e, általában az alábbi egyszerű kritérium alapján tudjuk gyorsan eldönteni:

2.2.3 Tétel. T 2.2.3

Adott egész számok akkor és csak akkor alkotnak teljes maradékrendszt modulo \(m\), ha

(i) számuk \(m\), és

(ii) páronként inkongruensek modulo \(m\).

Bizonyítás: Legyen \(T_m\) egy teljes maradékrendszer modulo \(m\). Mivel a modulo \(m\) maradékosztályok száma \(m\), és minden maradékosztályból egy elemet vettünk ki, ezért \(T_m\) elemszáma szükségképpen \(m\). Továbbá egyetlen maradékosztályból sem választottunk egynél több elemet, ezért \(T_m\) elemei páronként inkongruensek modulo \(m\).

Megfordítva, tekintsünk \(m\) darab páronként inkongruens számot modulo \(m\). A páronkénti inkongruencia miatt ezek csupa különböző maradékosztályba tartoznak, és mivel a számok \(m\), ezért \(m\) darab maradékosztályt reprezentálnak, azaz az összeset. Így ezek a számok valóban teljes maradékrendszt alkotnak modulo \(m\).

Ha egy teljes maradékrendszt a modulushoz relatív prim számmal végigszorzunk, és ehhez egy tetszőleges egész hozzáadunk, akkor ismét teljes maradékrendszt kapunk:

2.2.4 Tétel. T 2.2.4

Legyen \(\tau_1, \tau_2, \ldots, \tau_m\) teljes maradékrendszer modulo \(m\), \(\left\langle a, m \right\rangle = 1\) és \(b\) tetszőleges. Ekkor

\[a\tau_1 + b, a\tau_2 + b, \ldots, a\tau_m + b\]

is teljes maradékrendszer modulo \(m\).

Bizonyítás: Mivel az új rendszer elemszáma is \(m\), tehát a T 2.2.3 Tétel alapján azt kell még bizonyítani, hogy az elemei páronként inkongruensek mod \(m\).

Tegyük fel, hogy \(a\tau_i + b \equiv a\tau_j + b \pmod{m}\), megmutatjuk, hogy \(i = j\).

Mindkét oldalból \(b\) -t kivonva \(a\tau_i = a\tau_j \pmod{m}\) adódik.

Mivel \(\left\langle a, m \right\rangle = 1\), ezért a T 2.1.3A Tétel alapján egyszerűsíthetünk \(a\) -val: \(\tau_i \equiv \tau_j \pmod{m}\), és így valóban \(i = j\).

Megjegyezzük, hogy ha \(\left\langle a, m \right\rangle \neq 1\), akkor az \(a\tau_i + b\) számok sohasem alkotnak teljes maradékrendszt, lásd a 2.2.11 feladatot [41].

Most azt vizsgáljuk meg, hogy a modulushoz relatív prim egészek hogyan helyezkednek el az egyes maradékosztályokban. Megmutatjuk, hogy egy maradékosztálynak vagy az összes eleme relatív prim a modulushoz, vagy pedig egyetlen eleme sem relatív prim hozzá:

Legyen \(a \equiv b \pmod{m}\). Ekkor \(\left\langle a, m \right\rangle = 1 \iff \left\langle b, m \right\rangle = 1\).
Az alábbi tételben ennél erősebb állítást bizonyítunk:

**2.2.5 Tétel.** \( T \, 2.2.5 \)

\[ a \equiv b \pmod{m} \implies \{a, m\} = \{b, m\}. \]

**Bizonyítás:** A feltétel szerint \( b = a + mc \) teljesül alkalmas \( c \) egéssel.

Mivel itt a jobb oldalon \( a \) és \( m \) osztható \( \{a, m\} \)-mel, ezért \( \{a, m\} \mid b \). Ez azt jelenti, hogy \( \{a, m\} \)

közös osztója \( b \)-nek és \( m \)-nek, és így \( \{a, m\} \mid \{b, m\} \).

Ugyanígy adódik a fordított irányú \( \{b, m\} \mid \{n, m\} \) oszthatóság is, tehát valóban \( (a, m) = (b, m) \).

Fontos szerepet játszanak azok a maradékosztályok, amelyeknek az elemei relatív prímek a
modulushoz:

**2.2.6 Definíció.** \( D \, 2.2.6 \)

Az \( \{a\}_m \) maradékosztályt modulo \( m \) redukált maradékosztálynak nevezzük, ha \( \{a\}_m = \{b\}_m \).

Mint már említettük, a \( T \, 2.2.5 \) Tételből következik, hogy ha egy maradékosztálynak van olyan eleme, amely relatív prim a modulushoz, akkor a maradékosztály minden eleme ilyen. Ezért a \( D \, 2.2.6 \) Definíció nem függ attól, hogy az \( \{a\}_m \) maradékosztályt melyik elemével reprezentáltuk.

Most bevezetjük a számemlélet egyik legfontosabb függvényét:

**2.2.7 Definíció (Euler-féle \( \varphi \) -függvény).** \( D \, 2.2.7 \)

Tetszőleges \( n \) pozitív egész esetén \( \varphi(n) \) az \( 1, 2, \ldots, n \) számok közül az \( n \)-hez relatív prímek számát jelenti. \( ✤ \)

**Példa:** \( \varphi(1) = 1, \varphi(10) = 4, \varphi(11) = 10 - 1 \iff n \text{ prim.} \)

Világos, hogy \( \varphi(n) \) éppen a modulo \( n \) redukált maradékosztályok száma.

Az \( n \) kanonikus alakjából könnyen kiszámítható \( \varphi(n) \) értéke, ezt a képletet a 2.3 pontban tárgyaljuk.

Most a teljes maradékrendszer mintájára a redukált maradékrendszer fogalmát definiáljuk:

**2.2.8 Definíció.** \( D \, 2.2.8 \)

Ha rögzített \( n \) modulus mellett minden redukált maradékosztályból egy és csak egy elemet kiveszünk, az így kapott számokat modulo \( n \) redukált maradékrendszernek nevezzük. \( ✤ \)

**Példa:** \[ \{17, -5, 11, -11\} \text{ redukált maradékrendszer modulo } 12. \]

A legegyszerűbben úgy gyártathatunk redukált maradékrendszereket, ha a legkisebb nemnegatív maradékokból, illetve a legkisebb abszolút értékű maradékokból kiválasztjuk a modulushoz relatív prímeket.

A következőkben bebizonyítjuk a \( T \, 2.2.3 \) és \( T \, 2.2.4 \) Tételeknek a redukált maradékrendszerkre vonatkozó megfelelőit.

**2.2.9 Tétel.** \( T \, 2.2.9 \)

Adott egész számok akkor és csak akkor alkotnak redukált maradékrendszer modulo \( n \), ha
(i) számuk $\varphi(m)$,

(ii) páronként inkongruensek modulo $\mathfrak{m}$, és

(iii) valamennyien relatív prímek $\mathfrak{n}$-hez.

Bizonyítás: Legyen $\mathcal{R}_m$ egy redukált maradékrendszer modulo $\mathfrak{m}$. Mivel a modulo $\mathfrak{m}$ redukált maradékosztályok száma $\varphi(m)$, és minden maradékosztályból egy elemet vettünk ki, ezért $\mathcal{R}_m$ elemszáma szükségképpen $\varphi(m)$. Továbbá egyetlen maradékosztályból sem választottunk egynél több elemet, ezért $\mathcal{R}_m$ elemei páronként inkongruensek modulo $\mathfrak{m}$. Végül $\mathcal{R}_m$ minden eleme relatív prim $\mathfrak{n}$-hez, hiszen ezeket redukált maradékosztályokból választottuk.

Megfordítva, tekintsünk $\varphi(m)$ darab, az $\mathfrak{m}$-hez relatív prim számot, amelyek páronként inkongruensek modulo $\mathfrak{m}$. A páronkénti inkongruencia és az $\mathfrak{m}$-hez relatív primség miatt ezek csupá különböző redukált maradékosztályba tartoznak. Mivel a számuk $\varphi(m)$, ezért $\varphi(m)$ darab redukált maradékosztályt reprezentálnak, azaz az összeset. Így ezek a számok valóban redukált maradékrendszert alkotnak modulo $\mathfrak{m}$.

$\square$

2.2.10 Tétel. T 2.2.10

Legyen $\tau_1, \tau_2, \ldots, \tau_{\varphi(m)}$ redukált maradékrendszer modulo $\mathfrak{m}$ és $\{a, \mathfrak{m}\} = 1$. Ekkor $a\tau_1, a\tau_2, \ldots, a\tau_{\varphi(m)}$ is redukált maradékrendszer modulo $\mathfrak{m}$.

Bizonyítás: A T 2.2.9 Tétel (i)–(iii) kritériumát ellenőrizzük.

(i) Az új rendszer elemszáma is $\varphi(m)$.

(ii) $a\tau_i = a\tau_j \mod \mathfrak{m}$, $\{a, \mathfrak{m}\} = 1 \implies \tau_i = \tau_j \mod \mathfrak{m} \implies i = j$.

(iii) $\{a, \mathfrak{m}\} = 1$, $\{a\tau_i, \mathfrak{m}\} = 1 \implies \{a\tau_i, m\} = 1$.

Ha $\{a, \mathfrak{m}\} \neq 1$, akkor az $a\tau_i$ számok sohasem alkotnak redukált maradékrendszert, sőt ezen elemek egyike sem lesz relatív prim az $\mathfrak{m}$-hez.

A teljes maradékrendszerrel látottakhoz képest jelentős eltérés, hogy a redukált maradékrendszer elemeihez egy $b$ számot hozzáadva már általában nem kapunk redukált maradékrendszert, lásd a 2.2.12 feladatot [41].

Feladatok

Valamennyi feladatban feltesszük, hogy a modulus $\mathfrak{m} \geq 2$.

2.2.1 Határozzuk meg az $\mathfrak{m}$ modulust, ha tudjuk, hogy az alábbi elemek ugyanannak a modulo $\mathfrak{m}$ redukált maradékosztályának az elemei:

(a) 2 és 14;

(b) 18, 78 és 178;

(c) $a$ és $-a$.

2.2.2 Hány olyan

39
KONGRUENCIÁK

(a) teljes;
(b) redukált

maradékrendszer van modulo \( m \), amelynek minden \( a \) elemére \( 0 \leq a \leq 5m + 1 \) teljesül?

2.2.3 Melyek azok a mindkét irányban végletes számtani sorozatok, amelyekből kiválasztható egy modulo \( m \)
(a) maradékosztály;
(b) teljes maradékrendszer?

2.2.4 Milyen \( m \geq 2 \) esetén létezik olyan teljes maradékrendszer, amelynek elemei
(a) páratlan számok;
(b) összetett számok;
(c) négyzetszámok;
(d) (tízes számrendszerben) 1357-re végződő számok;
(e) mértani sorozatot alkotnak;
(f)(M [557]) × „csupaegyek” (azaz tízes számrendszerben minden számjegyük 1-es);
(g)(M [557]) × teljes hatványok?

2.2.5 Milyen \( m \geq 2 \) esetén létezik olyan redukált maradékrendszer, amelynek elemei
(a) 15-tel osztható számok;
(b) 15-tel nem osztható számok;
(c) négyzetszámok;
(d) (tízes számrendszerben) 1357-re végződő számok;
(e) teljes hatványok?

2.2.6 Melyek igazak az alábbi állítások közül?
(a) Ha \( \mathcal{r}_1, \mathcal{r}_2, \ldots, \mathcal{r}_k \) redukált maradékrendszer modulo 7, akkor \( \mathcal{r}_1, \mathcal{r}_2, \ldots, \mathcal{r}_k \) redukált maradékrendszer modulo 14 is.
(b) Ha \( \mathcal{m}_1, \mathcal{m}_2, \ldots, \mathcal{m}_k \) redukált maradékrendszer modulo 14, akkor \( \mathcal{m}_1, \mathcal{m}_2, \ldots, \mathcal{m}_k \) redukált maradékrendszer modulo 7 is.

2.2.7 (a) Milyen maradéket ad \( m \)-mel osztva egy modulo \( m \) teljes maradékrendszer elemeinek az összege?

(b) Legyen \( m \) páros, és \( a_1, a_2, \ldots, a_n \), valamint \( b_1, b_2, \ldots, b_n \) egy-egy teljes maradékrendszer modulo \( m \). Bizonyítsuk be, hogy az \( a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n \) elemek sohasem alkotnak teljes maradékrendszerzt modulo \( m \). Mit állíthatunk páratlan \( m \) esetén?

(c) Vizsgáljuk meg az analóg kérdéseket teljes maradékrendszekek helyett redukált maradékrendszekekre is.

2.2.8 (M [558]) (a) Egy kör alakú tisztas mentén \( m \) fa áll, mindegyiken egy-egy mökös. A mökusok össze szeretnének gyűlni egy fán, de csak úgy változtathatják a helyüket, hogy
KONGRUENCIÁK

két tetszőleges mókus egyidejűleg átugorhat egy-egy szomszédos fára. Ezt a lépést akárhányszor ismételhetik. Milyen \( m \) esetén tudnak összegyűlni a mókusok?

(b) Mi a helyzet akkor, ha a megengedett lépést a következőképpen módosítjuk: két tetszőleges mókus egyidejűleg átugorhat egy-egy szomszédos fára, azonban ellenkező körüljárási irányba kell ugorniuk.

2.2.9 (*) (a) Mely \( m \) -ek esetén alkotnak a \( 0; 0 + 1; 0 + 2; \ldots, 0 + 1 + 2 + \ldots + (m - 1) \) számok teljes maradékrendszert modulo \( m \)?

(b) Mely \( m \) -ek esetén létezik olyan \( a_1; \ldots; a_m \) teljes maradékrendszer modulo \( m \), amelyre az \( a_1, a_1 + a_2, a_1 + a_2 + a_3, \ldots, a_1 + a_2 + a_3 + \ldots + a_m \) számok is teljes maradékrendszert alkotnak modulo \( m \)?

2.2.10 Legyen \( k \mid m \). Melyek igazak az alábbi állítások közül?

(a) Bármely modulo \( k \) maradékosztály előáll modulo \( m \) maradékosztályok egyesítéseként.

(b) Bármely modulo \( k \) redukált maradékosztály előáll modulo \( m \) redukált maradékosztályok egyesítéseként.

(c) Bármely modulo \( k \) redukált maradékosztálynak van olyan részváltozó, amely egy modulo \( m \) redukált maradékosztályt alkot.

(d) Bármely modulo \( k \) redukált maradékrendszer kiegészíthető egy modulo \( m \) redukált maradékrendszerre.

(e) Bármely modulo \( m \) redukált maradékrendszerből kiválasztható egy modulo \( k \) redukált maradékrendszer.

2.2.11 Legyen \( r_1, r_2, \ldots, r_m \) teljes maradékrendszer modulo \( m \), \( \left( a, m \right) \neq 1 \) és \( b \) tetszőleges.

(a) Bizonyítsuk be, hogy \( ar_1 + b, \ldots, ar_r + b \) sohasem alkotnak teljes maradékrendszt modulo \( m \).

(b) Összesen hány modulo \( m \) maradékosztályt reprezentálnak az \( ar_1 + b, \ldots, ar_m + b \) elemek?

2.2.12 (M [558]*) Legyen \( r_1, r_2, \ldots, r_{\phi(m)} \) redukált maradékrendszer modulo \( m \).

(a) Adjuk meg az összes olyan \( a \) számot, amelyre az \( ar_1, \ldots, ar_{\phi(m)} \) elemek páronként inkongruenek modulo \( m \).

(b) Adjuk meg az összes olyan \( b \) számot, amelyre az \( r_1 - b, \ldots, r_{\phi(m)} + b \) elemek is redukált maradékrendszerenk ezeknek modulo \( m \).

2.2.13 (M [560]*) Milyen \( m \) és \( k \) számokhoz létezik olyan \( a_1; \ldots; a_m \) teljes maradékrendszer modulo \( m \) és \( b_1; \ldots; b_k \) teljes maradékrendszer modulo \( k \), hogy az \( a_i; b_j \) számok teljes maradékrendszerenk ezeknek modulo \( m; k \)?

2.2.14 (M [561]) Legyenek \( a \) és \( b \) pozitív egészek.

(a) Bizonyítsuk be, hogy

\[
T = \{ \bar{a}b - j \alpha \mid \bar{a} = 1, 2, \ldots, n; j = 1, 2, \ldots, b \}
\]

akkor és csak akkor alkot teljes maradékrendszt modulo \( ab \), ha \( \left( a, b \right) = 1 \).
(b) Legyen $r_1, \ldots, r_{\varphi(a)}$, illetve $s_1, \ldots, s_{\varphi(b)}$ redukált maradékrendszert modulo $a$, illetve modulo $b$. Bizonyítsuk be, hogy

$$R = \{ r_i b - s_j a \mid i = 1, 2, \ldots, \varphi(a), j = 1, 2, \ldots, \varphi(b) \}$$

akkor és csak akkor alakot redukált maradékrendszert modulo $ab$, ha $(a, b) = 1$.

(c) Mutassuk meg, hogy ha $(a, b) = 1$, akkor $\varphi(ab) = \varphi(a)\varphi(b)$.

### 2.3 Az Euler-féle $\varphi$-függvény

Az Euler-féle $\varphi$-függvényt a D 2.2.7 Definícióban értelmeztük: Tetszőleges $n$ pozitív egész esetén $\varphi(n)$ az $1, 2, \ldots, n$ számok közül az $n$-hez relatív prímek számát jelenti.

Ebből azonnal következett, hogy $\varphi(n)$ darab modulo $n$ redukált maradékosztály létezik, és egy modulo $n$ redukált maradékrendszer elemeinek a száma is $\varphi(n)$.

Most egy olyan képletet bizonyítunk, amely az $n$ kanonikus alakjának segítségével megadja $\varphi(n)$ értékét:

#### 2.3.1 Tétel

Legyen $n$ kanonikus alakja

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i}, \quad \text{ahol} \quad \alpha_i > 0.$$  

Ekkor

$$\varphi(n) = (p_1^{\alpha_1} - 1) \cdots (p_r^{\alpha_r} - 1) = \prod_{i=1}^{r} (p_i^{\alpha_i} - 1).$$

Felhívjuk a figyelmet arra, hogy $\varphi(n)$ fenti képlete csak akkor érvényes, ha az $n$ kanonikus alakjában az $\alpha_i$ kitevők valóban pozitívak (szemben például a $d(n)$-re az T 1.6.3 Tételben adott képlettel, amely akkor is igaz marad, ha megengedjük, hogy az $\alpha_i$ kitevők között a nulla is előforduljon).

A fenti képlet néhány másik, ekvivalens alakja:

$$\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i-1}(p_i - 1) = n \prod_{i=1}^{r} \left( 1 - \frac{1}{p_i} \right) = n \prod_{\substack{p \mid n \\text{prímtény}} \atop p \neq p_i} \left( 1 - \frac{1}{p} \right).$$

A T 2.3.1 Tételre két bizonyítást adunk. Egy harmadik bizonyítás leolvasható a 6.5.4b feladatból [193]. Emellett az első bizonyításban döntő fontosságú II. állítás két további igazolási móda is szerepel a 2.2.14 [41], illetve 2.6.10 feladatokban [61].

**Első bizonyítás:** A téttel az alábbi két állításra vezetjük vissza:

I. Ha $p$ prim (és $\alpha > 0$), akkor $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

II. Ha $(a, b) = 1$, akkor $\varphi(ab) = \varphi(a)\varphi(b)$.  

42
Ezekből a tételekben következik. Ugyanis II-ből a tényezők száma szerinti teljes indukcióval kapjuk, hogy ha az \( a_1, \ldots, a_r \) számok páronként relatív prímek, akkor \( \varphi(a_1 \ldots a_r) = \varphi(a_1) \cdots \varphi(a_r) \). Ha ezt \( a_i = p_i^{n_i} \)-re alkalmazzuk, és \( \varphi(p_i^{n_i}) \) helyére az I-ben szereplő értéket beírjuk, akkor éppen a bizonyítandó képlet adódik.

Rátérünk az I. állítás igazolására. Egy szám \( p^n \)-hoz akkor és csak akkor relatív prim, ha nem osztható \( p \)-vel. Ennél felfogva az \( 1, 2, \ldots, p^n \) egészek közül úgy kapjuk meg a \( p^n \)-hoz relatív primeket, ha elhagyjuk a \( p \)-vel oszthatókat. Ez utóbbiak a \( \varphi, 2p, \ldots, p^{n-1}p \), és így számuk \( \frac{p^n}{p} = p^{n-1} \). Ebből következik, hogy a megmaradók száma \( \varphi(p^n) = p^n - p^{n-1} \).

Nézzük most a II. állítás bizonyítását. (Mint már jeleztük, ennek két másik lehetséges módja szerepel a 2.2.14 [41], illetve 2.6.10 feladatban [61].)

A \( \varphi(ab) \) érték azoknak az \( ab \)-nél nem nagyobb pozitív egészeknek a számát jelenti, amelyek relatív primek \( ab \)-hez, azaz relatív primek \( a \)-hoz és \( b \)-hez is.

Jelöljük a modulo \( a \) redukált maradékosztályok legkisebb pozitív elemeit \( r_1, r_2, \ldots, r_{\varphi(a)} \)-val, és írjuk fel az \( ab \)-nél nem nagyobb pozitív egészek közül azokat, amelyek \( a \)-hoz relatív primek:

\[
\begin{array}{cccc}
  r_1 & r_2 & \cdots & r_{\varphi(a)} \\
  a + r_1 & a + r_2 & \cdots & a + r_{\varphi(a)} \\
  2a + r_1 & 2a + r_2 & \cdots & 2a + r_{\varphi(a)} \\
  \vdots & \vdots & \ddots & \vdots \\
  (b - 1)a + r_1 & (b - 1)a + r_2 & \cdots & (b - 1)a + r_{\varphi(a)}
\end{array}
\]

Ezek közül kell kiválasztani azokat a számokat, amelyek \( b \)-hez is relatív primek.

Tekintsük evégett az (1) táblázat egy tetszőleges oszlopát. Például az \( i \)-edik oszlop elemei a következők:

\[
r_1, a + r_1, 2a + r_1, \ldots, (b - 1)a + r_1.
\]

Ezek az elemek úgy jöttek létre, hogy a \( 0, 1, \ldots, b - 1 \) modulo \( b \) teljes maradékrendszer elemeit a \( b \)-hez relatív prim \( a \)-val megszoroztuk, majd az így kapott számokhoz \( r_i \)-t hozzáadunk. A T 2.2.4 Tétel alapján ekkor (2) is teljes maradékrendszer modulo \( b \), vagyis az (1) táblázat minden oszlopában egy-egy modulo \( b \) teljes maradékrendszer áll.

Mivel egy modulo \( b \) teljes maradékrendszerben \( \varphi(b) \) számú \( b \)-hez relatív prim elem szerepel, ezért az (1) táblázat minden oszlopában \( \varphi(b) \) darab olyan elem van, amely relatív prim \( b \)-hez.

Az (1) táblázatban az oszlopok száma \( \varphi(a) \), így a táblázatnak összesen \( \varphi(a) \varphi(b) \) eleme relatív prim a \( b \)-hez.

Ez azt jelenti, hogy az \( ab \)-nél nem nagyobb pozitív egészek között \( \varphi(ab) \) olyan van, amely \( a \)-höz és \( b \)-hez is, vagyis \( ab \)-hez relatív prim. Ez a szám másrészt definíció szerint éppen \( \varphi(ab) \), tehát valóban \( \varphi(ab) = \varphi(a)\varphi(b) \).

Második bizonyítás: A logikai szitaformulát alkalmazzuk.

Az \( 1, 2, \ldots, n \) egészek közül azoknak a számát kell meghatározni, amelyek relatív primek \( \varphi(b) \)-hez, azaz a \( b_1, b_2, \ldots, b_r \) primések egyikével sem oszthatók.
Ehhez az $1, 2, \ldots, n$ közül „ki kell szitálni a rossz tulajdonságúakat”, vagyis azokat, amelyek egy vagy több $p_j$-vel oszthatók.

Tekintsük először azokat az elemeket, amelyek egy adott $p_j$-vel oszthatók (függetlenül attól, hogy az $n$ többi prím tényezőjével osztható-e vagy sem). Ezek száma nyilván $n/p_j$.

Most nézzük azokat az egészeket, amelyek több, előre megadott $p_j$-vel oszthatók (ismét nem töröldve azzal, osztható-e az $n$ fennmaradó prím tényezőivel vagy sem). Egy egész akkor és csak akkor osztható adott prímek mindegyikével, ha osztható ezen prímek szorzatával. Ennél fogva például a $p_1$-gyel és $p_2$-vel is osztható elemek száma $n/(p_1p_2)$, a $p_1$-gyel, $p_3$-mal és $p_7$-tel oszthatóké $n/(p_1p_3p_7)$ stb.

Így a logikai szitaformula szerint

$$\varphi(n) = n - \frac{n}{p_1} - \frac{n}{p_2} - \cdots - \frac{n}{p_1p_2} - \cdots + \frac{n}{p_1p_2p_3} + \cdots + \frac{n}{p_1p_2p_3p_5} - \cdots \tag{3}$$

Közvetlen számolással ellenőrizhető, hogy (3) jobb oldala azonos az

$$n \prod_{i=1}^{x} \left(1 - \frac{1}{p_i}\right)$$

szorzattal, ez pedig a tételben megadott képletnek egy másik felírási módja.

### Feladatok

2.3.1 Mutassuk meg, hogy minden $n > 2$-re $\varphi(n)$ páros szám.

2.3.2 Határozzuk meg azokat az $n$-eket, amelyekre $\varphi(n)$ értéke

(a) 2;
(b) 4;
(c) 14;
(d) 60.

2.3.3 Melyik az a legkisebb $n$, amelyre $\varphi(n)$ osztható

(a) $2^{10}$-nel;
(b) $3^{10}$-nel?

2.3.4 Határozzuk meg $\varphi(100n)/\varphi(n)$ összes lehetséges értékét, ha $n$ végigfut a pozitív egészeken.

2.3.5 Bizonyítsuk be a következő állításokat.

(a) $k \mid n \implies \varphi(k) \mid \varphi(n)$ .

(b) $\varphi((a, b)) = [\varphi(a), \varphi(b)]$ és $[\varphi(a), \varphi(b)] = \varphi\{a, b\}$ .

(c) $\varphi\{a, b\} = \{\varphi(a), \varphi(b)\} \iff [\varphi(a), \varphi(b)] = \varphi\{a, b\}$ .
2.3.6 Bizonyítsuk be, hogy \( \phi(a)/\varphi(b) = a/b \) akkor és csak akkor teljesül, ha \( a \) és \( b \) pontosan ugyanazokkal a primékkal osztható.

2.3.7 Legyen \( n > 2 \). Melyek igazak az alábbi állítások közül?

(a) Ha \( \left( n, \varphi(n) \right) = 1 \), akkor \( n \) páratlan négyzetmentes szám.

(b) Ha \( n \) páratlan négyzetmentes szám, akkor \( \left( n, \varphi(n) \right) = 1 \).

2.3.8 (*) Bizonyítsuk be, hogy minden \( k \) pozitív egészhez létezik olyan \( n \), amelyre \( \left( n, \varphi(n) \right) = k \).

2.3.9 Igazoljuk, hogy minden \( n \)-re \( \varphi(n) + d(n) \leq n + 1 \). Mely \( n \)-ekre áll egyenlőség?

2.3.10 (a) Mutassuk meg, hogy ha \( \{a, b\} \neq 1 \), akkor \( \varphi(ab) > \varphi(a)\varphi(b) \) (tehát ebben az esetben sohasem áll fenn egyenlőség).

(b) A T. 2.3.1 Tétel első bizonyításának döntő része volt a II. állítás, azaz \( \{a, b\} = 1 \rightarrow \varphi(ab) = \varphi(a)\varphi(b) \) igazolása. Hol bukik meg az ott láttott gondolatmenet, ha \( a \) és \( b \) nem relatív primek?

(c) Bizonyítsuk be, hogy bármely \( a, b \) esetén

\[ \varphi(ab)\varphi(a, b) = \varphi(a)\varphi(b). \]

2.3.11 (a) Bizonyítsuk be, hogy ha \( n \) összetett szám, akkor \( n - \varphi(n) \geq \sqrt{n} \). Milyen \( n \)-ek esetén áll egyenlőség?

(b) Határozzuk meg azokat az \( n \)-eket, amelyekre \( n - \varphi(n) \) értéke

(b1) 1;

(b2) 6;

(b3) 7;

(b4) 10.

2.3.12 Mely egész számok szerepelnek az \( n/\varphi(n) \) függvény értékkészletében?

2.3.13 Bizonyítsuk be, hogy ha \( \varphi(n^2) = \varphi(k^2) \), akkor \( n = k \).

2.3.14 Mutassuk meg, hogy \( \sum_{d \mid n} \varphi(d) = n \).

2.3.15 Lássuk be, hogy \( \varphi(n) \to \infty \), ha \( n \to \infty \).

2.3.16 (*) Igazoljuk, hogy minden \( k \) természetes számhoz található olyan \( n \), amelyre \( \varphi(n) = \varphi(n + k) \).

2.3.17(*) Adjunk meg 1000 különböző egész számot, amelyekhez a \( \varphi \)-függvény ugyanazt az értéket rendeli.

2.3.18 (M [562]*) Határozzuk meg az összes olyan \( n \) pozitív egész, amelyhez létezik olyan \( k \), hogy \( \varphi(n^k) = k! \).
2.3.19 (M [562]* ) Milyen \( m \) esetén létezik olyan számtani sorozat, amely reduált maradékrendszerzrt alakot modulo \( m \)?

### 2.4 Euler–Fermat-tétel

#### 2.4.1 Tétel (Euler–Fermat-tétel) . T 2.4.1

\[
(a, m) = 1 \quad \implies \quad a^{\varphi(m)} \equiv 1 \pmod{m}.
\]

**Bizonyítás:** Legyen \( r_1, r_2, \ldots, r_{\varphi(m)} \) redukált maradékrendszer modulo \( m \).

Mivel \( (a, m) = 1 \), ezért az \( a r_1, a r_2, \ldots, a r_{\varphi(m)} \) elemek is redukált maradékrendszer alkotnak modulo \( m \).

Ez azt jelenti, hogy minden \( 1 \leq i \leq \varphi(m) \) -hez létezik egy és csak egy olyan \( 1 \leq j \leq \varphi(m) \), amelyre \( a r_i \equiv r_j \pmod{m} \). Jelöljük ezt az \( r_j \) -t \( s_i \)-vel:

\[
\begin{align*}
 r_1 & \equiv s_1 \pmod{m}, \\
 r_2 & \equiv s_2 \pmod{m}, \\
 & \vdots \\
 r_{\varphi(m)} & \equiv s_{\varphi(m)} \pmod{m}.
\end{align*}
\]

Itt az \( s_1, \ldots, s_{\varphi(m)} \) számok az \( r_1, \ldots, r_{\varphi(m)} \) számok egy permutációját alkotják.

Az (1)-beli kongruenciákat összeszorozva azt kapjuk, hogy

\[
a^{\varphi(m)} r_1 r_2 \cdots r_{\varphi(m)} \equiv s_1 s_2 \cdots s_{\varphi(m)} \pmod{m},
\]

azaz

\[
a^{\varphi(m)} r_1 r_2 \cdots r_{\varphi(m)} \equiv r_1 r_2 \cdots r_{\varphi(m)} \pmod{m}.
\]

A (2) kongruenciát \( (r_1, m) = 1 \) miatt az összes \( r_i \) -vel egyszerűsíthetjük, és ekkor a kívánt \( a^{\varphi(m)} \equiv 1 \pmod{m} \) adódik.

Tekintsük most azt a fontos speciális esetet, amikor a modulus egy \( p \) prímszámm. Ekkor \( \varphi(p) = p - 1 \) alapján a következő tételt kapjuk:

#### 2.4.1A Tétel (A „kis” Fermat-tétel egyik alakja) . T 2.4.1A

Ha \( p \) prim és \( (a, p) = 1 \), akkor \( a^{p-1} \equiv 1 \pmod{p} \).

Megjegyezzük, hogy egy \( p \) prim esetén az \( (a, p) = 1 \), a \( p \nmid a \) és az \( a \nmid 0 \pmod{p} \) feltételek ekvivalensek.

A T 2.4.1A Tételből könnyen nyerhető egy olyan kongruencia is, amely már minden \( a \) esetén fennáll:

#### 2.4.1B Tétel (A „kis” Fermat-tétel másik alakja) . T 2.4.1B

Ha \( p \) prim, akkor bármely \( a \) egész számra \( a^p \equiv a \pmod{p} \).

**Bizonyítás:** Ha \( p \nmid a \), akkor a T 2.4.1A Tétel alapján \( a^{p-1} \equiv 1 \pmod{p} \). Ezt a kongruenciát \( a \) -val beszorozva a kívánt \( a^p \equiv a \pmod{p} \) adódik.
Ha $p \mid q$, akkor $a \equiv 0 \pmod{p}$. Ezt $p$-edik hatványra emelve (vagy $a^{p-1}$-gyel beszorozva) kapjuk, hogy $a^p \equiv 0 \pmod{p}$, és így $a^p \equiv a \pmod{p}$ teljesül. $
$ Megjegyzések: 1. Az Euler–Fermat-tétel (T 2.4.1 Tétel) megfordítása is igaz, vagyis $(a, m) = 1$ az $a^p \equiv 1 \pmod{m}$ kongruencia fennállásának nemcsak elégséges, hanem egyben szükséges feltétele is. Sőt, ennél erősebb állítás is igaz: csak akkor létezik egyáltalán olyan $k > 0$ kiveő, amelyre $a^k \equiv 1 \pmod{m}$, ha $a$ és $m$ relatív primek. Az $a^k \equiv 1 \pmod{m}$ kongruenciából ugyanis a T 2.2.5 Tétel szerint $(a, m) = (1, m) = 1$ következik, és így $(a, m) = 1$-nek is teljesülne kell.

2. A kis Fermat-tétel második alakjának (2.4.1B Tétel) nincsen tetszőleges $m$ modulusra vonatkozó „természetes” megfelelője, azaz nincs az általános Euler–Fermat-tételnek olyan „egyszerű” változata, amely minden $a$ esetén érvényes lenne (lásd ezzel kapcsolatban a 2.4.15 feladatot [48]).

3. Mint a név is mutatja, a T 2.4.1A és B Tételek Fermat-tól származnak. A kis Fermat-tétel mindkét változata a T 2.4.1 Tétel felhasználása nélkül, közvetlenül is bizonyítható: a B variáns (a szerinti) teljes indukcióval igazolhatjuk, és innen az A variáns is könnyen következik (lásd a 2.4.16 feladatot [48]). A T 2.4.1 Tételt Euler fedezte fel, éppen a kis Fermat-tétel általánosításaként.

4. A kis Fermat-tételnél a „kis” jelző arra szolgál, hogy megkülönböztesse ezt az eredményt a számmelmélet egyik leghíresebb és csak a közelmúltban megoldott problémájától, a „nagy” Fermat-tételtől (vagy más néven Fermat-sejtéstől), amelyről a 7. fejezetben lesz szó.

Feladatok

2.4.1 Bizonyítsuk be, hogy bármely páratlan $n$-re $\frac{n!}{2^n} - 1$.

2.4.2 Határozzuk meg $1793^{8612}$ utolsó két jegyét (tízes számrendszerben).

2.4.3 Igazoljuk, hogy $n^{20} + 4n^{11} + 8n^{3}$ minden $n$-re osztható 13-mal.

2.4.4 Mutassuk meg, hogy bármely $n$ esetén $n^6 + 13$ és $n^2 + 21$ közül legalább az egyik összetett szám.

2.4.5 Lássuk be, hogy bármely $a$ egész számra $1703601900 \mid a^{32} - a^2$.

2.4.6 Bizonyítsuk be a következő állításokat:

(a) $11 \mid a^{30} - b^{30} + c^{30} \implies 11^{\phi(11)} \mid a^{30} + b^{30} - c^{30}$.

(b) $9 \mid a^{50} + b^{50} + c^{50} \implies 9^{\phi(9)} \mid a^{50} + b^{50} - c^{30}$.

2.4.7 Mutassuk meg, hogy $a^{38} - b^{38}$ akkor és csak akkor nem osztható 23-mal, ha $a$ és $b$ közül pontosan az egyik osztható 23-mal.

2.4.8 Legyen $p$ prim és $\gamma_1, \cdots, \gamma_p$ teljes maradékkrendszer modulo $p$. Bizonyítsuk be, hogy ekkor $\gamma_1^{2p-3}, \cdots, \gamma_p^{2p-3}$ is teljes maradékkrendszer modulo $p$.

2.4.9 (a) Legyen $p$ prim, $a$ egész, $i, j$ pozitív egész és $i + j \equiv 1 \pmod{p - 1}$. Lássuk be, hogy ekkor $a^i \equiv a^j \pmod{p}$.

(b) Hogyan általánosítható az (a)-beli állítás (prim helyett) tetszőleges $m$-re?
2.4.10 Melyek igazak az alábbi állítások közül? (A feladat tízes számrendszerre vonatkozik, és hatványon pozitív egész kitevős hatványt értünk.)

(a) 133-nak végtelen sok hatványa végződik 133-ra.
(b) 134-nek végtelen sok hatványa végződik 134-re.
(c) 136-nak végtelen sok hatványa végződik 136-ra.

2.4.11 Mutassuk meg, hogy az \( a, a + d, \ldots, a + kd, \ldots \) (különböző pozitív egészegyüttesből álló) végtelen számtani sorozat elemei között akkor és csak akkor szerepel az \( a \)-nak végtelen sok (pozitív egész kitevős) hatványa, ha \( d/(a, d) \) és \( a \) relatív prímek.

2.4.12 Oldjuk meg újra az 1.3.12a feladatot [14] az Euler–Fermat-tétel felhasználásával.

2.4.13 Igazoljuk, hogy egy \( n^2 + 1 \) alakú számokat minden pozitív páratlan osztója \( 4k + 1 \) aluk.

2.4.14 Tegyük fel, hogy \( a^{10} + b^{10} \) osztható 19-cel. Lássuk be, hogy ekkor \( a \) és \( b \) is osztható 19-cel.

2.4.15 Bizonyítsuk be a következő állításokat, és vizsgáljuk meg, hogyan kapcsolódnak ezek a kis Fermat-tételhez.

(a) Az \( a^{\varphi(m)} \equiv 1 \mod m \) kongruencia akkor és csak akkor teljesül minden \( a \)-ra, ha \( m \) négyzetmentes.
(b) Az \( a^{\varphi(n)} \equiv a^{\varphi(n) - \varphi(m)} \mod m \) kongruencia minden \( m \)-re és minden \( a \)-ra teljesül.
(c) Az \( a^{1729} = a \mod 1729 \) kongruencia minden \( a \)-ra teljesül.

2.4.16 Adjunk közvetlen bizonyítást a kis Fermat-tétel mindkét alakjára: először igazoljuk indukcióval a T 2.4.1B Tételt, majd ebből vezessük le a T 2.4.1A Tételt.

2.5 Lineáris kongruenciák

Ebben a pontban az ismeretlenes kongruenciák (vagy kongruenciaegyenletek) legegyszerűbb fajtájával, a lineáris kongruenciákkal foglalkozunk.

2.5.1 Definíció. \( D \ 2.5.1 \)

Legyenek \( a, b \) egészek és \( m \) pozitív egész. Ekkor az \( a x \equiv b \mod m \) kongruenciát lineáris kongruenciának nevezzük, és ennek egy megoldásán olyan \( s \) egész számot értünk, amelyet az \( x \) helyére beírva a kongruencia fennáll. ❖

Világos, hogy ha egy \( s \) szám megoldás, akkor az \( (s)n \) maradékosztály bármely másik eleme is megoldás. Így az összes megoldás megkereséséhez elegendő egy teljes maradékosztálysor elemei végigpróbálni, melyek adnak közülük megoldást; az összes megoldás ekkor az ezekkel kongruens egészek halmaza lesz.

Ennek alapján a lineáris kongruencia megoldásszámán a páronként inkongruens megoldások számát értjük, vagyis azt, hogy hány maradékosztályba tartoznak a megoldások, vagy (ismét kicsit más megfogalmazásban) azt, hogy egy teljes maradékosztálysor eleme elégíti ki a kongruenciát. Ugyanez a helyzett a magasabb fokú kongruenciák esetén is, ezért ezt a definíciót rögtön általánosan is megadjuk.

2.5.2 Definíció. \( D \ 2.5.2 \)

48
Legyen \( f \) egy egész együtthatós polinom. Ekkor az \( f(x) \equiv 0 \mod m \) kongruencia megoldásszámának egy modulo \( m \) teljes maradékkrendszer azon \( s \) elemeinek a számát értjük, amelyekre \( f(s) \equiv 0 \mod m \).

Mivel \( u \equiv v \mod m \Rightarrow f(u) \equiv f(v) \mod m \), ezért a definícióban megadott szám valóban nem függ attól, hogy a modulo \( m \) teljes maradékkrendszerek közül melyiket választottuk.

Térjünk vissza a lineáris kongruenciákra. Bárмely más típusú egyenlethez hasonlóan itt is a következő kérdésekre keressünk a válaszat:

(i) Mi a megoldhatóság szükséges és elégséges feltétele?
(ii) Mennyi a megoldásszám?
(iii) Hogyan lehet az összes megoldást valamilyen értelemben leírni, áttekinteni?
(iv) Milyen megoldási módszerekkel kaphatjuk meg a megoldásokat?

Először a megoldhatóság kérdésével foglalkozunk.

**2.5.3 Tétel.**

Am \( ax \equiv b \mod m \) kongruenciának akkor és csak akkor létezik megoldása, ha \( (a,m) \mid b \).

**Bizonyítás:** Am \( ax = b \mod m \) kongruencia megoldhatósága azt jelenti, hogy van olyan \( s \) egész, amelyre \( ax \equiv b \mod m \).

Ez tovább ekvivalens azzal, hogy van olyan \( s \) egész, amelyre \( ax + mj = b \) teljesül, vagyis \( a \) és \( t \) kielégíti az \( ax + mj = b \) lineáris diofantikus egyenletet.

Ezzel beláttuk, hogy az \( ax = b \mod m \) lineáris kongruencia akkor és csak akkor oldható meg, ha megoldható az \( ax + mj = b \) lineáris diofantikus egyenlet.

Az utóbbi megoldhatóságának szükséges és elégséges feltétele az T.1.3.6 Tétel szerint az, hogy \( (a,m) \mid b \) teljesüljön, tehát ugyanez a feltétele az \( ax = b \mod m \) kongruencia megoldhatóságának is.

A bizonyításból kiderült, hogy az \( ax \equiv b \mod m \) lineáris kongruencia és az \( ax + mj = b \) lineáris diofantikus egyenlet kölcsönösen visszavezethetők egymásra. (Sőt az \( ax + mj = b \) diofantikus egyenlet ugyanígy \( mj = b \mod |a| \) lineáris kongruenciává is „átalakítható", ha \( a \neq 0 \).

Ennek alapján bárмely, a lineáris kongruenciákkal kapcsolatos eredmény felhasználható a lineáris diofantikus egyenletek vizsgálatánál és viszont.

Ne feledezzünk meg azonban a jelentős eltérésekről sem: a lineáris kongruenciák megoldásai egész számok (illetve tulajdonképpen maradékosztályok), a lineáris diofantikus egyenletek pedig egész számpárak, egy lineáris kongruencia megoldásszáma véges, egy lineáris diofantikus egyenleté végében stb.

A következő tételben meghatározzuk a lineáris kongruenciánál a megoldásszámot, és együttal leírjuk, hogyan kapható meg egy megoldásból az összes többi.

**2.5.4 Tétel.**

I. Ha az \( ax \equiv b \mod m \) kongruencia megoldható, akkor a megoldásszáma \( (a,m) \).
II. Legyen \((n,m) = d\), \(m = dm_1\), és tegyük fel, hogy az \(s\) egész szám (az egyik) megoldása az 
\[ax \equiv b \pmod{m}\] kongruenciának. Ekkor az
\[s, \quad s + r_1, \quad s + 2r_1, \quad \ldots, \quad s + (d-1)r_1\] számok páronként inkongruensek modulo \(m\), kielégítik a kongruenciát, és az összes megoldás ezek valamelyikével kongruens modulo \(m\).

Bizonyítás: Az I. és II. állításokat egyszerre igazoljuk.
A feltétel szerint az \(s\) egész szám megoldás, vagyis
\[as \equiv b \pmod{m}\] Egy \(t\) egész szám akkor és csak akkor megoldás, ha
\[at \equiv b \pmod{m}\]
A (2) feltétel alapján (3) ekvivalens azzal, hogy
\[at \equiv os \pmod{r_1}\] A T 2.1.3 Tétel alapján (4) tovább ekvivalens
\[i = s \left( \frac{m}{(m,a)} \right), \quad \text{százz} \quad t = s \left( \frac{m}{m_1} \right)\]
teljesülésével. Ezt úgy írhatjuk, hogy
\[l = s + k_1 n_1,\] ahol \(k\) egész szám.

Ez azt jelenti, hogy az \(ax \equiv b \pmod{m}\) kongruencia összes megoldását az (5)-ben megadott \(t\) értékek szolgáltatják.

Így már csak azt kell igazolnunk, hogy az (5)-beli \(t\) értékek \(d\)-, darab különböző maradékosztályba tartoznak modulo \(m\), és (1)-ben éppen ezeknek a maradékosztályoknak egy-egy reprezentánsa szerepel.

Vizsgáljuk meg, mikor esik két ilyen \(t\) ugyanabba a maradékosztályba modulo \(m\). Legyen
\[t' = s + k'_1 n_1, \quad \text{és} \quad t'' = s + k''_1 n_1.\]
Ekkor
\[t' = t'' \pmod{m} \iff k'_1 n_1 = k''_1 n_1 \pmod{m} \iff k' = k'' \pmod{d}.\] Itt az első lépésben a \(t' \equiv t'' \pmod{m}\) kongruenciából kivontunk \(s\)-et, majd ismét a T 2.1.3 Tétel szabályai szerint egyszerűsíttettünk \(n_1\)-gyel, ekkor a modulus közben \(r_1/(m_1,m) = m/r_1 = d\) re változott.

(6) azt jelenti, hogy két \(t\) pontosan akkor esik ugyanabba a modulo \(m\) maradékosztályba, ha a megfelelő \(k\) kongruens modulo \(d\).
Így, ha $k$ végigfut a $0, 1, \ldots, d-1$ számokon, akkor az ezekhez tartozó
\[ i = s + kn_1 \pmod{m_1} \]
értékek a keresett modulo $m$ maradékosztályok egy-egy reprezentánsát alkotják. 

Külön kiemeljük azt a speciális esetet, amikor az $ax \equiv b \pmod{m}$ lineáris kongruenciában $(a, m) = 1$. Ekkor $(a, m) \mid b$ automatikusan teljesül, tehát a T 2.5.3 Tétel szerint a kongruencia biztosan megoldható, és a T 2.5.4 Tétel alapján a megoldásszám $(a, m) = 1$. Ezt az eredményt fontossága miatt külön tételként is megfogalmazzuk:

2.5.5 Tétel . T 2.5.5

Ha $(a, m) = 1$, akkor az $ax \equiv b \pmod{m}$ kongruencia bármely $b$ esetén megoldható és a megoldásszáma 1. 

A megoldási módszerek bemutatása előtt néhány fontos előzetes megjegyzést teszünk.

(A) Általában célszerű előre ellenőrizni a T 2.5.3 Tétel kritériuma alapján, hogy a kongruencia egyáltalán megoldható-e.

(B) Ha $(a, m) = 1$, akkor a lineáris kongruenciát csak egyetlen maradékosztály elemei elégtík ki, tehát ha találtunk egy megoldást, akkor készen is vagyunk. Általában is elég egyetlen megoldás megkeresése, mert akkor az összes megoldás megadása már könnyen megy a T 2.5.4/II Tétel alapján.

(C) A legtöbb esetben érdemes a megoldandó kongruenciát visszavezetni egy olyan lineáris kongruenciára, amelyen az $x$ együtthatója és a modulus már relativ prim. Ezt a következőképpen tehetjük meg.

Ha az $ax \equiv b \pmod{m}$ kongruencia megoldható, akkor $(a, m) \mid b$. Igy a $d = (a, m)$ jelöléssel
\[ a = da_1, \quad m = dm_1, \quad b = db_1 \quad \text{és} \quad (a_1, m_1) = 1. \]

Ekkor a kongruenciát „végigoszthatjuk” $d$ -vel (a modulust is beleértve): az $ax \equiv b \pmod{m}$ kongruencia a T 2.1.3 Tétel alapján „ekvivalens” az $a_1x_1 \equiv b_1 \pmod{m_1}$ kongruenciával, amelynél már $(a_1, m_1) = 1$ . (Ez az átalakítás tulajdonképpen annak felel meg, hogy az $ax \equiv b \pmod{m}$ kongruenciához tartozó $ax + mj = b$ diofantikus egyenletet elosztjuk $d$ -vel, és ekkor az $a_1x + m_1y = b_1$ diofantikus egyenletet kapjuk.)

Az előző bekezdésben az „ekvivalens” szó érdekes, arra utal, hogy ha a két kongruenciát ugyanazok az egész számok elégtík ki, azonban ezeket az elsőnél modulo $mn_1$ , a másodiknél pedig modulo $m_1$ maradékosztályokba kell besorolni. Így például a két kongruencia megoldásszáma sem lesz azonos (ha $d > 1$ ).

Most rátérünk a lineáris kongruenciák néhány megoldási módszerének az ismertetésére, amelyeket egy-egy példával illusztrálunk.

M1 Végigpróbálkodás. Egy modulo $mn$ teljes maradékkrendszer minden elemére megpiroszjálok, hogy kielégítő-e a kongruenciát. (Ezt csak nagyon kis modulus esetén érdemes alkalmazni.)

P1 $23x \equiv 11 \pmod{5}$ . Az egyszerűbb számolás érdekében a behelyettesítés előtt érdemes az együtthatók helyére velük kongruens, de kisebb (abszolút értékű) számokat írní: $3x \equiv 1 \pmod{5}$ vagy $-2x \equiv 1 \pmod{5}$ . Kipróbálva a $0, 1, 2, 3, 4$ (vagy $0, \pm 1, \pm 2$ ) értékeket azt kapjuk, hogy az
egyetlen megoldást az \( x \equiv 2 \mod{5} \) maradékosztály adja. [Mivel \( (23, 5) = 1 \) alapján eleve tudjuk, hogy csak egyetlen megoldás van, így annak megtalálása után a további értékeket természetesen nem kell már kipróbálni.]

**M2 Diofantikus egyenlet.** A lineáris kongruenciát a T 2.5.3 Tétel bizonyításában látott módon visszavezETJük egy diofantikus egyenlőtre, a diofantikus egyenletet megoldjuk, és a kapott megoldásokat „visszalakítva” megkapjuk a kongruencia megoldásait.

\[ \text{P2} \quad 15x \equiv 38 \mod{28} \quad \text{A megfelelő diofantikus egyenlet} \quad 15x + 28y = 38 \quad \text{Ezt 2-vel leosztva} \quad 9x + 14y = 19 \quad \text{adódik.} \]

Az T 1.3.6 Tétel bizonyítását követve állítsuk elő a 9 és a 14 legnagyobb közös osztóját 9\(n\) + 14\(v\) alakban. Az euklideszi algoritmusból vagy némi próbálgatás után kapjuk, hogy \(9 \cdot (-3) + 14 \cdot 2 = 1\). Ezt 19-cel beszorozva \(9 \cdot (-57) + 14 \cdot 38 = 19\) adódik, vagyis a \( 9x + 14y = 19\) diofantikus egyenlet egyik megoldása \( x = -57, y = 38 \).

Visszatérve a \( 15x \equiv 38 \mod{28} \) kongruenciára, ez azt jelenti, hogy \( x = -57 \) az egyik megoldás.

Az összes megoldást ezután a T 2.5.4/II Tétel szerint \( a = -57 \mod{28} \) és \( x = -43 \mod{28} \) maradékosztályok adják. (Ilt a = -57 és -43 reprezentánsok helyett irhatunk természetesen például -1-et, illetve 13-at.)

Megjegyezzük, hogy a lineáris diofantikus egyenletek megoldásánál inkább a 7.1 pontban szereplő eljárást érdemes alkalmazni, amely nemsok egy megoldást szolgáltat, hanem (paraméteres alakban) egyszerre megadja az egyenlet összes megoldását. (Tulajdonképpen az a módszer is az euklideszi algoritmus egy változata.)

**M3 Euler–Fermat-tétel.** Az \( a^x \equiv b \mod{n} \) kongruenciát a (C) megjegyzésben látott módon vezessük vissza az \( a^x \equiv b \mod{m_1} \) kongruenciára, ahol \( (a_1, m_1) = 1 \).

Ekkor az Euler–Fermat-tétel szerint \( a^x \equiv b \mod{m_1} \). Ennek alapján \( x = e_1^{\varphi(m_1)} \cdot b_1 \) megoldása a kongruenciának:

\[ a_1 \cdot a_1^{\varphi(m_1) - 1} b_1 = a_1^{e_1^{\varphi(m_1)} - 1} b_1 = b_1 \mod{m_1}. \]

Visszatérve az eredeti kongruenciára, ekkor \( x = e_1^{\varphi(m_1) - 1} b_1 \) annak is megoldása. Az összes megoldást ezután ismét (például) a T 2.5.4/II Tételből kaphatjuk meg.

\[ \text{P3} \quad 36x \equiv 81 \mod{21}. \quad \text{Itt} \quad (36, 21) = 3 \quad \text{így a feladatot visszavezethetjük a} \quad 12x = 27 \mod{7} \text{kongruenciára. Az együtthatókat redukálva} \quad -2x \equiv -1 \mod{7} \quad \text{adódik. Ennek megoldása} \quad x = (-2)^3 \cdot (-1) \equiv 4 \mod{7}. \quad \text{Tehát az eredeti kongruencia összes megoldása:} \quad x \equiv 4, 11, 18 \mod{21} . \]

Természetesen a \( 12x \equiv 27 \mod{7} \) kongruenciában az együtthatók redukciójánál választhatjuk a legkisebb nemnegatív maradékokat is a legkisebb abszolút értékű maradékok helyett. Ekkor az \( 5x \equiv 6 \mod{7} \) kongruenciához jutunk és \( x \equiv 5 \cdot 6 \mod{7} \) adódik.

Mivel \( (12, 7) = 1 \), ezért a \( 12x \equiv 27 \mod{7} \) kongruenciának egyetlen megoldása van modulo 7, tehát szükségképpen \( 5^2 \cdot 6 \equiv 4 \mod{7} \). Ennek a közvetlen igazolásának nem kell az \( 5^2 \) értékét ténylegesen kiszámolni, hanem a hatványozáskor mindig vehetjük a modulo 7 maradékokat:

\[ 5^2 = 25 \equiv 4 \mod{7}, \quad 5^4 = 4^2 \equiv 2 \mod{7}, \quad 5^5 = 5 \cdot 2 \equiv 3 \mod{7}, \]
KONGRUENCIÁK

és így valóban \(6 \cdot 5^3 = 6 \cdot 3 = 4 \pmod{7}\).

M4 Ügyeskedések. A kongruenciát ügyesen választott, a modulushoz relatív prim számokkal szorozta, illetve egyszerűsítve az eredetivel ekvivalens kongruenciákhoz jutunk, míg végül a megoldás(ok) nyilvánvalóan leolvasható(k).

\(p_4 \quad 80x \equiv 32 \pmod{108}\). Itt \(80, 108 = 4\), így a feladatot visszavezethetjük a \(20x \equiv 8 \pmod{27}\) kongruenciára.

Mivel \(\{4, 27\} = 1\), ezért a 4-gyel történő egyszerűsítés ekvivalens lépés: \(5x \equiv 2 \pmod{27}\).

Most két módszert is mutatunk arra, hogy az \(5x \equiv 2 \pmod{27}\) kongruenciában hogyan „szabadulhatunk meg” az 5 együttthatótól.

I. Osztás: Ahhoz, hogy az 5-tel egyszerűsíthessünk, írjuk a jobb oldalon a 2 helyére a vele kongruens \(-5\):

\[ 5x \equiv -25 \pmod{27} \]. Mivel \((5, 27) = 1\), innen \(x = -5 \pmod{27} \) adódik.

II. Szorzás: Olyan szorzót keresünk, hogy a beszorzás után az \(x\) együtthatója 1-gyel (vagy \(-1\)-gyel) legyen kongruens modulo 27. (Ekkor ez a szorzó biztosan relatív prim a 27-hez, ezért a beszorzás most automatikusan ekvivalens lépést jelent.) Szorozzuk be a \(5x \equiv 2 \pmod{27}\) kongruenciát például 11-gyel: ekkor \(55x \equiv 22 \pmod{27}\) és \(55 \equiv 1 \pmod{27}\) alapján \(x = 22(-5) \pmod{27}\) adódik.

Az eredeti kongruencia megoldásai tehát: \(x = -5, 22, 49, 76 \pmod{108}\).

Az egyes módszereket összehasonlítva első ránézésre talán az M3 vagy az M4 tűnhet a legkényelmesebbnek. Kiderül azonban, hogy nagy modulusok esetén szinte kizárólag az M2 használható. Erről részletesebben az 5.7 pontban lesz szó.

Feladatok

2.5.1 Oldjuk meg a P1–P4 példákat az M2–M4 módszerek mindegyikével.

2.5.2 Oldjuk meg az alábbi kongruenciákat:

(a) \(24x \equiv 60 \pmod{51}\);
(b) \(100x \equiv 88 \pmod{116}\);
(c) \(555x \equiv 5555 \pmod{5555}\);
(d) \(2^k+1)x \equiv 2^{k+1}+1 \pmod{2^{k+2}}+1\);
(e) \(10x^{30} + 8x^{20} - 9x^{10} + 7x \equiv 0 \pmod{19}\);
(f) \(13x^{11} \equiv 27 \pmod{100}\).

2.5.3 Határozzuk meg azt a két legkisebb pozitív egész, amelynek 13-szorosát hétbet számrendszerben felirva az utolsó előtti jegy 4, az utolsó jegy pedig 3.

2.5.4 Számítsuk ki 3\(^{27}\) utolsó két jegyét (tízes számrendszerben).

2.5.5 Az alábbi feltételek mindegyikéről döntsük el, hogy elégséges-e az \(ux \equiv b \pmod{m}\) kongruencia megoldhatóságához.
KONGRUENCIÁK

(a) \( (a, m) \mid (a, b) \).

(b) \( (a, b) \mid (a, m) \).

(c) \( a, m, b \) számtani sorozat.

(d) \( a, m, b \) mértani sorozat.

(e) \( a, b, m \) számtani sorozat.

(f) \( a, b, m \) mértani sorozat.

2.5.6 Melyek igazak az alábbi állítások közül?

(a) Az \( ax \equiv b \pmod{m} \) kongruencia megoldásszáma legfeljebb \( b \), ha \( b > 0 \).

(b) Ha az \( ax \equiv b \pmod{m} \) kongruencia megoldható, akkor megoldható az \( a^2x \equiv b^2 \pmod{m^2} \) kongruencia is.

(c) Ha az \( a_1x \equiv b_1 \pmod{m_1} \) és \( a_2x \equiv b_2 \pmod{m_2} \) kongruenciák megoldhatók, akkor megoldható az \( a_1a_2x \equiv b_1b_2 \pmod{m_1m_2} \) kongruencia is.

2.5.7 (M [563]) Legyen \( a \) és \( m \) rögzített, és jelöljük \( f(b) \)-vel az \( ax \equiv b \pmod{m} \) kongruencia megoldásszámát. Számítsuk ki a \( \sum_{b=1}^{m} f(b) \) összegét.

2.6 Szimultán kongruenciarendszerek

Szimultán kongruenciarendszerek azt nevezzük, amikor ugyanarra az ismeretlenekre egyidejűleg több, különböző modulus szerinti kongruenciafeltételt is előírunk:

\[
\begin{align*}
&f_1(x) \equiv 0 \pmod{m_1}, \quad f_2(x) \equiv 0 \pmod{m_2}, \quad \ldots, \quad f_k(x) \equiv 0 \pmod{m_k},
\end{align*}
\]

ahol \( f_1, \ldots, f_k \) egész együtthatós polinomok.

Egy ilyen rendszer megoldhatóságához nyilván szükséges, hogy minden egyes kongruencia különböző megoldható legyen. Az egyes kongruenciákat megoldva így elég az

\[
\begin{align*}
x &\equiv c_1 \pmod{m_1}, \quad x \equiv c_2 \pmod{m_2}, \quad \ldots, \quad x \equiv c_k \pmod{m_k}
\end{align*}
\]

alakú (speciális lineáris) rendszereket vizsgálnunk.

Először a két kongruenciából álló rendszerekkel foglalkozunk.

2.6.1 Tétel. T 2.6.1

I. Az

\[
\begin{align*}
x &\equiv c_1 \pmod{m_1} \\
x &\equiv c_2 \pmod{m_2}
\end{align*}
\]

szimultán kongruenciarendszer akkor és csak akkor oldható meg, ha

\[
\begin{align*}
(m_1, m_2) &\mid c_1 - c_2.
\end{align*}
\]

54
II. Megoldhatóság esetén az összes megoldás egy maradékosztályt alkot modulo $[m_1, m_2]$. Ez más megfogalmazásban azt jelenti, hogy ha az $s$ egész szám a szimultán kongruenciarendszer egy megoldása, akkor az alábbi $t$ értékek adják az összes megoldást:

$$t = s \mod \left[ m_1, m_2 \right], \quad \text{ahol } k \text{ egész}.$$ 

A tétel bizonyítása egyúttal módszert is szolgáltat a megoldások megkeresésére; kiderül, hogy egy lineáris diofantikus egyenletet (vagy ami ezzel egyenértékű, egy lineáris kongruenciát) kell megoldani.

**Bizonyítás:** I. A kongruencia definíciója alapján (1) átírható az

$$x = c_1 + z_1 m_1, \quad x = c_2 + z_2 m_2$$

(2)

alakba, ahol $z_1$ és $z_2$ egész számok.

A (2) feltétel ekvivalens teljesülésével. (3)-at átrendezve

$$c_1 - c_2 = z_2 m_2 - z_1 m_1$$

adódik.

Ez azt jelenti, hogy az (1) szimultán kongruenciarendszer a (4) lineáris diofantikus egyenletre vezethető vissza.

Az utóbbi megoldhatóságának szükséges és elégséges feltétele az T 1.3.6 Tétel szerint az, hogy $\left\langle n_1, m_2 \right\rangle \mid c_1 - c_2$ teljesüljen, tehát ugyanez a feltétele (1) megoldhatóságának is.

Mint a bizonyítás előtt jeleztük, egyúttal módszert is nyertünk a megoldások megkeresésére: a (4) diofantikus egyenletet, vagy egy ennek megfelelő lineáris kongruenciát kell megoldani.

II. Legyen $s$ egy megoldás, azaz

$$s \equiv c_1 \mod m_1, \quad s \equiv c_2 \mod m_2.$$ 

Egy $t$ egész szám definíció szerint pontosan akkor megoldás, ha

$$t \equiv c_1 \mod m_1, \quad t \equiv c_2 \mod m_2.$$ 

(6)

(5) alapján a (6) feltétel azzal ekvivalens, hogy

$$t \equiv s \mod m_1, \quad t \equiv s \mod m_2$$

(7)

teljesül. Írjuk át (7)-et oszthatóságra, és használjuk fel a legkisebb közös többszörös tulajdonságait (T 1.6.6/T. Tétel):

$$\frac{m_1}{m_2} \mid t - s \quad \text{és} \quad \frac{m_1}{m_2} \mid t - s \quad \text{és} \quad t \equiv s \mod \left[ m_1, m_2 \right].$$

Külön kiemeljük azt a speciális esetet, amikor az (1) szimultán kongruenciarendszer $m_1$ és $m_2$ modulusai relatív prímek. Ekkor az $\left\langle n_1, m_2 \right\rangle \mid c_1 - c_2$ feltétel automatikusan teljesül, tehát a T 2.6.1 Tétel alapján a kongruenciarendszer biztosan megoldható, és a megoldások egyetlen
maradékosztályt alkotnak modulo \( m_1 m_2 \). Ezt az eredményt fontossága miatt külön tételként is megfogalmazzuk:

**2.6.1A Tétel.** T 2.6.1A

Ha \( \langle m_1, m_2 \rangle = 1 \), akkor az

\[
x \equiv c_1 \pmod{m_1} \\
x = c_2 \pmod{m_2}
\]

szimultán kongruenciarendszer bármilyen \( c_1 \) és \( c_2 \) egész szám esetén megoldható, és a megoldások egyetlen maradékosztályt alkotnak modulo \( m_1 m_2 \).

A T 2.6.1A Tételből következik, hogy ha \( m_1 \) és \( m_2 \) relatív prímek, akkor hiába tudjuk, hogy mennyi egy számnak az \( m_1 \)-gyel való osztási maradéka, ez semmilyen támpontot sem jelent az \( m_2 \) szerinti osztási maradékkal kapcsolatban: a két modulusra vonatkozó maradék (egy jól meghatározott valószínűségszámítási értelemben) teljesen független egymástól. Így például egy szám utolsó számjegye vagy számjegyei a 10-zel vagy a 10 valamely hatványával való osztási maradékot jelentik, és ennél folyva semmilyen információt sem adhatnak arra vonatkozóan, hogy mi az adott szám maradéka 3-mal, 7-tel vagy 13-mal osztva, hiszen ezek a modulusok relatív prímei a 10-hez.

A több kongruenciából álló szimultán kongruenciarendszerek közül csak azzal az esettel foglalkozunk, amikor a modulusok páronként relatív prímek (az általános esetre vonatkozóan lásd a 2.6.13 feladatot [62]). Az idevágó téttel lényegében már Szun Cu kínai matematikus is ismerte mintegy 2000 évevel ezelőtt(!), ezért ezt kínai maradéktételnek is szokás nevezni.

**2.6.2 Tétel (Kínai maradéktétel).** T 2.6.2

Legyenek az \( m_1, \ldots, m_k \) modulusok páronként relatív prímei. Ekkor az

\[
x \equiv c_1 \pmod{m_1} \\
x = c_2 \pmod{m_2} \\
\vdots \\
x = c_k \pmod{m_k}
\]

szimultán kongruenciarendszer bármilyen \( c_1, \ldots, c_k \) egész esetén megoldható, és a megoldások egyetlen maradékosztályt alkotnak modulo \( m_1 m_2 \cdots m_k \).

*Előb bizonyítás:* A tétel könnyen adódik a 2.6.1A Tételből \( k \) szerinti teljes indukcióval.

A \( k = 2 \) eset éppen maga a T 2.6.1A Tétel.

Tegyük fel, hogy \( k - 1 \) kongruenciából álló rendszerekre az állítás igaz, és tekintsük a \( k \) kongruenciából álló (8) rendszert. Itt az első \( k - 1 \) kongruenciát kielégítő egész számok az indukciós feltevés szerint egyetlen maradékosztályt alkotnak modulo \( m_1 m_2 \cdots m_{k-1} \), vagyis az első \( k - 1 \) kongruencia helyett egyetlen \( x = c \pmod{m_1 m_2 \cdots m_{k-1}} \) kongruencia írható, ahol \( c \) alkalmaz egész szám. Így (8) ekvivalens az

\[
x = c \pmod{m_1 m_2 \cdots m_{k-1}}
\]

szimultán kongruenciarendszerrel. (9)-re ismét a T 2.6.1A Tételt alkalmazva éppen a \( k - 1 \)-ra vonatkozó állítást kapjuk.

*Második bizonyítás:* Csak a megoldhatóságra adunk új bizonyítást, mégpedig a(z egyik) megoldást (valamilyen értelemben) elő is állítjuk.
Az eljárás némileg emlékeztet a Lagrange-féle interpolációs polinomok konstrukciójára.

Először azt a speciális esetet tekintjük, amikor (8)-ban az egyik \( c_i \) értéke 1, a többi \( c_j \) pedig 0, majd az itt kapott eredményt felhasználjuk az általános eset megoldásához.

Nézzük meg mindezt részletesen. Legyen
\[
M = m_1 \ldots m_k \quad \text{és} \quad M_i = \frac{M}{m_i}, \quad i = 1, 2, \ldots, k.
\]

Mivel \( m_1, \ldots, m_k \) modulusok páronként relatív prímek, ezért
\[
(M_i, m_i) = 1, \quad i = 1, 2, \ldots, k. \tag{10}
\]

I. Rögzítsünk egy \( 1 < i < r \) indexet, és oldjuk meg a feladatot először abban a speciális esetben, amikor (8)-ban \( c_i = 1 \), és \( j \neq i \) -re \( c_j = 0 \).

Az \( x = 0 \pmod{m_j} \) kongruenciákat azt jelentik, hogy \( x \) minden \( j \neq i \) -re osztható \( m_j \) -vel. Az \( m_j \) modulusok páronként relatív prímek, ezért ez ekvivalens azzal, hogy \( x \) osztható az \( m_j \) számok szorzatával, vagyis \( M_i \cdot \text{vel}: x = M_i \cdot z \).

Írjuk be ezt \( x \) helyére a fennmaradó \( x = 1 \pmod{m_i} \) kongruenciában:
\[
M_i \cdot z \equiv 1 \pmod{m_i}. \tag{11}
\]

Ez \( z \) -re nézve lineáris kongruencia, amely (10) alapján megoldható.

Legyen a \( b_i \) egész szám megoldása (11)-nek. Ekkor az előzőek alapján \( x = b_i M_i \) megoldása (8)-nak.

II. Tekintsük meg az általános esetet, amikor (8)-ban valamennyi \( c_i \) tetszőleges. Megmutatjuk, hogy ekkor
\[
x = c_1 b_1 M_1 + \cdots + c_k b_k M_k \quad \text{(ahol) } M_i b_i \equiv 1 \pmod{m_i}, i = 1, \ldots, k \tag{12}
\]

megoldása a (8) szimultán kongruenciarendszernek.

Ellenőrizzük például az \( x \equiv c_i \pmod{m_3} \) kongruencia teljesülését. A (12) összegben \( M_3 \) kivételével valamennyi \( M_j \) osztható \( m_3 \)-mal, továbbá \( b_3 M_3 = 1 \pmod{m_3} \), ezért valóban
\[
c_1 b_1 M_1 + \cdots + c_k b_k M_k = c_3 b_3 M_3 = c_3 \pmod{m_3} \quad \square
\]

A T 2.6.2 Tétel fontos következménye, hogy tetszőleges összetett modulusú kongruencia visszavezethető prímhatvány modulusú kongruenciákra. Legyen ugyanis \( m \) kanonikus alakja \( m = p_1^{e_1} \cdots p_r^{e_r} \). Ekkor az
\[
f(x) \equiv 0 \pmod{m} \tag{13}
\]

kongruencia ekvivalens az
\[
f(\bar{x}) \equiv 0 \pmod{p_1^{e_1}}
\]
\[
f(\bar{x}) \equiv 0 \pmod{p_2^{e_2}}
\]
\[
\vdots
\]
\[
f(\bar{x}) \equiv 0 \pmod{p_r^{e_r}} \tag{14}
\]

szimultán kongruenciarendszerrel.
A (14) rendszerben minden kongruenciát külön-külön megoldunk. Ha valamelyik nem oldható meg, akkor nyilván (13)-nak sincs megoldása. Ha mindegyik megoldható, akkor legyen \( h_1, \ldots, h_n \) egy-egy megoldásuk. Ekkor az

\[
x \equiv h_1 \pmod{p_1^{n_1}} \\
x \equiv h_2 \pmod{p_2^{n_2}} \\
\vdots \\
x \equiv h_n \pmod{p_n^{n_n}}
\]

szimultán kongruenciarendszert megoldva az eredeti (13) kongruencia egy megoldásához jutunk. Az összes megoldást úgy kapjuk, ha \( h_1, \ldots, h_n \) végigfut a (14)-beli kongruenciák összes lehetséges megoldásrendszerein.

**P1 példa:** Oldjuk meg a

\[
10x^{84} + 3x + 7 \equiv 0 \pmod{245} \quad (15)
\]
kongruenciát.

Az előzőek alapján (15) ekvivalens a

\[
10x^{84} + 3x + 7 \equiv 0 \pmod{5} \quad (16) \\
10x^{84} + 3x + 7 \equiv 0 \pmod{49} \quad (17)
\]
szimultán kongruenciarendszerrel.

A (16) kongruencia \( 10 \equiv 0 \pmod{5} \) miatt ugyanaz, mint a \( 3x + 7 \equiv 0 \pmod{5} \) lineáris kongruencia. Ennek egyetlen megoldása

\[
x \equiv 1 \pmod{5} \quad (16a)
\]

A (17) kongruenciánál a megoldások keresésénél két esetet érdemes megkülönböztetni:

(i) \( \langle x, 49 \rangle = 1 \) ;

(ii) \( \langle x, 49 \rangle \neq 1 \).

Az (i) esetben az Euler–Fermat-tétel szerint

\[
x^{84} \equiv x^{2^{(49-1)}} \equiv 1 \pmod{49}.
\]

Így ebben az esetben (17) ekvivalens a \( 3x - 17 \equiv 0 \pmod{49} \) lineáris kongruenciával. Ennek egyetlen megoldása

\[
x \equiv -22 \pmod{49} \quad (17)
\]

A (ii) eset azt jelenti, hogy \( 7 \mid x \). Ekkor \( x^{84} \equiv 0 \pmod{49} \). Így ebben az esetben (17) ekvivalens a \( 3x + 7 \equiv 0 \pmod{49} \) lineáris kongruenciával. Ennek egyetlen megoldása (a \( 7 \mid x \) feltételt is kielégítő)

\[
x \equiv 14 \pmod{49} \quad (17b)
\]

A (15) kongruencia megoldásait ezek szerint az
KONGRUENCiÁK

\[ x = 1 \pmod{5} \quad (16a) \]
\[ x = -22 \pmod{49} \quad (17a) \]

illetve az

\[ x = 1 \pmod{5} \quad (16a) \]
\[ x = 14 \pmod{49} \quad (17b) \]

szimultán kongruenciarendszer megoldásaiból kapjuk meg.

A megoldásokat meghatározhatjuk a T 2.6.1 Tétel bizonyításánál jelzett eljárással, de gyakran kényelmesebben az alábbi módszer.

Az első kongruenciarendszerben a nagyobbik modulus szerinti (17a) kongruenciából

\[ x = 49z - 22 \quad (18) \]

Írjuk be (18)-at a (16a) kongruenciába, ekkor

\[ 49z - 22 \equiv 1 \pmod{5} \]

adódik. Ebből

\[ z \equiv 2 \pmod{5}, \quad \text{azaz} \quad z = 5w + 2. \quad (19) \]

Visszahelyettesítve (19)-et (18)-ba azt kapjuk, hogy \[ x = 245w + 78 \]. Ez azt jelenti, hogy az első kongruenciarendszer megoldása \[ x \equiv 76 \pmod{245} \].

Hasonlóan nyerjük, hogy a második kongruenciarendszer megoldása \[ x \equiv 161 \pmod{245} \].

Tehát a (15) kongruencia összes megoldása

\[ x \equiv 76 \pmod{245} \implies x \equiv 161 \pmod{245}. \]

Végül a kínai maradéktétel egy számítástechnikai alkalmazását mutatjuk be. Sok olyan művelet van, amelyet a számítógép egész számok összeadásának, kivonásának és szorzásának sorozatából épít fel, azt ilyen alaplépésekre vezeti vissza. Ezért igen lényeges, milyen gyorsan lehet ezeket az alapműveleteket elvégezni.

Tekintsük például az összeadást. A szokásos számrendszeres felírás esetén a számjegyek összeadását nem lehet egymástól függetlenül elvégezni, mert az átvitelek jelentősen befolyásolhatják az eredményt. Az ún. maradékszámrendszerben viszont az egyes „számjegyekkel” teljesen függetlenül végezhetjük a műveleteket. Ezt elsősorban olyanok szokták alkalmaznai, ha sok párhuzamos processzor áll rendelkezésre.

A módszer lényege a következő. Tegyük fel, hogy a számolás során csak \( N \)-nél kisebb abszolút értékű egészek fordulhatnak elő. (Ez nem jelent semmiféle megszorítást, hiszen bármely számítógép csak egy adott korlátig képes a számokat ábrázolni és velük műveleteket végezni.) Legyen \( r_1 = r_2, \ldots, r_r \) az első \( r \) darab ( pozitív ) primszám szorzata, ahol \( r \)-et úgy választjuk meg, hogy \( n > 2N \) teljesüljön.

Ekkor egy \( N \)-nél kisebb abszolút értékű egész szám megegyezik a modulo \( n \) legkisebb abszolút értékű maradékával. Ehelyett pedig tekinthetjük a szám modulo \( P_i \) maradékinak a rendszerét, ezek lesznek a szám „számjegyei" maradékszámrendszerben.

A „számjegyek” tulajdonképpen egy szimultán kongruenciarendszert jelentenek, ahol a \( P_i \) modulusok páronként relatív prímek, és így ezekből a modulo \( n \) maradék, vagyis maga a szám egyértelműen rekonstruálható.
KONGRUENCIÁK

Két szám összeadásakor vagy szorzásakor a megfelelő maradékokat (azaz a „számjegyeket”) kell összeadni, illetve összeszorozni („átvitel” nincs, a különböző modulusokhoz tartozó műveletek egymástól függetlenül végezhetők), majd az így kapott modulo \( p_i \) maradékok rendszeréből kell a modulo \( n \) maradékot, vagyis magát a számot meghatározni.

**P2 példa:** Illusztrációként legyen \( N = 1000 \), és végezzük el a \( 27 \cdot 34 \) szorzást maradékszámrendszerben.

Ekkor

\[ n = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310 \]

megfelel. A 27 maradékaik a 2, 3, 5, 7 és 11 primekkel osztva rendre 1, 0, 2, 6 és 5, tehát a 27 maradékszámrendszeres felírása

\[ 27 = (1, 0, 2, 6, 5). \]

Hasonlóan

\[ 34 = (0, 1, 4, 6, 1). \]

A \( 27 \cdot 34 \) szorzás elvégzéséhez összeszorozzzuk az egyes „számjegyeket” („átvitel” nincs), a szorzatokat redukáljuk modulo \( 2310 \), majd megoldjuk az így adódó szimultán kongruenciarendszert:

\[ 27 \cdot 34 = (1, 0, 0, 1, 2, 4, 6, 0, 5, 1) = (0, 0, 3, 1, 5), \]

és az

\[ x = 0 \pmod{2} \]
\[ x \equiv 0 \pmod{3} \]
\[ x = 3 \pmod{5} \]
\[ x \equiv 1 \pmod{7} \]
\[ x = 5 \pmod{11} \]

szimultán kongruenciarendszer megoldása

\[ x \equiv 918 \pmod{2310}. \]

Tehát \( 27 \cdot 34 = 918 \).

Ha több műveletet végzünk, akkor természetesen folyamatosan lehet a maradékszámrendszeres alakkal dolgozni, és csak a végeredményt érdemes „visszaváltani” a számok szokásos alakjába.

Megemlítjük még, hogy a szimultán kongruenciarendszereket hasonló módon lehet alkalmazni (racionális együttáthatós) lineáris egyenletrendszerek megoldásánál is. A módszer lényege, hogy az egyenletrendszert különböző prim modulusok szerint tekintjük, majd az így kapott megoldásokból előállítjuk az egyenletrendszer megoldását a modulusok szorzatára nézve, ami megfelelő feltételek esetén magát a keresett megoldást is megadja, ha elég sok modulusat választunk. Az eljárás előnye, hogy szemben pl. a hagyományos Gauss-kiküszöböléssel, itt nem keletkeznek túl nagy (vagy túl kicsi) számok, és ezért nem fenyeget a túlsordulás veszélye.

**Feladatok**

(Ha más kikötést nem teszünk, akkor a feladatok tízes számrendszerre vonatkoznak.)
2.6.1 (a) Egy százlábú meg akarja számolni a lábait. Tudja, hogy legfeljebb 250 lába van. Ha 11-esével számolja öket, akkor 5 marad ki, ha 15-ösével, akkor 3. Hánylábú a százlábú?

(b) Egy másik százlábú is megrigyli ezt a módszert. Neki 12-esével számolva 4 marad, 15-ösével számolva pedig 8. Bizonyítsuk be, hogy elszámolta magát.

2.6.2 Egy szám utolsó jegye 20-as alapú számrendszerben „tizenegyes”. Mi lehet az utolsó jegye (a) 9-es; (b) 8-as alapú számrendszerben?

2.6.3 Oldjuk meg az alábbi kongruenciákat:

(a) \[ 2x^{10} + 3x + 4 \equiv 0 \pmod{176} \];

(b) \[ 21x^{65} + 16x^{31} + 11x + 6 \equiv 0 \pmod{333} \];

(c) \[ 3x^3 + 3x + 7 \equiv 0 \pmod{105} \].

2.6.4 Legyenek \(a\), \(b\) és \(c\) páronként relatív prim, 1-nél nagyobb egészek. Milyen maradéket ad

(a) \(a^b\)-vel osztva \(a^{\varphi(b)} + b^{\varphi(a)}\);

(b) \(ab^c\)-vel osztva \(a^{\varphi(bc)} + b^{\varphi(ac)} + c^{\varphi(ab)}\) ?

2.6.5 Határozzuk meg \(1234^{1987}\) utolsó három számjegyét.

2.6.6 Gondoltam egy egész számot 200 és 2000 között. Ha a szám 501-edik és 201-edik hatványát összeadom, majd ehhez hozzáadom magát a számot, akkor az eredmény 998-ra végződik. Melyik számra gondoltam?

2.6.7 Melyek azok az (a) kétjegyű; (b) háromjegyű pozitív egészek, amelyek négyzete is ugyanerre a két, illetve három számjegyre végződik?

2.6.8 (a) Hány olyan huszonegyjegyű pozitív egész létezik, amelynek minden hatványában ugyanaz az utolsó húsz számjegy, mint az eredeti számban volt?

(b) Hány olyan huszonegyjegyű pozitív egész létezik, amelynek minden páratlan hatványában ugyanaz az utolsó húsz számjegy, mint az eredeti számban volt?

2.6.9 (M [563]) Mennyi lesz a pontos idő (óra/perc) éjfél után \(3^{34\cdot87}\) perccel?

2.6.10 (a) Legyen \((a, b) = 1\) és \(v_1, \ldots, v_r(c)\), illetve \(s_1, \ldots, s_r(b)\) reduált maradékkrendszer modulo \(a\), illetve modulo \(b\). Jelöljük \(c_{ij}\)-vel az

\[
x \equiv r_i \pmod{a}
\]

\[
x = s_j \pmod{b}
\]

szimultán kongruenciarendszer (egy) megoldását, \(i = 1, \ldots, \varphi(a)\), \(j = 1, \ldots, \varphi(b)\). Mutassuk meg, hogy a \(c_{ij}\) számok reduált maradékkrendszert alkotnak modulo \(ab\). A bizonyítás során csak a reduált maradékkrendszer definióját használjuk (D 2.2.8 Definíció), és ne támaszkodjunk a T 2.2.9 Tételre, illetve a jelen feladat (b) részére.

(b) Bizonyítsuk be (újra): \((a, b) = 1 \implies \varphi(ab) = \varphi(a)\varphi(b)\).

2.6.11 Igazoljuk, hogy a négyzetmentes számok sorozatában tetszőlegesen nagy hétzegok is előfordulnak. Pontos megfogalmazásban ez azt jelenti, hogy bármely \(K\)-hoz létezik \(K\) olyan egymást követő pozitív egész, amelyek egyike sem négyzetmentes.
2.6.12 (*) (a) Bizonyítsuk be, hogy az alábbi két szimultán kongruenciarendszer bármely $u, b, c$ pozitív egész esetén megoldható.

\[ \begin{align*} x &\equiv a + b \pmod{c} \\
x &\equiv b + c \pmod{a} \\
x &\equiv c + a \pmod{b} \end{align*} \]

(b) Mutassuk meg, hogy az

\[ \begin{align*} x &\equiv a + b \pmod{c} \\
x &\equiv b + c \pmod{a} \\
x &\equiv c + a \pmod{b} \end{align*} \]

szimultán kongruenciarendszer akkor és csak akkor oldható meg, ha $\langle a, b \rangle = \langle b, c \rangle = \langle c, a \rangle$.

2.6.13 (*) Mutassuk meg, hogy az

\[ x \equiv c_1 \pmod{m_1}, \quad x \equiv c_2 \pmod{m_2}, \quad \ldots, \quad x \equiv c_k \pmod{m_k} \]

szimultán kongruenciarendszer (ahol az $m_i$ modulusok nem feltétlenül páronként relatív primek) akkor és csak akkor oldható meg, ha minden $1 \leq i < j \leq k$ esetén $\langle m_i, m_j \rangle = |c_i - c_j|$ teljesül.

2.6.14 Van-e olyan $f(x)$ egész együtthatós polinom, amelyre az $f(x) \equiv 0 \pmod{30}$ kongruencia megoldásszáma 14?

2.6.15 (a) Bizonyítsuk be, hogy akkor és csak akkor léteznek olyan számok, amelyek egyszerre alkotnak teljes maradékrendszert modulo $n$ és redukált maradékrendszert modulo $k$, ha $\varphi(k) = n$ és $(k, n) = 1$.

(b) Bizonyítsuk be, hogy akkor és csak akkor léteznek olyan számok, amelyek egyszerre alkotnak redukált maradékrendszert modulo $n$ és modulo $k$ is, ha $\varphi(n) = \varphi(k)$.

2.6.16 (a) Bizonyítsuk be, hogy tetszőleges $a_1$, $a_2$ és $a_3$ különböző egész számokhoz végelen sok olyan $n$ természetes szám létezik, amelyre $a_1 + n$, $a_2 + n$ és $a_3 + n$ páronként relatív primek.

(b) Adjunk meg olyan $a_1$, $a_2$, $a_3$ és $a_4$ különböző egészeket, hogy az $a_i + n$, $i = 1, 2, 3, 4$ számok semmilyen $n$ természetes szám esetén se legyenek páronként relatív primek.

(c) Mutassuk meg, hogy tetszőleges $a_1$, $a_2$, $a_3$ és $a_4$ különböző egész számokhoz végelen sok olyan $n$ természetes szám létezik, amelyre minden $i \neq j$ esetén $\langle a_i + n, a_j + n \rangle \leq 2$.

(d) Igazoljuk, hogy tetszőleges $a_1$, $a_2$, $a_3$ és $a_4$ különböző egész számokhoz végelen sok olyan $n$ természetes szám létezik, amelyre minden $1 \leq i < j < k \leq 4$ esetén

\[ \langle a_i + n, a_j + n, a_k + n \rangle = 1. \]

(e) Igazak maradnak-e a (c) és (d) részben szereplő állítások, ha négy helyett öt, illetve hat $G_i$ számot veszünk?
2.7 Wilson-tétel

2.7.1 Tétel (Wilson-tétel).

Ha \( P \) (pozitív) prim, akkor \( (p-1)! \equiv -1 \pmod{p} \).

Mivel az \( 1, 2, \ldots, p-1 \) számok redukált maradékszorzatot alkotnak modulo \( P \), és bármely modulo \( P \) redukált maradékszorzat elemeinek a szorzata ugyanaz a modulus \( P \) vel osztva, ezért a Wilson-tételt a következő formában is megfogalmazhatjuk:

Ha \( P \) (pozitív) prim, akkor egy modulo \( P \) redukált maradékszorzat elemeinek a szorzata \(-1\)-gyel kongruens modulo \( P \).

Az összetett modulusra vonatkozó általánosításokat a 2.7.1 feladatban [64], a csoportelméleti vonatkozásokat a 2.8 pontban tárgyaljuk.

Bizonyítás: A tétel \( P = 2 \) és \( P = 3 \) esetén nyilván igaz.

Megmutatjuk, hogy ha \( P \geq 5 \), akkor a \( 2, 3, \ldots, p-2 \) számok pára állíthatók úgy, hogy az egyes párokon az elemek szorzata legyen kongruens modulo \( P \). Ebből a tétel már következik, hiszen ekkor

\[
(p-1)! = 2 \cdot 3 \cdot \ldots \cdot (p-2) \cdot 1 \cdot (p-1) = 1 \cdot 1 \cdot (p-1) = -1 \pmod{p}.
\]

A pára állítást illusztráljuk először \( p = 11 \) -re. A 2 pártja a \( 2x \equiv 1 \pmod{11} \) kongruenciából kapjuk. Ennek egyetlen megoldása \( x \equiv 6 \pmod{11} \), azaz a 2 pára a 6. Itt a 2 és a 6 valóban kölcsönösen összetartoznak, „egymás párja”, hiszen \( 2 \cdot 6 = 12 \equiv 1 \pmod{11} \).

Hasonlóan továbbhaladva a 3–4, majd az 5–9, végül a 7–8 párokat kapjuk. Ennek alapján

\[
10! = (2 \cdot 6) \cdot (3 \cdot 4) \cdot (5 \cdot 9) \cdot (7 \cdot 8) \cdot 1 \cdot 10 \equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot (11) = -1 \pmod{11}.
\]

Most nézzük mindezt általánosan. A pára állításhoz a következőket kell igazolni:

(i) Minden \( 2 \leq a \leq p-2 \) egészhez pontosan egy olyan \( \hat{b} = f(a) \) létezik, amelyre

\[
a \hat{b} \equiv 1 \pmod{p} \quad \text{és} \quad 2 \leq \hat{b} \leq p-2.
\]

(ii) Ha \( f(a) = \hat{b} \), akkor \( f(\hat{b}) = a \), azaz \( a \) és \( \hat{b} \) valóban „egymás párja”.

(iii) \( f(a) \neq a \), azaz „egyik elem párja sem űnmaga”.

(i) Az \( ax \equiv 1 \pmod{p} \) kongruencia \( (a, \theta) = 1 \) miatt megoldható, és egyetlen \( b \) megoldása van a \( 0, 1, 2, \ldots, p-1 \) teljes maradékszorzatban. Mivel \( x = 0 \), \( 1 \), illetve \( p-1 \) esetén \( ax = 0 \), \( a \), illetve \( -a \pmod{p} \), így ezekre az \( x \) értékekre \( ax \neq 1 \pmod{p} \), tehát \( \hat{b} \) valóban a megadott \( 2 \leq \hat{b} \leq p-2 \) intervallumba esik.

(ii) Az \( f(a) = \hat{b} \) feltétel azt jelenti, hogy \( ab \equiv 1 \pmod{p} \). Az \( f(\hat{b}) \) érték a \( b\hat{b} \equiv 1 \pmod{p} \) kongruencia megoldása adja. Ezt a kongruenciát \( \hat{b} = c \) nyilván kielégíti, továbbá (i)-ből tudjuk, hogy ennek a kongruenciának a \( 2 \leq \hat{b} \leq p-2 \) intervallumban pontosan egy megoldása van. Ezért valóban \( f(\hat{b}) = c \).
(iii) A $b = c$ feltétel azt jelentené, hogy $a^2 \equiv 1 \pmod{p}$. Ezt oszthatóságra átírva, majd $P$ prim tulajdonságát felhasználva

$$p \mid (a - 1)(a + 1) \implies p \mid a - 1 \text{ vagy } p \mid a + 1 \implies c \equiv \pm 1 \pmod{p}$$

következik. Ez viszont ellentmond a $2 \leq c \leq p - 2$ feltételnek. ■

A Wilson-tétel egy-egy további bizonyítása szerepel a T 3.1.2 Tétel után, valamint a 3.3.6 feladatban [83].

### Feladatok

(Prímszámon végig pozitív primet értünk.)

#### 2.7.1 A Wilson-tétel általánosítása összetett modulusra. Legyen $\mathfrak{m}$ összetett szám. Milyen maradékot ad $\mathfrak{m}$-mel osztva

(a) $(\mathfrak{m} - 1)!$;

(b) $\varphi(\mathfrak{m})!$;

(c) egy redukált maradéktrendszer elemeinek a szorzata?

#### 2.7.2 Mely $\mathfrak{m} > 0$ egészre teljesül $(\mathfrak{m} - 6)! \equiv 1 \pmod{\mathfrak{m}}$?

#### 2.7.3 Legyen $\mathfrak{m} > 2$ és $a_1, \ldots, a_\mathfrak{m}$, illetve $b_1, \ldots, b_\mathfrak{m}$ az $1, 2, \ldots, \mathfrak{m}$ számok két tetszőleges permutációja.

(a) Mutassuk meg, hogy ha $\mathfrak{m}$ prim, akkor van olyan $\hat{i} \neq \hat{j}$, amelyre

$$\mathfrak{m} \mid a_i b_j - a_j b_i.$$

(b) Igazoljuk ugyanezt az állítást tetszőleges összetett $\mathfrak{m}$-re is.

#### 2.7.4 Legyen $P$ egy $4k - 1$ alakú prímszám. Bizonyítsuk be, hogy ekkor

$$\left(\frac{P - 1}{2}\right)! = \pm 1 \pmod{P}.$$

#### 2.7.5 Lássuk be, hogy bármely $P$ prímszámra

$$P^P \mid (P^2 - 1)! - P^{P-1}.$$

#### 2.7.6 Legyen $P > 3$ prim. Milyen maradékot ad $3(P - 3)!$, ha $P$-vel maradékosan elosztjuk?

#### 2.7.7 Milyen maradékot ad $99!$, ha 10100-zal maradékosan elosztjuk?

#### 2.7.8 Számítsuk ki $(n! + 3, (n + 2)! + 6)$ lehetséges értékeit, ha $n$ végeggen a természetes számokon.

#### 2.7.9 Milyen $\mathfrak{m}$-ekre létezik

(a) teljes;

(b) redukált

maradéktrendszer $k!$ alakú számokból?
2.7.10 Legyen \( a_1, \ldots, a_{31} \) reduált maradékkrendszer modulo 31. Lássuk be, hogy
\[
31 \mid (a_1 a_2 a_3)^3 + (a_1 a_4 \ldots a_{31})^27.
\]

2.7.11 Legyen \( p > 2 \) prim. Képezzünk egy egész számokból álló, \( p - 1 \) tagú számtani sorozatot, és szorozzuk össze az elemeit. Milyen maradéket adhat ez a szorzat \( P \)-vel osztva?

2.7.12 Oldjuk meg az \( x^m(z - x)^l = 1 \) (modul \( x \)) kongruenciát, ahol \( 0 < x < z \) egész számok.

2.7.13 (*) Melyek azok a \( P \) prímek, amelyekre \( (p - 1)! + 1 \) a \( P \)-nek ( pozitív egész kitevős) hatvanya?

## 2.8 Műveletek maradékosztályokkal

Ebben a pontban a modulo \( m \) maradékosztályok között összeadást és szorzást értelmezünk és ezek tulajdonságait vizsgáljunk. Az \( m > 1 \) modulust végig rögzítettnek tekintjük.

### 2.8.1 Definíció

Az \( \langle a \rangle \) és \( \langle b \rangle \) maradékosztályok összegén az \( \langle a + b \rangle \), szorzatán pedig az \( \langle ab \rangle \) maradékosztályt értjük, azaz
\[
\langle a \rangle \cdot \langle b \rangle = \langle ab \rangle.
\]

Be kell látnunk, hogy a fenti módon valóban műveleteket definiáltunk, azaz mind az összeadásnál, mind pedig a szorzásnál bármely két modulo \( m \) maradékosztályhoz egyértelműen hozzárendelünk egy modulo \( m \) maradékosztályt.

A problémát az jelenti, hogy a maradékosztályokra vonatkozó összeadást és szorzást a reprezentánsok segítségével adtuk meg, és így azt kell igazolni, hogy ez nem függ attól, hogy az egyes maradékosztályokban melyik reprezentánsat választottuk.

Nézzük az összeadást. Azt kell megmutatni, hogy ha \( \langle a \rangle \cdot \langle a' \rangle \) és \( \langle b \rangle \cdot \langle b' \rangle \), akkor \( \langle a + b \rangle = \langle a' + b' \rangle \). Ez valóban teljesül, ugyanis
\[
\begin{align*}
\langle a \rangle \cdot \langle b \rangle &= \langle a + b \rangle \\
\langle a' \rangle \cdot \langle b' \rangle &= \langle a' + b' \rangle.
\end{align*}
\]

Hasonlóan járhatunk el a szorzás esetében is.

Felhívjuk a figyelmet arra, hogy számos olyan, az egész számokon értelmezett művelet van, amelyek megfelelőíít nem lehet a reprezentánsok segítségével a maradékosztályok körében értelmezni. Ennek illusztrálására egy egyszerű példát mutatunk, további példák szerepelnek a 2.8.6 feladatban [69].

Legyenek \( a \) és \( b \) egész számok, és jelölje \( \max \{a, b\} \) közülük a nagyobbikat, illetve a közös értéküket, ha \( a = b \). Ez a maximumképzés bármely két egész számhoz egyértelműen hozzárendel egy egész számot, tehát művelet az egész számok körében.

Azonban a modulo \( m \) maradékosztályok körében a \( \max \{a, b\} \) egyenlőséggel nem tudunk műveletet értelmezni, ugyanis az egyenlőség jobb oldalán más és más maradékosztályt kap(hat)unk, ha az \( \langle a \rangle \cdot \langle b \rangle \), illetve \( \langle a \rangle \cdot \langle b \rangle \) maradékosztályt egy másik elemével reprezentáljuk. Például legyen a modulus \( m = 9 \), a két maradékosztály pedig
KONGRUENCIÁK

\[ A = \{3\}_9 = \{12\}_9 \text{ és } B = \{10\}_9 = \{1\}_9 \]. Ekkor \(1_{\text{max}}(A, B)\) egyrészét \(1_{\text{max}}(3,10)\) lenne, másrészt \(1_{\text{max}}(12,1) = \{12\}_9\) lenne, azonban \(\{10\}_9 \neq \{12\}_9\).

Most rátérünk a modulo \(\mathfrak{m}\) maradékosztályok körében értelmezett összeadás és szorzás legfontosabb tulajdonságaira.

Könnyen adódik, hogy az egész számoknál megismert tulajdonságok nagy része a maradékosztályok körében is érvényben marad:

2.8.2 Tétel. T 2.8.2

A modulo \(\mathfrak{m}\) maradékosztályok körében

— az összeadás associatív és kommutatív;

— a \((0)\) nullelem, azaz minden \((a)_m -ra \{0\}_m + \{a\}_m = \{a\}_m + \{0\}_m = \{a\}_m\);

— az \((a)\) nellen tetített \((-a)\), azaz \((-a)_m + \{a\}_m = \{a\}_m + \{-a\}_m = \{0\}_m\);

— a szorzás associatív és kommutatív;

— az \((1)\) egységelem, azaz minden \((a)\) -ra \((1)_m \cdot \{a\}_m = \{a\}_m \cdot (1)_m = \{a\}_m\);

— érvényes a distributivitás.

Bizonyítás: Valamennyi állítás azonnal következik a műveletek definíciójából és az egész számok megfelelő tulajdonságából. Nézzük példaként az összeadás kommutativitását:

\[
\{a\}_m + \{b\}_m = \{a + b\}_m = \{b + a\}_m = \{b\}_m + \{a\}_m
\]

(az első és a harmadik egyenlőség a maradékosztályok közötti összeadás definíciójából, a második egyenlőség pedig az egész számok összeadásának kommutativitásából adódik).

A T 2.8.2 Tételben felsorolt tulajdonságok azt jelentik, hogy a modulo \(\mathfrak{m}\) maradékosztályok az összeadásra és szorzásra nézve egységelemes, kommutatív gyűrűt alkotnak.

Megjegyezzük, hogy — mint bármely gyűrűben — a maradékosztályok körében a kivonás is elvégezhető, azaz bármely \((a)\) \(\{b\}_m\) esetén pontosan egy olyan \((c)\) létezik, amelyre \((a)_m = \{b\}_m + \{c\}_m\); a keresett \((c)_m\) maradékosztályt az \((a)_m \cdot (-1)\) alakban kaphatjuk meg. (A kivonás elvégezhetőségét az egész számok kivonására támaszkodva is beláthatjuk, ekkor \((c)_m = (a - b)_m\) adódik.)

Most megvizsgáljuk, hogy mely maradékosztályoknak létezik a szorzásra nézve inverze (multiplikatív inverze), azaz mely \((a)\) esetén létezik olyan \((c)\) maradékosztály, amelyre

\[
\{c\}_m \cdot \{a\}_m = \{a\}_m \cdot \{c\}_m = \{1\}_m.
\]

Az (1) feltétel azt jelenti, hogy \(\{ac\}_m = \{1\}_m\), azaz \(ac \equiv 1 \pmod{m}\), vagyis az \(a\) redukált maradékosztály legyen. Így beláttuk az alábbi tételt:

2.8.3 Tétel. T 2.8.3

A modulo \(\mathfrak{m}\) maradékosztályok között pontosan a redukált maradékosztályoknak létezik (multiplikatív) inverze.
Megjegyezzük, hogy bármely asszociatív művelet esetén egy elemnek csak egy inverze lehet. Így egy redukált maradékosztály inverze is egyértelmű. (Ez egyébként a T 2.5.5 Tételből is következik.)

Kommutatív testen egy olyan (legalább kételemű) kommutatív, egységelemes gyűrűt értünk, amelyben a nullelemen kívül minden elemnek létezik inverze. A T 2.8.3 Tétel szerint a modulo \( \mathbb{Z}_m \) maradékosztályok körében ez akkor és csak akkor teljesül, ha minden nemnulla maradékosztály redukált, azaz \( \mathbb{Z}_m \) prim. Így a következő tételt kaptuk:

**2.8.4 Tétel.** T 2.8.4

A modulo \( \mathbb{Z}_m \) maradékosztályok akkor és csak akkor alkotnak testet, ha \( m \) prim. ♦

A modulo \( \mathbb{Z}_m \) maradékosztályok körében előfordulhat, hogy két nemnulla maradékosztály szorzata a nulla maradékosztály, például \( \langle 5 \rangle_{10} \cdot \langle 4 \rangle_{10} = \langle 0 \rangle_{10} \). Egy \( \langle a \rangle_m \neq \langle 0 \rangle_m \) maradékosztályt — a (kommutatív) gyűrükben értelmezett általános fogalommal megfelelően — *nullosztonak* nevezünk, ha

\[
\text{van olyan } b \neq 0 \pmod m, \text{ azaz } (a, m) = 1.
\]

Az előző példa szerint tehát a \( \langle 4 \rangle_{10} \) maradékosztály nullosztó.

**2.8.5 Tétel.** T 2.8.5

Az \( \langle a \rangle_m \neq \langle 0 \rangle_m \) maradékosztály akkor és csak akkor nullosztó, ha \( \langle a \rangle_m \) *nem* redukált maradékosztály, azaz \( (a, m) \neq 1 \). ♦

Az \( \langle a \rangle_m \neq \langle 0 \rangle_m \) feltételt az \( a \) reprezentánsra vonatkozóan az \( m \equiv a \), illetve \( (a, m) < m \) kikötést jelenti.

**Bizonyítás:** A nullosztó (2)-beli definícióját átírva kapjuk, hogy \( \langle a \rangle_m \neq \langle 0 \rangle_m \) pontosan akkor nullosztó, ha

\[
\text{van olyan } b \neq 0 \pmod m, \text{ azaz } ab \equiv 0 \pmod m, \quad \text{ha } (a, m) = 1.
\]

Mivel az \( ax \equiv 0 \pmod m \) kongruenciának \( x \equiv 0 \pmod m \) mindig megoldása, ezért (3) azzal ekvivalens, hogy az \( ax \equiv 0 \pmod m \) kongruencia megoldásszámá 1-nél nagyobb. Mivel ez a megoldásszám éppen \( (a, m) \), így \( \langle a \rangle_m \neq \langle 0 \rangle_m \) valóban akkor és csak akkor nullosztó, ha \( (a, m) > 1 \).

A T 2.8.5 Tételből azonnal következik, hogy a modulo \( m \) maradékosztályok körében akkor és csak akkor található nullosztó, ha \( m \) összetett szám.

Végül röviden kitérünk a maradékosztályok néhány csoportelméleti vonatkozására.

Egy \( G \) halmazt akkor nevezünk *csoportnak*, ha értelmezve van \( G \) -n egy asszociatív művelet, létezik egységelem és minden elemnek van inverze. Ha a művelet kommutatív, akkor *kommutatív* vagy *Abel-csoportról* beszélünk.

Ennek alapján a modulo \( m \) maradékosztályok az összefüggésre, a redukált maradékosztályok pedig a szorzásra kommutatív csoportot alkotnak (ez utóbbi abból következik, hogy két redukált maradékosztály szorzata, valamint egy redukált maradékosztály inverze is redukált maradékosztály).

Az Euler–Fermat-tétel a következő általános csoportelméleti tétel speciális esetének tekinthető: Egy véges \( G \) csoport bármely \( a \) elemére \( a^{\varphi(G)} \) a csoport egységelemével egyenlő (ahol \( |G| \) a csoport elemszámát jelöli). Ez a csoportelméleti tétel kommutatív \( G \) esetén az Euler–Fermat-tétel mintájára igazolható (lásd a 2.8.7 feladatot [69]), tetszőleges \( G \) -re pedig az ún. Lagrange-tételből következik.
A Wilson-tétel általánosításaként azt a kérdést lehet megvizsgálni, hogy egy véges kommutatív csoport elemeinek a szorzata a csoport melyik elemével egyenlő (lásd a 2.8.8 feladatot [69]).

Feladatok

2.8.1 Milyen \( m \) esetén létezik olyan nemnulla maradékosztály, amely önmagának az ellentettje?

2.8.2 Tekintsük a modulo 100 maradékosztályok gyűrűjét.

(a) Mi a (13) maradékosztály multiplikatív inverze?

(b) Hány nullosztó van?

(c) A \( \{40\} \) maradékosztálynak hány nullosztópárja van, azaz hány olyan \( (i) \neq (0) \) maradékosztály létezik, amelyre \( \{40\} \cdot (i) = \{0\} \)?

(d) Van-e olyan \( (c) \) maradékosztály, amelyre \( \{35\} \cdot (c) = \{90\} \)?

2.8.3 Hány olyan modulo \( m \) maradékosztály van, amelynek önmaga a multiplikatív inverze, ha \( \forall a \) értéke

(a) 47;

(b) 30;

(c) 800;

(d) * tetszőleges?

2.8.4 Legyen \( m \) összetett szám, és tekintsük a modulo \( m \) maradékosztályok gyűrűjét.

(a) Mutassuk meg, hogy ha \( \{a\} \) nullosztó, akkor tetszőleges \( \{c\} \)-re \( \{a\} \cdot \{c\} \) nullosztó vagy \( \{0\} \).

(b) Lássuk be, hogy ha \( \{a\} \cdot \{c\} \) nullosztó, akkor \( \{a\} \) és \( \{c\} \) közül legalább az egyik nullosztó.

(c) Melyek azok az \( m \)-ek, amelyekre bármely két nullosztó összege is nullosztó vagy \( \{0\} \)?

(d) Határozzuk meg az összes nullosztó összegét, illetve szorzatát.

(e) Mely \( m \)-ek esetén létezik olyan \( \{a\} \neq \{0\} \), amelyre \( \{a\}^2 = \{0\} \)?

2.8.5 (a) Legyen \( H \) a modulo 20 maradékosztályok közül a „4-gyel oszthatók” halmaza, azaz

\[
H = \{\{0\}_{20}, \{4\}_{20}, \{8\}_{20}, \{12\}_{20}, \{16\}_{20}\}.
\]

Bizonyítsuk be, hogy \( H \) a maradékosztályok összeadására és szorzására kommutatív testet alkot.

(b) Legyen \( K \) a modulo 40 maradékosztályok közül a „4-gyel oszthatók” halmaza, azaz

\[
K = \{\{0\}_{40}, \{4\}_{40}, \ldots, \{36\}_{40}\}.
\]

Mutassuk meg, hogy \( K \) a maradékosztályok összeadására és szorzására kommutatív gyűrűt alkot, amely azonban nem test, a szorzásra nézve nincs egységelem, sőt \( K \) minden nemnulla eleme nullosztó.

(c)(M) [563] * Általánosítsuk (minél jobban) a feladatot.
2.8.6 Vizsgáljuk meg minél részletesebben, lehet-e a modulo $m$ maradékosztályokra a pozitív reprezentánsok segítségével értelmezni

(a) a legnagyobb közös osztót: $\text{lko}(a_m, b_m) = (\text{lko}(a, b))_m$;

(b) a köbre emelést: $(a)_m^3 = (a^3)_m$;

(c) a köbgyökverzést: $\sqrt[3]{(a)_m} = (\sqrt[3]{a})_m$;

(d) a számú közép képzését: $\left(\frac{(a)_m + (b)_m}{2}\right) = \left(\frac{a + b}{2}\right)_m$;

(e) a hatványozást: $(a)_m^b = (a^b)_m$.

2.8.7 Az Euler–Fermat-tétel általánosítása. Jelölje a $G$ véges kommutatív csoport elemszámát $|G|$, egységelemét $e$. Bizonyítsuk be, hogy bármely $a \in G$ elemre $a^{|G|} = e$.

2.8.8 (*) A Wilson-tétel általánosítása. Jelölje $S$ egy $G$ véges kommutatív csoport elemeinek a szorzatát és $e$ az egységelemet. Mutassuk meg, hogy ha $G$-ben pontosan egy olyan $c \neq e$ elem van, amelyre $c^2 = e$, akkor $S = e$, minden más esetben pedig $S = e$. 
3. fejezet - MAGASABB FOKÚ KONGRUENCIÁK

A fejezet elején néhány általános észrevételt teszünk a prim modulusú ismeretlenes kongruenciákra vonatkozóan. Ezután a rend, a primitív gyök és a diszkrit logaritmus legfontosabb tulajdonságait tárgyaljuk, majd ezek felhasználásával a modulo $\mathcal{P}$ „gyökvonás” kérdését, azaz a prim modulusú binom kongruenciákat tekintjük át. Szerepeltejük König és Rados, valamint Chevalley egy-egy nevezetes tételeit is. Végül megmutatjuk, hogyan lehet az összetett modulusú kongruenciákat prímhatvány, illetve prim modulusú kongruenciákrá visszavezetni.

3.1 Megoldásszám és redukció

Legyen $m$ rögzített pozitív egész, $\bar{f}$ tetszőleges egész együttthatós polinom, és tekintsük az $f(x) \equiv 0 \pmod{m}$ ismeretlenes kongruenciát.

A lineáris kongruenciákhoz hasonlóan megoldáson egy olyan $s$ egész számot értünk, amelyet az $x$ helyére beírva a kongruencia fennáll. Itt is világos, hogy ha egy $s$ szám megoldás, akkor az $(\bar{s})_m$ maradékosztály minden eleme megoldás, hiszen $s = r \pmod{m}$ esetén $\bar{f}(s) = \bar{f}(r) \pmod{m}$.

Ennek alapján megoldásszámának a páronként inkongruens megoldások számát értjük, vagyis azt, hogy hány maradékosztálya tartoznak a megoldások (lásd a D 2.5.2 Definíciót). Az is nyilvánvaló, hogy $\bar{f}$ együttthatóra vonatkozóan is csak az számít, hogy melyik maradékosztályokba tartoznak modulo $m$.

Mindezek alapján gyakran kényelmesebb és természetesebb, ha mind az együttthatókat, mind pedig a megoldásokat (egész számok helyett) modulo $m$ maradékosztályokként kezeljük. Ez más szóval azt jelenti, hogy $\bar{f}$-et a modulo $m$ maradékosztályok $\mathbb{Z}_m$ gyűrűje feletti polinomnak tekintjük, és az $f(x) \equiv 0 \pmod{m}$ kongruencia megoldásai az $\bar{f}$-hez tartozó polinomfüggvények a $\mathbb{Z}_m$-beli gyökei. Ennek megfelelően definiáljuk az $\bar{f}$ polinom modulo $m$ vett fokszámát is:

3.1.1 Definíció . D 3.1.1

Az $\bar{f} = a_0 + a_1 x + \cdots + a_n x^n$ polinom modulo $m$ vett fokszáma (vagy foka) $k$, ha $a_k \neq 0 \pmod{m}$, de minden $i > k$ esetén $a_i \equiv 0 \pmod{m}$. Ha minden $i$-re $a_i \equiv 0 \pmod{m}$, akkor $\bar{f}$-nek modulo $m$ nincs foka. ◻

Példa: az $\bar{f} = 6 + 12x + 15x^2 + 21x^3$ polinomnak modulo 5 a foka 3, modulo 7 a foka 2 és modulo 3 nincs foka.

A pont további részében prim modulusú kongruenciákkal foglalkozunk.

3.1.2 Tétel . T 3.1.2

Ha $\mathcal{P}$ prim és az $\bar{f}$ polinom modulo $\mathcal{P}$ vett foka $k$, akkor az $f(x) \equiv 0 \pmod{p}$ kongruencia megoldásszáma legfeljebb $k$. ◻

Bizonyítás: Az előzetes megfigyelések szerint tekintsük $\bar{f}$-et a modulo $\mathcal{P}$ maradékosztályok $\mathbb{Z}_\mathcal{P}$ gyűrűje feletti polinomként, ekkor a kongruencia megoldásszáma az $\bar{f}$-hez tartozó polinomfüggvény $\mathbb{Z}_\mathcal{P}$-beli gyökeinek a száma.

Mivel $\mathbb{Z}_\mathcal{P}$ a T 2.8.4 Tétel szerint kommutatív test, ezért a T 3.1.2 Tétel állítása azonnal következik az alábbi jól ismert klasszikus algebrai tételből: Ha egy $\mathcal{T}$ kommutatív test feletti polinom foka $k$, akkor a megfelelő polinomfüggvények legfeljebb $k$ gyöke lehet $\mathcal{T}$-ben. ◻
A T 3.1.2 Tétel állítása összetett modulusra nem igaz, pl. a
\[ 10x - 15 = 0 \pmod{25} \]
elsőfokú kongruencia megoldásszáma 5, az
\[ x(x - 1)(x - 2)(x - 3) = 0 \pmod{24} \]
negyedfokú kongruencia megoldásszáma 24 stb.

A T 3.1.2 Tétel segítségével újabb bizonyítást nyerhetünk a Wilson-tételre (T 2.7.1 Tétel): Ha \( P \) prim, akkor \( (p - 1)! \equiv -1 \pmod{p} \).

Az állítás \( p = 2 \)-re nyilvánvaló. Legyen \( P > 2 \), és tekintsük az
\[ f = x^{p-1} - 1 - (x - 1)(x - 2) \cdots (x - (p - 1)) = a_0 + a_1x + \cdots + a_{p-2}x^{p-2} \]
polinomot. Az \( f(x) \equiv 0 \pmod{p} \) kongruenciának a kis Fermat-tétel szerint az \( x = 1, 2, \ldots, p - 1 \) (páronként inkongruens) számok valamennyien megoldásai, tehát a megoldásszám legalább \( p - 1 \)
. Ha \( f \)-nek modulo \( P \) létezne foka, akkor ez a fok legfeljebb \( p - 2 \) lehetne, ami ellentmond a T 3.1.2 Tételnél. Ebből következik, hogy \( f \)-nek modulo \( P \) nincs foka, vagyis valamennyi együtthatója 0 modulo \( P \). Speciálisan
\[ a_0 = -1 - (-1)^{p-1}(p-1)! \equiv -1 - (p-1)! = 0 \pmod{p}, \]
ami éppen a Wilson-tétel állítása.

Mivel egy modulo \( m \) kongruencia megoldásszáma legfeljebb \( m \), ezért a T 3.1.2 Tétel állítása semmitmondó, ha \( f \) modulo \( P \) vett foka \( P \) vagy annál nagyobb. Azonban az \( f(x) \equiv 0 \pmod{p} \) kongruencia vizsgálata ebben az esetben is „redukálható” egy legfeljebb \( p - 1 \)-edfokú kongruenciára az alábbi értelmében:

3.1.3 Tétel . T 3.1.3

Bármely \( P \) prim és \( f \) egész együththatós polinom esetén létezik olyan \( g \) egész együththatós polinom, hogy

(i) a \( g \) modulo \( P \) vett foka legfeljebb \( p - 1 \) vagy \( g \) minden együtthatója 0 modulo \( P \); és

(ii) minden \( e \) egész számmá \( f(e) \equiv g(e) \pmod{p} \). $

Más megfogalmazásban a T 3.1.3 Tétel azt jelenti, hogy a \( \mathbb{F}_p \) test felett bármely \( f \) polinomhoz található olyan legfeljebb \( p - 1 \)-edfokú \( g \) polinom (megengedve a nullpolinomot is), hogy a két polinomhoz ugyanaz a polinomfüggvény tartozik.

A tételből nyilvánvalóan következik, hogy az \( f(x) \equiv 0 \pmod{p} \) és \( g(x) \equiv 0 \pmod{p} \) kongruenciáknak ugyanazok a megoldásai, és így a T 3.1.2 Tétel szerint a megoldásszám legfeljebb annyi, mint a \( g \) modulo \( P \) vett foka.

Első bizonyítás: Írjunk \( f \)-ben mindenütt \( x^p \) helyére mindaddig \( x \) -et, amíg ez csak lehetséges. Így végül egy olyan \( g \) polinomhoz jutunk, amelynek (modulo \( P \) vett) foka legfeljebb \( p - 1 \) vagy minden
együttthatója 0 modulo \( p \). Mivel a kis Fermat-tétel szerint bármely \( c \) -re \( c^p \equiv c \pmod{p} \), ezért \( f(c) \equiv g(c) \pmod{p} \) is teljesül. □

Második bizonyítás: Oszzuk el \( f \) -et maradékosan \( x^p - x \)-szel; mivel \( x^p - x \) főegyüttthatója 1, ezért a hányados és a maradék is egész együttthatós lesz. Megmutatjuk, hogy a keletkezett maradék megfelel \( \mathcal{G} \)-nek. Valóban, legyen

\[
f = (x^p - x)h + g,
\]

ahol \( \mathcal{G} \) foka legfeljebb \( p - 1 \) vagy \( \mathcal{G} \) a nullpolinom. Ekkor bármely \( c \) egész számra

\[
f(c) = (c^p - c)h(c) + g(c) \equiv 0 + g(c) \pmod{p} \] □

Megjegyzések:
1. A második bizonyításban a maradékos osztást végezhetjük a \( \mathbb{Z}_p \) test feletti polinomok körében is, csak ez kicsit nehézesebb.
2. Mindkét bizonyítás együttal konkrét algoritmust is ad a megfelelő \( \mathcal{G} \) előállítására (sót, tulajdonképpen ugyanannak az eljárásnak a kétféle megközelítéséről van szó).
3. Egy harmadik bizonyítást kaphatunk az ún. interpolációs polinomok segítségével, ez azonban \( \mathcal{G} \) gyakorlati előállítására nemigen alkalmas (lásd a 3.1.8 feladatot [73]).
4. A T 3.1.3 Tételt kiegészíthetjük azzal, hogy (megfelelő értelemben tekintve) csak egy ilyen tulajdonságú \( \mathcal{G} \) polinom létezik (lásd a 3.1.9 feladatot [73]).

Feladatok

3.1.1 Határozzuk meg az alábbi kongruenciák megoldásszámát:

(a) \( x^{109} + x = 0 \pmod{101} \);

(b) \( x^{109} + x = 0 \pmod{100} \);

(c) \( 21x^9 + 18x^6 + 15 \equiv 0 \pmod{77} \);

(d) \( x(x^2 - 1)(x^2 - 4) \equiv 0 \pmod{60} \).

3.1.2 Bizonyítsuk be, hogy \( c \) akkor és csak akkor megoldása az \( f(x) \equiv 0 \pmod{m} \) kongruenciának, ha van olyan \( h \) egész együttthatós polinom, amelyre az \( f - (x - c)h \) polinom minden együttthatója osztható \( m \)-mel.

3.1.3 Jelöljük az \( f(x) \equiv 0 \pmod{m} \) kongruencia megoldásszámát \( N(f, m) \) -mel. Melyek igazak az alábbi állítások közül?

(a) \( N(fg, m) \leq N(f, m) + N(g, m) \).

(b) \( N(fg, m) \leq N(f, m) + N(g, m) + 1000 \).

(c) \( N(fg, 13) \leq N(f, 13) + N(g, 13) \).

(d) \( N(fg, 13) = N(f, 13) + N(g, 13) \).
3.1.4 (a) Adjunk meg olyan \( f \) polinomot, amelynek a modulo 37 vett foka 13 és az \( f(x) \equiv 0 \ (\text{mod} \ 37) \) kongruencia megoldásszáma 12.

(b) Hány olyan \( f \) van, amely teljesíti az (a)-beli feltételeket és minden együthatója az \( 1, 2, \ldots, 37 \) számok közül kerül ki?

3.1.5 Legyen \( p \) prim, és jelöljük az \( f(x) = 0 \ (\text{mod} \ p) \) kongruencia megoldásszámát \( r \) -rel. Lássuk be, hogy

\[
\tau = -\sum_{i=1}^{p} f(i)^{p-1} \ (\text{mod} \ p).
\]

3.1.6 Legyen \( p > 2 \) prim és \( 1 \leq j \leq p - 2 \). Bizonyítsuk be, hogy az \( 1, 2, \ldots, p - 1 \) számokból képezett összes \( j \) tényezős szorzat összege osztható \( p \)-vel.

3.1.7 Legyen \( p > 2 \) prim és

\[
f = a_0 + a_1 \omega + \cdots + a_{p-1} \omega^{p-1}, \quad \text{al. ol.} \quad a_0 \not\equiv 0 \ (\text{mod} \ p).
\]

Bizonyítsuk be, hogy az \( f(x) \equiv 0 \ (\text{mod} \ p) \) kongruencia redukálható egy legfeljebb \( p - 2 \) -edfokú kongruencia vizsgálatára az alábbi értékeken: megadható olyan \( h \) polinom, amelynek a modulo \( p \) vett foka legfeljebb \( p - 2 \) vagy minden együthatója \( \equiv 0 \ (\text{mod} \ p) \), és minden \( (v, p) = 1 \) esetén \( f(v) = h(v) \ (\text{mod} \ p) \) teljesül.

3.1.8 Bizonyítsuk be a T 3.1.3 Tételben szereplő \( \theta \) létezését a Lagrange- vagy Newton-féle interpolációs polinomok felhasználásával.

3.1.9 Bizonyítsuk be, hogy a T 3.1.3 Tétel követelményeit kielégítő \( \theta \) mint \( \mathbb{Z}_p \) feletti polinom egyértelmű, azaz az együthatói modulo \( P \) egyértelműen meg vannak határozva.

3.1.10 Lássuk be, hogy a T 3.1.3 Tétel összetett modulus esetén is érvényben marad.

### 3.2 Rend

Az Euler–Fermat-tételből következik, hogy ha \( \{a, m\} = 1 \), akkor van olyan \( t \) pozitív egész, amelyre \( a^t \equiv 1 \ (\text{mod} \ m) \); ilyen kivétő például a \( \varphi(m) \) vagy annak bármely többszöröse. A további vizsgálatokban kitüntetett szerepet játszik a legkisebb ilyen tulajdonságú \( t \) pozitív egész, amelyet az \( a \) rendjének nevezzük modulo \( m \):

#### 3.2.1 Definíció

Legyen \( \{a, m\} = 1 \). A \( k \) pozitív egész az \( a \) rendjének nevezzük modulo \( m \), ha \( a^k \equiv 1 \ (\text{mod} \ m) \), de bármely \( 0 < i < k \) esetén \( a^i \not\equiv 1 \ (\text{mod} \ m) \).

Az \( a \) rendjét \( a_m(a) \)-val jelöljük. Például \( a_7(2) = 3 \), \( a_7(3) = 4 \) stb. Ha nem okoz feltevést, akkor a modulusra utaló indexet el is hagyhatjuk. Az „\( a \) rendje” helyett — a rend szó latin megfelelőjével — az „ordo \( a \)” kifejezést is szokás használni.

Az Euler–Fermat-tételből következik, hogy minden \( \{a, m\} = 1 \) esetén létezik az \( a \) -nak rendje és \( a_m(a) \leq \varphi(m) \).
A rend fogalma csak \( (a, m) = 1 \) esetén értelmezhető: ha \( (a, m) \neq 1 \), akkor egyáltalán nem létezik olyan \( k > 0 \) kitevő, amelyre \( a^k \equiv 1 \pmod{m} \) teljesülne (lásd a T 2.4.1B Tétel utáni 1. megjegyzést).

A rend definíciójából világos, hogy

\[
a \equiv b \pmod{m} \implies a_{\alpha}(a) - a_{\alpha}(b),
\]

teht egy redukált maradékosztály valamennyi elemének ugyanaz a rendje.

Az alábbi tételben összefoglaljuk a rend legfontosabb tulajdonságait.

3.2.2 Tétel. \( \text{T 3.2.2} \)

Legyenek \( i, u, v \) nemnegatív egészek és \( (a, m) = 1 \).

(i) \( a^i \equiv 1 \pmod{m} \iff a_{\alpha}(a) \mid i \).

(ii) \( a^u \equiv a^v \pmod{m} \iff u \equiv v \pmod{\varphi(a)} \).

(iii) Az \( a \)-nak \( a_{\alpha}(a) \) darab páronként inkongruens pozitív egész kitevős hatványa létezik modulo \( m \).

(iv) \( a_{\alpha}(a) \mid \varphi(m) \).

Bizonyítás: (i) Ha \( t = q_{\alpha}(a) \), akkor

\[
a^t = (a_{\alpha}(a))^t \equiv 1^t \equiv 1 \pmod{m}.
\]

A megfordításhoz osszuk el a \( t \) számot maradékosan modulo \( m \).

(ii) Legyen \( u \geq v \). Ekkor \( (a, m) = 1 \) és (i) felhasználásával

\[
a^u \equiv a^v \pmod{m} \iff a^{u-v} \equiv 1 \pmod{m} \iff a_{\alpha}(a) \mid u-v \iff u = v \pmod{\varphi(a)}.
\]

(iii) Ez azonnal következik (ii)-ből.

(iv) Az Euler–Fermat-tétel szerint \( a^\varphi(m) \equiv 1 \pmod{m} \), és így (i) alapján \( a_{\alpha}(a) \mid \varphi(m) \).

Példa: Számitsuk ki a 13 rendjét modulo 59.

A 13 és 59 relatív prímek, tehát \( a_{13}(13) \) létezik. Mivel \( a_{13}(13) \mid \varphi(59) \) és \( \varphi(59) = 58 \), ezért

\[
a_{13}(13) = 1, 2, 29, vagy 58.
\]

Nyilván \( 13 \neq 1 \pmod{59} \), \( 13^2 \neq 1 \pmod{59} \), és így \( a_{13}(13) \) értéke csak 29 vagy 58 lehet. Ennek megfelelően, ha \( 13^2 \equiv 1 \pmod{59} \), akkor a rend 29, ha pedig \( 13^2 \neq 1 \pmod{59} \), akkor a rend 58.
A $13^{21}$ maradékát modulo 59 ismételt négyzetre emelések segítségével határozhatjuk meg:

\[
13^2 = 189 \equiv -8 \mod{59} \\
13^4 = (-8)^2 = 5 \mod{59} \\
13^8 = 5^2 = 25 \mod{59} \\
13^{16} = 25^2 = -24 \mod{59}
\]

és így

\[
13^{29} = 13^{16} \cdot 13^8 \cdot 13^4 \cdot 13 \equiv (-24) \cdot 25 \cdot 5 \cdot 13 = -(-60) \cdot 25 \equiv (-10) \cdot 6 \equiv -1 \mod{59}.
\]

Tehát $\varphi(13) = 58$. (Megjegyezzük, hogy $13^{58}$ maradékát modulo 59 semmiképpen sem kellett külön kiszámítani, de az Euler–Fermat-tételből eleve is tudtuk, hogy ez a maradék 1.)

Végül megemlítjük, hogy a D 3.2.1 Definíció a csoportbeli elemrend fogalmának a speciális esete, és a T 3.2.2 Tétel megfelelője is igaz tetszőleges csoportban.

**Feladatok**

(Ha az index nélküli $o(a)$ jelölést használjuk, akkor ez vagy a feladatban szereplő $\mathfrak{m}$, illetve $P$ modulusra, vagy pedig ilyenek hiányában tetszőleges modulusra vonatkozik.)

3.2.1 Számítsuk ki a következő rendeket:

(a) $o_{17}(155)$  
(b) $o_{100}(199)$  
(c) $o_{35}(2)$  
(d) $o_{17}(43)$

3.2.2 Van-e olyan $a$, amelyre $o_m(a) = 4$, ha $\mathfrak{m}$ értéke (a) 11; (b) 12; (c) 17?

3.2.3 Melyek azok az $\mathfrak{m}$ modulusok, amelyekre $o_m(2) = 6$?

3.2.4 Legyen $(a, \mathfrak{m}) = 1$, $o_{\mathfrak{m}}(a) = k$ és $i \geq 0$. Mutassuk meg, hogy

(a) $o_{\mathfrak{m}}(a^i) \mid k$  
(b) $o_{\mathfrak{m}}(a^i) = k \iff (i, k) = 1$  
(c) $o_{\mathfrak{m}}(a^i) = k/(i, k)$

3.2.5 Mik $o(a)$ lehetséges értékei, ha $o(a^3)$ értéke (a) 10; (b) 12?

3.2.6 (M [564]) Legyen $p > 2$ prím. Igazoljuk: $o_p(a) = o_p(-a) \iff a \mid o_p(a)$.

3.2.7 Tegyük fel, hogy $a^5, a^{13}$ és $a^{24}$ pontosan két redukált maradékosztályba tartoznak modulo $\mathfrak{m}$. Számítsuk ki $o_{\mathfrak{m}}(a)$ értékét.
3.2.8 Tegyük fel, hogy $p$ prím és $\alpha_p(\varepsilon) = 3$.

(a) Lássuk be, hogy $1 + a + a^2 = 0 \pmod{p}$.

(b) Számfaktorok ki $\alpha_p(1 + \varepsilon)$ értékét.

3.2.9 (M [565]) Tegyük fel, hogy $p > 5$ prím és $a^{2p-10} \equiv -1 \pmod{p}$, Számfaktorok ki $\alpha_p(\varepsilon)$ értékét.

3.2.10 (a) Lássuk be, hogy az $a^k - 1 \pmod{m}$ és $a^k \equiv 1 \pmod{m}$ kongruenciák egyidejűleg pontosan akkor teljesülnek, ha $a^{\text{ord}_m(k)} \equiv 1 \pmod{m}$.

(b) Az (a) rész felhasználásával adjunk új bizonyítást az 1.3.13 feladatra [15].

3.2.11 Igazoljuk, hogy ha $n$ páratlan, akkor $(a^n - 1, a^k + 1) \leq 2$.

3.2.12 Legyen $p > 2$ prím, $(a, p) = 1$. Mutassuk meg, hogy akkor és csak akkor létezik olyan $s$, amelyre $a^s = -1 \pmod{p}$, ha $a^s$ páros. Mennyiben változik a helyzet, ha $p$ helyett egy $mn$ összetett modulust veszünk?

3.2.13 Bizonyítsuk be, hogy

(a) $(a, m) = 1, d \mid m \implies a_d(e) = a_{m_d(e)}$;

(b) $(a, mn) = 1 \implies a_{m_d(e)}(m) = [a_{mn}(e), a_{m_d(e)}(m)]$.

3.2.14 Az $1, 2, \ldots, 999$ számok között hány másodrendű elem van mod 1000?

3.2.15 (*) Legyen $o(\varepsilon) = \alpha$, $o(\hat{\varepsilon}) = \beta$. Igazoljuk, hogy

(a) $o(\varepsilon \beta) = uv \iff (u, v) = 1$ ;

(b) $[u, v]_{\varepsilon \beta} \mid o(\varepsilon \beta) | [u, v]$ .

3.2.16 (*) Tegyük fel, hogy $a^{\varepsilon(\hat{\varepsilon})} \equiv j^{\varepsilon(\hat{\varepsilon})} \pmod{m}$. Lássuk be, hogy $o(\varepsilon) = o(\hat{\varepsilon})$.

3.2.17 Bizonyítsuk be, hogy $\gamma | \chi(a^n - 1)$ bármely $n > 1$ és $n > 0$ esetén teljesül.

3.2.18 (*) Legyen $(a_1, \ldots, a^p(m))$ redukált maradékrrendszer modulo $m$. Mutassuk meg, hogy $\sum_{i=1}^{p} o_{\varepsilon(\hat{\varepsilon})} \varepsilon(\hat{\varepsilon})$ mindig páratlan szám.

3.2.19 Legyen $p$ prím és $(a, p) = 1$. Milyen maradékot ad $p$-vel osztva az alábbi összeg és szorzat:

(a) $a + a^2 + \cdots + a^{o(a)}$ ;

(b) $a \cdot a^2 \cdots a^{o(a)}$ ?

3.2.20 Tizedes törtek. Csak a tizedesvessző után következő jegysorozattal foglalkozunk, ezért elegendő $0 < \alpha < 1$ számokat tekintenünk. A feladatban kizárruk azokat a végtelen tizedes törteket, amelyekben egy határtól kezdve minden számjegy 9-es. Egy tizedes tört véges, ha csak véges sok
jegyből áll; ezt a legrövidebb alakban írjuk fel, azaz az utolsóként szereplő tizedesjegy nem nulla. Egy végként tizedes tört szakaszos, ha a tizedesjegyek sorozata egy határtól kezdve periodikus, ezen belül tiszta szakaszos, illetve vegyes szakaszos, attól függően, hogy a periodicitás (azaz az első szakasz) közvetlenül a tizedesvessző után, illetve csak később kezdődik. A racionalis számok \( \frac{a}{b} \) közönséges tört alakjában feltesszük, hogy \( b > 0 \) és \( (a, b) = 1 \).

(a) Mutassuk meg, hogy egy \( \alpha \) valós szám tizedestört-alakja akkor és csak akkor véges vagy végként szakaszos, ha \( \alpha \) racionalis.

(b) Az \( \frac{a}{b} \) racionalis szám tizedestört-alakja akkor és csak akkor véges, ha \( b \) kanonikus alakjában legfeljebb a 2 és az 5 primszámok szerepelnek: \( b = 2^r 5^s \). Ekkor a tizedesvessző után szereplő jegyek száma \( k = \max(r, s) \), azaz \( b \mid 10^k \), de \( b \nmid 10^{k-1} \).

(c) Az \( \frac{a}{b} \) racionalis szám tizedestört-alakja akkor és csak akkor tiszta szakaszos, ha \( (b, 10) = 1 \). Ekkor a (legkisebb) szakasz hossza \( o_5(10) \).

(d) Az \( \frac{a}{b} \) racionalis szám tizedestört-alakja akkor és csak akkor vegyes szakaszos, ha \( (b, 10) > 1 \), de a \( b \)-nek létezik a 2-től és 5-től különböző primosztója is: \( u = 2^r 5^s t \), ahol \( (t, 10) = 1 \), \( t > 1 \) és \( k = \max(r, s) > 0 \). Ekkor a(z első) szakasz a tizedesvessző utáni \( k + 1 \)-edik jegyben kezdődik és hossza \( o_5(10) \).

3.3 Primitív gyök

Mint láttuk, az Euler–Fermat-tételből következik, hogy bármely \( (a, m) = 1 \) esetén \( \varphi(m) \leq \varphi(m) \). Különösen fontos az az eset, amikor itt egyenlőség teljesül:

3.3.1 Definíció . D 3.3.1

Egy \( g \) számot primitív gyöknek nevezünk modulo \( m \), ha \( o_m(g) = \varphi(m) \).

A definícióból világos, hogy egy primitív gyök szükségszükséggel relatív prim az \( m \) modulushoz, továbbá egy redukált maradékosztálynak vagy minden eleme primitív gyök, vagy pedig egyetlen eleme sem az.

Példák:

P1 A 3 primitív gyök modulo 10, mert \( o_{10}(3) = \varphi(10) = 4 \).

P2 A 2 nem primitív gyök modulo 31, mert \( o_{31}(2) = 5 < \varphi(31) = 30 \).

P3 Modulo 12 egyáltalán nem létezik primitív gyök: elég például a \( \{ \pm 1, \pm 5 \} \) redukált maradékrészlet elemének a rendjét megvizsgálni, és itt az 1 rendje 1, a többi elemé 2, vagyis mindegyik rend kisebb, mint \( \varphi(12) = 4 \).

Amikor egy \( a \) számról (ahol \( (a, m) = 1 \)) el akarjuk dönteni, hogy primitív gyök-e modulo \( m \), akkor \( a^{\varphi(m)} \equiv 1 \pmod{m} \) fennállását fölösleges ellenőrizni, hiszen ez az Euler–Fermat-tétel miatt biztosan igaz. Az \( a^{\varphi(m)} \equiv 1 \pmod{m} \) összefüggés alapján azt kell megvizsgálni, hogy a \( \varphi(m) \) valamely \( d < \varphi(m) \) osztójára teljesül-e \( a^d \equiv 1 \pmod{m} \); ha van ilyen \( d \), akkor \( a \) nem primitív gyök, ha nincs ilyen \( d \), akkor pedig \( a \) primitív gyök. Könnyen látszik, hogy a \( \varphi(m) \) osztói közül is elég a „maximálisakkat” tekinteni, vagyis azokat, amelyek \( \varphi(m)/q \) alakúak, ahol \( q \) primszám.
A primitív gyökök alkalmazhatósága elsősorban az alábbi egyszerű tételben megfogalmazott tulajdonságon alapul:

3.3.2 Tétel. T 3.3.2

Egy \( q \) szám akkor és csak akkor primitív gyök az \( \mathcal{m} \) modulusra nézve, ha \( 1, q, q^2, \ldots, q^{\varphi(\mathcal{m})-1} \) reduált maradékrrendszer alkotnák modulo \( \mathcal{m} \).

Bizonyítás: Tegyük fel, hogy \( q \) primitív gyök, azaz \( \omega, (q) = \varphi(\mathcal{m}) \). Ekkor a T 3.2.2 Tétel (ii) állítása alapján \( 1, \mathcal{m}, \mathcal{m}^2, \ldots, \mathcal{m}^{\varphi(\mathcal{m})-1} \) párkonként inkongruensek modulo \( \mathcal{m} \), továbbá számuk \( \varphi(\mathcal{m}) \) és \( (q, \mathcal{m}) = 1 \) miatt valamennyien relatív primnek \( \mathcal{m} \)-hez. A T 2.2.9 Tétel szerint így valóban reduált maradékrendszert alkotnak mod \( \mathcal{m} \).

A megfordításhoz tegyük fel, hogy a fenti \( q \)-hatványok reduált maradékrrendszer alkotnák mod \( \mathcal{m} \). Ekkor \( (q, \mathcal{m}) = 1 \), tehát \( \omega, (q) \leq \varphi(\mathcal{m}) \). Továbbá \( q, q^2, \ldots, q^{\varphi(\mathcal{m})-1} \) egyike sem lehet kongruens a szintén a megadott reduált maradékrendszerben szereplő 1-gyel, tehát \( \omega, (q) = \varphi(\mathcal{m}) \). ●

A következőkben azt vizsgáljuk meg, milyen \( \mathcal{m} \) modulus esetén létezik primitív gyök. Megjegyezzük, hogy ezt csoportelméleti terminológiával úgy is fogalmazhatjuk, hogy mely \( \mathcal{m} \)-esetén lesz a modulo \( \mathcal{m} \) reduált maradékosztályok multiplikatív csoportja ciklikus.

Először azt igazoljuk, hogy prim modulus esetén mindig létezik primitív gyök:

3.3.3 Tétel. T 3.3.3

Ha \( P \) prim, akkor modulo \( P \) létezik primitív gyök. ●

A T 3.3.3 Tétel általánosításaként megmutatható, hogy nemcsak a modulo \( P \) maradékosztályok körében, hanem bármely véges elemszámú testben található olyan elem, amelynek a hatványai előállítják a test összes nemnulla elemtét.

A T 3.3.3 Tételre két bizonyítást adunk. Emellett egy harmadik gondolatmenetet is vázolunk a 3.3.14 feladatban [84]. Mindhárom bizonyítás — értelmszerű módosításokkal — alkalmas az imént említett általánosabb tétel igazolására is.

Első bizonyítás: Ha \( P = 2 \), akkor \( q = 1 \) (vagy bármely páratlan szám) primitív gyök.

Legyen \( P > 2 \) és \( P - 1 \) összes különböző primosztója legyen \( q_1, \ldots, q_s \).

Tegyük fel indirekt, hogy nem létezik primitív gyök, azaz bármely \( 1 \leq i \leq P - 1 \) esetén \( \omega, (i) = \frac{d_i}{p} \). Mivel \( d_i \mid P - 1 \), ezért van a \( P - 1 \)-nek olyan \( q \) primosztója, amelyre \( d_i \mid (P - 1)/q \). Ekkor \( q^{(P - 1)/q} = 1 \mod P \). Ez azt jelenti, hogy a reduált maradékrendszer bármely eleme gyöke az

\[
\hat{f} = (x^{(P - 1)/q} - 1) \ldots (x^{(P - 1)/q} - 1)
\]

polinommal képzett \( \hat{f}(x) = 0 \mod P \) kongruenciának. Továbbá \( \hat{f}(0) = (-1)^s \not\equiv 0 \mod P \), tehát a kongruencia megoldásszáma pontosan \( P - 1 \).

Végezzük el (1)-ben a szorzásokat. Ekkor \( \hat{f} \) olyan \( \pm x^k \) tagok összegeként áll elő, ahol

\[ a k \text{ kitevő } k\text{-különböző } (P - 1)/q_j\]-kre az (esetleg csak egytagú) összege, 

78
illetve $k = 0$. Alkalmazzuk most a T 3.1.3 Tétele első bizonyításában szereplő redukciós eljárast: írjunk $x^p$ helyére $x^p$-et, amíg ez csak lehetséges. A keletkezett $g$ polinom legfeljebb $p - 1$ -edfokú és minden $c$-re $f(c) \equiv g(c) \pmod{p}$.

Ez azt jelenti, hogy a $g(x) \equiv 0 \pmod{p}$ kongruencia megoldásszáma is pontosan $p - 1$, és így a T 3.1.2 Tétel szerint a $g$ polinom modulo $p$ vett foka pontosan $p - 1$ kell hogy legyen.

Ekkor $g$-ben szükségképpen szerepel $x^p - 1$-es tag. A redukciós eljárás során ez a tag csak olyan, az $f$-ben előforduló $x^p$ tag(ok)ból keletkezhetett, amely(ek)ben

$$a_k \text{ kitevő } k = (p - 1)t \text{ alakú, } a_{\text{kol} \ t > 0 \text{ egész}},$$

hiszen a $(p - 1)$-nél nagyobb) kitevőket mindig $p - 1$-gyel csökkentettük.

A (2) és (3) összevetéséből kapjuk, hogy (mondjuk)

$$t = \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_r}.$$  

A (4) egyenlőséget $d_2 \cdots d_r$-rel beszorozva minden tag egész szám lesz, kivéve a jobb oldal első tagját, és így ellentmondásra jutottunk.

Második bizonyítás: Jelölje $\tilde{h}(d)$ az $1, 2, \ldots, p - 1$ elemek közül azoknak az $i$-knek a számát, amelyekre $a_i(i) = d_i$. Ekkor nyilván $\tilde{h}(d) = 0$, ha $d \not\equiv p - 1$, továbbá

$$\sum_{d \not\equiv p - 1} \tilde{h}(d) = p - 1.$$  

Megmutatjuk, hogy bármely $d$-re

$$\tilde{h}(d) \leq \varphi(d).$$  

Ha nincs $d$-edrendű elem, akkor (6) fennáll, hiszen $0 = \tilde{h}(d) < \varphi(d)$.

Feltételejük tehát, hogy valamely $a$-ra $\alpha_p(a) = d$. Ekkor az $a, a^2, \ldots, a^d$ elemek páronként inkongruensek modulo $p$, és $(a^i)^d = (a^d)^i \equiv 1 \pmod{p}$ miatt valamennyien gyökei az $x^d \equiv 1 \pmod{p}$ kongruenciának.

Mivel ennek a kongruenciának a megoldásszáma nem lehet $d$-nél nagyobb, ezért ha valamely $c$-re $c^d \equiv 1 \pmod{p}$ teljesül, akkor a $c$ az $a, a^2, \ldots, a^d$ számok valamelyikével kongruens.

Minden $d$-edrendű szám is gyöke az $x^d \equiv 1 \pmod{p}$ kongruenciának, tehát minden $d$-edrendű szám is $a, a^2, \ldots, a^d$ valamelyikével kongruens. A 3.2.4b feladat [75] szerint $\alpha_p(a^i) = \alpha_p(c) = d$ akkor és csak akkor teljesül, ha $(i, d) = 1$, ennél fogva az $a, a^2, \ldots, a^d$ számok között éppen $\varphi(d)$-nek a rendje lesz $d$, azaz $\tilde{h}(d) = \varphi(d)$. Ezzel (6)-ot beláttuk.

Felhasználva (5)-öt és (6)-ot, továbbá a 2.3.14 feladatban [45] bizonyított $\sum_{d \not\equiv p - 1} \varphi(d) = p - 1$ egyenlőséget azt kapjuk, hogy

$$p - 1 = \sum_{d \not\equiv p - 1} \tilde{h}(d) \leq \sum_{d \not\equiv p - 1} \varphi(d) = p - 1,$$
ami nyilván csak úgy teljesülhet, ha minden $d \mid p - 1$-re $\varphi(d) = \varphi(p)$.

Ezzel beláttuk, hogy egy mod $\mathcal{P}$ redukált maradéktrendszerben a $d$-edrendű elemek száma $\varphi(d)$.

Ezt speciálisan $d = p - 1$-re alkalmazva adódik, hogy a primitív gyökök száma $\varphi(p - 1)$ (tehát létezik primitív gyök).

Megjegyzés: A második bizonyításban (látszólag) erősebb állítást bizonyítottunk be: a primitív gyök létezésén túlmenően megkaptuk a (páronként inkongruens) primitív gyökök, sőt még általánosabban bármely adott $d$-re a $d$-edrendű elemek számát. Ez a „többleteredmény” azonban könnyen következik a primitív gyök (bármilyen módon igazolt) létezéséből a T 3.3.2 Tétel és a 3.2.4 [75]b, illetve 3.2.4c feladat [75] felhasználásával (lásd a 3.3.9 feladatot [83]).

Az így adódó eredményeket fontosságuk miatt külön tételként is megfogalmazzuk:

3.3.4 Tétel. T 3.3.4

Legyen a modulus egy $\mathcal{P}$ prímszám.

(i) Egy primitív gyök $i$-edik hatványa akkor és csak akkor primitív gyök, ha $(i, p - 1) = 1$.

(ii) A páronként inkongruens primitív gyökök száma $\varphi(p - 1)$.

(iii) Általánosan is igaz, hogy ha $d \mid p - 1$, akkor egy mod $\mathcal{P}$ redukált maradéktrendszer elemei között a $d$-edrendű elemek száma $\varphi(d)$.

A következő tételben pontosan meghatározunk, mely $\mathcal{M}$ modulusokra létezik primitív gyök:

3.3.5 Tétel. T 3.3.5

Az $\mathcal{M} > 1$ modulusra nézve akkor és csak akkor létezik primitív gyök, ha $\mathcal{M} = \mathcal{P}^\alpha, 2^{\alpha}, 2$ vagy 4, ahol $\mathcal{P} > 2$ prim és $\alpha > 0$.

Bizonyítás: Az $\mathcal{M} = \mathcal{P}$ és $\mathcal{M} = 2$ esetet a T 3.3.3 Tétel tartalmazza, ha pedig $\mathcal{M} = 4$, akkor $\mathcal{G} = 3$ primitív gyök. A többi esetre a bizonyítást az alábbi lépésekben végezzük.

(L1) Modulo $\mathcal{P}^2$ létezik primitív gyök.

(L2) Ha $\alpha > 2$, akkor modulo $\mathcal{P}^\alpha$ létezik primitív gyök.

(L3) Modulo $2^{\alpha}$ létezik primitív gyök ($\alpha > 0$).

(N1) Ha $\mathcal{M}$ osztható 4-gyel és van páratlan prímosztója, vagyha $\mathcal{M}$-nek van (legalább) két különböző páratlan prímosztója, akkor nem létezik primitív gyök modulo $\mathcal{M}$.

(N2) Ha $\mathcal{M} = 2^{\alpha}$, ahol $\alpha > 2$, akkor nem létezik primitív gyök modulo $\mathcal{M}$.

(L1) Legyen $\mathcal{G}$ primitív gyök modulo $\mathcal{P}$. Megmutatjuk, hogy $\mathcal{G}$ és $\mathcal{G} \mid \mathcal{P}$ közül legalább az egyik primitív gyök lesz modulo $\mathcal{P}^2$ is.

Egyrésztt

$$a_{\mathcal{P}^2}(\mathcal{G}) \mid \mathcal{P}(\mathcal{G}^\mathcal{P}),$$

másrésztt a 3.2.13a feladat [76] alapján
A \( \varphi(p^2) = \varphi(p - 1) \) és \( \omega(p^2) = p - 1 \) összefüggéseket beírva azt kapjuk, hogy
\[
\varphi(p^2) | \omega(p^2) \quad \text{és} \quad \varphi(p^2) | p(p - 1).
\]
Így \( \omega(p^2) = p - 1 \) vagy \( \omega(p^2) = \varphi(p - 1) \).

A második esetben \( \varphi \) (definíció szerint) primitív gyök modulo \( P^2 \).

Ha \( \omega(p^2) = p - 1 \), akkor megmutatjuk, hogy \( \varphi \mid P \) primitív gyök modulo \( P^2 \).

Az előző gondolmatenetet \( \varphi \) helyett \( \varphi \mid P \) -re megismételve adódik, hogy \( \omega(\varphi + p) \) értéke is csak \( p - 1 \) vagy \( \varphi(p - 1) \) lehet. Így elég azt igazolni, hogy \( \omega(\varphi + p) = \varphi(p - 1) \). A hatványozást elvégezve kapjuk, hogy
\[
(\varphi + p)^{p-1} = \varphi^{p-1} + (p-1)p\varphi^{p-2} + \left(\frac{p-1}{2}\right)p^2\varphi^{p-2} + \ldots
\]

A jobb oldalon az első tag a feltételezésünk szerint \( \varphi \)-gyel kongruens modulo \( P^2 \), továbbá a harmadik tag kezdve minden tag osztható \( P^2 \)-tel. Így
\[
(\varphi + p)^{p-1} \equiv \varphi^{p-1} + (p-1)p\varphi^{p-2} \equiv 1 - p\varphi^{p-2} \equiv 1 \pmod{P^2}.
\]

(L.2) Bebizonyítjuk, hogy ha \( \varphi \) primitív gyök modulo \( P^2 \), akkor primitív gyök modulo \( P^\alpha \) is, tetszőleges \( \alpha \geq 2 \)-re. Az (L1) részben láttott gondolmatenethez hasonlóan elég azt megmutatni, hogy
\[
\varphi(\varphi^\alpha; 1 - 1) \neq 1 \pmod{P^\alpha}.
\]

Ezt a következő formában igazoljuk:
\[
g^{\alpha - 2; (1 - 1)} = 1 + \omega_p \alpha^{-1}, \quad \text{ahol} \quad p \mid \omega_p. \quad (7)
\]

A (7) összefüggést \( \alpha \) szerinti teljes indukcióval bizonyítjuk.

Az \( \alpha = 2 \) esetben valóban \( g^{2; 1} = 1 + 2^2 \), ez a kis Fermat-tétel, és itt \( P \mid 2 \), mert \( \varphi \) primitív gyök modulo \( P^2 \).

Tegyük fel most, hogy (7) teljesül valamely \( \alpha \geq 2 \) esetén; belátjuk, hogy ekkor \( (\alpha \hbox{ helyett}) \alpha + 1 \)-re is fennáll. Emeljük (7)-et \( P \)-edik hatványa:
\[
g^{\alpha - 2; (1 - 1)} = (1 + \omega_p \alpha^{-1})^{\alpha - 1} = 1 + \omega_p \alpha^{-1} + \left(\frac{\alpha - 1}{2}\right) \omega_p^2 \alpha^{-1} + \ldots \quad (8)
\]

Itt a harmadik tag osztható a \( P \) -nek \( 1 + 2(\alpha - 1) \geq \alpha + 1 \)-edik hatványával, a további tagokban pedig szintén legalább ekkora a \( P \) kitevője. Ennélfogva
\[
g^{\alpha - 2; (1 - 1)} = 1 + \omega_p \alpha^{-1} + \omega_p^{\alpha - 1} = 1 + \omega_p \alpha^{-1}, \quad \text{ahol} \quad P \nmid \omega_p, \quad (7)
\]

azaz (7) valóban fennáll \( \alpha + 1 \)-re is.
(L3) Legyen \( g \) primitív gyök modulo \( \mathbb{Z}^r \). Jelöljük \( h \)-val a \( g \) és \( g + \ell^r \) közül azt, amelyik páratlan; belátjuk, hogy \( h \) primitív gyök modulo \( \mathbb{Z}^{2r} \).

Mivel bármely \( i \)-re \( h^i \equiv 1 \pmod{2} \), ezért

\[
    i^r \equiv 1 \pmod{p^r} \iff h^r \equiv 1 \pmod{2p^r}.
\]

Ez azt jelenti, hogy

\[
    a_{2p^r}(h) = a_p(h) = \varphi(p^r) = \varphi(2p^r).
\]

(N1) Megmutatjuk, hogy tetszőleges \( \langle u, \tau \rangle = 1 \) esetén található olyan \( 0 < r < \varphi(m) \), amelyre \( a^r \equiv 1 \pmod{m} \), és így \( a \) nem lehet primitív gyök.

A szóban forgó \( \tau \)-ek felirhatók \( \tau = uv \) alakban, ahol \( \langle u, v \rangle = 1 \) és \( u > 2, v > 2 \). Igazolni fogjuk, hogy \( r = [\varphi(u), \varphi(v)] \) megfelel.

Az \( u > 2 \), \( v > 2 \) feltétel miatt \( \varphi(u) \) és \( \varphi(v) \) páros (lásd a 2.3.1 feladatot [44]), tehát \( \langle \varphi(u), \varphi(v) \rangle > 2 \). Ebből következik, hogy

\[
    r = [\varphi(u), \varphi(v)] \leq \frac{\varphi(u) \varphi(v)}{2} = \frac{\varphi(m)}{2}.
\]

Emellett, \( \varphi(u) | r \) miatt \( a^r \equiv 1 \pmod{u} \), és ugyanez érvényes mod \( v \) is, ezért \( a^r \equiv 1 \pmod{|u,v|} \), azaz mod \( \tau \) is teljesül.

(N2) Megmutatjuk, hogy ha \( \alpha \geq 3 \), akkor bármely páratlan \( a \)-ra

\[
    a^{2^{\alpha-2}} \equiv 1 \pmod{2^{\alpha}}, \quad \text{és az} \quad a^{2^{\alpha-2}} \leq 2^{\alpha-2} < \varphi(2^{\alpha}). \quad (8)
\]

Az \( \alpha \) szerinti teljes indukcióval bizonyítunk. Ha \( \alpha = 3 \), akkor valóban

\[
    2^5 = 8 \mid a^2 - 1 = (a - 1)(a + 1).
\]

Tegyük most fel, hogy (8) ilyen valamely \( \alpha \)-ra; belátjuk, hogy ekkor \( \alpha + 1 \)-ra is fennáll. Az

\[
    a^{2^{\alpha-1}} - 1 = \left(a^{2^{\alpha-2}} - 1\right)\left(a^{2^{\alpha-2}} + 1\right)
\]

szorzatban az első tényező az indukciós feltevés szerint osztható \( 2^{\alpha-1} \)-val, a második tényező osztható 2-vel, így a szorzat valóban osztható \( 2^{\alpha+1} \)-gyel. □

**Feladatok**

3.3.1 Határozzuk meg az összes primitív gyököt modulo \( \mathbb{Z}^m \), ha \( m \) értéke

(a) 7;
(b) 10;
(c) 18.

3.3.2 Adjunk meg egy olyan számot, amely egyszerre primitív gyök mod 11 és mod 14 is.
3.3.3 Adjunk meg
(a) egy primitív gyököt mod 625;
(b) egy olyan primitív gyököt mod 5, amely nem primitív gyök mod 625.

3.3.4 Melyek igazak az alábbi állítások közül?
(a) Ha \( g \) primitív gyök mod 11, akkor \( g \) primitív gyök mod 22.
(b) Ha \( g \) primitív gyök mod 22, akkor \( g \) primitív gyök mod 11.
(c) Ha \( g \) primitív gyök mod \( n \), akkor \( g^3 \) is primitív gyök mod \( n \).
(d) Ha \( g^3 \) primitív gyök mod \( n \), akkor \( g \) is primitív gyök mod \( n \).
(e) Ha \( g \) primitív gyök mod \( n \), akkor \( g^2 \cdot (m-1) \) is primitív gyök mod \( n \).
(f) Ha \( \langle a, 34 \rangle = 1 \) és \( a^b \neq 1 \pmod{34} \), akkor \( a \) primitív gyök mod 34.
(g) Ha \( \langle a, 25 \rangle = 1 \) és \( a^{10} \neq 1 \pmod{25} \), akkor \( a \) primitív gyök mod 25.

3.3.5 Legyen a modulus egy (tetszőleges, de rögzített) \( p > 2 \) primszám.
(a) Mutassuk meg, hogy két primitív gyök szorzata sohasem primitív gyök.
(b) Bizonyítsuk be, hogy létezik három olyan primitív gyök, amelyeknek a szorzata is primitív gyök.
(c) Mely \( P \) primek esetén igaz, hogy bármely három primitív gyök szorzata is primitív gyök?

3.3.6 Adjunk új bizonyítást a Wilson-tételre a primitív gyök felhasználásával.

3.3.7 Legyen \( p > 2 \) prim. Milyen maradékon keresztül az \( 1^k + 2^k + \cdots + (p-1)^k \) összeg \( P \)-vel osztva?

3.3.8 Legyen \( p > 2 \) prim. Milyen maradékon keresztül \( P \)-vel osztva az összes (páronként inkongruens) primitív gyök szorzata? (A primitív gyökök összegére vonatkozóan lásd a 6.5.9c feladatot [194].)

3.3.9 (a) Legyen \( P \) prim, \( d \mid P-1 \), \( g \) primitív gyök mod \( P \) és \( \langle u, P \rangle = 1 \). Bizonyítsuk be, hogy

\[
\alpha_u(a) = d \iff u = y^2 \pmod{p}, \text{ahol} \quad y = \frac{(a-1)}{d} \text{és} \langle t, d \rangle = 1.
\]

(b) Határozzuk meg az (a) rész felhasználásával egy modulo \( P \) redukált maradéknövekben a \( d \)-edrendű elemek számát.

3.3.10 (M [565]*) Legyen \( p > 2 \) prim és \( \langle a, p \rangle - \langle b, p \rangle = 1 \). Bizonyítsuk be, hogy \( \alpha_x(a) = \alpha_x(b) \) akkor és csak akkor teljesül, ha van olyan \( r \) és \( s \) pozitív egész, amelyre \( a \equiv b^r \pmod{p} \) és \( b \equiv a^s \pmod{p} \).

3.3.11 Hogyan általánosítható a T 3.3.4 Tétel olyan összetett modulusra, amelyre nézve létezik primitív gyök?

3.3.12 Legyen \( m = 2^\alpha \), ahol \( \alpha \geq 3 \). Bizonyítsuk be az alábbi állításokat:

(a) \( \alpha_x(5) = 2^{\alpha-2} \).
(b) Az $5^k \equiv -1 \pmod{m}$ kongruencia nem oldható meg.

(c) $A \pm 5^k, 0 \leq k < \varphi(m)/\alpha$ számok redukált maradékkonkruezet alkotnak modulo $\eta$.

*Megjegyzés:* A T 3.3.5 Tételből tudjuk, hogy $\eta = \mathcal{P}^\alpha$, $\alpha > 3$ esetén nem létezik primitív gyök. A feladat (c) része — kissé pongyolán fogalmazva — azt fejezi ki, hogy az 5 „majdnem” primitív gyök ezekre a modulusokra.

3.3.13 (*) Legyen az $\eta > 1$ páratlan szám kanonikus alakja $\eta = \mathcal{P}_1^{\eta_1} \cdots \mathcal{P}_v^{\eta_v}$. Mutassuk meg, hogy léteznek olyan $\eta_1, \ldots, \eta_v$ egészek, hogy az

$$a_1^{k_1} \cdots a_v^{k_v}, \quad 0 \leq k_i < \varphi(p_i^{\eta_i}), \quad i = 1, 2, \ldots, r$$

számok redukált maradékkonkruzet alkotnak modulo $\eta$. Fogalmazzuk meg és bizonyítsuk be a megfelelő állítást páros $\eta$-erre is.

3.3.14 Legyen $p > 2$ prim. Adjunk új bizonyítást modulo $\mathcal{P}$ primitív gyök létezésére az alábbi gondolmatmenet alapján.

(a) Mutassuk meg, hogy ha az $f$ egész együthatós polinomra $f \mid x^p - 1$, akkor az $f(x) \equiv 0 \pmod{\mathcal{P}}$ megoldásszáma pontosan az $f$ fokszámával egyenlő.

(b) Tegyük fel, hogy $q^{\bar{g}} \mid p - 1$, ahol $\bar{g}$ prim és $\bar{g} > 0$. Bizonyítsuk be, hogy az

$$f_1 = x^p - 1 \quad \text{és} \quad f_2 = x^{q^{\bar{g}}} - 1$$

polinomokra az $f_1(x) \equiv 0 \pmod{\mathcal{P}}$, illetve $f_2(x) \equiv 0 \pmod{\mathcal{P}}$ kongruenciák megoldásszáma pontosan $q^{\bar{g}}$, illetve $q^{\bar{g}-1}$.

(c) $A$ (b) rész jelöléseit és eredményét használva mutassuk meg, hogy van olyan $e$, amelyre $o_{\mathcal{P}}(e) = q^{\bar{g}}$.

(d) $A$ (c) rész és a 3.2.15a feladat [76] felhasználásával igazoljuk, hogy minden $d \mid p - 1$ esetén léteznek $d$-edrendű elem modulo $\mathcal{P}$.

3.4 Diszkrét logaritmus (index)

Ebben és a következő pontban feltesszük, hogy a modulus egy $\mathcal{P}$ prímszám. Megjegyezzük, hogy az itt szereplő fogalmak és eredmények tetszőleges olyan modulusra is átvithetők, amelyekre nézve létezik primitív gyök.

Legyen $\eta$ primitív gyök mod $\mathcal{P}$. A T 3.3.2 Tétel szerint az $1, \eta, \ldots, \eta^{p-2}$ számok redukált maradékkonkruezet alkotnak mod $\mathcal{P}$, és így bármely $(\eta, \mathcal{P}) = 1$ esetén pontosan egy olyan $0 \leq k \leq p - 2$ kitevő létezik, amelyre $a \equiv \eta^k \pmod{\mathcal{P}}$. Mindez lehetővé teszi a „logaritmus” bevezetését.

### 3.4.1 Definíció

Legyen $\eta$ primitív gyök mod $\mathcal{P}$ és $(\eta, \mathcal{P}) = 1$. Ekkor az $a$-nak a $\eta$ alapú diszkrét logaritmusán vagy indexén azt a $0 \leq k \leq p - 2$ számot értjük, amelyre $a \equiv \eta^k \pmod{\mathcal{P}}$. 📊
Jelölés: $\text{ind}_p(a)$. Mivel a $\mathcal{P}$ modulus általában rögzített, ezért legtöbbször az erre utaló jelzést elhagyjuk; $\text{ind}_\phi(a)$. Ha a $\mathcal{G}$ primitív gyök is egyértelmű, akkor simán $\text{ind}_\phi(a)$-t írunk.

Az előzetes megjegyzés szerint $(a, \phi) = 1$ esetén $\text{ind}_\phi(a)$ létezik és egyértelmű. Egy $a$ szám diszkrét logaritmusa természetesen függ attől, hogy melyik $\mathcal{G}$ primitív gyök szerint vesszük.

Ha $a \equiv b \pmod{\mathcal{P}}$, akkor nyilván $\text{ind}_\phi(a) = \text{ind}_\phi(b)$, tehát (rögzített $\mathcal{G}$ mellett) egy redukált maradékosztály minden elemének ugyanaz a diszkrét logaritmus.

Sokszor fel fogjuk használni a

$$g^s \equiv g^t \pmod{\mathcal{P}} \iff s \equiv t \pmod{\mathcal{P} - 1}$$

összefüggést (amelő a T 3.2.2 Tétel (ii) állításából következik $m = \mathcal{P}$, $a = g$ és $\omega(g) = \mathcal{P} - 1$ szereposztással).

Ennek megfelelően, ha az összes olyan $j \geq 0$ egész keressük, amelyre $g^j \equiv a \pmod{\mathcal{P}}$, akkor ezek a $j$ értékek éppen egy modulo $\mathcal{P} - 1$ maradékosztály nemnegatív elemei lesznek. Más megfogalmazásában:

$$g^j \equiv a \pmod{\mathcal{P}} \iff j \equiv \text{ind}_\phi(a) \pmod{\mathcal{P} - 1}.$$

(Szokás ennek alapján a diszkrét logaritmust úgy is értelmezni, hogy ezt a modulo $\mathcal{P} - 1$ maradékosztályt nevezik az $a$ elem $\mathcal{G}$ alapú diszkrét logaritmusának.)

A diszkrét logaritmusra is érvényesek a logaritmusazonosságok megfelelői (lásd a 3.4.3 [86]-3.4.4 feladatokat [86]).

A diszkrét logaritmus segítségével oldjuk meg a következő pontban a modulo $\mathcal{P}$ „gyökvonás” problémáját, emellett egy kriptográfiai alkalmazást is tárgyalunk az 5.8.6 feladatban [165].

Illusztrációként mellékelünk egy „exponenciális” és egy „logaritmus”-táblázatot (indextáblázatot), amely a $\mathcal{P} = 13$ modulusra és a $g = 2$ primitív gyökre vonatkozik.

<table>
<thead>
<tr>
<th>$j$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^j \pmod{13}$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>3</td>
<td>6</td>
<td>12</td>
<td>11</td>
<td>9</td>
<td>5</td>
<td>10</td>
<td>7</td>
</tr>
<tr>
<td>$\text{ind}_\phi(a)$</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>$\text{ind}_\phi(a)$</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>9</td>
<td>5</td>
<td>11</td>
<td>3</td>
<td>8</td>
<td>10</td>
<td>7</td>
<td>6</td>
</tr>
</tbody>
</table>

**Feladatok**

Valamennyi feladatban a $\mathcal{G}$ és $\mathcal{H}$ primitív gyökök egy $\mathcal{P} > 2$ prim modulusra vonatkoznak, $\mathcal{E}$ és $\mathcal{B}$ relatív primek $\mathcal{P}$-hez, és ha külön nem jelezzük, akkor $\mathcal{G}$ alapú indexről van szó.

3.4.1 Mely $\mathcal{P}$ prímekre lesz $\text{ind}_{\mathcal{P}}(2) = 3$?

3.4.2 Számítsuk ki az alábbi diszkrét logaritmusokat:

(a) $\text{ind}_\mathcal{G}(1)$;

(b) $\text{ind}_\mathcal{G}(-1)$;

(c) $\text{ind}_\mathcal{G}(-g)$.

85
3.4.3 Bizonyítsuk be az alábbi „logaritmusazonosságokat”:

(a) \( \text{ind}(a^b) \equiv \text{ind}(a) \cdot \text{ind}(b) \mod p - 1 \); 
(b) \( \text{ind}(a^k) \equiv k \cdot \text{ind}(a) \mod p - 1 \).

3.4.4 Bizonyítsuk be, hogy a \( q \) alapú indexről a \( h \) alapú indexre az alábbi („szokásos”) módon lehet áttérni:

(a) \( \text{ind}_q(h \cdot \text{ind}_h g) \equiv 1 \mod p - 1 \); 
(b) \( \text{ind}_q(a) \equiv \text{ind}_q g \cdot \text{ind}_q a \mod p - 1 \).

3.4.5 Melyik az a legkisebb \( s \) pozitív egész, amelyre \( p - 1 \mid s \cdot \text{ind} a \)?

3.4.6 Bizonyítsuk be, hogy \( a \) akkor és csak akkor primitív gyök mod \( p \), ha \( (\text{ind}_q a, p - 1) = 1 \).

3.4.7 Bizonyítsuk be az alábbi állításokat.

(a) \( (\text{ind}_q c, p - 1) = 1 \iff (\text{ind}_h a, p - 1) = 1 \); 
(b) \( (\text{ind}_q a, p - 1) = (\text{ind}_q c, p - 1) \).

3.4.8 Legyenek \( a, b, c \) tetszőleges primitív gyökök modulo \( p \). Igazoljuk, hogy ekkor

\[ a^{\text{ind}_h c} \]

is primitív gyök mod \( p \).

3.4.9 (M [565]*) Mutassuk meg, hogy \( \text{ind}_q(a) = \text{ind}_q(b) \) akkor és csak akkor teljesül, ha van olyan \( q \) és \( h \) primitív gyök, amelyre \( \text{ind}_q b = \text{ind}_h a \).

3.4.10 Keressük meg az alábbi prímekhez a legkisebb pozitív primitív gyököt és készítsünk indextáblázatot: (a) \( 7 \); (b) \( 11 \); (c) \( 17 \).

3.4.11 (*) Bizonyítsuk be, hogy bármely \( p \) prímhez és \( a \) egészhez végére sok olyan \( k \) pozitív egész található, amelyre \( a = k^k \mod p \).

### 3.5 Binom kongruenciák

A pozitív valós számok körében a gyökölés elvégzéséhez a szám logaritmusát elosztjuk a gyököt a kalkulátorok (így vonnak gyököt a kalkulátorok is). Hasonló módon használható a diszkrét logaritmus is a modulo \( p \) gyököléshez, azaz az \( x^k \equiv a \mod p \) kongruencia megoldásához (ahol \( P \) prim szám). Az ilyen kongruenciákat kéttagú vagy binom kongruenciának nevezzük. Az általános \( cx^k \equiv d \mod p \) binom kongruencia, ahol \( c \neq 0 \mod p \), szintén ilyen \( x^k \equiv a \mod p \) alakra hozható: a megfelelő \( a \) értéket a \( cy \equiv d \mod p \) lineáris kongruencia (mod \( p \) egyértelmű) megoldása szolgáltatja.

Az \( \{a, p\} \neq 1 \) esetben \( a \equiv 0 \mod p \), azaz az \( x^k \equiv 0 \mod p \) kongruenciáról van szó; ennek könnyen láthatóan \( x \equiv 0 \mod p \) az egyetlen megoldása.
Így a továbbiakban feltesszük, hogy \((a, p) = 1\).

3.5.1 Tétel. T 3.5.1

Legyen \(p\) prim és \((a, p) = 1\). Az

\[ x^k \equiv a \pmod{p} \tag{1} \]

kongruencia akkor és csak akkor oldható meg, ha

\[ a^{\frac{k}{p-1} \cdot \frac{1}{2}} \equiv 1 \pmod{p}. \tag{2} \]

Megoldhatóság esetén a (páronként inkongruens) megoldások száma \(\frac{k}{p-1}\).

A (2) feltétel ekvivalens azzal, hogy

\[ \frac{k}{p-1} \mid \text{ind}_p a \tag{3} \]

teljesül, ahol \(\mathcal{G}\) egy tetszőleges primitív gyököt jelent modulo \(p\).

Bizonyítás: A \(\mathcal{G}\) primitív gyök szerinti diszkrit logaritmust fogjuk használni.

Keressük a megoldást \(x \equiv g^{\text{ind}_p a} \pmod{p}\) alakban. Ekkor az (1) kongruencia átírható a

\[ g^{k \cdot \text{ind}_p a} \equiv g^{\text{ind}_p a} \pmod{p} \]

alakba, amely a már sokszor használt \(g' = g' \pmod{p} \iff s \equiv t \pmod{p-1}\) összefüggés alapján tovább ekvivalens

\[ k \cdot \text{ind}_p x \equiv \text{ind}_p a \pmod{p-1} \tag{4} \]

teljesülésével.

A (4) az \(\text{ind}_p x\) -re nézve egy lineáris kongruencia, amely a T 2.5.3 Tétel szerint akkor és csak akkor oldható meg, ha (3) teljesül, tehát ugyanez az (1) kongruencia megoldhatóságának a szükséges és elégséges feltétele is.

A (4) kongruencia modulo \(p - 1\) páronként inkongruens megoldásainak az (1) kongruencia modulo \(p\) páronként inkongruens megoldásai feltének meg és viszont, tehát a két kongruenciának ugyanannyi a megoldásszáma: a T 2.5.4 Tétel alapján ez \(\frac{k}{p - 1}\).

Végül megmutatjuk a (2) és (3) feltételek ekvivalenciáját. Mivel

\[ a^{\frac{k}{p-1} \cdot \frac{1}{2}} \equiv \left(g^{\text{ind}_p a}\right)^{\frac{p-1}{2}} - g^{(p-1)\frac{\text{ind}_p a}} \pmod{p}, \tag{5} \]

ez\(a^{(p-1)/2} \pmod{p}\) pontosan akkor teljesül, ha (5) utolsó tagjában a \(\mathcal{G}\) kitevője a \(p - 1\)-nek egész számú többszöröse, azaz ha \(\{k, p-1\} \mid \text{ind}_p a\).

Megjegyzések: 1. A tétel bizonyításából együttal megoldási módszert is kaptunk, feltéve, hogy rendelkezésünkre áll egy indextáblázat.

2. A (3)-ban szereplő \(\text{ind}_p a\) érték természetesen más és más (lehet), attól függően, hogy melyik \(\mathcal{G}\) primitív gyököt választottuk. Mivel azonban az (1) kongruencia megoldhatósága nem függ \(\mathcal{G}\)-től,
ezért a (3)-ban megadott feltétel is független a $\mathcal{G}$ -től: vagy minden primitív gyökre teljesül, vagy pedig egyikre sem. (Mindez egyébként a 3.4.7b feladatból [86] is következik.)

**Példa:** Oldjuk meg az $5^{22} \equiv 6 \ (\text{mod} \ 13)$ kongruenciát.

Az $5^{22} \equiv 6 \ (\text{mod} \ 13)$ kongruencia (egyetlen) megoldása $y \equiv 9 \ (\text{mod} \ 13)$. Ennek megfelelően az $x^{22} \equiv 9 \ (\text{mod} \ 13)$ kongruenciát kell megoldanunk.

A T 3.5.1 Tétel bizonyításában láttuk, hogy ez a kongruencia a

$$22 \cdot \text{ind} \ x \equiv \text{ind} \ 9 \ (\text{mod} \ 12)$$

kongruenciával ekvivalens.

A 13 modulusra nézve a 2 primitív gyök, és a megfelelő „exponenciális” és „logaritmus”-táblázatok a 3.4 pont végén találhatók. Innen $\text{ind} \ 9 = 8$.

Az így nyert

$$22 \cdot \text{ind} \ x = 8 \ (\text{mod} \ 12)$$

lineáris kongruencia $(22, 12) \mid 8$ miatt megoldható és a (páronként inkongruens) megoldások száma $(22, 12) = 2$. A megoldások:

$$\text{ind} \ x \equiv 2 \ (\text{mod} \ 12) \quad \text{és} \quad \text{ind} \ x \equiv 8 \ (\text{mod} \ 12).$$

Az „exponenciális” táblázatot használva ebből

$$x \equiv 4 \ (\text{mod} \ 13) \quad \text{és} \quad x \equiv 9 \ (\text{mod} \ 13)$$

adódik.

Megjegyezzük, hogy nem szükséges az $5^{9} \equiv 6 \ (\text{mod} \ 13)$ kongruenciát külön megoldani, hanem rögtön áttérhetünk az indexre:

$$\text{ind} \ 5 + 22 \cdot \text{ind} \ x \equiv \text{ind} \ 6 \ (\text{mod} \ 12), \quad \text{azaz} \quad 9 + 22 \cdot \text{ind} \ x \equiv 5 \ (\text{mod} \ 12).$$

Ily módon egy lépésben jutottunk el a $22 \cdot \text{ind} \ x \equiv 6 \ (\text{mod} \ 12)$ lineáris kongruenciához.

**3.5.2 Definíció.**

D 3.5.2

Legyen $\mathcal{P}$ prim és $(\alpha, \mathcal{P}) = 1$. Az $\alpha$ számot (a $\mathcal{P}$-re nézve) $\hat{k}$-adik hatványmaradéknak nevezzük, ha az $x^k \equiv \alpha \ (\text{mod} \ \mathcal{P})$ kongruencia megoldható, és $\hat{k}$-adik hatvány-nemmaradéknak nevezzük, ha az $x^k \equiv \alpha \ (\text{mod} \ \mathcal{P})$ kongruencia nem oldható meg.

**3.5.3 Tétel.**

T 3.5.3

Legyen $\mathcal{P}$ prim és $(\alpha, \mathcal{P}) = 1$. Az $\alpha$ szám (a $\mathcal{P}$-re nézve) akkor és csak akkor $\hat{k}$-adik hatványmaradék, ha

$$\alpha^{\frac{\varphi(\mathcal{P})}{\deg \alpha}} \equiv 1 \ (\text{mod} \ \mathcal{P}), \quad \text{illetve} \quad \frac{k \varphi(\mathcal{P}) - 1}{\deg \alpha} \mid \text{ind}_\mathcal{P} \alpha,$$

ahol $\mathcal{G}$ tetszőleges primitív gyök modulo $\mathcal{P}$. 

88
A (páronként inkongruens) \( k \)-adik hatványmaradékok száma \( \phi(k, p - 1) \).

**Bizonyítás:** Az első állítás a T 3.5.1 Tétel (egy részének) átfogalmazása.

A második állítás abból következik, hogy a \( k \)-adik hatványmaradékok épén a

\[
\sum_{x=1}^{k-1} x^{pk-1} \equiv 1 \pmod{p}
\]

kongruencia megoldásai, és ennek a kongruenciának a megoldásszáma szintén a T 3.5.1 Tétel szerint

\[
\left( \frac{p-1}{(k, p-1)^2} \right) p - 1 \equiv \frac{p-1}{(k, p-1)}
\]

**Feladatok**

Valamennyi feladatban a modulus egy \( p > 2 \) prím.

### 3.5.1

Oldjuk meg az alábbi kongruenciákat. (A 11, 13 és 17 modulusok esetén használjuk fel a 3.4 pont végén, illetve a 3.4.10 feladat [86] útmutatásánál szereplő indextáblázatokat is.)

(a) \( 3x^{30} \equiv 2 \pmod{101} \).

(b) \( x^{59} \equiv 2 \pmod{101} \).

(c) \( 2x^{50} \equiv 50 \pmod{23} \).

(d) \( 5x^4 \equiv 14x^2 \pmod{17} \).

(e) \( 4x^2 + 7x^4 \equiv 0 \pmod{13} \).

(f) \( 4x^{27} + 5x^{20} + 7x^{17} + 9x^9 + 3 \equiv 0 \pmod{11} \).

### 3.5.2

Határozzuk meg az alábbi kongruenciák megoldásszámát.

(a) \( (x^{30} - 1)(x^{45} - 1) \equiv 0 \pmod{73} \).

(b) \( 1 + x + x^2 + \cdots + x^k \equiv 0 \pmod{31} \).

### 3.5.3

Mely \( a \) számokra oldható meg az

\[ 1 - x + \cdots + x^{p-2} \equiv a \pmod{p} \]

kongruencia?

### 3.5.4

Mutassuk meg, hogy ha \( g \) primitív gyök, akkor az \( x^k \equiv g \pmod{p} \) kongruenciának legfeljebb egy megoldása van.

### 3.5.5

Jelölje \( x^k \equiv 1 \pmod{p} \) összes (páronként inkongruens) megoldását \( b_1, b_2, \ldots, b_r \). Legyen \( (a, p) = 1 \) és az \( x^k \equiv a \pmod{p} \) kongruencia egy megoldása \( c \). Hogyan kaphatjuk meg az \( x^k \equiv a \pmod{p} \) kongruencia összes megoldását?

### 3.5.6

Határozzuk meg az
(a) \( p - 1 \) -edik;

(b) \( (p - 1)/2 \) -edik

hatványmaradékokat mod \( P \).

3.5.7 Melyek azok a \( k \) értékek, amelyekre a \( k \) -adik gyökvonás modulo \( P \) egyértelműen elvégezhető, azaz amelyekre az \( x^k \equiv a \mod{p} \) kongruenciának bármely \( a \) esetén pontosan egy megoldása van?

3.5.8 Mely primekre létezik teljes maradékrrendszer csupa köbszámából?

3.5.9 Bizonyítsuk be, hogy

(a) két \( k \) -adik hatványmaradék szorzata mindig \( k \) -adik hatványmaradék;

(b) egy \( k \) -adik hatványmaradék és egy \( k \) -adik hatvány-nemmaradék szorzata mindig \( k \) -adik hatvány-nemmaradék.

3.5.10 Mi a szükséges és elégséges feltétele annak, hogy létezzen \( k \) -adik hatvány-nemmaradék és bármely két \( k \) -adik hatvány-nemmaradék szorzata \( k \) -adik hatványmaradék legyen?

3.5.11 Milyen maradéket ad \( P \) -vel osztva az összes (páronként inkongruens) \( k \) -adik hatványmaradék (a) összege; (b) szorzata?

3.5.12 (M [S66]) Bizonyítsuk be, hogy \( a \) akkor és csak akkor lesz egyszerre \( 20 \) -adik és \( 50 \) -edik hatványmaradék modulo \( P \), ha \( 1 \pmod{1} \)-adik hatványmaradék modulo \( P \). Általánosítsuk a feladatot.

### 3.6 Chevalley-tétel, Kőnig–Rados-tétel

Ebben a pontban prim modulusú kongruenciákra vonatkozó két nevezetes tételt tárgyalunk. Elsőként olyan

\[
x_i(x_1, x_2, \ldots, x_i) \equiv 0 \mod{p}, \quad i = 1, 2, \ldots, k \tag{1}
\]

kongruenciarendszerekkel foglalkozunk, ahol \( P \) prim, \( k \geq 1 \) és

\[
f_i(x_1, x_2, \ldots, x_i), \quad i = 1, 2, \ldots, k
\]

olyan egész együttthatós, \( t \) -változós polinomok, amelyek konstans tagja 0, azaz

\[
f_i(0, 0, \ldots, 0) = 0, \quad i = 1, 2, \ldots, k. \tag{2}
\]

A (2) felételből azonnal kapjuk, hogy \( x_1 \equiv x_2 \equiv \cdots \equiv x_t \equiv 0 \mod{p} \) kielégíti az (1) kongruenciarendszert, ezt a továbbiakban trivialis megoldásnak nevezzük.

Chevalley tétel arra vonatkozik, hogy az \( f_i \) polinomok fokszámára tett alkalmazás kikötés esetén az (1) rendszernek létezik nemtrivialis megoldása is. (Egy \( x_1^{n_1} \cdots x_t^{n_t} \) tag fokszáma \( n_1 + \cdots + n_t \), egy polinom fokszáma pedig a benne szereplő nemnulla együttthatós tagok fokszámának a maximuma.)

3.6.1 Tétel (Chevalley tétel) . \( T \) 3.6.1

Ha az (1)-ben szereplő \( f \) polinomokra teljesül (2) és fokszámaik összege kisebb a változók számánál, azaz
akkor (1)-nek létezik nemtriviális megoldása.

**Példák:** Az

\[
x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 \equiv 0 \pmod{23}
\]

\[
x_1^3 + 2x_1x_2 + 3x_2x_3 + 4x_3x_4 + 5x_4^2 \equiv 0 \pmod{23}
\]

kongruenciarendszernek létezik nemtriviális megoldása, azaz olyan, ahol nem mindegyik \(x_i\) osztható 23-mal. (Ilt \(k = 2\) és \(5 = t > 1 + 3 = \deg f_1 + \deg f_2\).)

A T 3.6.1 Tételt \(k = 1\), azaz egyetlen polinom esetén is jól alkalmazhatjuk: pl. bármely \(P\) prim esetén a

\[
p \mid x_1^3 + 3x_2^3 + 5x_3^3 + 7x_4^3 + 9x_1x_2 + 11x_3x_4
\]

oszthatóság úgy is megvalósul, hogy legalább az egyik \(x_i\) nem osztható \(P\)-vel. (Most \(t = 4\) és \(\deg f = 3\).)

**Bizonyítás:** Tegyük fel indirekt, hogy a kongruenciarendszernek csak triviális megoldása van.

Vezessük be az alábbi két \(t\)-változós polinomot:

\[
F(x_1, x_2, \ldots, x_t) = \prod_{i=1}^{k} \left(1 - f_i^{p-1}(x_1, x_2, \ldots, x_t)\right),
\]

\[
G(x_1, x_2, \ldots, x_t) = \prod_{j=1}^{t} \left(1 - x_j^{p-1}\right).
\]

A kis Fermat-tétel szerint

\[
x_j \equiv 0 \pmod{p} \implies x_j^{p-1} \equiv 1 \pmod{p}.
\]

Ebből azonnal következik, hogy \(G\)-be tetszőleges \(c_1, \ldots, c_t\) egész számokat behelyettesíve

\[
G(c_1, c_2, \ldots, c_t) = \begin{cases} 
1 \pmod{p}, & \text{ha } c_1 = \cdots = c_t = 0 \pmod{p}; \\
0 \pmod{p}, & \text{ egyébként.}
\end{cases}
\]

(Megmutatjuk, hogy ugyanez érvényes \(F\)-re is, azaz

\[
F(c_1, c_2, \ldots, c_t) = \begin{cases} 
1 \pmod{p}, & \text{ha } c_1 = \cdots = c_t = 0 \pmod{p}; \\
0 \pmod{p}, & \text{ egyébként.}
\end{cases}
\]

Legyen először

\[
c_1 \equiv \cdots \equiv c_t \equiv 0 \pmod{p}
\]

Ekkor (2) alapján minden \(i\)-re

\[
f(c_1, \ldots, c_t) \equiv 0 \pmod{p},
\]
azaz $F(c_1, \ldots , c_i)$ minden tényezője és így maga $F(c_1, \ldots , c_i)$ is 1-gyel kongruens modulo $p$.

Vegyük most a másik esetet, azaz amikor a $c_1, \ldots , c_i$ számok közül legalább az egyik nem osztható $P$-vel. Mivel az indirekt feltevés szerint (1)-nek csak triviális megoldása létezik, ezért $c_1, \ldots , c_i$ nem megoldás, vagyis legalább egy $i$-re

$$f_i(c_1, \ldots , c_i) \neq 0 \pmod{p}.$$ 

Ebből ismét a kis Fermat-tétel alapján következik, hogy

$$f_i^{p-1}(c_1, c_2, \ldots , c_i) \equiv 1 \pmod{p}.$$ 

Ez azt jelenti, hogy $F(c_1, \ldots , c_i)$ egyik tényezője, és így maga $F(c_1, \ldots , c_i)$ is osztható $P$-vel. Ezzel (5) igazolását befejeztük.

A (4) és (5) képletek alapján tetszőleges $c_1, \ldots , c_i$ egész számokra

$$F(c_1, \ldots , c_i) \equiv G(c_1, \ldots , c_i) \pmod{p}. \quad (6)$$

A továbbiakban valamennyi polinomot a modulo $P$ test feletti $t$ -változós polinomnak fogunk tekinteni.

Ekkor (6) azt fejezi ki, hogy az $F$ és $G$ polinomok minden helyettesítési értéke megegyezik (vagyis $F$ -hez és $G$ -hez ugyanaz a polinomfüggvény tartozik; véges test esetén azonban ebből maguknak, a polinomoknak, azaz az együttáthatóknak az egyenlősége nem következik).

Nevezzük egy $H$ polinom redukált alakjának azt a polinomot, amelyet $H$-ből úgy kapunk, hogy $H$-ban mindenhol $x_i^n$ helyére $x_i$-t írunk, ameddig csak lehetséges. Nyilván $H^*$ minden tagjában bármelyik $x_i$ kitevője legfeljebb $p - 1$ , továbbá $H$ és $H^*$ minden helyettesítési értéke megegyezik. A változók száma szerinti teljes indukcióval könnyen megmutatható, hogy ha a $H$ és $K$ polinomok minden helyettesítési értéke megegyezik, akkor a $H^*$ és $K^*$ polinomok (formálisan is) egyenlők (azaz $H^*$-nak és $K^*$-nak ugyanazok a megfelelő együttáthatók).

Láttuk, hogy az $F$ és $G$ polinomok minden helyettesítési értéke megegyezik, ezért az előzőek szerint ekkor az $F^*$ és $G^*$ polinomok egyenlők. Így $\deg G^* = \deg F^*$ is teljesül. Azonban $G = G^*$ és (3) miatt

$$\deg G^* = \deg G = (p - 1)t > (p - 1) \left( \sum_{i=1}^{k} \deg f_i \right) = \deg F > \deg F^*,$$

ami ellentmondás. ♦

A pont második részében egy olyan eredményt bizonyítunk, amely az $f(x) \equiv 0 \pmod{p}$ kongruencia megoldásszámba pontos képletet ad az együttáthatók segítségével. Ez a König Gyulától és Rados Gusztávtól származó tétel inkább csak elvi jelentőségű, a megoldásszám gyakorlati kiszámítására nemigen használható.

3.6.2 Tétel (König–Rados-tétel) .

Legyen $P$ prim és

$$f = a_0 + a_1z + \cdots + a_{n-2}z^{n-2}$$
olyan egész együtthatós polinom, amelyre \( a_0 \neq 0 \mod p \). Ekkor az

\[ f(x) \equiv 0 \mod p \]

kongruencia megoldásszáma \( n - 1 - r \), ahol \( r = r(A) \) az alábbi \((p-1) \times (p-1)\)-es \( A \) ciklikus mátrixnak a modulo \( P \) test feletti rangját jelöli:

\[
A = \begin{pmatrix}
a_0 & a_1 & \cdots & a_{p-2} \\
a_{p-2} & a_0 & \cdots & a_{p-3} \\
\vdots & \vdots & \ddots & \vdots \\
a_1 & a_2 & \cdots & a_0
\end{pmatrix}
\]

Megjegyzések:
1. A tételből azonnal adódik, hogy az \( f(x) \equiv 0 \mod p \) kongruencia akkor és csak akkor oldható meg, ha az \( A \) mátrix rangja \( n - 1 \) kisebb, azaz \( \det A \equiv 0 \mod p \).
2. Az \( f \) -re tett kikötések nem jelentenek lényeges megszorítást; egy tetszőleges polinom esetén a megoldásszám meghatározását visszavezethetjük a König–Rados-tételre, lásd a 3.6.11 feladatot [95].

Bizonyítás: Az alábbi elemi lineáris algebrai tételeket fogjuk felhasználni. Ezek egy \( \mathbb{F} \) kommutatív test feletti \( n \times n \)-es mátrixokra vonatkoznak, és \( r(B) \) jelöli a \( B \) mátrix rangját; esetünkben \( n = p - 1 \) és \( \mathbb{F} \) a modulo \( P \) test.

(i) Legyenek \( t_1, t_2, \ldots, t_n \) a \( \mathbb{F} \) test különböző elemei. Ekkor a

\[
V = V(t_1, t_2, \ldots, t_n) = \begin{pmatrix}
t_1 & t_2 & \cdots & t_n \\
t_1^2 & t_2^2 & \cdots & t_n^2 \\
\vdots & \vdots & \ddots & \vdots \\
t_1^{n-1} & t_2^{n-1} & \cdots & t_n^{n-1}
\end{pmatrix}
\]

Vandermonde-mátrix rangoja \( r(V) = n \).

(ii) Ha \( r(B) = \gamma \), azaz \( B \) invertálható, akkor tetszőleges \( C \) -re \( r(BC) = r(C) \).

A (ii) összefüggés a bármely \( M, N \) mátrixra érvényes

\[
r(MN) \leq \min\{r(M), r(N)\}
\]

egyenlőtlenségből adódik; ennek alapján egyrészt \( r(CB) \leq r(C) \), másrészt \( r(C) - r(\{(CB)B^{-1}\}) \leq r(CB) \).

Rátérve a T 3.6.2 Tétel bizonyítására, jelöljük az \( f(x) = 0 \mod p \) kongruencia megoldásszámát \( s \) -sel, legyen \( V = V(1, 2, \ldots, p - 1) \), és tekintsük a \( D = AV \) mátrixot. Az (i) és (ii) segéd tételeink alapján

\[
r(D) = r(A) = r. \tag{7}
\]

Az \( AV \) mátrixszorzást elvégezve a \( D \) mátrix első sorának \( j \) -edik eleme

\[
d_{1j} = a_0 + a_1 j + a_2 j^2 + \cdots + a_{p-2} j^{p-2} = f(j)
\]

93
lesz. A második sor $j$-edik elemének egyszerű felirásához azt is felhasználjuk, hogy $j^{p-1} \equiv 1 \pmod{p}$:

$$d_{i\ell} = a_{\ell-2} + a_{i} j + a_{i,1} j^2 + \cdots + a_{i,p-3} j^{p-2} \equiv
= a_{\ell-2} j^{p-1} + a_{i} j + a_{i,1} j^2 + \cdots + a_{i,p-3} j^{p-2} = j^{p-1} \cdot f(j) \pmod{p}.$$

Hasonlóan adódik, hogy az $i$-edik sor $j$-edik eleme

$$d_{ij} = j^{i-1} \cdot f(j) \pmod{p}.$$

Így azt kaptuk (a kongruenciák helyett a modulo $P$ testbeli egyenlőséget irva), hogy

$$D = AV = \begin{pmatrix}
    f(1) & f(2) & f(3) & \cdots & f(p-1) \\
    f(1) & 2f(2) & 3f(3) & \cdots & (p-1)f(p-1) \\
    f(1) & 2^2f(2) & 3^2f(3) & \cdots & (p-1)^2f(p-1) \\
    \vdots & \vdots & \vdots & \ddots & \vdots \\
    f(1) & 2^{p-2}f(2) & 3^{p-2}f(3) & \cdots & (p-1)^{p-2}f(p-1)
\end{pmatrix}.$$

A $D$ mátrix $j$-edik oszlopa pontosan akkor lesz minden elem 0, ha $f(j) \equiv 0 \pmod{p}$, vagyis a $D$ csupa 0 oszlopainak a száma éppen $s$. A többi oszlop a $V$ különböző oszlopainak a nemnulla skalárszorosa, tehát ezek az $(i)$ segédítél szerint lineárisan függetlenek. Ez azt jelenti, hogy $\tau(D) = p - 1 - s$. Ezt (7)-tel összevetve éppen a tétel állítását kapjuk. 

Feladatok

3.6.1 Melyik ismert téttelt kapjuk a Chevalley-tételnek abban a speciális esetében, ha mindegyik $j_i$ polinom elsőfokú?

3.6.2 Bizonyítsuk be, hogy az $ax^2 + by^2 + cz^2 = 0 \pmod{p}$ kongruenciának bármely $p$ prim és $a, b, c$ egész esetén létezik nemtriviális megoldása.

3.6.3 (a) Mutassuk meg, hogy bármely $n > 1$-hez található három olyan egész szám, amelyek $s$ négyzetösszegére $n|s^s$, de $n^2 \not| s$.

(b) Lássuk be, hogy $(n, s/n) = 1$ is elérhető.

3.6.4 Mutassuk meg, hogy bármely $p$ prímszámnak létezik olyan (nemnulla) többszöröse, amely kisebb, mint $p^{4/4}$, és felírheto legfeljebb öt egész szám negyedik hatványának az összegeként.

3.6.5 (*) (a) Legyenek $q_1, \ldots, q_k$ különböző prímszámok és $c_1, \ldots, c_t$ olyan különböző pozitív egészek, amelyek egyikének sincs a $G_i$-től különböző prímosztója. Bizonyítsuk be, hogy ha $t > 2k + 1$, akkor a $c_i$ számok közül kiválásztható néhány különböző (esetleg csak egy, esetleg az összes) úgy, hogy a szorzatuk köbzsám legyen.

(b) Általánosítsuk az (a) részt köbszámok helyett $m$-edik hatványokra, ahol $m$ tetszőleges prímszám.

3.6.6 (*) Mutassuk meg, hogy $2n - 1$ egész számból mindig kiválasztható $n$ olyan, amelyek összege sosztható $n$-nel.
3.6.7 Bizonyítsuk be a Chevalley-tétel következő általánosítását. Hagyjuk el a tétel feltételei közül azt, hogy az $f_i$ polinomok konstans tagja 0, a többi feltétel változatlan marad. Ekkor a szóban forgó kongruenciarendszer megoldásaira a következők igazak:

(a) Ha van megoldás, akkor legalább két megoldás van.
(b) A megoldásszám osztható $P$-vel.

3.6.8 Legyen $p > 2$ prim, $(a^b, p) = 1$. A König–Rados-tétel illusztrációjaként határozzuk meg az $f(x) \equiv 0 \pmod{p}$ kongruenciák megoldásszámát az alábbi $f$ polinomok esetén:

(a) $ax - b$;
(b) $1 + x + \cdots + x^{p-2}$;
(c) $x^{p-2} - \omega$.

3.6.9 Olvassuk le a König–Rados-tételből, hogy az alábbi kongruenciák megoldhatók:

(a) $x^k \equiv 1 \pmod{p}$, ahol $p$ páratlan prim és $1 \leq k \leq p - 2$;
(b) $x^2 = -1 \pmod{p}$, ahol $p$ prim és $p = 1 \pmod{4}$.

3.6.10 Legyen $p > 3$ prim, $(a_0, p) = (a_1, p) = (a_{p-2}, p) = 1$ és

$$f = a_0 + a_1x + \cdots + a_{p-3}x^{p-3} + a_{p-2}x^{p-2} + a_{p-1}x^{p-1},$$
$$g = a_1 + a_2x + \cdots + a_{p-2}x^{p-2} + a_{p-1}x^{p-1},$$
$$h = a_{p-2} + a_{p-3}x + \cdots + a_1x^{p-1} + a_0x^p.$$

Bizonyítsuk be, hogy az

$$f(x) \equiv 0 \pmod{p}, \quad g(x) \equiv 0 \pmod{p} \quad \text{és} \quad h(x) \equiv 0 \pmod{p}$$

kongruenciák mindegyikének ugyanannyi a megoldásszáma.

3.6.11 Legyen $g = b_0 + b_1x + \cdots + b_{n}x^n$ tetszőleges egész együtthatós polinom. Hogyan vezethetjük vissza a $g(x) \equiv 0 \pmod{p}$ kongruencia megoldásszámának a meghatározását a König–Rados-tételre az $n > p - 2$ és/vagy $b_0 \equiv 0 \pmod{p}$ esetben?

3.7 Prímhatvány modulusú kongruenciák

A 2.6 pontban láttuk, hogy tetszőleges összetett modulusú kongruencia visszavezethető primhatvány modulusú kongruenciákra a kínai maradéktétel segítségével. Most azzal foglalkozzunk, hogyan vezethető vissza alkalmas feltételek teljesülése esetén egy primhatvány modulusú kongruencia a prim modulusú esetére.

Legyen $p$ prim, $k$ pozitív egész, $f$ egy egész együtthatós polinom, és tekintsük az

$$f(x) \equiv 0 \pmod{p^k}$$

kongruenciát. Ha $e$: megoldása (1)-nek, akkor $e$: nyilván az

$$f(x) \equiv 0 \pmod{p}$$
kongruenciát is kielégíti. Ezért (1) megoldásait a (2) kongruencia megoldásaiból kiindulva fogjuk megkeresni.

3.7.1 Tétel. T 3.7.1

Legyen \( c \) megoldása (2)-nek, és tegyük fel, hogy \( f'(c) \not\equiv 0 \pmod{p} \), ahol \( f' \) az \( f \) polinom deriváltját jelöli. Ekkor (1)-nek pontosan egy olyan \( x \equiv c_k \pmod{p^k} \) megoldása létezik, amelyre \( c_k \equiv c \pmod{p} \).

A bizonyítás egyúttal eljárást is ad \( c_k \) előállítására, és az is kiderül, mi a helyzet akkor, ha \( f'(c) \equiv 0 \pmod{p} \).

**Bizonyítás:** Fel fogjuk használni az alábbi összefüggést:

\[
j \geq 1 \implies f(a + tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}}.
\]

Ennek igazolásához tekintsük \( f(a + tp^j) \) előállítását a Taylor-formula segítségével:

\[
f(a + tp^j) = f(a) + tp^j f'(a) + \frac{t^2 p^{2j} f''(a)}{2!} + \ldots + \frac{t^j p^j f^{(j)}(a)}{j!}
\]

ahol \( n \) az \( f \) polinom foka. Itt mindegyik \( f^{(r)}(a)/r! \) egész szám, ugyanis bármely \( x \)-tag \( r \)-edik deriváltja \( s(s-1)\ldots(s-r+1)x^{s-r} \) (ha \( s \geq r \)), és \( r \) szomszédos egész szám szorzata mindig osztható \( r! \)-sal (lásd az 1.1.17b feladatot [4]). Ebből következik, hogy (4) jobb oldalán a harmadik tagtól kezdve minden tag osztható \( p^{j+1} \)-gyel, tehát (3) valóban teljesül.

A T 3.7.1 Tételt \( k \)- szerinti teljes indukcióval bizonyítjuk. A \( k = 1 \) eset (a deriváltra vonatkozó feltétel nélkül is) nyilvánvaló.

Tegyük fel, hogy az állítás \( k - 1 \)-re igaz: ez azt jelenti, hogy az

\[
f(x) \equiv 0 \pmod{p^{k-1}}
\]

kongruenciának \( x \equiv c_{k-1} \pmod{p^{k-1}} \) az egyetlen olyan megoldása, amelyre \( c_{k-1} \equiv c \pmod{p} \).

Keressük meg a (1) kongruenciának a \( c_k \equiv c \pmod{p} \) feltételt is teljesítő megoldását. Nyilván \( c_k \) kielégíti (5)-öt is, tehát \( c_k \equiv c_{k-1} \pmod{p^{k-1}} \), azaz

\[
c_k = c_{k-1} + tp^{k-1}.
\]

Helyettesítsük be (6)-ot az (1) kongruenciába, és használjuk fel (3)-at (\( a = c_{k-1} \), \( j = k - 1 \) szereposztással). Ekkor az

\[
f(c_k) = f(c_{k-1} + tp^{k-1}) \equiv f(c_{k-1}) + tp^{k-1}f'(c_{k-1}) \equiv 0 \pmod{p^k}
\]

kongruenciához jutunk. Itt az indukciós feltevés miatt \( p^{k-1} \mid f'(c_{k-1}) \). A (7) kongruenciát \( p^{k-1} \)-gyel egyszerűsítve és \( c_{k-1} \equiv c \pmod{p} \) felhasználásával

\[
\frac{f(c_{k-1})}{p^{k-1}} + tf'(c) \equiv 0 \pmod{p}
\]
adódik. Ez lineáris kongruencia \( t \)-re, amelynek az \( f'(c) \neq 0 \pmod{p} \) feltétel miatt pontosan egy \( t \equiv t_0 \pmod{p} \) megoldása létezik. Innen \( t = t_0 + sp \), amit (6)-ba visszahelyettesítve kapjuk, hogy
\[
c_k = c_{k-1} + t_0p^{k-1} + sp^k, \quad \text{azaz} \quad c_k \equiv c_{k-1} + t_0p^{k-1} \pmod{p^k}.
\]
Ezzel beláttuk, hogy \( c_k \) létezik és mod \( p^k \) egyértelmű.

A bizonyítás alapján \( c = c_1 \)-ből kiindulva egymás után előállíthatjuk a \( c_2, c_3, \ldots \) értékeket, vagyis a \( c_k \) meghatározására egy rekurziós módszert kaptunk. (A \( c_k \) értékekre akár „ képletet” is nyerhetünk, lásd a 3.7.4 feladatot [99].)

Ha \( f'(c) \equiv 0 \pmod{p} \), akkor a (8) kongruenciának vagy minden \( t \) megoldása, vagy pedig egyáltalán nincs megoldása, attól függően, hogy \( p^k | f'(c_k-1) \) vagy sem. Ez azt jelenti, hogy az (5) kongruencia egy \( c_k-1 \) megoldásából vagy \( P \) darab megfelelő \( c_k \) értéket kapunk, vagy pedig egyet sem. Ilyenkor tehát a fenti rekurziós típusú eljárás alkalmazása jóval bonyolultabb.

Példa: Oldjuk meg az \( x^5 + 2x \equiv 22 \pmod{125} \) kongruenciát.

Először megoldjuk az
\[
f(x) = x^5 - 2x - 22 \equiv 0 \pmod{5}
\]
kongruenciát. A \( 0, \pm 1, \pm 2 \) modulo 5 teljes maradvérendszer elemeit behelyettesítsük, hogy az összes megoldás
(i) \( x \equiv 2 \pmod{5} \) és
(ii) \( x \equiv -1 \pmod{5} \).
(i) Az \( x \equiv 2 \pmod{5} \) esetben
\[
f'(2) = 3 \cdot 2^2 + 2 = -1 \pmod{5},
\]
ezért alkalmazhatjuk a T 3.7.1 Tételt.

Az \( x^5 + 2x - 22 = 0 \pmod{25} \) kongruenciában az \( x = 2 + 5t \) helyettesítést elvégezve a fentiek alapján
\[-10 + (5t) \cdot 14 \equiv 0 \pmod{25}, \quad \text{azaz} \quad -2 - t \equiv 0 \pmod{5}
\]
adódik, ahonnan \( t \equiv -2 \pmod{5} \), vagyis \( t = 5k - 2 \). Innen
\[
x = 2 + 5t = 2 + 5(5k - 2) = -8 + 25k.
\]
Ez azt jelenti, hogy az
\[
x^5 + 2x - 22 \equiv 0 \pmod{25}
\]
kongruenciának az \( x \equiv 2 \pmod{5} \) feltételt is kielégítő egyetlen megoldása \( x \equiv -8 \pmod{25} \).

Hasonlóan haladunk tovább az \( 5^2 \) modulusról az \( 5^3 \) modulusra. Írjuk be az
\[
x^5 + 2x - 22 \equiv 0 \pmod{125}
\]
kongruenciába \( x \) helyére a kapott \( x = -8 + 25s \) kifejezést. Ekkor
\[
-50 + (25s) \cdot 191 \equiv 0 \pmod{125}
\]
adódik. Innen \( s \equiv -2 \pmod{5} \), tehát
\[
x = -8 + 25s = -58 + 125s, \quad \text{azaz} \quad x = -58 \pmod{125}.
\]
(ii) Az \( x \equiv -1 \pmod{5} \) esetben \( f'(x) \equiv 0 \pmod{125} \), és így a bizonyítás után tett megjegyzés szerint minden lépésben azt kell vizsgálnunk, hogy a (8) kongruenciában a megfelelő \( f(c_\ell - 1) \) érték osztható-e \( p^k \)-val vagy sem.

Mivel \( f(-1) \equiv 0 \pmod{25} \), ezért minden \( x \equiv -1 \pmod{5} \) érték kielégíti az \( x^5 + 2x - 22 \equiv 0 \pmod{25} \) kongruenciát, azaz a megoldások
\[
x \equiv -1, 4, 9, 14 \text{és } 19 \pmod{25}.
\]
Ezek közül csak az utolsó kettőre lesz \( f(x) \) osztható 125-tel is, vagyis az \( x^5 + 2x - 22 \equiv 0 \pmod{125} \) kongruenciát
\[
x \equiv 14 \pmod{25} \quad \text{és} \quad x \equiv 19 \pmod{25}
\]
elégítik ki (ez \( 2 \cdot 5 = 10 \) maradékosztályt jelent modulo 125).

Összefoglalva, az \( x^2 + 2x \equiv 22 \pmod{125} \) kongruencia összes megoldását az alábbi 11 modulo 125 maradékosztály adja:
\[
-58, \quad 14 + 25j \quad \text{és} \quad 19 + 25j, \quad \text{ahol} \quad 0 \leq j \leq 4.
\]

Feladatok

3.7.1 Határozzuk meg az alábbi kongruenciák megoldásszámát:

(a) \( x^{30} + x^3 \equiv 8 \pmod{3^{20}} \);
(b) \( x^{93} + x^3 \equiv 8 \pmod{3^{20}} \);
(c) \( x^{60} \equiv 1 \pmod{73^{20}} \);
(d) \( x^{73} \equiv 1 \pmod{73^{20}} \);
(e) \( x(x - 1)(x - 2) \equiv 0 \pmod{10^{20}} \).

3.7.2 Legyen \( P \) prím, továbbá \( \alpha \) és \( \beta \) olyan pozitív egészek, amelyek nem oszthatók \( P \)-vel. Bizonyítsuk be, hogy ha az \( x^n \equiv \alpha \pmod{P} \) kongruencia megoldható, akkor bármely \( k \) esetén megoldható az \( x^n \equiv \alpha \pmod{P^k} \) kongruencia is.

3.7.3 Mely, a modulushoz relatív prím \( \alpha \) értékek esetén oldhatók meg az alábbi kongruenciák? Határozzuk meg a megoldásszámot is.
(a) \( x^{10} \equiv a \pmod{11^5} \);

(b) \((M \ [567]) \ast x^2 \equiv a \pmod{2^5} \).

3.7.4 Tegyük fel, hogy teljesülnek a T 3.7.1 Tétel feltételei, és legyen \( t \) egy olyan szám, amelyre \( \gcd(t', p) = 1 \). Bizonyítsuk be, hogy a \( c_k \) értékek az alábbi rekurzióval állíthatók elő:

\[
c_1 = c \quad \text{és} \quad c_k = c_{k-1} - tf(c_{k-1}), \quad \text{ha} \ k > 1.
\]

3.7.5 Oldjuk meg az \( x^6 + 4x = d \pmod{7^3} \) kongruenciát, ahol \( d \) értéke

(a) 3;

(b) 2;

(c) 72.
4. fejezet - LEGENDRE- ÉS JACOBI- SZIMBÓLUM

A prím modulusú másodfokú kongruenciák kezelésének alapvető eszköze a Legendre-szimbólum. Ennek tárgyalása során bebizonyítjuk többek között a nevezetes Gauss-lemmát és kvadratikus reciprocitási téttel is. A fejezet végén a Legendre-szimbólum általánosításával, a Jacobi- szimbólummal foglalkozunk.

4.1 Másodfokú kongruenciák

Ebben a pontban végig feltesszük, hogy \( p > 2 \) prim és \( \left( \frac{a}{p} \right) = 1 \).

A D 3.5.2 Definíció \( k = 2 \) speciális eseteként először definiáljuk a kvadratikus maradék, illetve kvadratikus nemmaradék fogalmát.

4.1.1 Definíció . \[ D 4.1.1 \]

Legyen \( p > 2 \) prim és \( \left( \frac{a}{p} \right) = 1 \). Az \( a \) számot aszerint nevezzük kvadratikus maradéknak, illetve kvadratikus nemmaradéknak modulo \( p \) , hogy az \( x^2 \equiv a \ (\text{mod} \ p) \) kongruencia megoldható-e, vagy sem. \( \Diamond \)

Az \( a \equiv 0 \ (\text{mod} \ p) \) számokat nem soroljuk sem a kvadratikus maradékok, sem a kvadratikus nemmaradékok közé.

4.1.2 Tétel . \[ T 4.1.2 \]

(i) Az \( a \) szám akkor és csak akkor kvadratikus maradék modulo \( p \) , ha \( a^{(p-1)/2} = 1 \ (\text{mod} \ p) \). Ezzel ekvivalens, hogy az \( a \) (bármyel primitív gyök szerinti) indexe páros.

(ii) Az \( a \) szám akkor és csak akkor kvadratikus nemmaradék modulo \( p \) , ha \( a^{(p-1)/2} \equiv -1 \ (\text{mod} \ p) \). Ezzel ekvivalens, hogy az \( a \) (bármyel primitív gyök szerinti) indexe páratlan.

(iii) A (páronként inkongruens) kvadratikus maradékok száma, illetve kvadratikus nemmaradékok száma egyaránt \( \left( p - 1 \right)/2 \).

(iv) Ha \( a \) kvadratikus maradék, akkor az \( x^2 \equiv a \ (\text{mod} \ p) \) kongruenciának két (páronként inkongruens) megoldása van. \( \Diamond \)

Bizonyítás: (i) és (ii) a T 3.5.3 Tételnek, (iv) pedig a T 3.5.1 Tétel egyik állításának a \( k = 2 \) speciális esete.

(i) alapján az is adódik, hogy \( a \) akkor és csak akkor kvadratikus nemmaradék, ha \( a^{(p-1)/2} \neq 1 \ (\text{mod} \ p) \), illetve ha az \( a \) indexe páratlan. Így (ii)-höz már csak az

\[ a^{\frac{p-1}{2}} \neq 1 \ (\text{mod} \ p) \iff a^{\frac{p-1}{2}} \equiv -1 \ (\text{mod} \ p) \quad (1) \]

ekvivalenciát kell igazolni. Mivel \( e^{k-1} \equiv 1 \ (\text{mod} \ p) \) és \( p \) prim, ezért csak \( a^{(p-1)/2} \equiv \pm 1 \ (\text{mod} \ p) \) lehetséges. Emellett \( p > 2 \) miatt \( 1 \neq -1 \ (\text{mod} \ p) \), és így (1) valóban teljesül. \( \blacksquare \)

4.1.3 Definíció . \[ D 4.1.3 \]
Az \( \left( \frac{a}{p} \right) \) Legendre-szimbólumot a következőképpen értelmezzük:

\[
\left( \frac{a}{p} \right) = \begin{cases} 
1, & \text{ha } a \text{ kvadratikus maradék } \pmod{p}; \\
-1, & \text{ha } a \text{ kvadratikus nemmaradék } \pmod{p}.
\end{cases}
\]

**Megjegyzés:** Időnként hasznos a Legendre-szimbólum definícióját a \( p \mid a \) esetre is kiterjeszteni, mégpedig az \( \left( \frac{a}{p} \right) = 1 \) értelmezéssel (lásd például a 4.1.15 feladatot [103]). Ha azonban ezt külön nem jelezzük, akkor a továbbiakban automatikusan az \( (a,p) = 1 \) feltételre szorítkozunk.

**Példa:** \( \left( \frac{5}{11} \right) = 1 \), mert az \( x^2 \equiv 2 \pmod{11} \) kongruencia megoldható; az egyik megoldás \( x \equiv 3 \pmod{11} \). A megoldhatóságot a

\[
2^{\frac{3-1}{2}} = 2^1 = 1 \pmod{11}
\]

feltétel ellenőrzésével is beláthatjuk.

A Legendre-szimbólum definícióját a T 4.1.2 Tétellel összevetve kapjuk, hogy bármely \( a \) esetén

\[
a^{\frac{x-1}{2}} = \left( \frac{a}{x} \right) \pmod{p}.
\]

A Legendre-szimbólum néhány fontos tulajdonságát az alábbi tételben foglaljuk össze.

**4.1.4 Tétel.**

(i) \( a \equiv b \pmod{p} \) \( \implies \) \( \left( \frac{a}{p} \right) = \left( \frac{b}{p} \right) \).

(ii) \( \left( \frac{ab}{p} \right) = \left( \frac{a}{p} \right) \left( \frac{b}{p} \right) \).

(iii) \( \left( \frac{-1}{p} \right) = \begin{cases} 
1, & \text{ha } p \equiv 1 \pmod{4}; \\
-1, & \text{ha } p \equiv -1 \pmod{4}.
\end{cases} \)

**Bizonyítás:** Mindhárom állítás azonnal adódik (2)-ből, ezt csak (ii)-re részletezzük:

\[
\left( \frac{ab}{p} \right) = (ab)^{\frac{x-1}{2}} = a^{\frac{x-1}{2}} b^{\frac{x-1}{2}} = \left( \frac{a}{p} \right) \left( \frac{b}{p} \right) \pmod{p}.
\]

Így

\[
K = \left( \frac{ab}{p} \right) - \left( \frac{a}{p} \right) \left( \frac{b}{p} \right)
\]

eygérészt osztható \( p > 2 \) -vel, másrészt \( K \) értéke csak 0 vagy 1 lehet, vagyis valóban \( K = 0 \). □

A T 4.1.4 Tétel alapján a Legendre-szimbólum számolása visszavezethető a \( \left( \frac{2}{p} \right) \) és \( \left( \frac{q}{p} \right) \) értékek meghatározására, ahol \( q > 2 \) a \( p \)-től különböző prím. Az erre vonatkozó eredményeket a következő pontban tárgyaljuk.
Feladatok

(A $P$ végig egy 2-nél nagyobb prímszámot jelöl.)

4.1.1 Bizonyítsuk be három különböző módon, hogy $(r, P) = 1$ esetén a $r^2$ kvadratikus maradék mod $P$.

4.1.2 Számítsuk ki az alábbi Legendre-szimbólumok értékét:

(a) \( \left( \frac{39}{13} \right) \);

(b) \( \left( \frac{37}{19} \right) \);

(c) \( \left( \frac{160}{17} \right) \).

4.1.3 Számítsuk ki az

\[ \left( \frac{1}{P} \right), \left( \frac{2}{P} \right), \ldots, \left( \frac{p-1}{P} \right) \]

Legendre-szimbólumok összegét és szorzatát.

4.1.4 Lássuk be, hogy bármely kvadratikus maradék az

\[ 1^2, 2^2, \ldots, \left( \frac{P-1}{2} \right)^2 \]

számok közül pontosan eggyel kongruens modulo $P$.

4.1.5 Igazoljuk, hogy ha $a^2 + b^2$ osztható 77-tel, akkor osztható 5929-cel is.

4.1.6 Legyen $P$ egy $4k + 1$ alakú prím. Bizonyítsuk be, hogy az $x^2 \equiv -1 \,(\text{mod } P)$ kongruencia megoldásai

\[ x = \pm \left( \frac{P-1}{2} \right)! \,(\text{mod } P). \]

4.1.7 Legyen $P$ egy $4k + 3$ alakú prím és $a$ kvadratikus maradék mod $P$. Bizonyítsuk be, hogy az $x^2 \equiv a \,(\text{mod } P)$ kongruencia megoldásai

\[ x = \pm a^{\frac{P+3}{4}} \,(\text{mod } P). \]

4.1.8 (a) Bizonyítsuk be, hogy ha $\alpha_k(a)$ páratlan, akkor $a$ kvadratikus maradék mod $P$.

(b) Mely $P$ primek esetén igaz a fenti állítás megfordítása?

4.1.9 (a) Bizonyítsuk be, hogy egy primitív gyök szükségképpen kvadratikus nemmaradék modulo $P$.

(b) Mely $P$ primek esetén igaz a fenti állítás megfordítása?

4.1.10 Tegyük fel, hogy $(r, 97) = 1$, a $c$ kvadratikus nemmaradék és nem primitív gyök mod 97. Számítsuk ki $\alpha_{97}(c)$ értékét.
4.1.11 Bizonyítsuk be, hogy ha

(a) \( p = 4k - 1 \);
(b) \( p = 4k + 1 \), akkor az \( x^2 \equiv k \pmod{p} \) kongruencia megoldható.

4.1.12 Mutassuk meg, hogy bármely \( P \) esetén az alábbi mod \( P \) kongruenciák közül legalább az egyik biztosan megoldható:

\[
\begin{align*}
72^2 &
= 30, \\
52^2 &
= 33, \\
43^2 &
= 70, \\
32^2 &
= 105 \quad \text{és} \\
22^2 &
= 165.
\end{align*}
\]

4.1.13 Oldjuk meg az alábbi kongruenciákat:

(a) \((\text{M}[567])\) \(3x^2 + 5x + 5 \equiv 0 \pmod{13} \);
(b) \(7x^2 + 8x \equiv 5 \pmod{17} \);
(c) \(6x^2 - x^2 + 3x \equiv 0 \pmod{23} \);
(d) \(2x^2 + 5x + 1 \equiv 0 \pmod{19} \).

4.1.14 Jelöljük \( \mu(p) \) -vel a legkisebb olyan pozitív egész, amely kvadratikus nemmaradék mod \( P \).

Például \( \mu(5) = 2, \mu(7) = 3 \) . Bizonyítsuk be, hogy

(a) \( \mu(p) \) mindig primszám;
(b) \( \mu(p) < 1 + \sqrt{p} \).

4.1.15 Terjesszük ki a Legendre-szimbólum definícióját a \( \mu(u) \) esetre az \( \frac{(u)}{p} = 0 \) értelmezéssel. Legyen továbbá

\[
S(u, p) = \sum_{i=1}^{p-1} \left( \frac{i+u}{p} \right).
\]

Bizonyítsuk be, hogy

(a) \( S(0, p) = p - 1 \);
(b) \( \mu(p) = 1 \implies S(u, p) = S(1, p) \);
(c) \( \sum_{u=0}^{p-1} S(u, p) = 0 \);
(d) \( S(1, p) = -1 \).

4.1.16 Jelölje \( M(p) \) azoknak az \( 1 \leq \omega \leq p - 2 \) értékeknek a számát, amelyekre \( u \) és \( u + 1 \) is kvadratikus maradék mod \( P \).

(a) Bizonyítsuk be, hogy

\[
4M(p) = \sum_{\omega=1}^{p-2} \left( \frac{\omega}{p} \right) + 1 \left( \frac{\omega+1}{p} \right) + 1.
\]
(b) Mutassuk meg, hogy $M(p)$ „körülbelül“ $p/4$; ha $p = 4k \pm 1$, akkor $M(p) = k - 1$.

### 4.2 Kvadratikus reciprocitás

Ebben a pontban is feltesszük, hogy $p > 2$ prim. A $\left(\frac{2}{p}\right)$ és $\left(\frac{q}{p}\right)$ Legendre-szimbólumokra vonatkozó tételeket fogunk bizonyítani, ahol $q > 2$ a $P$-től különböző prim. Mindkét eredményhez szükségünk lesz az alábbi lemmára:

#### 4.2.1 Tétel (Gauss-lemma).

Legyen $(a,p) = 1$, és tekintsük az $a, 2a, \ldots, \frac{p-1}{2}a$ számok modulo $p$ vett legkisebb pozitív maradékait. Jelölje $u$ ezek közül a $\frac{p}{2}$-nél nagyobbak számát. Ekkor

$$\left(\frac{a}{p}\right) = (-1)^{v}.$$  

**Bizonyítás:** Az adott $\frac{p-1}{2}$ szám legkisebb pozitív maradékai közül a $\frac{p}{2}$-nél kisebbeket jelölje $r_1, \ldots, r_u$, a $\frac{p}{2}$-nél nagyobbakat pedig $p - r_1, \ldots, p - r_u$ (ahol $u + v = \frac{p-1}{2}$). Így bármely $1 \leq t \leq \frac{p-1}{2}$ esetén alkalmas $i$ -vel vagy $j$ -vel

$$i = \begin{cases} \text{vagy } r_i, & (i \text{ osztja } p) \\ \text{vagy } p - s_j, & i \text{ osztja } p \end{cases}$$  \hspace{1cm} (1)

teljesül. Itt az $r_i$ és $s_j$ számok valamennyien az $1, 2, \ldots, \frac{p-1}{2}$ értékek közül kerülnek ki.

Megmutatjuk, hogy az $r_i$ és $s_j$ számok mind különbözők, és így valamilyen sorrendben az $1, 2, \ldots, \frac{p-1}{2}$ számokkal egyeznek meg.

Ha valamely $i \neq k$ -ra $r_i = r_k$, akkor alkalmas $1 \leq \lambda < \mu \leq \frac{p-1}{2}$ számokkal

$$\lambda a \equiv r_i - r_k \equiv \mu a \pmod{p}$$

teljesül. Mivel $(a, p) = 1$, ezért $a$ -val egyszerűsítve $\lambda \equiv \mu \pmod{p}$ adódik, ami ellentmondás.

Hasonlóan jutunk ellentmondásra két $s_j$ egyenlőségéből is.

Végül, ha $r_i = s_j$, akkor

$$\lambda a \equiv r_i - s_j \equiv -\mu a \pmod{p},$$

azaz $p \mid (\lambda + \mu)$ . Azonban $(a, p) = 1 \text{ és } 0 < \lambda + \mu < p$, így egyik tényleg sem osztható $p$ -vel, ami ellentmond a $p$ prim voltának.

Szorozzuk most össze az (1) kongruenciákat:

$$\left(\frac{p-1}{2}\right)_{\lambda \equiv 1} = r_1 \ldots r_u (p - s_1) \ldots (p - s_v) \equiv (-1)^{v} r_1 \ldots r_u s_1 \ldots s_v = (-1)^{v} \left(\frac{\frac{p-1}{2}}{2}\right) \pmod{p}. \hspace{1cm} (2)$$

104
A (2) kongruenciát a \( p \)-hez relatív prim \( \left( \frac{\nu - 1}{2} \right) \)-sal egyszerűsíte adódik

\[
\nu \equiv \left( \frac{\nu - 1}{2} \right) \equiv (-1)^\nu \pmod{p}, \quad \text{azaz} \quad \left( \frac{\nu}{p} \right) = (-1)^\nu.
\]

A Gauss-lemma segítségével könnyen meghatározhatjuk, hogy a 2 mely primekre nézve lesz kvadratikus maradék.

4.2.2 Tétel. T 4.2.2

\[
\left( \frac{\nu}{p} \right) = \begin{cases} 
1, & \text{ha} \ p \equiv 1 \pmod{8}; \\
-1, & \text{ha} \ p \equiv 3 \pmod{8}.
\end{cases}
\]

Bizonyítás: A Gauss-lemmát alkalmazzuk \( \nu = 2 \)-re: megvizsgáljuk, hogy a \( \nu \)-nél nagyobb \( \nu \) számok közül hány nagyobb \( \frac{\nu}{2} \)-nél.

A számok száma összesen \( \frac{\nu - 1}{2} \), ebből a \( \frac{\nu}{2} \)-nél kisebbek száma \( \left( \frac{\nu - 1}{2} \right) \), tehát a keresett \( \nu \) érték

\[
\nu = \frac{\nu - 1}{2} = \left( \frac{\nu - 1}{4} \right).
\]

Ha \( \nu = 8k + 1 \), akkor így \( \nu = 4k - 2k = 2k \), vagyis \( \left( \frac{2}{p} \right) = \left( -1 \right)^{2k} = 1 \).

Hasonlóan kapjuk a tétel állítását a \( p = 8k \pm 3 \) és \( 8k - 1 \) esetekben is. ■

Könnyen ellenőrizhető, hogy a T 4.2.2 Tétel a

\[
\left( \frac{2}{p} \right) = (-1)^{(\nu - 1)/8}
\]

alakban is felírható.

Most ráterünk a Legendre-szimbólumokra vonatkozó legfontosabb eredmény kimondására és igazolására.

4.2.3 Tétel (Kvadratikus reciprocitási tétel). T 4.2.3

Ha \( \nu > 2 \) és \( q > 2 \) két különböző prim, akkor

\[
\left( \frac{\nu}{p} \right) \left( \frac{\nu}{q} \right) = (-1)^{\frac{\nu - 1}{2} \cdot \frac{\nu - 1}{2}},
\]

azaz

\[
\left( \frac{\nu}{pq} \right) = \begin{cases} 
\left( \frac{\nu}{p} \right), & \text{ha} \ p = q = 1 \pmod{4}; \\
\left( \frac{\nu}{q} \right), & \text{egyéb esetek}.\ 
\end{cases}
\]

Bizonyítás: Az alábbi két állítást fogjuk igazolni:

(A) Ha \( \left( \nu, p \right) = 1 \) és \( \nu \) páratlan, akkor

105
\[
\left( \frac{\omega}{p} \right) = (-1)^w, \quad \text{ahol} \quad w = \sum_{l=1}^{\frac{p-1}{2}} \left\lfloor \frac{lu}{p} \right\rfloor.
\] (4)

(B) Ha \( b \) és \( c \) páratlan, 1-nél nagyobb, relatív prim számok, akkor

\[
\left( \frac{c}{b} \right) = \left( \frac{c}{b} \right)^{\frac{b-1}{2}} \left( \frac{c}{b} \right)^{\frac{b-1}{2}} = \left( \frac{b-1}{2} \right) \left( \frac{c-1}{2} \right).
\] (5)

Ezekből a T 4.2.3 Tétel már következik: (4) alapján

\[
\left( \frac{q}{p} \right) \left( \frac{\nu}{q} \right) = (-1)^z, \quad \text{ahol} \quad z = \sum_{\mu=1}^{\frac{p-1}{2}} \left\lfloor \frac{\nu q}{p} \right\rfloor = \sum_{v=1}^{\frac{p-1}{2}} \left\lfloor \frac{\nu q}{q} \right\rfloor,
\]
és itt (5) szerint

\[ z = \frac{p-1}{2}, \quad \frac{q-1}{2}, \]

tehát (3) valóban teljesül.

(A) bizonyításánál a Gauss-lemmára (T 4.2.1 Tétel) támaszkodunk. Az ottani jelöléseket fogjuk használni. Elég azt igazolnunk, hogy

\[
\omega = \sum_{t=1}^{\frac{p-1}{2}} \left\lfloor \frac{tu}{p} \right\rfloor = u \mod 2.
\] (6)

Az (1) kongruenciákat a maradékos osztás alapján a következőképpen írhatjuk át egyenlőséggé:

\[
\tau_a = \left\lfloor \frac{ta}{p} \right\rfloor + \begin{cases} v; & \text{vagy } r; \\ v-p-s_j; & \text{vagy } p-s_j. \end{cases}
\] (7)

A (7) egyenlőségeket \( t = 1, 2, \ldots, \frac{p-1}{2} \)-re összegezve

\[
\left( 1 + 2 + \cdots + \left\lfloor \frac{p-1}{2} \right\rfloor \right) a = p \sum_{t=1}^{\frac{p-1}{2}} \left\lfloor \frac{tu}{p} \right\rfloor + \sum_{i=1}^{u} r_i = \sum_{j=1}^{v} (p-1) + \sum_{j=1}^{v} r_j
\]

adódik. Ezt átrendezve, és felhasználva, hogy \( r_1, \ldots, r_v, s_1, \ldots, s_v \) az \( 1, 2, \ldots, \frac{p-1}{2} \) számok egy permutációját alkotják, a következő összefüggést kapjuk:

\[
\left( 1 + 2 + \cdots + \left\lfloor \frac{p-1}{2} \right\rfloor \right) (u - 1) + 2 \sum_{j=1}^{v} s_j = p \left( \sum_{i=1}^{(p-1)/2} \left\lfloor \frac{tu}{p} \right\rfloor + v \right).
\] (8)

Mivel \( a \) páratlan, ezért (8) bal oldala páros szám, és így (\( p > 2 \) miatt) (6) valóban teljesül.

(B) bizonyításához tekintsük a sikon a

\[ A = \left( \frac{1}{2}, \frac{1}{2} \right), \quad B = \left( \frac{b}{2}, \frac{1}{2} \right), \quad C = \left( \frac{b}{2}, \frac{c}{2} \right) \quad \text{és} \quad D = \left( \frac{1}{2}, \frac{c}{2} \right). \]
pontok által meghatározott \( T \) téglalapot. Ekkor (5) jobb oldalán nyilván a \( T \) belsejébe eső egész koordinátájú pontok (az ún. rácspontok) száma áll.

Megmutatjuk, hogy (5) bal oldala is a fenti rácspontok számával egyenlő. Vágjuk ketté a \( T \) téglalapot az \( A \) és \( C \) csúcsokat összekötő \( y = \frac{1}{2}x \) egyenletű átlóval. Magára az átlóra \( (b, c) = 1 \) miatt nem esik rácspont.

Most megszámoljuk az \( \overline{ABC} \) („alsó”) háromszög belsejébe eső rácspontok számát, jelöljük ezt \( u \) -nel. Vizsgáljuk meg, hány rácspont helyezkedik el az \( x = \nu \) egyenletű („függőleges”) egyenesnek a háromszögbe eső részén. Ezeknek a rácspontoknak az első koordinátája \( \nu \). A második koordinátát \( y \)-nal jelölve az \( 1 \leq y < \frac{1}{2} \nu \) egyenlőtlenségnek kell teljesülnie. Az ilyen \( y \)-ok száma tehát \( \left\lfloor \frac{1}{2} \nu \right\rfloor \). Az \( \overline{ABC} \) háromszög belsejébe eső rácspontok számát innen úgy kapjuk, hogy a \( \left\lfloor \frac{1}{2} \nu \right\rfloor \) értékeket összegezzük \( \nu = 1, 2, \ldots, \frac{b - 1}{2} \)-re, azaz

\[
\nu = \sum_{\nu=1}^{(b-1)/2} \left[ \frac{\nu c}{b} \right].
\]

Ez éppen az (5) bal oldalán szereplő második összeg.

Hasonlóan igazolható, hogy ha az \( \overline{ACD} \) háromszög belsejébe eső rácspontokat az \( y = \frac{1}{2}x \) („vízszintes”) egyenesek mentén számoljuk meg, akkor az (5) bal oldalán szereplő első összeget kapjuk. Ezzel (5)-öt beláttuk, és így a T 4.2.3 Tétel bizonyítását befejeztük. □

Az alábbi példával azt illusztráljuk, hogyan használhatók a T 4.1.4, T 4.2.2 és T 4.2.3 Tételek a Legendre-szimbólum értékének meghatározásánál.

**Példa:** Megoldható-e az \( x^2 \equiv 198 \pmod{1997} \) kongruencia? (Az 1997 prímszám.)

A 198 kanonikus alakja \( 198 = 2 \cdot 3^2 \cdot 11 \), ezért

\[
\left( \frac{198}{1997} \right) = \left( \frac{2}{1997} \right) \left( \frac{3^2}{1997} \right) \left( \frac{11}{1997} \right) = -1 \cdot 1 \cdot (-1) = 1.
\]

Mivel \( 1997 \equiv -3 \pmod{8} \), így a T 4.2.2 Tétel szerint \( \left( \frac{2}{1997} \right) = -1 \). Mivel \( 1997 \equiv 1 \pmod{4} \), így a T 4.2.3 Tétel, majd \( 1997 \equiv -3 \pmod{11} \), stb. felhasználásával

\[
\left( \frac{11}{1997} \right) = \left( \frac{1997}{11} \right) = \left( \frac{-3}{11} \right) = \left( \frac{5}{11} \right) = (-1) \left( \frac{11}{5} \right) = (-1) \left( \frac{1}{5} \right) = -1.
\]

Tehát

\[
\left( \frac{198}{1997} \right) = (-1) \cdot 1 \cdot (-1) = 1,
\]

vagyis az \( x^2 \equiv 198 \pmod{1997} \) kongruencia megoldható.

Nagyon nagy számok esetén a fenti módszer problematikus pontja az, amikor az eljárással közben keletkező Legendre-szimbólumok „számítási” faktorizálni kell, amiire nem ismeretes gyors algoritmus. A következő pontban látni fogjuk, hogy ez a probléma a Jacobi-szimbólum segítségével kiküszöbölhető.
Feladatok

4.2.1 Melyek oldhatók meg az alábbi kongruenciák közül:

(a) \( x^2 \equiv 66 \pmod{191} \);
(b) \( x^2 \equiv 71 \pmod{83} \);
(c) \( x^2 \equiv 94 \pmod{101} \);
(d) \( x^2 \equiv 30 \pmod{77} \);
(e) \( x^2 \equiv 38 \pmod{187} \);
(f) \( 2x^2 + 3x + 5 \equiv 0 \pmod{101} \).

4.2.2 Milyen \( p > 2 \) primekre oldhatók meg az alábbi kongruenciák:

(a) \( x^2 \equiv -2 \pmod{p} \);
(b) \( x^2 \equiv 3 \pmod{p} \);
(c) \( x^2 \equiv -3 \pmod{p} \);
(d) \( x^2 \equiv 5 \pmod{p} \);
(e) \( x^4 \equiv 4 \pmod{p} \);
(f) \( x^4 \equiv -4 \pmod{p} \);
(g) \( x^8 \equiv 16 \pmod{p} \);
(h) \( x^8 \equiv 81 \pmod{p} \).

4.2.3 Bizonyítsuk be, hogy ha \( 1999 \mid a^2 + b^2 \), akkor \( 1999 \mid a \) és \( 1999 \mid b \).

4.2.4 (*) Bizonyítsuk be, hogy van olyan \( c \), amelyre \( 43^{100} \mid 2c^8 + 1 \).

4.2.5 Mutassuk meg, hogy

(a) egy \( 8c^2 - 1 \) alakú (pozitív) számnak minden prímosztója \( 8k \pm 1 \) alakú és biztosan van \( 8k - 1 \) alakú prímosztója;

(b) egy \( 12c^2 - 1 \) alakú (pozitív) számnak minden prímosztója \( 12k \pm 1 \) alakú és biztosan van \( 12k - 1 \) alakú prímosztója;

(c) egy \( c^2 + 4 \) alakú páratlan számnak biztosan van \( 8k + 5 \) és \( 3 \mid c \) esetén \( 12k + 5 \) alakú prímosztója is (ez a két prímosztó lehet ugyanaz).

4.2.6 Legyenek \( \nu_1, \nu_2, \nu_3, \nu_4, \nu_5 \) különböző páratlan primek, \( P = \nu_1 \cdots \nu_3 \) és \( a_i = P/\nu_i \), \( i = 1, 2, 3, 4, 5 \).
(a) Igazoljuk, hogy az
\[ x_i^2 \equiv a_i \pmod{p_i}, \quad i = 1, 2, 3, 4, 5 \]
kongruenciák közül a megoldhatók száma akkor és csak akkor páros, ha
\[ \sum_{i=1}^{5} \left( \frac{-1}{p_i} \right) = \pm 1. \]

(b) Tegyük fel, hogy a
\[ x_i^2 \equiv a_i \pmod{m} \quad (m > a_i), \quad i = 1, 2, 3, 4, 5 \]
kongruenciák mindegyike megoldható. Lássuk be, hogy ekkor
\[ \sum_{i=1}^{5} \left( \frac{-1}{p_i} \right) \geq 3. \]

4.2.7 (a) Bizonyítsuk be, hogy 19 egymást követő egész szám négyzetének az összege nem lehet teljes hatvány.

(b) Mutassuk meg, hogy az (a)-beli állítás 19 helyett bármilyen \(12k + 5\) alakú prímszámra is igaz.

4.2.8 (M [568]**) Adjunk meg olyan \( f \) egész együthattós polinomot, amelyre az \( f(x) = 0 \)
eyenletnek nincs racionális gyöke, de az \( f(x) \equiv 0 \pmod{m} \) kongruencia minden \( m \)-re megoldható.

4.3 Jacobi-szimbólum

4.3.1 Definíció . D 4.3.1

Legyen \( m > 1 \) páratlan szám, \( m = p_1 \cdots p_r \), ahol a \( p_i \) számok (nem feltétlenül különböző) pozitív
prímek. Legyen továbbá \( (a, m) = 1 \). Ekkor az \( \left( \frac{a}{m} \right) \) Jacobi-szimbólumot mint az \( \left( \frac{a}{m} \right) \) Legendre-
szimbólumok szorzatát értelmezzük:

\[ \left( \frac{a}{m} \right) = \left( \frac{a}{p_1} \right) \cdots \left( \frac{a}{p_r} \right). \]

Példa: \( \left( \frac{1}{10} \right) = \left( \frac{1}{2} \right)^2 \left( \frac{1}{5} \right) = \left( \frac{1}{5} \right) = -1. \)

Ha \( m \) prim, akkor a Jacobi-szimbólum megegyezik a Legendre-szimbólummal. Ennél fogva nem
okozhat problémát, ha mindkettőt ugyanúgy jelöljük.

A primeknél tapasztaltakkal szemben összetett \( m \) esetén az \( x^2 \equiv a \pmod{m} \) kongruencia
megoldhatósága nem karakterizálható az \( \left( \frac{a}{m} \right) \) Jacobi-szimbólum segítségével (lásd a
4.3.2 feladatot [111]).

A Jacobi-szimbólum ugyanakkor „átöröktí” a Legendre-szimbólumnak a T 4.1.4, T 4.2.2 és T
4.2.3 Tételekben tárgyalt tulajdonságait:

4.3.2 Tétel . T 4.3.2
Tegyük fel, hogy a szereplő Jacobi-szimbólumok értelmesek, azaz a „nevező” egy 1-nél nagyobb páratlan szám, amely relatív prim a „számlálóhoz” (tehát pl. (v)-ben \( m \) és \( n \) relatív prim, 1-nél nagyobb páratlan számok).

(i) \( a \equiv b \pmod{m} \Rightarrow \left( \frac{a}{m} \right) = \left( \frac{b}{m} \right) \).

(ii) \( \left( \frac{a^2}{m} \right) = \left( \frac{a}{m} \right)^2 \), \( \left( \frac{a}{mn} \right) = \left( \frac{a}{m} \right) \left( \frac{a}{n} \right) \).

(iii) \( \left( \frac{1}{m} \right) = \begin{cases} 1, & \text{ha } m \equiv 1 \pmod{4}; \\ -1, & \text{ha } m \equiv -1 \pmod{4}. \end{cases} \)

(iv) \( \left( \frac{2}{m} \right) = \begin{cases} 1, & \text{ha } m \equiv \pm 1 \pmod{8}; \\ -1, & \text{ha } m \equiv \pm 3 \pmod{8}. \end{cases} \)

(v) \( \left( \frac{n^2}{m} \right) = \begin{cases} -\left( \frac{n}{m} \right), & \text{ha } n \equiv m \equiv -1 \pmod{4}; \\ \left( \frac{n}{m} \right), & \text{egyébként}. \end{cases} \)

Bizonyítás: Valamennyi tulajdonság következik a Jacobi-szimbólum definíciójából és a Legendre-szimbólum megfelelő tulajdonságából. Ezt részletesen megmutatjuk (v)-re (azaz a reciprocitási tétel megfelelőjére), a többi hasonlóan igazolható.

Legyen \( n = p_1 \cdots p_r \), \( \nu = q_1 \cdots q_s \) (ahol \( p_i \neq q_j \)). Ekkor a Jacobi-szimbólum definíciója és a Legendre-szimbólum multiplikativitása (vagy a jelen tétel (ii) tulajdonságai) alapján

\[
\left( \frac{n}{m} \right) = \prod_{1 \leq j \leq r} \left( \frac{p_j}{m} \right), \quad \left( \frac{\nu}{m} \right) = \prod_{1 \leq j \leq s} \left( \frac{q_j}{m} \right). \tag{1}
\]

Legyen a \( p_i \cdot q_j \)-k közül \( \ell \) darab, a \( q_j \cdot p_i \)-k közül \( v \) darab \( 4k - 1 \) alakú. Erre az \( uv \) számú \( p \cdot q \) párra

\( \left( \frac{p_i}{q_j} \right) = -\left( \frac{q_j}{p_i} \right) \), az összes többi párra pedig \( \left( \frac{x}{y} \right) = \left( \frac{y}{x} \right) \). Ezért (1) alapján

\[
\left( \frac{\nu}{m} \right) = \left( \frac{n}{m} \right) \iff \nu \text{ páratlan } \iff \\
\quad \nu \text{ és } v \text{ páratlan } \iff \nu v = n = -1 \pmod{4}.
\]

Példa: Megoldható-e az \( x^2 \equiv 23 \pmod{11239} \) kongruencia? (A 11239 prím szám.)

Az \( \left( \frac{23}{11239} \right) \) Legendre-szimbólumot Jacobi-szimbólumként, a T.4.3.2 Tétel felhasználásával számíthatuk ki. Ennek az lesz az előnye, hogy a „számlálódból” mindig csak a legnagyob kettőhatványokat kell leválasztani, a páratlan részt nem kell faktorizálni, hanem azonnal lehet a reciprocitást alkalmazni.

\[
\begin{align*}
\left( \frac{23}{11239} \right) &= \left( \frac{2}{11239} \right) \left( \frac{1171}{11239} \right) \left( \frac{11239}{1171} \right) = \left( \frac{-1}{1171} \right) \left( \frac{471}{1171} \right) = \left( \frac{-1}{1171} \right) \left( \frac{471}{471} \right) = \left( \frac{471}{471} \right) = 1.
\end{align*}
\]

A kongruencia tehát megoldható.

Vegyük észre, hogy a fenti eljárás az euklideszi algoritmus egy variánsának tekinthető.
A Jacobi-szimbólum a prímtesztelésnél is fontos szerephez jut (lásd az T 5.7.4 Tételt).

**Feladatok**

4.3.1 Számítsuk ki az alábbi Jacobi-szimbólumokat:

(a) \( \left( \frac{1234567}{2345} \right) \);  
(b) \( \left( \frac{31}{35} \right) \);  
(c) \( \left( \frac{560}{1999} \right) \);  
(d) \( \left( \frac{1113}{11351} \right) \).

4.3.2 Legyen \( m \geq 1 \) páratlan szám és \( (a, m) = 1 \).

(a) Bizonyítsuk be, hogy ha az \( x^2 = a \pmod{m} \) kongruencia megoldható, akkor \( \left( \frac{a}{m} \right) = 1 \).

(b) Mutassunk példát, hogy az (a)-beli állítás megfordítása nem igaz.

(c) Melyek azok az \( m \)-ek, amelyekre az (a)-beli állítás megfordítása is igaz?

4.3.3 Bizonyítsuk be, hogy ha \( p \) prim és \( p = a^2 + b^2 \), akkor az

\[ x^2 = a \pmod{p} \quad \text{és} \quad x^2 = b \pmod{p} \]

kongruenciák közül legalább az egyik megoldható.

4.3.4 Számítsuk ki a Jacobi-szimbólumokból képezett alábbi összegeket:

(a) \( \sum_{k=1}^{111} \left( \frac{2}{k+1} \right) \);  
(b) \( \sum_{k=1}^{111} \left( \frac{k}{2k+1} \right) \).

4.3.5 Legyenek az \( a, m, n \) számok 1-nél nagyobbak, \( m \) és \( n \) páratlan, továbbá \( (a, m) = (a, n) = 1 \).

(a) Bizonyítsuk be, hogy ha \( a \equiv 0 \pmod{4} \), akkor

\[ m = n \pmod{a} \implies \left( \frac{a}{m} \right) = \left( \frac{a}{n} \right). \]

(b) Mutassuk meg, hogy ha \( a \equiv 2 \pmod{4} \), akkor létezik olyan \( m \) és \( n \), hogy

\[ m = n \pmod{a}, \quad \text{de} \quad \left( \frac{a}{m} \right) \neq \left( \frac{a}{n} \right). \]

4.3.6 Legyen \( mn \geq 1 \) páratlan szám. Számítsuk ki a Jacobi-szimbólumokból képezett alábbi összeget és szorzatot:

\[ \sum_{1 \leq i \leq m} \left( \frac{i}{m} \right) \];
4.3.7 (a) Adjuk meg az összes olyan $m > 1$ páratlan számot, amelyre bármely $(a, m) = 1$ esetén az $\left( \frac{a}{m} \right)$ Jacobi-szimbólum értéke 1.

(b) * (M [568]) Adjuk meg az összes olyan $a$ egészt, amelyre bármely $m > 1$ páratlan szám és $(a, m) = 1$ esetén az $\left( \frac{a}{m} \right)$ Jacobi-szimbólum értéke 1.
5. fejezet - PRÍMSZÁMOK

A prímszámok a matematika egyik legegyszerűbben megadott, ugyanakkor talán legtitokzatosabb
halmazát alkotják. Már Euklidész Elemei című könyvében szerepel annak bizonyítása, hogy végtelen
sok prímszám van, azonban ma sem tudjuk, hogy például végtelen sok ikerprím létezik-e. Néhány
ilyen híres, egyszerűen megfogalmazható, ugyanakkor reménytelenül nehéz megoldatlan probléma
bemutatása után speciális alakú primekkel foglalkozunk: a Fermat- és Mersenne-primekkel, illetve
számtani sorozatok prímszámaiaval. A prímszámok eloszlásával kapcsolatban alsó és felső becslést
adunk az ő -nél nem nagyobb prímszámok számára, továbbá a szomszédos primek közötti hézagot,
valamint a primek reciprokösszegét vizsgáljuk. Végül azt a kérdéskört tanulmányozzuk, hogy hogyan lehet
egy nagy számról a gyakorlatban is előtérbe puszista (legalábbis jelenlegi tudásunk szerint), és bemutatjuk az ezen az eltérésen
alapuló, széles körben alkalmazott nyilvános titkosírást, az RSA-sémat.

5.1 Klasszikus problémák

Ebben a fejezetben primen végig pozitív prímszámot értünk (a „prímszám” szó tulajdonképpen pozitív
felbonthatatlan szám értelemben szerepel majd általában), és ő -vel mindig (pozitív) prímszámot
jelölünk (tehát például  a 0,1 intervallumba eső primek sorozatát jelenti).

Először az ókori görög matematika két nevezetes eredményét tárgyaljuk.

5.1.1 Tétel . T 5.1.1

A prímszámok száma végtelen.

Bizonyítás: Tegyük fel indirekt, hogy csak véges sok prímszám létezik, legyenek ezek
p₁(= 2), ..., pᵣ. Tekintsük az  a = p₁ ... pᵣ + 1 számot.

Az  nyilván a p₁, ..., pᵣ prímszámok egyikével sem osztható.

Ugyanakkor minden 1-nél nagyobb számnak, így  -nak is létezik prímosztója. Ez szükségképpen
különbözik a p₁, ..., pᵣ primektől, ami ellentmond az indirekt feltevések.

Megjegyzés: A bizonyításból az is leolvasható, hogy

\[ p_n < \sqrt{2^n}, \]

ahol  az  n.-edik prímszámot jelöli (5.1.9a feladat [117]). Ennél lényegesen jobb felső becslést
fogunk megadni az 5.4 pontban.

Most az eratosthenesi szitaét mutatjuk be. Ez egy olyan eljárás, amellyel előállíthatjuk egy adott  számig az összes prímszámot.

5.1.2 Tétel (Eratosthenesi szita) . T 5.1.2

Írjuk fel 2-tól  -ig az egész számokat. Az első lépésben karikázzuk be a 2-t, majd húzzuk át azokat
a számokat, amelyek a 2 többszörösei és 2-nél nagyobbak: 4, 6, 8, .... Ezután karikázzuk be azt a
legkisebb számot, amely még nincs megjelölve (azaz nincs bekarikázva és nincs áthúzva); ez a 3, majd
húzzuk át ennek a nála nagyobb többszöröseit: 6, 9, .... (a 6-ot, 12-t stb. már másodsor húzzuk át).

Ismételjük meg a fentieket mindig a legkisebb még jelölten számmal, ha ez a szám még legfeljebb
\[ \sqrt{N} \]. Ha már minden  nél nem nagyobb számot megjelöltünk, akkor álljunk meg.
Ekkor a bekarikázott és a jelölhetetlen számok együttesen éppen az \( \sqrt{N} \)-nél nem nagyobb prímszámokat adják (a bekarikázottak lesznek a \( \sqrt{N} \)-nél nem nagyobb, a jelölhetetlenek pedig a \( \sqrt{N} \) és \( N \) közötti primek). ♦

**Bizonyítás:** Az áthúzott számok nyilván összetettnek hiszen van egy náluk kisebb, de \( 1 \)-nél nagyobb osztója.

A bekarikázott számokról teljes indukcióval igazoljuk, hogy felbonthatlanok. Az első bekarikázott szám, a 2 felbonthatatlan. Legyen \( s \leq \sqrt{N} \) a \( k \)-adik bekarikázott szám, és tegyük fel, hogy az első \( k - 1 \) bekarikázott szám alkotja az összes \( s \)-nél kisebb felbonthatatlan számot. Ekkor \( s \)-nek ezek egyike sem osztója (hiszen \( s \)-et egyszer sem húztuk át), tehát \( s \) nem osztható egyetlen náluk kisebb felbonthatatlan számmal sem, és így \( s \) szükségképpen felbonthatatlan.

Legyen végül \( t \) egy tetszőleges jelölhetetlen szám. Ha \( t \) összetett lenne, akkor (pl. az 1.4.7a-b feladat [18] szerint) \( t \)-nek lenne olyan \( p \) felbonthatatlan osztója, amelyre \( p \leq \sqrt{t} \leq \sqrt{N} \). Ez azonban ellentmond annak, hogy \( t \) nem osztható a bekarikázott számok, azaz a \( \sqrt{N} \)-nél nem nagyobb felbonthatatlan számok egyikével sem. ♦

Most a prímszámokkal kapcsolatos néhány nevezetes megoldatlan problémát ismertetünk. Ezek egy részével a fejezet további pontjaiban részletesebben is foglalkozunk majd.

**Ikerprímek:**

\[ \{3, 5\}, \{5, 7\}, \{11, 13\}, \{17, 19\}, \ldots : \text{előfordul-e végig sokszor?} \]

**Megjegyzések:**

1. A 2005-ben ismert legnagyobb ikerprímpár a Járai Antal és munkatársai által talált \( 168890873904775 \cdot 2^{171930} + 1 \) (ezek a számok a tízes számrendszerben 51779 jegyűek).

2. A 2 helyett bármilyen más rögzített \( 2k \) páros számra is megoldatlan, hogy van-e végig sok olyan primpár, amelyben a két prim különbsége éppen \( 2k \) . További általánosítástként primpárokat helyett primhármasokat, primnégyeseket stb. is vizsgálhatunk: könnyen adódik, hogy \( n_1, n_2 + 2 \) és \( n + 4 \) mindegyikére csak \( n = 3 \) esetén prim, azonban nagyon is elképzelhető, hogy végig sok olyan \( n \) van, amelyre \( n, n + 2 \) és \( n + 6 \) mindhárman primek, vagy akár \( n, n + 2, n + 6 \) és \( n + 8 \) mindegyikére prim stb. (Vó. az 1.4.1 [17] és 5.1.1 feladatokkal [116].)

3. Az ikerprimprobléma úgy is megfélemlíthető, hogy a szomszédos primek különbsége vajon végig sokszor lesz-e „nagyon kicsi“. Egy másik irányú nevezetes sejtés, hogy két egymást követő négyzetszám között mindig található primprímszám, vagyis a szomszédos primek különbsége nem nőhet „túl gyorsan“. A szomszédos primek közötti hézaggal részletesebben az 5.5 pontban foglalkozunk.

4. Az ikerprimek (ha végig sokan vannak is) mindenképpen „nagyon ritka” helyezkednek el a primek között; például az ikerprimek reciprokösszege konvergens, míg a primeké divergens (lásd az 5.6 pontot).

5. Egy további érdekes eredmény, hogy végig sok olyan \( P \) prim létezik, amelyre \( P + 2 \) vagy prim, vagy pedig két prim szorzata (azaz „csak egyetlen lépés” hiányzik az ikerprimprobléma bizonyításához).

**Goldbach-sejtés:**

\[ 4 = 2 + 2, \quad 6 = 3 + 3, \quad 8 = 5 + 3, \quad 10 = 7 + 3, \quad 12 = 7 + 5, \ldots : \text{felírható-e 4-től kezdve minden páros szám két prímszám összegeként?} \]

**Megjegyzések:**

114
1. A fenti problémát szokás „páros” Goldbach-sejtésnek is nevezni, megkülönböztetésül a „páratlan” Goldbach-tól, amely arra vonatkozik, hogy a 7-től kezdve minden páratlan szám felírható három prim összegeként. Ez utóbbi állítás egyrészt azonnal következik a „páros” Goldbachból (lásd az 5.1.2 feladatot [116]), másrészt sikerült már lényegében bebizonyítani (Vinogradov, 1937): minden eléggő nagy páratlan szám előáll három prim összegeként. (Sajnos az „elég nagy” helyére egyelőre nem tudunk egy olyan explicit korlátot tenni, hogy az annál kisebb páratlan számokra számítógéppel ellentmondani lehessen az előállíthatóságot.)

2. A („páros”) Goldbach-sejtéssel kapcsolatos néhány részvételek:

(A) Minden páros szám legfeljebb 6 prímszám összege. (Az első ilyen típusú tételt a 6 helyett néhány szerel Schinzelmann igazolta 1930-ban.)

(B) Minden eléggő nagy páros szám felírható $p + m$ alakban, ahol $p$ prim és $m$ vagy prim, vagy pedig két prim szorzata. (Az első ilyen típusú tételt, ahol alkalmas rögzített $k$-val legfeljebb $k$ darab prim szorzata, Rényi Alfréd igazolta 1947-ben.)

(C) Csak (a megfelelő értelmen vett) „ritka kivétel” lehet azok a páros számok, amelyek esetleg nem írhatók fel két prim összegeként. (A „ritka” jelző egyelőre sajnos nem helyettesíthető a „véges sok” kifejezéssel.)

Hosszú számtani sorozatok:

$\{3, 5, 7\}, \{5, 11, 17, 23, 29\}, \{7, 13, 37, 97, 127, 157\}, \ldots$ : van-e akármillő hosszú (nemkonstans) számtani sorozat csupa prímszámból?

Itt örömmel számolhatunk be arról, hogy 2004-ben Ben Green és Terence Tao bebizonyították, hogy a válasz igen.

Megjegyzések:

1. A 2005-ben ismert leghosszabb számtani sorozatnak, amely csupa prímszámokból áll, 23 tagja van: $562113387530397 + 44540738095800k, \quad k = 0, 1, \ldots, 22$.

2. Egy végtelen számtani sorozat már nem állhat csupa prímszámokból (lásd az 1.4.2 feladatot [17]), de szerepel benne végtelen sok prim, ha a kezdőtagja és a differenciája reláti primok (Dirichlet tétele, lásd az 5.3 pontot).

Speciális alakú prímek:

- Létezik-e végtelen sok $2^k - 1$, illetve $2^k + 1$ alakú prim (Mersenne-, illetve Fermat-prímek, lásd az 5.2 pontot)?

- Létezik-e végtelen sok $n^2 + 1$ alakú prim (vő. az 1.4.6 feladattal [17])?

- Létezik-e végtelen sok prim a (tízes számrendszerben) csupa egyes számjegyet tartalmazó számok, a 333...31 alakú számok, a Fibonacci-számok stb. között?

Prímképletet:

Megadható-e olyan „gyakorlati szempontból is használható” képlet, amely minden $n$-re előállítja az $n$-edik prímcszámot, vagy legalábbis olyan, a természetes számokon értelmezett, a gyakorlatban is kiszámítható (végtelen sok értékű) függvény, amelynek minden helyettesítési értéke prim?
Megjegyzések:

1. Általános vélekedés szerint ilyen képletre nemigen van remény. Az 5.1.9 [117]b és 5.5.9b feladatokban [140] szereplő képletek éppen a gyakorlati kiszámíthatóság követelményének nem felelnek meg.

2. Már Euler észrevette, hogy \( n^2 + n + 41 \) minden \( 0 \leq n < 39 \) esetén prim (azonban \( n = 40 \)-re összetett). Ebből azonnal adódik, hogy

\[
(n - 40)^2 + (n - 40) + 41 = n^2 - 79n + 1601
\]

minden \( 0 \leq n \leq 79 \) esetén prim. Ha nemcsak egész, hanem racionális együttíthatós polinomokat is megengedünk, akkor akármilyen hosszú ilyen prímsorozatot tudunk gyártani (5.1.7 feladat [117]). Másfelől azonban egy (nemkonstans) polinom biztosan nem alkalmas prímképletnek, mert nem vehet fel minden egész helyen primet (5.1.8 felada [117]t).

3. Meglepő ugyanakkor az alábbi (szintén csak elméleti szempontból jelentős) eredmény: Megadható olyan többváltozós, egész együttíthatós polinom, amelynek a változók nemnegatív értékein felvett pozitív helyettesítési értékei megegyeznek a (pozitív) prímszámok halmazával. (Ez a polinom ugyanazt a primet több helyen is felveheti, valamint negatív értékeket is felvesz.)

Ilyen polinom létezését először Matijaszevics igazolta 1970-ben. Matijaszevics ekkor oldotta meg Hilbert tizedik problémáját: (mások munkáját betetőve) bebizonyította, hogy nem létezik olyan általános algoritmus, amelynek a változók nemnegatív értékein felvett pozitív helyettesítési értékei megegyeznek a (pozitív) prímszámok halmazával. (Ez a polinom ugyanazt a primet több helyen is felveheti, valamint negatív értékeket is felvesz.)

Feladatok

Lásd az 1.4.1 [17]–1.4.7 feladatokat [18] is.

5.1.1 Tegyük fel, hogy az \( r_1, \ldots, r_k \) egészekhez végzélen sok olyan \( u \) létezik, amelyre az \( u + r_1, \ldots, u + r_k \) számok mindegyike prim. Bizonyítsuk be, hogy ekkor az \( r_1, \ldots, r_k \) számok semmilyen \( m > 1 \) modulovala sem tartalmazhatnak teljes maradékkrendszert modulo \( m \).

5.1.2 Bizonyítsuk be, hogy

(a) a „páros” Goldbach-sejtésből következik a „páratlan”, továbbá
(b) a „páros” Goldbach-sejtés ekvivalens azzal az állítással, hogy minden \( u \geq 6 \) egész szám felírható három prim összegeként.

5.1.3 Mely páros számok írhatók fel két (pozitív) összetett szám összegeként? És melyek két páratlan (pozitív) összetett szám összegeként?

5.1.4 Határozzuk meg azokat a prímeket, amelyeknek az összege és a különbsége is prímszám.

5.1.5 Tekintsünk egy csupa prímszámú és álló számtani sorozatot, jelöljük a tagok számát \( u \) -nel, a differenciáciat pedig \( d \) -vel. Bizonyítsuk be, hogy

(a) ha \( u = 4 \), akkor \( 6 \mid d \);
(b) ha \( u = 6 \), akkor \( 30 \mid d \);
(c) (M [569]) általában, \( d \) osztható az összes \( u \) -nél kisebb prímszámmal.
Megjegyzés: A példaként megadott 23 tagú számtani sorozat differenciája

\[ 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 39889. \]

5.1.6 Bizonyítsuk be, hogy a „Speciális alakú prímek” c. résznél felsorolt valamennyi típusú számból végére sok összetett szám létezik.

5.1.7 Legyen \( k \) tetszőleges pozitív egész. Lássuk be, hogy van olyan \( f \) racionális együthatós polinom, amelyre bármely \( 1 \leq i \leq k \) esetén \( f(i) \) éppen az \( i \) -edik prímszám.

5.1.8 (a) Legyen \( f \) egész együthatós, egyváltozós, nemkonstans polinom. Mutassuk meg, hogy \( f(n) \) nem lehet minden \( n \) természetes számra prím.

(b) Igazoljuk ugyanezt

(b1) racionális együthatós;

(b2) komplex együthatós;

(b3) többváltozós polinomokra is.

5.1.9 Jelölje \( p_n \) az \( n \) -edik prímszámot.

(a) Bizonyítsuk be, hogy \( p_n < 2^{p_n} \).

(b) Legyen

\[ a = \sum_{i=3}^{\infty} \frac{p_i}{10^{2^{p_i}}} = 0,000020000000000300 \ldots, \]

azaz \( c \) egy olyan tízdecis tört, amelyben sorra a primek tízes számrendszerbeli alakját írjuk le, amelyeket megfelelő számú 0 jeggyel választunk el egymástól (hogy „biztosan ne érjenek egymásba”). Mutassuk meg, hogy

\[ p_n = \left| 10^{2p_n} c \right| - \left| 10^{2p_n} - 2^{p_n}-1 \right| \cdot \left| 10^{2^{p_n}-1} c \right|, \]

(c) Miért nem alkalmazható a (b)-beli formula \( p_n \) tényleges meghatározására?

5.1.10 Adjunk meg olyan \( K \) számot, amelyre igaz az alábbi állítás:

\[ 10^4 \leq c \leq 10^8 \] feltételt kielégítő \( c \) számokra \( c \) akkor és csak akkor prím, ha \( (c,K) = 1 \).

5.2 Fermat- és Mersenne-prímek

Ebben a pontban a \( 2^k + 1 \) és \( 2^k - 1 \) alakú prímekkel foglalkozunk, az előbbieket Fermat-prímeknek, az utóbbieket Mersenne-prímeknek nevezzük. Amint az előző pontban már említettük, megoldatlan, hogy létezik-e végére sok Fermat-, illetve Mersenne-prím.

Az 1.4.4 feladatban [17] láttuk, hogy ha \( 2^k + 1 \) prim, akkor \( k \) szükségképpen kettőhatvány, ha pedig \( 2^k - 1 \) prim, akkor \( k \) maga is prim. Így elég az \( \Gamma_k = 2^{2^k} + 1 \) Fermat-számokat és az \( M_p = 2^p - 1 \) (ahol \( P \) prim) Mersenne-számokat vizsgálnunk.
Először a Fermat-számokkal foglalkozunk. Fermat azt hitte, hogy $F_n$ mindig prímet ad (nem ez a híres Fermat-sejtés, azzal a 7. fejezetben foglalkozunk majd). A $0 < n < 4$ értékekre $F_n$ valóban prim (ezek a primek a 3, 5, 17, 257 és 65537), azonban Euler megmutatta, hogy $F_5 = 2^{2^{16}} + 1$ már összetett, ugyanis osztható 641-gyel.

Ma (2005-ben) már tudjuk, hogy $F_n$ összetett szám 5 ≤ $n ≤ 32$ és néhány nagyobb $n$ esetén. A rekord $F_{101000}$ (amely a tízes számrendszerben több, mint $10^{120000}$ jegyből áll!), ez osztható $1207 \cdot 2^{101008} + 1$-gyel. Az $n > 4$ értékekre (egyelőre) nem találtuk primet az $F_n$ számok között. Nem tudjuk, hogy $F_{34}$ prim-e. Nem ismerjük $F_{14}$ egyetlen nemtrivialis osztóját sem (noha tudjuk, hogy összetett szám). $F_2$, $F_3$ és $F_5$ primitívgyos felbontását megadjuk a könyv végén található, a Fermat-számokra vonatkozó táblázatban (rajtuk kívül csak $F_2$, $F_3$, $F_{10}$ és $F_{11}$ teljes felbontása ismert).

A Fermat-prím megjelenését a szabálysok sokszögek szerkesztésénél játszanak szerepet: Gauss tétele szerint egy szabályos $N$-szög akkor és csak akkor szerkeszthető (euklideszi szerkesztéssel), ha $(3 \leq N)$ kanonikus alakja $N = 2^a \cdot p_1 \cdots p_v$, ahol $\alpha > 0$, $v > 0$ és a $p_i$ számok különböző Fermat-prímek.

Az első néhány érték $N = 3, 4, 5, 6, 7, 10, 12, 15, 16, 17, 20, \ldots$ A Fermat-számok vizsgálatában az alábbi két tétel nyújt gyakorlati segítséget. Az T 5.2.1 Tétel a Fermat-számok prímosztóinak keresését teszi hatékonyabbá, az T 5.2.2 Tétel alapján pedig (viszonylag) gyorsan ellenőrizhető, hogy egy Fermat-szám prim-e vagy összetett.

### 5.2.1 Tétel

#### T 5.2.1

$F_n$ bármely (positív) osztója $k \cdot 2^{n+1} + 1$, sőt $n \geq 2$ esetén $\tau \cdot 2^{k+2} + 1$ alakú.

Feltehetőleg Euler is ezt a tételt használta $F_5$ összetettségének a kimutatására: $F_5$ prímosztói csak a $128k + 1$ alakú primek közül kerülhetnek ki. Ezek közül az első kettő a 257 és a 641, és ez utóbbi osztója is $F_5$-nek.

**Bizonyítás:** Az állítást először arra az esetre igazoljuk, ha az osztó egy $p$ prímszám. Ekkor $p \mid F_n$ átírható a

$$2^{2^n} \equiv -1 \pmod p$$  

alakba. Ezt négyzetre emelve

$$2^{2^{n+1}} \equiv 1 \pmod p$$  

adódik. A T 3.2.2(i) Tétel szerint

$$2^j \equiv 1 \pmod p \iff a_p(2) \mid j.$$  

Ennek megfelelően a (2) kongruenciából azt kapjuk, hogy

$$a_p(2) \mid 2^{n+1},$$

uyanakkor az (1) kongruencia alapján

$$a_p(2) \mid 2^n;$$

118
PRÍMSZÁMOK

hiszen nyilván \( p > 2 \) és így \(-1 \neq 1 \pmod{p}\). Ebből következik, hogy

\[
\alpha_p(2) = 2^{n+1}.
\]

Az \( \alpha_p(2) \mid p - 1 \) összefüggésből kapjuk, hogy \( 2^{n+1} \mid p - 1 \), azaz alkalmas \( k \) egésszel \( p = k2^{n+1} + 1 \).

Ha \( n \geq 2 \), akkor az előzőek alapján egyúttal \( p = 8n + 1 \) alakú, és így

\[
\left( \frac{2}{p} \right) = 1, \quad \text{azaz} \quad 2^{\frac{p-1}{2}} = 1 \pmod{p}.
\]

Ebből következik, hogy

\[
\alpha_p(2) = 2^{n+1} \mid \frac{p-1}{2},
\]

vagyis alkalmas \( r \) egésszel \( p = r2^{n+2} + 1 \).

A fenti eredményeket átírhatjuk \( p = 1 \pmod{2^{n+1}} \), illetve \( n \geq 2 \) esetén \( p \equiv 1 \pmod{2^{n+2}} \) alakba is.

Legyen végül \( d \mid F_p \) tetszőleges. Írjuk fel \( d \cdot t \) (nem feltétlenül különböző) prímszámok szorzataként (ha \( d > 1 \)); \( d = p_1 \cdots p_s \). Az előzőekben azt igazoltuk, hogy mindegyik \( d \) -re \( p_i \equiv 1 \pmod{2^{n+1}} \) . Ezeket a kongruenciákat összeszorozva kapjuk, hogy \( d \equiv 1 \pmod{2^{n+1}} \) is teljesül. A \( 2^{n+2} \) modulusra vonatkozó állítás ugyanily bizonyítható.

**5.2.2 Tétel (Pepin-teszt)**. T 5.2.2

Az \( n \geq 1 \) esetben \( F_n \) akkor és csak akkor prim, ha

\[
3^{(F_n-1)/2} = -1 \pmod{F_n}.
\]  

Bizonyítás: Tegyük fel először, hogy \( F_n \) prim. Ekkor (3) éppen azt jelenti, hogy a 3 kvadratikus nemmaradék modulo \( F_n \), azaz

\[
\left( \frac{3}{F_n} \right) = -1.
\]

Ennek igazolásához felhasználjuk, hogy \( n \geq 1 \) miatt \( 2^{2^a} = 4^t \) alakú, és így

\[
F_n = 1 \pmod{4}, \quad \text{továbbá} \quad F_n = 4^t + 1 \equiv -1 \pmod{3}.
\]

Ezért a kvadratikus reciprocitási tétel alapján

\[
\left( \frac{3}{F_n} \right) = \left( \frac{F_n}{3} \right) = \left( \frac{-1}{3} \right) = -1.
\]

A megfordításhoz tegyük fel, hogy (3) teljesül. Ezt négyzetre emelve

\[
3^{F_n-1} \equiv 1 \pmod{F_n}
\]

adódik. A (4), illetve (3) kongruenciából
következik. Mivel $F_n - 1$ kettőhatvány, ezért ebből azt nyerjük, hogy

$$a_{F_n}(3) \mid F_n - 1,$$

illetve

$$a_{F_n}(3) \mid \frac{F_n - 1}{2}$$

Ez azt is jelenti, hogy $F_n - 1 \mid \varphi(F_n)$. Mivel $\varphi(F_n) \leq F_n - 1$, így csak $F_n - 1 = \varphi(F_n)$ lehetséges, ami azzal ekvivalens, hogy $F_n$ prím.

Az T 5.2.2 Tétel alapján $F_n = 2^{2^n} + 1$ összetettségét a következőképpen lehet kimutatni: $3^{2^n}$ modulo $F_n$ vett maradékát 31 négyzetre emeléssel és az eredményt mindig modulo $F_n$ redukálva kiszámoljuk, és kiderül, hogy ez a maradék nem $-1$. Sőt, tulajdonképpen pusztán a kis Fermat-tétel segítségével is célhoz érhetünk: 32 ilyen négyzetre emeléses és redukciós lépészel kapjuk, hogy

$$3^{2^{2^n} - 1} \neq 1 \pmod{F_n},$$

tehát $F_n$ nem lehet prim. Így Fermat akár a saját tételével is megcáfolhatta volna a Fermat-számok prim voltára vonatkozó sejtését (az imént jelzett számolás mennyisége nem jelentett volna akadályt, hiszen abban a korban rendszeresen végeztek ennek jólóval nagyobb számításokat is papírral és ceruzával).

Az T 5.2.2 Tétel általában is hatékony eszközt jelent a Fermat-számok prím vagy összetett voltának az eldöntésére: a (3) feltétel teljesülését ismételt négyzetre emelésekkel (és az eredményt mindig modulo $F_n$ redukálva) gyorsan ellenőrizni tudjuk, összessen $2^{2^n - 1} \approx \log_2 F_n$ ilyen lépést kell végezni. Sajnos, a gyakorlati alkalmazásának gátat szab az a tény, hogy a Fermat-számok iszonyú sebességgel nőnek, $F_n \approx 2^{2^n} - 1$, és így a legjobb számítógépek sem képesek megbirkózni már viszonylag kis $n$ értékekkel sem.

Most rátérünk az $M_p = 2^p - 1$ (ahol $p$ prim) Mersenne-számok vizsgálatára. Könnyen látszik, hogy ezek nem lesznek mindig prímek, a legkisebb összetett számot $p = 11$ esetén kapjuk:

$$2^{11} - 1 = 2047 = 25 \cdot 89.$$  

A Mersenne-primek jelentőségét többek között a páros tökéletes számokkal való kapcsolatuk adja, lásd a T 6.3.2 Tételt. A névadó Mersenne a 17. század jelentős francia „tudományos vezetője”. Fermat, Descartes és más vezető tudók intenzív levezetőpartnere volt, aki a minél nagyobb tökéletes számok előállítása reményében keresett ilyen típusú primeket.


Több mint kétszáz évig senki sem tudta, vajon Mersenne listája helyes-e vagy sem. Az első hibát 1876-ban(!) fedezte fel a szintén francia Lucas: megmutatta, hogy $2^{67} - 1$ összetett. Itt külön érdekesség, hogy a számot nem sikerült tényezőkre bontania, csak az összetettség tényét igazolta (a részben róla elnevezett T 5.2.4 Tétel segítségével). Végül 1903-ban az amerikai Cole találta meg a

$$193707721 \cdot 76183257287$$

felbontást, miután sok évig minden vasárnap délutánját ennek a problémának szentelte.

Mersenne listájában később további négy hibát találtak: a hiányzó $2^{11} - 1$, $2^{17} - 1$ és $2^{61} - 1$ is prim, ugyanakkor $2^{2^{27} - 1} - 1$ összetett.

Közülük az utolsó, a 2005 decemberében felfedezett a legnagyobb ismert prim. Ez a számjegyből áll (tízes számvízszberben).

A könyv végén, a Mersenne-számokra vonatkozó táblázatban megadjuk a 10 és 100 közötti (prim) kitevőkhöz tartozó összetett Mersenne-számok primitív egen belül felfontságát.

Most az T 5.2.1 és T 5.2.2 Tételek Mersenne-számokra vonatkozó megfelelőit tárgyaljuk.

5.2.3 Tétel. T 5.2.3

Legyen \( p > 2 \) prim. Ekkor \( M_p \) bármely (positív) osztója egyszerre \( 2kp + 1 \) és \( 8r \pm 1 \) alakú. 

Példa: Legyen \( p = 37 \). Ekkor \( M_{37} = 2^{37} - 1 \) tetszőleges \( q \) primosztója egy részett \( 94k + 1 \), más rész \( 8r \pm 1 \) alakú. Az így adódó

\[
x = 1 \mod 94, \quad x \equiv \pm 1 \mod 8
\]

szimultán kongruenciarendszereket megoldva

\[
x \equiv 1 \mod 95\quad \text{és}\quad x \equiv 1 \mod 376
\]

adódtik. Az ilyen alakú primek

\[
q = 1129, 1223, 2351, \ldots
\]

Ezek közül \( 2351 \mid M_{37} \), tehát \( M_{37} \) összetett.

Könnyen lehet, hogy \( M_{17} \)-nek ezt a primosztóját Mersenne is megtalálta, vagyis tudatosan hagyta ki a \( p = 47 \) értéket a listájáról (és nem csak arról van szó, hogy szerencsésen tippelt).

Bizonyítás: A Fermat-számoknál látottakhoz hasonlóan most is elég az állítást primosztókra igazolni.

Tegyük fel, hogy a \( q \) primre

\[
q \mid 2^p - 1, \quad \text{azaz} \quad 2^p \equiv 1 \mod q.
\]

Ekkor \( \alpha_q(2) \mid p \), továbbá nyilván \( \alpha_q(2) \neq 1 \), tehát \( \alpha_q(2) = p \).

Innen kapjuk, hogy \( p \mid q - 1 \), azaz \( q = bp + 1 \) alakú. Mivel \( q \) és \( p \) páratlan, ezért \( t \) páros, vagyis \( q = 2kp + 1 \) alakú.

A \( q = 8r \pm 1 \) állításhoz azt kell igazolnunk, hogy a 2 kvadratikus maradék mod \( q \). Ez a \( 2^p \equiv 1 \mod q \) kongruenciából \( p \) páratlanságának és a Legendre-szimbólum tulajdonságainak felhasználásával a következőképpen adódtik:

\[
\left( \frac{2}{q} \right) = \left( \frac{2^p}{q} \right) = \left( \frac{1}{q} \right) = 1, \quad \text{másra}
\]

5.2.4 Tétel (Lucas–Lehmer-teszt). T 5.2.4
Legyen $p > 2$ prim, továbbá $a_1 = 4$ és $a_{i+1} = a_i^2 - 2$, ha $i \geq 1$. Ekkor $M_p$ pontosan akkor prim, ha

$$M_p \mid a_{p-1}.$$  \hfill (5)

** Példa:** Legyen $p = 5$ . Ekkor

$$a_1 = 4, \quad a_2 = 14, \quad a_3 = 194 = 8 \pmod{31} \quad \text{és} \quad a_4 = 62 = 0 \pmod{31},$$

tehát $M_5$ 31 prim.

Az (5) feltétel teljesülésének ellenőrzésekor elég mindig az $a_i$-knek csak a modulo $M_p$ vett maradékát kiszámítani, összesen $p - 2 \approx \log_2 M_p$ négyzetre emelési (valamint kivonási és redukciós) lépést kell végrehajtani.

**Bizonyítás:** Az $a + b\sqrt{3}$ ( $a,b$ egész) alakú számok a szokásos műveletekre egy (kommutatív, egységelemeles, nullosztómentes) gyűrűt alkotnak, jelöljük ezt $\mathbb{H}$-val. A bizonyításban a $\mathbb{H}$-beli oszthatóság, kongruencia és rendfogalom elemi tulajdonságait használjuk fel (ezek $\mathbb{H}$-ban is ugyanúgy érvényesek, mint az egész számoknál). Megjegyezzük, hogy $\mathbb{H}$-ban a számelmélet alaptétele is igaz (lásd a T 10.3.6 Tételt, illetve a 10.3.1 feladatot [337]), azonban a bizonyítás során erre nem lesz szükségünk.

I. Teljes indukcióval könnyen igazolható, hogy bármely $k$-ra

$$a_k = (2 + \sqrt{3})^{2^k-1} + (2 - \sqrt{3})^{2^k-1}.$$  

Ennek alapján az (5) feltétel ekvivalens az

$$M_p \mid (2 + \sqrt{3})^{2^p-2} + (2 - \sqrt{3})^{2^p-2}.$$  \hfill (6)

oszthatósággal. A jobb oldalon $(2 - \sqrt{3})^{2^p-2}$-t kiemelve (6) átírható az alábbi alakba:

$$M_p \mid (2 - \sqrt{3})^{2^p-2} \left( (2 + \sqrt{3})^{2^p-1} + 1 \right).$$  \hfill (7)

Használjuk fel, hogy a (7)-beli oszthatóság pontosan akkor teljesül az egész számok körében, mint amikor $\mathbb{H}$-ban (lásd az 5.2.10 feladatot [125]), továbbá $(2 - \sqrt{3})(2 + \sqrt{3}) = 1$ miatt a $2 \pm \sqrt{3}$ számok egész kitevős hatványai egységek $\mathbb{H}$-ban. Ennek megfelelően (7) és így (5) is ekvivalens a

$$(2 + \sqrt{3})^{2^p-1} = -1 \pmod{M_p}$$  \hfill (8)

kongruenciával.

Mindezek alapján az T 5.2.4 Tétel átfogalmazható a következő alakba: $M_p$ akkor és csak akkor prim, ha (8) teljesül.

II. Szükségünk lesz a következő lemmára: Ha $q > 3$ tetszőleges prímszám, akkor

$$\omega + b\sqrt{3} = a + \left( \frac{3}{\omega} \right) b\sqrt{3} \pmod{q}.$$  \hfill (9)

A lemma bizonyítása: A binomiális tétel alapján

122
A kis Fermat-tétel szerint
\[ a^d \equiv a \pmod{q} \quad \text{és} \quad b^d \equiv b \pmod{q}, \]
továbbá
\[ \left( \frac{q}{1}, \frac{q}{2}, \ldots, \frac{q}{q-1} \right) \]
mindegyike osztható \( q \)-val, és végül
\[ 3^{(q-1)/2} \equiv \left( \frac{3}{q} \right) \pmod{q}. \]
Ezeket (10)-be beírva éppen (9) adódik.

III. Most megmutatjuk, hogy ha (8) fennáll, akkor \( M_p \) prim. A (8) kongruenciát négyzetre emelve kapjuk, hogy
\[ (2 + \sqrt{3})^{2^p} \equiv 1 \pmod{M_p}. \]
Legyen \( q \) az \( M_p \) egy prímosztója (nyilván \( q > 3 \)). Ekkor a (11) és (8) kongruenciák \( M_p \) helyett a \( q \) modulusra is teljesülnek. Ebből (az T 5.2.1 és T 5.2.2 Tételek bizonyításánál is használt gondolatmenet szerint) következik, hogy \( \alpha_q(2 + \sqrt{3}) = 2^p \).

Ha \( \left( \frac{3}{q} \right) = 1 \), akkor (9) felhasználásával kapjuk, hogy
\[ (2 + \sqrt{3})^{q-1} - (2 - \sqrt{3})(2 + \sqrt{3})^q \equiv (2 - \sqrt{3})(2 + \sqrt{3}) = 1 \pmod{q}, \]
és így
\[ \alpha_q(2 + \sqrt{3}) = 2^p \leq q - 1. \]
Ez azonban \( q \leq M_p = 2^p - 1 \) miatt lehetetlen.

Ha \( \left( \frac{3}{q} \right) = -1 \), akkor hasonlóan adódik, hogy
\[ (2 + \sqrt{3})^{q+1} \equiv (2 - \sqrt{3})(2 + \sqrt{3}) = 1 \pmod{q}, \]
és így
\[ \alpha_q(2 + \sqrt{3}) = 2^p \leq q + 1. \]
Ezt a \( q \leq M_p = 2^p - 1 \) egyenlőtlenséggel összevetve kapjuk, hogy \( q = M_p \), vagyis \( M_p \) prim.

IV. Végül belátjuk, hogy ha \( M_p \) prim, akkor (8) teljesül.

Fel fogjuk használni, hogy \( M_p \equiv -1 \pmod{8} \) miatt
\[
\left( \frac{2}{M_p} \right) = 1, \tag{12}
\]
továbbá \( M_p \equiv 1 \pmod{3} \) és \( M_p \equiv -1 \pmod{4} \) alapján, a reciprocitási tétele felhasználásával
\[
\left( \frac{3}{M_p} \right) = -\left( \frac{M_p}{3} \right) = -\left( \frac{1}{3} \right) = -1. \tag{13}
\]
Induljunk ki a
\[
2(2 + \sqrt{3}) = (1 + \sqrt{3})^2
\]
egyenlőségből, és emeljük mindkét oldalt \( \left( \frac{M_p}{\sqrt{3}} + 1 \right)^2 = 2^{\phi - 1} \)-edik hatványra:
\[
2^{(M_p+1)/2} \cdot (2 + \sqrt{3})^{2^{\phi - 1}} = (1 + \sqrt{3})^{M_p + 1}. \tag{14}
\]
A (14) egyenlőség bal oldalának első tényezőjére (12)-t is felhasználva kapjuk, hogy
\[
2^{(M_p+1)/2} = 2 \cdot 2^{(M_p-1)/2} = 2 \left( \frac{2}{M_p} \right) = 2 \pmod{M_p}, \tag{15}
\]
a (14) jobb oldalán pedig a (9) kongruenciát az \( a + b\sqrt{3} = 1 + \sqrt{3} \) és \( q = M_p \) szereposztással alkalmazva, valamint (13)-at is felhasználva
\[
(1 + \sqrt{3})^{M_p+1} = (1 + \sqrt{3})(1 + \sqrt{3})^{M_p} = (1 + \sqrt{3})(1 + \left( \frac{3}{M_p} \right) \sqrt{3}) = (1 + \sqrt{3})(1 - \sqrt{3}) = -2 \pmod{M_p} \tag{16}
\]
adódik. A (15) és (16) összefüggéseket (14)-be beirva azt nyerjük, hogy
\[
2(2 + \sqrt{3})^{2^{\phi - 1}} \equiv -2 \pmod{M_p}. \tag{17}
\]
Szorozzuk meg (17)-et \( 2^{\phi - 1} \)-gyel. Ekkor \( 2^x \equiv 1 \pmod{M_p} \) miatt éppen a bizonyítani kívánt (8) kongruenciát jutunk.

**Feladatok**

5.2.1 (a) Igazoljuk, hogy \( F_{n+1} = F_0F_1 \ldots F_n + 2 \).

(b) Mutassuk meg, hogy a Fermat-számok páronként relatív prímek (vö. az 1.3.14 feladattal [15]).

(c) A (b) rész felhasználásával adjunk új bizonyítást arra, hogy a primek száma végtelen.

(d) Adjunk új bizonyítást az 5.1.9a feladat [117] állítására.

5.2.2 Bizonyítsuk be, hogy az T 5.2.2 Tétel \( n \geq 2 \) esetén akkor is érvényben marad, ha a (3) képletben a 3 helyére 5-öt vagy 10-et írunk.

5.2.3 Legyen \( n \geq 2 \). Mutassuk meg, hogy \( K_n = 5 \cdot 2^n + 1 \) akkor és csak akkor prim, ha
\[
3^{K_n-1)/2} \equiv -1 \pmod{K_n}.
\]
5.2.4 Bizonyítsuk be, hogy \( \varphi(N) \) akkor és csak akkor kettőhatvány, ha \( N = 2^\alpha p_1 \cdots p_k \), ahol \( \alpha > 0 \), \( r > 0 \) és a \( p_i \) számok különböző Fermat-prímek.

5.2.5 (M [569]) Hány olyan \( k \) létezik, amelyre szabályos \( 2^k - 1 \)-szög szerkeszthető?

5.2.6 Keressük meg az alábbi számok legkisebb prímosztóját:
(a) \( 2^{20} - 1 \);
(b) \( 2^{29} - 1 \);
(c) \( 2^{17} - 1 \);
(d) \( 2^{13} - 1 \).

5.2.7 (M [569]) Bizonyítsuk be, hogy \( M_p \) akkor és csak akkor osztható \( 2p + 1 \)-gyel, ha \( 2p + 1 \) prim és \( p \equiv 3 \ (\text{mod} \ 4) \). (Illusztráció: \( 11 \equiv 3 \ (\text{mod} \ 4) \), \( 2 \cdot 11 + 1 = 23 \) prim, és valóban \( 23 \mid 2^{11} - 1 \).)

5.2.8 Tegyük fel, hogy egy \( q \) prímszámtára \( q^2 \) osztója egy Fermat-számnak vagy egy Mersenne-számnak. Mutassuk meg, hogy ekkor
\[
2^{q - 1} \equiv 1 \ (\text{mod} \ q^2).
\]

Megjegyzés: Megoldatlan probléma, hogy a feladat feltétele egyáltalán teljesülhet-e; könnyen elképzelhető ugyanis, hogy valamennyi Fermat- és Mersenne-szám négyzetmentes. Az is megoldatlan, hogy a fenti kongruenciát egyáltalán hány \( q \) prim elégteti ki, nem kizárt, hogy a jelenleg ismert 1093-on és 3511-en kívül nincs is több ilyen tulajdonságú \( q \).

5.2.9 (M [569]) A 8 és a 9, a 16 és a 17, illetve a 31 és a 32 szomszédos primhatványok (a prímeket is primhatványnak tekintjük). Jellemezzük az összes ilyen \( n, n + 1 \) számpárt.

5.2.10 Jelölje \( H \) az \( a + b\sqrt{3} \) (\( a, b \) egész) alakú számok gyűrűjét (lásd az T 5.2.4 Tétel bizonyítását), és legyenek \( k \) és \( n \) egész számok. Mutassuk meg, hogy a \( k \mid n \) oszthatóság akkor és csak akkor teljesül \( H \)-ban, ha az egész számok körében is fennáll.

5.2.11 (*) Az is megoldatlan probléma, hogy a Fermat-számok között végteles sok összetett szám van-e. Ugyanígy megoldatlan, hogy a \( H_n = 6^{2^n} + 1 \) számok között végteles sok prim, illetve hogy végteles sok összetett szám található-e. Mutassuk meg azonban, hogy az \( P_n \) és \( H_n \) számsorozatok közül legalább az egyikben végteles sok összetett szám fordul elő.

5.3 Prímszámok számtani sorozatokban

Számtani sorozaton egész számokból álló, pozitív differenciájú, végteles számtani sorozatot fogunk érteni:
\[
a + kd, \quad \text{ahol} \ d > 0 \ \text{és} \ a \ \text{egészek}, \ k = 0, 1, 2, \ldots
\]

Az 5.1 pontban láttuk, hogy egy ilyen sorozat nem állhat csupa prímszámomból. Ha \( (a, d) = t > 1 \), akkor a sorozat minden eleme osztható \( t \)-vel, így a sorozatban legfeljebb egy (pozitív) prim található. Ha azonban \( (a, d) = 1 \), akkor a sorozatban végteles sok prim fordul elő:
5.3.1 Tétel (Dirichlet-tétel).

Ha a \(d > 0\) és \(a\) egészek relatív prímek, akkor az \(a + kd\), \(k = 0, 1, 2, \ldots\) számtani sorozat végig tartalmaz sok prímet.

Ezt a tételt jelély általánosságában nem bizonyíthatjuk be, csak néhány speciális esetet igazoljuk.

5.3.2 Tétel.

Az \(4k - 3\) alakú prímek száma végtelen.

Bizonyítás: Az T 5.1.1 Tétel bizonyításának a gondolatmenetét követjük. Tegyük fel indirekt, hogy csak véges sok ilyen prímszám létezik, legyenek ezek \(p_1, \ldots, p_r\). Tekintsük az \(A = 4p_1 \cdots p_r - 1\) számot.

Az \(A\) nyilván nem osztható a \(p_1, \ldots, p_r\) prímeik egyikével sem.

Írjuk fel \(A\) prímtényezők szorzatát ként: \(A = a_1 \cdots a_s\) (\(s = 1\), illetve \(q_i = q_j\) is megengedett). Mivel \(A\) páratlan, ezért mindegyik \(a_i > 2\). Továbbá nem lehet minden \(q_i = 1 \pmod{4}\), ugyanis ezeket a kongruenciákat összesorozva \(A \equiv 1 \pmod{4}\) adóná, ami ellentmondás. Ebből következik, hogy a \(q_i\) primek között kell lennie \(4k + 3\) alakúaknak is. Ez szükségképpen különbözik a \(p_1, \ldots, p_r\) primektől, ami ellentmond az indirekt feltevésnek.

5.3.3 Tétel.

Az \(4k - 1\) alakú prímek száma végtelen.

Bizonyítás: Az euklideszi gondolatmenetet tovább kell finomítanunk. Tegyük fel indirekt, hogy csak véges sok ilyen prímszám létezik, legyenek ezek \(p_1, \ldots, p_r\). Tekintsük az \(A = (2p_1 \cdots p_r)^2 + 1\) számot.

Az \(A\) nyilván nem osztható a \(p_1, \ldots, p_r\) primeik egyikével sem.

Legyen \(q\) az \(A\) tetszőleges prímosztója. Nyilván \(q > 2\). A \(q \mid A\) oszthatóságot átírhatjuk a

\[ (2p_1 \cdots p_r)^2 \equiv -1 \pmod{q} \]

alakba. Ebből következik, hogy az \(x^2 \equiv -1 \pmod{q}\) kongruencia megoldható, vagyis \(q \equiv 1 \pmod{4}\). Így egy újabb \(4k + 1\) alakú prímet találtunk, ami ellentmondás.

A kvadratikus kongruenciák felhasználásával a Dirichlet-tétel számos további speciális esete is előírható, lásd az 5.3.3 feladatot [128].

Most a Dirichlet-tételt tetszőleges olyan számtani sorozatra igazoljuk, amelynek a kezdőtagja 1:

5.3.4 Tétel.

Bármely rögzített \(m > 0\) esetén az \(mk + 1\), \(k = 0, 1, 2, \ldots\) számok között végig tartalmaz sok prímet.

Bizonyítás: Fel fogjuk használni a körösségi polinomokra és a polinomok többszörös gyökeire vonatkozó alábbi összefüggéseket:

(i) Az \(m\) -edik körösségi polinom, \(\Phi_m\), az az \(1\) főgyűthető polinom, amelynek gyökei az \(m\) -edik primitív komplexx egységgyökök. \(\Phi_m\) fokszáma tehát \(\varphi(m)\). Példák:
Megmutatható, hogy $\Phi_n$ egész együtthatós, továbbá

$$
\Phi_n \mid x^n - 1, \quad \forall x \mid x^n - 1 = \prod_{d \mid n} \Phi_d.
$$

(ii) Legyen $T$ tetszőleges kommutatív test, $f \in \mathbb{T}[x]$. Az $\alpha \in \mathbb{T}$ elemet az $f$ polinom többszörös gyökének nevezzük, ha $(x - \alpha)^2 \mid f$. Ez pontosan akkor teljesül, ha $f'(\alpha) = f''(\alpha) = 0$, ahol $f'$ az $f$ polinom (formálisan képzett) deriváltját jelöli.

Az iménti fogalmak és tételek felhasználásával először az alábbi, önmagában is érdekes lemmát igazoljuk:

Legyen $c$ egész szám és $q$ prímszám. Ekkor $a_n(c) = m$. Ekkor $m \mid q - 1$, és így nyilván $q' \mid m$.

Helyettesítsünk (1)-ben $\alpha$ helyére $c$-t:

$$
e^m - 1 = \prod_{d \mid m} \Phi_d(c).
$$

Mivel $a_n(c) = m$, ezért $\nu(c) \equiv 1 \pmod{q}$, és így (3) bal oldala osztható $q$-val. A $q$ prim, tehát a jobb oldalon valamilyen $\Phi_d(c)$ tényező osztható $q$-val. Ekkor $\Phi_d(c) \mid e^m - 1$ miatt $e^m \equiv 1 \pmod{q}$. Tegyük fel indirekt, hogy $a_n(c) = t < m$. Ekkor $t \mid m$ és $e^t \equiv 1 \pmod{q}$.

A megfordításnál a $q' \mid \Phi_m(c)$ és $q' \mid m$ feltételekből indulunk ki. Ekkor $\Phi_m(c) \mid e^m - 1$ miatt $e^m \equiv 1 \pmod{q}$. Tegyük fel indirekt, hogy $a_n(c) = t < m$. Ekkor $t \mid m$ és $e^t \equiv 1 \pmod{q}$. A (3) összefüggést $\forall n$ helyett $t$-re alkalmazva azt kapjuk, hogy van olyan $d \mid t$, amelyre $q' \mid \Phi_d(c)$.

Az előzőknek, hogy az eredeti (3) jobb oldalán legalább két tényező osztható $q$-val.

A továbbiakban az (1)-beli $e^m - 1 = \prod_{d \mid m} \Phi_d$ egyenlősségét a $\mathbb{Z}_q$ modulo $q$ test felett fogjuk tekinteni. Ebben a felfogásban az előző bekezdés utolsó mondata úgy fogalmazható meg, hogy a $c$ (mint $\mathbb{Z}_q$-beli elem) a $\prod_{d \mid m} \Phi_d$ szorzat legalább két tényezőjének gyöke. Mivel ez a szorzat $e^m - 1$-gyel egyenlő, ezért a $c$ legalább kétszeres gyöke az $f = x^m - 1 \in \mathbb{Z}_q[x]$ polinomnak. Ekkor (ii) szerint $f'(c) = m e^{m-1} = 0$ ( $\mathbb{Z}_q$-ban).

Mivel $q' \mid m$ és $q' \mid c$, azaz a $\mathbb{Z}_q$ testben $e \neq 0$ és $c \neq 0$, ezért $m e^{m-1}$ sem lehet 0, ami ellentmond az előzőknek. Ezzel a lemmát bizonyítását befejeztük.

Rátérve az T 5.3.4 Tétel bizonyítására, tegyük fel indirekt, hogy csak véges sok $nk + 1$ alakú prim van (esetleg egy sincs), legyenek ezek $p_1, \ldots, p_r$. Legyen $c = \nu p_1 \cdots p_r$, ahol $\nu$ tetszőleges pozitív egész ($\nu = 0$-ra $c = \nu m$). Nyilván elég nagy $\nu$ esetén $\Phi_n(c) > 1$. 

127

PRÍMSZÁMOK
Legyen $q$ a $\Phi_m(c)$ egy tetszőleges prímosztója. Ekkor $\Phi_m(c)|c^m-1$ miatt $\langle q, c \rangle = 1$, és ennél fogva $q \nmid m$ is teljesül. Így a lemma szerint $\nu_q(c) = m$.

Ebből következik, hogy $n|mq - 1$, azaz $q = mk + 1$ alakú. Végül $\langle q, c \rangle = 1$ miatt $q \nmid \lambda$, ami ellentmond annak, hogy $a_1 \ldots p_r$ az összes $mk + 1$ alakú prim. $\blacksquare$

**Feladatok**

5.3.1 A modulo 9999 maradékosztályok közül hányban található pozitív prímszám?

5.3.2 Miért nem lehet az T 5.3.2 Tétel bizonyítását közvetlenül átvinni az T 5.3.3 Tételre is, $\Lambda = 4p_1 \ldots p_r + 1$-et véve?

5.3.3 Az általános Dirichlet-tétel felhasználása nélkül mutassuk meg, hogy az alábbi számtani sorozatokban végtelen sok prímszám van:

(a) $6k + 5$;
(b) $8k + 3$;
(c) $8k + 5$;
(d) $8k + 7$;
(e) $10k + 9$;
(f) $12k + 5$;
(g) $12k + 7$;
(h) $12k + 11$.

5.3.4 Hány olyan prímszám létezik, amelynek tízes számrendszerben az utolsó négy számjegye 4321?

5.3.5 Írjuk le a tízdesvessző után rendre a prímszámokat. Bizonyítsuk be, hogy az így keletkező szám irracionális.

5.3.6 Mely $a, b, c$ pozitív egészek esetén lesz végtelen sok prím az $a + bk + ce$ alakú számok között, ahol $k = 0, 1, 2, \ldots$, $n = 0, 1, 2, \ldots$ ?

5.3.7 (a) Mutassuk meg, hogy minden $c \neq 0$ egészhez létezik olyan $P$ prim, amelyre a $c$ kvadratikus maradék mod $P$.

(b) Mely $c$ egészhez létezik olyan $P$ prim, amelyre a $c$ kvadratikus nemmaradék mod $P$?

5.3.8 Bizonyítsuk be, hogy minden $u > 1$-hez található olyan $u$-edfokú együttható $f$ polinom, amely reducibilis a racionális test felett, és alkalmas $\omega_1, \ldots, \omega_n$ (különböző) pozitív egészek mindegyikére $f(\omega_i)$ pozitív prímszám.

5.3.9 Mutassuk meg (az általános Dirichlet-tétel felhasználása nélkül), hogy ha bármely $a$ és $d$ relatív prim pozitív egészek esetén létezik $a + kd$ alakú prim, akkor mindig végtelen sok ilyen prim is létezik. (Ez azt jelenti, hogy az általános Dirichlet-tétel bizonyításánál az igazi nehézséget nem a végtelen sok prim garantálása okozza, hanem az, hogy egyáltalán van a kívánt alakú prímszám.)
5.4 Becslések $\pi(x)$ -re

Az $x$ -nél nem nagyobb (pozitív) prímek számát $\pi(x)$ -szel jelöljük. Például $\pi(1) = 0$, $\pi(6,7) = 3$, $\pi(20) = 8$. Nyilván elég $\pi(x)$ -nek a pozitív egész $x$ -eken felvett értékeivel foglalkozni.

Annak ellenére, hogy a prímek igen szabálytalanul helyezkednek el a természetes számok között, a $\pi(x)$ függvény közeli viselkedése jól leírható. Ez az ún. prímszámtétel, amelyet bizonyítás nélkül közelünk:

5.4.1 Tétel (Prímszámtétel) . T 5.4.1

Jelölje $\log$ a természetes logaritmust. Ekkor

$$\lim_{x \to \infty} \frac{\pi(x)}{\log x} = 1,$$

azaz $\pi(x)$ és $\frac{x}{\log x}$ aszimptotikusan egyenlők.

Megjegyzések: 1. A prímszámtétel a $\pi(x)$ és $\frac{x}{\log x}$ mennyiségek arányára, és nem a különbségére vonatkozik, ez utóbbi akár milyen nagy is lehet.

2. A prímszámtétel azt fejezi ki, hogy $x$ -ig „körülbelül” $\frac{x}{\log x}$ prím van. Hogy ez „sok” vagy „kevés”, az attól függ, mihez hasonlítjuk. Az összes pozitív egészhez viszonyítva a prímszámok „ritkán” helyezkednek el, hiszen

$$\lim_{x \to \infty} \frac{\pi(x)}{\log x} = \lim_{x \to \infty} \frac{x}{\log x} = \lim_{x \to \infty} \frac{1}{\log \sqrt{x}} = 0.$$  

Ugyanakkor a prímszámok sokkal „sűrűbben” fordulnak elő, mint például a négyzetszámok, hiszen az utóbbiak száma $x$ -ig $\sqrt{x}$, és

$$\lim_{x \to \infty} \frac{\pi(x)}{\sqrt{x}} = \lim_{x \to \infty} \frac{x}{\sqrt{x}} = \lim_{x \to \infty} \frac{\sqrt{x}}{\log x} = \infty.$$  

3. A prímszámtételt először a 18. század végén sejtette meg egymástól függetlenül Legendre és Gauss. Gauss ekkor csak 15 éves volt, és az ö sejtésében az $\frac{x}{\log x}$ függvény helyett a

$$\text{Li}(x) = \int_2^x \frac{dt}{\log t}$$

logaritmus integrál szerepelt, amelyről később kiderült, hogy a $\pi(x)$ -et az $\frac{x}{\log x}$ -nál még sokkal pontosabban közelíti. A prímszámtétel bizonyításához vezető utat mintegy 70 évvel később Riemann jelölte ki, a bizonyítás pedig először de la Vallée Poussinnek és Hadamard-nak sikerült egymástól függetlenül 1896-ban. 1949-ben Erdős és Selberg talált ún. elemi (azaz mélyebb analízist nem használó) bizonyítást a prímszámtételre.

A prímszámtételből könnyen nyerhetünk aszimptotikát az $n$ -edik prímszámra:

5.4.2 Tétel . T 5.4.2

Jelölje $p_n$ az $n$ -edik prímszámot. Ekkor
PRÍMSZÁMOK

\[ \lim_{n \to \infty} \frac{\varphi_n}{n \log n} = 1. \tag{1} \]

Bizonyítás: Mivel \( \pi(p_n) = \frac{n}{\log n} \), így a prímszámtétel szerint

\[ \lim_{n \to \infty} \frac{\pi(p_n)}{\log p_n} = \lim_{n \to \infty} \frac{n \log \varphi_n}{\log p_n} - 1. \tag{2} \]

Az (1) bal oldalán szereplő sorozat reciproka

\[ \frac{n \log n}{p_n} = \frac{n \log \varphi_n}{\log p_n} \frac{\log n}{\log p_n} \tag{3} \]

alaka írható, ezért (2) alapján (1) igazolásához azt kell megmutatni, hogy (3) jobb oldalon a második tört határértéke is 1, azaz

\[ \lim_{n \to \infty} \frac{\log n}{\log p_n} = 1. \tag{4} \]

Ha a (2) összefüggést „logaritmáljuk”, akkor

\[ \lim_{n \to \infty} \log \left( \frac{n \log p_n}{p_n} \right) = \lim_{n \to \infty} \left( \log n - \log \log p_n - \log p_n \right) = 0 \tag{5} \]

adódik. Mivel \( 1/(\log n) \) korlátos, így (5)-ből kapjuk, hogy

\[ \lim_{n \to \infty} \left( \frac{\log n}{\log p_n} + \frac{\log \log p_n}{\log p_n} - 1 \right) = 0. \tag{6} \]

Itt

\[ \lim_{n \to \infty} \frac{\log \log p_n}{\log p_n} = 0, \]

ezért (6)-ből következik (4), és így (1) is.

A pont hátralevő részében egy, a prímszámtételnél gyengébb eredményt bizonyítunk:

5.4.3 Tétel . \( T \) 5.4.3

Léteznek olyan \( c_1 \) és \( c_2 \) pozitív konstansok és olyan \( a_0 \), hogy minden \( x \geq a_0 \) esetén

\[ c_1 \frac{x}{\log x} < \pi(x) < c_2 \frac{x}{\log x}. \tag{T} \]

Megjegyzések: 1. Az T 5.4.3 Tétel azt fejezi ki, hogy a \( \pi(x) \) „nagyságrendje” megegyezik az \( x/\log x \) függvény nagyságrendjével. Számos kérdés tisztázásához már ez a tétel is elegendő, lád például az T 5.4.1 Tétel utáni 2. megjegyzésben szereplő sűrűségi összehasonlításokat.

2. Az T 5.4.1 és T 5.4.3 Tételeket összevetve, a prímszámtétel szerint a \( \pi(x) \) és \( x/\log x \) függvények hányadosa 1-hez tart, az T 5.4.3 Tétel pedig azt állítja, hogy ez a hányados (elég nagy \( x \)-ekre) két pozitív konstans közé esik. Ebből rögtön következik, hogy az T 5.4.3 Tételben a (7) egyenlőség eleve csak olyan \( c_1 \), \( c_2 \) konstansokkal lehet igaz, amelyekre \( c_1 \leq 1 \) és \( c_2 \geq 1 \). Továbbá, a prímszámtétel úgy éppen azt jelenti, hogy az T 5.4.3 Tétel becsleléi \( bármely \) \( 0 < c_1 < 1 \) és \( c_2 > 1 \) konstansokkal fennállnak, azaz \( bármely \) \( 0 < c_1 < 1 \) és \( c_2 > 1 \) konstansokhoz található olyan \( a_0 \),

130
hogy a (7) egyenlőtlenség minden \( x \geq x_0 \)-ra teljesüljön. (Sőt, azt is bebizonyították, hogy \( a_1 = 1 \) is választható.)

3. Az T 5.4.3 Tételben \( x_0 = 2 \) is vehető („rosszabb” \( \epsilon_1 \) és \( \epsilon_2 \), lásd az 5.4.2 feladatot [134].

4. Az T 5.4.3 Tételt először Csebisev bizonyította be 1850-ben. Az alábbiakban az alsó becsélésre Erdős, a felső becslesre pedig Erdős és Kalmár közös bizonyítását mutatjuk be.

Bizonyítás: I. Alsó becslés \( \pi(x) \)-re.

Szükségünk lesz az alábbi segédtétellek:

**5.4.4 Lemma**. L 5.4.4

Az \( \binom{n}{k} \) binomiális együttható bármely prímhatvány osztója kisebb vagy egyenlő, mint \( n \).

*A lemma bizonyítása:* Legyen \( \binom{n}{k} \) kanonikus alakja

\[
\binom{n}{k} = \frac{n!}{k!(n-k)!} = \prod_{\nu \leq n} p^{\beta_{n,\nu}}. \tag{8}
\]

Azt kell igazolnunk, hogy \( \sum_{\nu} \beta_{n,\nu} \leq n \), azaz \( \beta_{n,\nu} \leq \log_{e} n \).

Tekintsünk egy rögzített \( P \) prímet, és jelöljük \( \log_{e} n \) értékét \( t \)-vel. A \( P \) kitevőjét \( n! \)-ban, \( k! \)-ban és \( (n-k)! \)-ban a Legendre-formulával (1.6.8 Tétel) határozhatjuk meg. Ennek alapján \( \binom{n}{k} \)-ban a \( P \) kitevője

\[
\beta_{n,\nu} = \frac{n}{\nu} + \frac{n}{2\nu} + \cdots + \frac{n}{\nu^k} - \left( \frac{n}{\nu} + \frac{n}{2\nu} + \cdots + \frac{n}{n-1\nu} \right) - \left( \frac{n}{\nu} - \frac{k}{\nu} + \frac{k}{2\nu} - \cdots + \frac{k}{n-k\nu} \right).
\]

Itt mind a \( t \) oszlophoz az egymás alatt álló tagok előjelésszegének alakú. Könnyen látható, hogy egy ilyen előjelésszeg értéke mindig 0 vagy 1 (lásd az 5.4.1 feladatot [134]), és így \( \beta_{n,\nu} \leq \frac{1}{t} \).

Most ráterünk \( \pi(x) \) alsó becsélésének a bizonyítására. A (8) jobb oldalán (legfeljebb) \( \tau^{\binom{n}{k}} \) darab prímhatvány szorzata áll, és az L 5.4.4 Lemma alapján ezek mindegyike kisebb vagy egyenlő, mint \( n \). Ebből azonnal következik, hogy

\[
\binom{n}{k} = \prod_{\nu \leq n} p^{\beta_{n,\nu}} \leq n^{\pi(n)}. \tag{9}
\]

A (9) egyenlőtlenségeket \( k = 0, 1, \ldots, n \)-re összegezve a

\[
2^n = \sum_{k=0}^{n} \binom{n}{k} \leq (n+1)n^{\pi(n)}
\]

eyenlőtlenséghoz jutunk. Ezt logaritmálva

\[
\log_2 2 \leq \log(n+1) + \pi(n) \log n.
\]
adó dik, ahonnan $\pi(n)$ et kifejezve kapjuk, hogy

$$\pi(n) \geq \log 2 \cdot \frac{\tau_n}{\log n} - \frac{\log(n + 1)}{\log n}. \quad (10)$$

Mivel (10) jobb oldalán a második tag korlátos, ezért elég nagy $n$ -re kisebb, mint (például) $0.01 n / \log n$, és így

$$\pi(n) > (\log 2 - 0.01) \frac{\tau_n}{\log n}.$$  

II. Felső becslés $\pi(n)$ - re.

Itt is szükségünk lesz egy segédtételre, amely az $\pi(n)$ -nél nem nagyobb prímszámok szorzatára ad felső becslést:

5.4.5 **Lemma** . L 5.4.5

Tetszőleges $n > 0$ egészre

$$\prod_{\substack{p \leq n \in \mathbb{P} \setminus \{2\}}} p < 4^n. \quad (11)$$

*A lemma bizonyítása:* Az állítást teljes indukcióval igazoljuk.

Az $n = 1, 2$ és $3$ értékekre (11) nyilván teljesül.

Tegyük fel, hogy az egyenlőség az $n = 1, 2, \ldots, m$ értékek ($m \geq 3$ ) esetén teljesül, és megmutatjuk, hogy ekkor $n = m + 1$ -re is fennáll.

Ha $m$ páratlan, akkor $m + 1$ egy 2-nél nagyobb páros szám, tehát összetett. Így az indukciós feltevést $n = m$-re alkalmazva kapjuk, hogy

$$\prod_{\substack{p \leq m + 1 \in \mathbb{N} \setminus \{2\}}} p = \prod_{\substack{p \leq m \in \mathbb{N}}} p < 4^m < 4^{m + 1}.$$  

Legyen most $m$ páros, $m = 2k$, azaz $m + 1 = 2k + 1$. Ekkor a kérdéses szorzatot a következőképpen bontjuk két részre:

$$\prod_{\substack{p \leq 2k + 1 \in \mathbb{N} \setminus \{2\}}} p = \prod_{\substack{p \leq k + 1 \in \mathbb{N}}} p \cdot \prod_{\substack{p \leq 2k + 1 \setminus 2k \in \mathbb{N}}} p. \quad (12)$$

A (12) jobb oldalán szereplő első tényezőre az $n = k + 1$ -re vonatkozó indukciós feltevés szerint

$$\prod_{\substack{p \leq k + 1 \in \mathbb{N} \setminus \{2\}}} p < 4^{k + 1}. \quad (13)$$

A (12) jobb oldalán levő második tényezőt a $\binom{2k + 1}{k}$ binomiális együttható segítségével becsülikjuk. Mivel

$$\binom{2k + 1}{k} = \frac{(2k + 1)(2k) \cdots (k + 2)}{k!}$$
számlálójában minden $k + 2 \leq p \leq 2k + 1$ prímszám szerepel, azonban a nevező ezen prímek egyikével sem osztható, ezért $\left(\binom{2k+1}{k}\right)$ (mely egész szám) osztható ezen prímek mindegyikével, vagyis a szorzatukkal is. Azaz

$$\prod_{k + 2 \leq i \leq 2k + 1} p\left|\binom{2k + 1}{k}\right|,$$

és így

$$\prod_{k \mid 2 \leq i \leq 2k + 1} p \leq \binom{2k + 1}{k}.$$  \hspace{1cm} (14)

Továbbá

$$\binom{2k + 1}{k} = \frac{1}{2} \left(\binom{2k + 1}{k} + \binom{2k + 1}{k - 1}\right) < \frac{1}{2} \cdot 2^{2k+1} = 4^k. \hspace{1cm} (15)$$

A (14) és (15) egyenlőtlenségekből

$$\prod_{k + 2 \leq i \leq 2k + 1} p < 4^k \hspace{1cm} (16)$$

következik. Végül (13)-at és (16)-ot (12)-be beírva kapjuk a kívánt

$$\prod_{p \leq 2k + 1} p < 4^{2k + 1}$$

eyenlőtlenséget. \hfill \blacksquare

Most rátérünk $\pi(x)$ felső becslésének a bizonyítására. A (11) egyenlőtlenség bal oldalán a tényezők száma $\pi(n)$. Mivel $\pi(n)$-re felső becslést keresünk, az első ötlet az, hogy minden tényező helyére a legkisebb prímet, a 2-t írjuk. Ebből azonban sajnos csak

$$2^{\pi(n)} < \prod_{p \leq n} p < 4^n$$

következik, ami a (triviálisnál is rosszabban) $\pi(n) < 2n$ becslést adja.

A javítás kulcsa az, hogy a (11) bal oldalán álló szorzatot úgy csökkentjük, hogy először elhagyjuk a kis prímeket, majd (lényegében) a megmaradó tényezők legkisebbikét írjuk mindegyik tényező helyére:

$$\prod_{p \leq n} p \geq \prod_{\sqrt{n} < p \leq n} p \geq \sqrt{n}^{\pi(\sqrt{n}) - \pi(\sqrt{n})}. \hspace{1cm} (17)$$

A (17) és (11) egyenlőtlenségeket összevetve

$$\sqrt{n}^{\pi(\sqrt{n}) - \pi(\sqrt{n})} < 4^n$$

következik. Ezt logaritmálva

$$\left(\pi(n) - \pi(\sqrt{n})\right) \log(\sqrt{n}) < n \log 4$$

adódik, ahonnan $\pi(n)$-et kifejezve kapjuk, hogy
Végül, mivel \( \pi(\sqrt{n}) < \sqrt{n} \), és

\[
\lim_{n \to \infty} \frac{\sqrt{n}}{\log n} = \lim_{n \to \infty} \frac{\log n}{\sqrt{n}} = 0,
\]

ezért elég nagy \( n \) -re \( \pi(\sqrt{n}) \) kisebb, mint (például) 0,01\( n / \log n \), és így (18)-ből

\[
\pi(n) < (2 \log 4 + 0,01)\frac{n}{\log n}
\]

következik. §

Feladatok

Valamennyi feladatban \( P \) prímszámot jelöl, \( P_n \) az \( n \) -edik prímszám, továbbá \( u_n \sim \varepsilon_n \) azt jelenti, hogy \( u_n \) és \( \varepsilon_n \) aszimptotikusan egyenlő, azaz \( \lim_{n \to \infty} u_n / \varepsilon_n = 1 \).

5.4.1 Igazoljuk, hogy az \(|a + b| - |a| - |b|\) kifejezés értéke bármely \( a, b \) valós szám esetén 0 vagy 1.

5.4.2 Mutassuk meg, hogy az T 5.4.3 Tételben \( x \) 2 is vehető, azaz alkalmas \( \varepsilon_1' \) és \( \varepsilon_2' \) pozitív konstansokkal a (7)-nek megfelelő egyenlőtlenség minden \( x \geq 2 \) valós számra teljesül.

5.4.3 (*) Milyen alsó és felső becsléseket nyerhetünk \( P_n \) -re, ha (az T 5.4.1 Tétel helyett) az T 5.4.3 Tételt használjuk fel?

5.4.4 Igazoljuk a prímszámtétel felhasználásával a következő becsléseket.

(a) \( \sum_{\nu \leq u} \log p \sim n \).

(b) Az \( n \) -nél nem nagyobb prímszámok szorzata „körülbelül” \( \varepsilon n \) az alábbi értékmérő szerint (v. az L 5.4.5 Lemmával): Bármely \( \varepsilon > 0 \) esetén létezik olyan \( n_0, \) hogy minden \( n > n_0 \)-ra

\[
e^{(1-\varepsilon)n} < \prod_{p \leq u} p < e^{(1+\varepsilon)n}.
\]

5.4.5 (*) Legyen \( 1 \leq a_1 < a_2 < \cdots \) a természetes számok tetszőleges részsorozata, és jelölje \( A(n) \) a sorozat \( u \) -nél nem nagyobb elemeinek a számát, azaz \( A(n) = \sum_{a_1 \leq a} 1 \). Bizonyítsuk be, hogy az alábbi négy állítás ekvivalens.

(i) \( A(n) \sim n / \log n \).

(ii) \( u_n \sim n \log n \).

(iii) \( \sum_{a_1 \leq a} \log a \sim n \).

(iv) Bármely \( \varepsilon > 0 \) esetén létezik olyan \( n_0, \) hogy minden \( n > n_0 \)-ra

\[
e^{(1-\varepsilon)n} < \prod_{a_1 \leq a} a_i < e^{(1+\varepsilon)n}.
\]
Megjegyzés: A feladat azt mutatja, hogy az T 5.4.1 és T 5.4.2 Tételekben, valamint az 5.4.4 feladatban [134] szereplő állítások a prímszámok sorozatánál általánosabb sorozatok esetén is szorosan összefüggnek egymással.

5.4.6 (*) Jelöljük $\mathcal{S}(n)$-nel az $\sum_{p \leq n} p$ . Bizonyítsuk be az alábbi becséléseket $\mathcal{S}(n)$-re:

(a) Léteznek olyan $c_3$ és $c_4$ pozitív konstansok, hogy minden $n > 1$ -re

$$c_3 \frac{n^2}{\log n} < \mathcal{S}(n) < c_4 \frac{n^2}{\log n}.$$  

(b) $\mathcal{S}(n) \sim \frac{n^2}{(2\log n)}$.

5.4.7 (a) Mutassuk meg, hogy bármely $K'$-höz található olyan páros szám, amely legalább $K'$-féleképpen írható fel két prímszám összegeként.  

(b) Lássuk be a hasonló állítást összeg helyett különbségre is.

5.4.8 Igazoljuk, hogy

$$\pi(n) = \sum_{j=2}^{n} \left( \left\lfloor \frac{\lfloor \frac{1}{2} \rfloor+1}{j} \right\rfloor - \left\lfloor \frac{\lfloor \frac{1}{2} \rfloor+1}{j} \right\rfloor \right).$$

Alkalmass-e ez a képlet a $\pi(n)$ gyakorlati kiszámítására?

5.5 Hézag a szomszédos prímek között

Először megmutatjuk, hogy a szomszédos prímszámok között tetszőlegesen nagy hézagok is előfordulnak:

5.5.1 Tétel. \hspace{0.5cm} T 5.5.1

Bármely $K'$ pozitív egészhez meg lehet adni $K'$ egymást követő összetett számot. ♦  

Bizonyítás: Legyen $N > K'$ tetszőleges, és tekintsük az $a_i = N! + i$ számokat, $i = 2, 3, \ldots, K' + 1$ . Ekkor nyilván $i | a_i$, és $a_i > i$ , tehát valamennyi $a_i$ összetett. ♦  

Megjegyzés: A bizonyításban $N!$ helyett az $N - nél nem nagyobb prímek szorzatát is vehetjük volna.  

Az T 5.5.1 Tételt általánosítva most azt bizonyítjuk be, hogy a szomszédos prímek közötti két egymás utáni hézag is tetszőlegesen nagy lehet, azaz olyan prímek is léteznek, amelyeket mindkét oldalról sok összetett szám vesz körül (az ilyen prímeket izolált prímeknek szokták nevezni).

5.5.2 Tétel. \hspace{0.5cm} T 5.5.2

Bármely $K'$ pozitív egészhez meg lehet adni olyan $P$ prímet, amelyre a $p \pm 1, p \pm 2, \ldots, p \pm K'$ számok valamennyien összetettek. ♦  

Bizonyítás: Válasszunk egy olyan $q$ prímet, amelyre $q \geq K' + 2$, és legyen

$$d = 2 \cdot 3 \cdot (q - 2) \cdot (q - 1) \cdot (q + 1) \cdot (q + 2) \cdot (2q - 2) = \frac{(2q - 2)!}{q}.$$
Ekkor \( (q, d) = 1 \), és így Dirichlet tétele szerint létezik (végtermékenő) olyan \( k > 0 \), amelyre \( p = q + dk \) prímszám. Megmutatjuk, hogy egy ilyen \( p \) megfelel a téttal állításának.

Tetszőleges \( 1 \leq j \leq q - 2 \) esetén

\[
p = j - q + kd \pm j = (q \pm j) + \frac{k(2q - 2)!}{q!} = (q \pm j)(1 + c_j),
\]

ahol \( c_j \) pozitív egész, tehát valóban valamennyi \( p \pm j \) szám összetett.

Most Csebisev nevezetes tételét igazoljuk: egy szám és a kétszerese közé mindig esik prímszám.

**5.5.3 Tétel (Csebisev tétele).** T 5.5.3

Bármely \( n \geq 1 \) egész esetén létezik olyan \( p \) prim, amelyre \( n < p \leq 2n \).

A tételt nyilván következik, hogy az állítás (egeszek helyett) \( n \geq 1 \) valós számokra is igaz marad.

A tételt szokás Bertrand-posztulátumnak is nevezni, mert sejtésként először Bertrand fogalmazta meg 1845-ben, abban a hajszálnivalóval erősödő formában, hogy \( n > 3 \) esetén létezik olyan \( P \) prim, amelyre \( n < p \leq 2n - 2 \). (Ez az alak is igaz, sőt ennél jóval élesebb eredmények is, lást az T 5.5.4 és T 5.5.5 Tételek (A) állításait.) Az T 5.5.3 Tételt Csebisev bizonyította be 1852-ben. Az alábbi bizonyítás Erdős Páltól származik.

**Bizonyítás:** A bizonyítás alapötlete az, hogy az \( \binom{2n}{n} \) binomiális együtthatóval. A továbbiakban feltesszük, hogy \( n \geq 5 \).

I. Írjuk fel \( \binom{2n}{n} \) kanonikus alakját, és bontsuk ezt három tényező szorzatára a szereplő prímek nagysága szerint, az alábbi módon:

\[
\binom{2n}{n} = \prod_{\nu \leq 2n,} p^{\nu} \cdot \prod_{\nu = \sqrt{2n},} \frac{p^{\nu}}{\nu} \cdot \prod_{\nu = 1,} \frac{p^{\nu}}{\nu \sqrt{2n} \nu}.
\]  

Jelölje az \( 1 \) jobb oldalán álló tényezőket rendre \( A \), \( B \), illetve \( C \). A tétel bizonyításához elég azt igazolni, hogy \( C > 1 \), hiszen ekkor biztosan létezik az \( n + 1 \leq p \leq 2n \) feltételt kielégítő \( p \) prim. (Könnyen megmutatható az is, hogy \( C \)-ben minden \( \nu \) kifejezése értéke 1, azaz \( C \) éppen az \( n \) és \( 2n \) közötti prímek szorzata, lást az 5.5.7a feladatot [140].)

A \( C > 1 \) egyenlőtlenség belátásához felső becsleést keresünk \( A \), \( B \), \( C \)-re, valamint alsó becsleést \( \binom{2n}{n} \)-re.

II. Alsó becsleás \( \binom{2n}{n} \)-re: Mivel bármely \( 0 \leq k \leq 2n \) esetén \( \binom{2n}{k} \leq \binom{2n}{n} \) (lásd az 5.5.5 feladatot [140]), ezért

\[
(2n + 1) \binom{2n}{n} > \sum_{\nu = 0}^{2n} \binom{2n}{\nu} = 2^{2n},
\]

azaz

\[
\binom{2n}{n} > \frac{4^n}{2n + 1}.
\]

136
III. Felső becslés 4-ra: Az L 5.4.4 Lemma alapján \( p^\nu \leq 2n \), és így

\[
A = \prod_{\nu \leq \sqrt{2n}} p^\nu \leq (\nu!)^{\sqrt{2n}} < (\nu!)^{\sqrt{2n}}. \tag{3}
\]

IV. Felső becslés B-re: Ismét az L 5.4.4 Lemma alapján \( p^\nu \leq 2n \), és ebből \( \nu > \sqrt{2n} \) miatt \( \nu \leq 1 \) következik.

Megmutatjuk, hogy \((\nu > 2 \text{ és}) \ 2n/3 < \nu \leq \tau_1 \) esetén \( \nu = 0 \). Ez azért igaz, mert

\[
\left( \frac{2n}{\nu} \right) = \frac{2n(2n-1) \ldots (\nu+1)}{\nu!}
\]

nevezője és számlálója is egy ilyen \( P \)-nek pontosan az első hatványával osztható: a nevezőben csak a \( \frac{1}{\nu} \), a számlálóban pedig csak a \( \frac{1}{\nu} \) tényezőben szerepel a \( \frac{1}{\nu} \).

A fentiek alapján

\[
B = \prod_{\nu < \sqrt{2n} \times \nu \leq \sqrt{2n}} p^\nu = \prod_{\sqrt{2n} < \nu \leq 2n/3} p^\nu \leq \prod_{\sqrt{2n} < \nu \leq 2n/3} p. \tag{4}
\]

A (4) egyenlőtlenség és az L 5.4.5 Lemma alapján kapjuk, hogy

\[
B < \prod_{\nu < 2n/3} p < 4^{2n/3}. \tag{5}
\]

V. A (2), (3) és (5) becsléseket (1)-be beírva és \( C \)-t kifejezve kapjuk, hogy

\[
C > \frac{A^n}{(2n+1)(2n)\sqrt{2n} \cdot 4^{2n/3}} \geq \frac{4^{n/3}}{(2n+1)^{1+\sqrt{2n}}}. \tag{6}
\]

A \( C > 1 \) egyenlőtlenség igazolásához elég azt megmutatnunk, hogy a (6) jobb oldalán álló \( s_n \) kifejezés logaritmusa pozitív. Mivel

\[
\log s_n = \frac{n \log 4}{3} - (1 + \sqrt{2n}) \log(2n+1) \rightarrow \infty, \quad \text{ha} \quad n \rightarrow \infty, \tag{7}
\]

ezért minden \( n \) esetén \( \log s_n > 0 \). Könnyen adódik, hogy például \( n > 511 \) esetén \( s_n > 0 \).

VI. Végül az \( n \leq 511 \) értékekre közvetlenül ellenőrizhetjük a tétele állítását. Ehhez elegendő a 2-ből kiindulva olyan prímszám-sorozatot készítenünk, amelynek bármiely eleme kisebb, mint a megelőző elemnek a kétszerese. Egy ilyen sorozat például a következő: 2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631. (Az éppen a Csebisev-tételből következik, hogy ilyen tulajdonságú végtelen sorozat is létezik.)

A Csebisev-tétellel kapcsolatban felvethetjük a következő általánosabb „hézagfüggvény” problémát:

Milyen \( h(n) \) függvényekre igaz, hogy minden \( n \) esetén \( \log h(n) \) nyílt intervallumban található primszám?

A Csebisev-tétel szerint \( h(n) = \nu \) megfelel, az T 5.5.1 Tétel alapján viszont a \( \hat{h}(\nu) \) nem választható konstans függvénynek, hiszen az \( (\nu, \nu + K) \) intervallum bármilyen rögzített \( K \) esetén végtelen sok \( \hat{h}(\nu) \) -re „primmentes”.

137
Megoldatlan probléma, hogy milyen nagyságrendű a „lehető legjobb” \( h(n) \). Erre vonatkozóan a következő eredmények ismertek (ezeket bizonyítás nélkül közöljük):

**5.5.4 Tétel.** T 5.5.4

(A) Legyen \( \theta = 0,5351 \). Ekkor minden elég nagy \( n \)-re az \((n, n + \theta n)\) intervallum tartalmaz prímszámot.

(B) Végtelen sok olyan \( n \) pozitív egész létezik, amelyre az

\[
\left( n, n + \frac{\log n \cdot \log \log n \cdot \log \log \log n}{(\log \log n)^2} \right)
\]

intervallum nem tartalmaz prímszámot.

Az T 5.5.4 Tétel mindkét állítása igen mély eredmény (például jóval élesebbek, mint a prímszám-tételből leolvasható következtetések, lásd az T 5.5.5 Télelt), ennek ellenére hatalmas űr tátong közöttük; a \( h(n) \) választható \( n^\theta \)-nak, és nem választható egy \( \log n \)-nél „nem sokkal nagyobb” függvénynek. Bizonyos valószínűségi megfontolások alapján azt lehet sejteni, hogy a \((\log n)^2\) függvény „környékén” várható a választóvonal.

Érdekességgént megjegyezzük, hogy (A)-ból még az az 5.1 pontban már említett, ártatlannak látszó sejtés sem következik, hogy két egymást követő négyzetszám között mindig található prímszám.

Ehhez az (A)-beli \( \theta \)-nak \( \frac{1}{2} \)-re történő leszorítása szükséges, amit még az ún. Riemann-sejtés felhasználásával sem sikerült igazolni.

Az alábbiakban azt mutatjuk meg, hogy a prímszám-tétel segítségével mennyire élesíthetők az T 5.5.3 és T 5.5.1 Tételek eredményei.

**5.5.5 Tétel.** T 5.5.5

(A) Bármely \( \varepsilon > 0 \) -hoz létezik olyan \( \eta \)-tól függő \( \eta_0 \), hogy minden \( n > \eta_0 \) esetén az \((n, (1 + \varepsilon)n)\) intervallum tartalmaz prímszámot.

(B) Bármely \( 0 < \varepsilon < 1 \) esetén végtelen sok olyan \( n \) pozitív egész létezik, amelyre az \((n, n + (1 - \varepsilon) \log n)\) intervallum nem tartalmaz prímszámot.

\[\text{Bizonyítás: Az (A) részhez azt kell igazolnunk, hogy minden elég nagy } n \text{-re}
\]

\[
\pi((1 + \varepsilon)n) - \pi(n) > 0.
\]

(8)

A prímszám-tétel szerint minden elég nagy \( n \)-re egyrészt

\[
\pi(n) < \left( 1 + \frac{\varepsilon}{4} \right) \cdot \frac{\tau_2}{\log n},
\]

másrészt

\[
\pi((1 + \varepsilon)n) > \left( 1 - \frac{\varepsilon}{4} \right) \cdot \frac{\tau_2}{\log((1 - \varepsilon)\tau_2)}
\]

(10)

teljesül, továbbá nyilván
PRÍMSZÁMOK

\[ \log\left(1 + \varepsilon n\right) = \log(1 + \varepsilon) + \log n < \left(1 + \frac{\varepsilon}{4}\right) \log n. \quad (11) \]

(9), (10) és (11) alapján

\[ \pi\left(1 + \varepsilon n\right) - \pi(n) > \left(1 - \frac{\varepsilon}{4}\right) - \left(1 + \frac{\varepsilon}{4}\right) = \frac{n}{\log n}, \quad (12) \]

(12) jobb oldalán az \(\frac{n}{\log n}\) együtthatója

\[ \frac{\left(1 - \frac{\varepsilon}{4}\right) - \left(1 + \frac{\varepsilon}{4}\right)}{1 + \frac{\varepsilon}{4}} > 0 \]

(hiszen feltehető, hogy \(\varepsilon < 4/5\)), és így (12)-ből következik (8).

A (B) állítást indirekt bizonyítjuk. Tegyük fel, hogy van olyan \(\varepsilon > 0\) és olyan \(n_0\), hogy minden \(n > n_0\) esetén az \(n, \pi(n) + (1 - \varepsilon) \log n\) intervallum tartalmaz prímszámont.

Legyen \(N\) egy (nagy) rögzített egész, és tekintsük az \(n_0\) és \(N\) közötti prímszámatokat: \(n_0 < p_r < p_{r-1} < \cdots < p_k \leq N\). Ekkor az indirekt feltevés alapján az alábbi egyenlőtlenségeket kapjuk:

\[
\begin{align*}
p_{r+1} &< p_r + (1 - \varepsilon) \log p_r, \\
p_{r+2} &< p_{r+1} + (1 - \varepsilon) \log p_{r+1}, \\
&
\end{align*}
\]

\[ (13) \]

A (13)-beli egyenlőtlenségeket összeadva a \(p_{r+1}, \cdots, p_k\) tagok kiesnek, és

\[ p_{k+1} < p_r + (1 - \varepsilon) \sum_{j=r}^{k} \log p_j \quad (14) \]

adódik.

A \(p_k\) definíciója szerint \(p_{k-1} > N\), ezért az ellentmondáshoz elég azt megmutatnunk, hogy (14) jobb oldala viszont kisebb, mint \(N\).

Ehhez (14) jobb oldalát a következőképpen becsüljük felülől:

\[ p_r + (1 - \varepsilon) \sum_{j=r}^{k} \log p_j < p_k + (1 - \varepsilon) \pi(N) \log N. \quad (15) \]

A prímszámtétel szerint elég nagy \(N\) esetén

\[ \pi(N) < \left(1 + \frac{\varepsilon}{4}\right) \frac{N}{\log N}, \quad (16) \]

továbbá (elég nagy \(N\)-re) nyilván

\[ p_k < \frac{\varepsilon N}{4}. \quad (17) \]
A (16) és (17) egyenlőtlenségeket (15)-be beírva azt nyerjük, hogy (14) jobb oldala kisebb, mint
\[ (1 - \frac{c}{4})(1 + \frac{c}{4}) + \frac{c}{4}N < (1 - \frac{c}{2})N < N, \]
amivel megkapjuk a már jelzett ellentmondást. ■

Feladatok

5.5.1 Bizonyítsuk be, hogy \( n > 1 \) esetén \( n! \) nem lehet teljes hatvány.

5.5.2 Igazoljuk, hogy bármely két szomszédos pozitív egész közül legalább az egyik felírható csupa különböző prímszám összegeként (egytagú összeget is megengedünk).

5.5.3 Mutassuk meg, hogy végig telen sok olyan prím van, amelynek (tízes számrendszerben)
(a) az első számjegye 1-es;
(b) az első ezer számjegye 4-es.

5.5.4 Bizonyítsuk be, hogy ha \( 1 \leq k < n \), akkor az alábbi összegek értéke nem lehet egész szám:
(a) \( \sum_{j=1}^{n} \frac{1}{j} \)
(b) \( \sum_{j=1}^{n} \frac{1}{j} \)

5.5.5 Mutassuk meg, hogy a \( \binom{2n}{k} \), \( 0 \leq k \leq 2n \), binomiális együtthatók közül \( \binom{2n}{n} \) a legnagyobb.

5.5.6 Adjunk meg egy bizonyítást az T 5.5.2 Tételre az alábbi gondolatmenet alapján: Válasszunk \( 2K \) darab \( K \)-nél nagyobb prímszámot, legyenek ezek \( p_1, \ldots, p_K \), \( q_1, \ldots, q_K \), és tekintsük az
\[ x \equiv j \pmod{p_j}, \quad x \equiv -j \pmod{q_j}, \quad j = 1, 2, \ldots, K \]
szimultán kongruenciarendszert. Mutassuk meg, hogy ennek megoldásai között található (végig telen sok) \( P \) prímszám, és ezek kielégíti a tétel feltételeit.

5.5.7 (a) Bizonyítsuk be, hogy \( \binom{2n}{n} \) minden \( n + 1 \leq p \leq 2n \) prímszámnak pontosan az első hatványával osztható.

(b) Mutassuk meg, hogy ha \( p > 3 \) prím és \( 2n/5 < p < n/2 \), akkor \( \binom{2n}{n} \) nem osztható \( P \) -vel. Hogyan átalánosítható ez az észrevétel?

5.5.8 Mutassuk meg, hogy \( n \geq 2 \) esetén a Csebisev-tételre adott bizonyításból az alábbi élesebb eredmény is következik: Az \( n \) és \( 2n \) közötti prímek száma nagyobb, mint \( c n / \log n \), ahol \( c \) alkalmas pozitív konstant.

5.5.9 \( (M[570]) \) (a) Az T 5.5.4 Tétel (A) részének a felhasználásával lássuk be, hogy bármely két elég nagy, egymást követő köbszám között található prímszám.

(b) * Bizonyítsuk be, hogy létezik olyan \( \alpha > 1 \) valós szám, amelyre \( \alpha^{1/n} \) minden \( n \) pozitív egész esetén prímszám.

(c) Miért nem alkalmas a (b)-beli képlet nagy prímszámok gyakorlati előállítására?
5.5.10 Vizsgáljuk meg, hogy milyen, az T 5.5.5 Tétel (B) állításához hasonló jellegű eredményeket nyerhetünk, ha a prímszámtétel helyett az alábbiakra támaszkodunk:

(a) T 5.4.3 Tétel;

(b) az T 5.5.1 Tétel bizonyítása;

(c) az T 5.5.1 Tétel bizonyítása utáni megjegyzés.

5.5.11 (*) Bizonyítsuk be, hogy bármely \( \varepsilon > 0 \) -höz vég.tlen sok olyan \( n \) pozitív egész létezik, amelyre \( p_{n+1} - p_n < (1 + \varepsilon) \log n \) . (A szokásos módon \( p_n \) az \( n \) -edik prímszámot jelöli.)

Megjegyzés: Az 5.1 pontban tárgyalt ikerprimprobléma úgy is fogalmazható, vajon vég.tlen sokszor teljesül-e \( p_{n+1} - p_n = 2 \) . Örülési szenzációt jelentett, amikor 2005-ben Goldston, Motohashi, Pintz János és Yildirim bebizonyítottak, hogy a \( \{p_{n+1} - p_n\} / \log n \) sorozatnak létezik 0-hoz tartó részsorozata (ami látszólag „alig” erősebb, mint az 5.5.11 feladat [141] állítása). 2013-ban pedig Zhang újabb áttörést ért el: megmutatta, hogy \( p_{n+1} - p_n \)-nek létezik korlátos(!) részsorozata (2014-ben a legjobb korlát 250 körül van).

5.6 A prímek reciprokösszege

Ebben a pontban bebizonyítjuk, hogy a prímszámok reciprokából képzett vég.tlen sor divergens. Ez azt jelenti, hogy a prímszámok reciprokái „lassan” fognak, azaz maguk a prímszám növekednek, vagyis a prímek „viszonylag sűrű” helyezkednek el a pozitív egészek között. Összehasonlíttásképpen, a négyszetszámok reciprokából képzett vég.tlen sor convergens, azaz a négyszetszámok a pozitív egészkek egy „ritka” részsorozatát alkotják (vö. az T 5.4.1 Tétel utáni 2. megjegyzéssel).

A prímszám reciprokösszegének divergenciájára három bizonyítást adunk. Az első mutatja, hogy ez a tény a prímszámtételtől (sőt már az T 5.4.3 Tételből is) következik. A második Erdős Pál szellemes indirekt gondolatmenete. A harmadik Euler bizonyítása, aki először mondta ki és igazolta ezt a téttel.

Végül megmutatjuk, hogy az \( x \) -nél nem nagyobb prímkövet is konvergálják az adott számon, hogy az \( \log \log x \) függvénnyel.

5.6.1 Tétel .  T 5.6.1

A prímszám reciprokából képzett vég.tlen sor divergens, azaz

\[
\sum_{p} \frac{1}{p} = \infty. \quad \blacktriangleleft
\]

Első bizonyítás: Azt kell igazolnunk, hogy

\[
\lim_{n \to \infty} \frac{1}{\log \log n} \sum_{j=1}^{n} \frac{1}{p_j} = \infty,
\]

ahol \( p_j \) a \( j \) -edik prímszámot jelöli.

Az T 5.4.2 Tétel (vagy az 5.4.3 feladat [134]) szerint létezik olyan \( c \) és \( n_0 \), hogy minden \( j \geq n_0 \) esetén \( p_j <cj \log j \) . Ebből következik, hogy

\[
\sum_{j=1}^{n} \frac{1}{p_j} > \frac{1}{c} \sum_{j=\infty}^{n_0} \frac{1}{j \log j}. \quad \blacktriangleleft
\]
Rajzoljunk minden $a_0 \leq j \leq n$ egész számhoz egy olyan téglalapot, amelynek az alapja az $x$ tengely $[j, j+1]$ szakasza, magassága pedig $1/(\log j)$ . Ekkor a téglalapok területének összege éppen a (2) jobb oldalán szereplő összeg (az $1/x$ szorzó nélkül).

Mivel az $1/(x \log x)$ függvény ($x > 1$ esetén) monoton csökken, ezért az $[n_0, n + 1]$ intervallumon a függvény görbe a téglalapok alakta alakzatban halad. Emiatt a függvény görbe alatti terület kisebb, mint a téglalapok területének az összege, azaz

$$\sum_{j=n_0}^{n} \frac{1}{j \log j} > \int_{n_0}^{n+1} \frac{dx}{x \log x}. \quad (3)$$

A (3) jobb oldalán szereplő integrált kiszámítva

$$\int_{n_0}^{n+1} \frac{dx}{x \log x} = \left[ \log \log x \right]_{n_0}^{n+1} = \log \log (n+1) - \log \log n_0 \quad (4)$$

adódik. A (3) és (4) összefüggések felhasználásával a (2) egyenlőtlenségből

$$\sum_{j=n_0}^{n} \frac{1}{j} > \frac{1}{e} \left( \log \log (n+1) - \log \log n_0 \right) \quad (5)$$

következik. Mivel

$$\lim_{n_0 \to \infty} \log \log n = \infty,$$

ezért $n \to \infty$ esetén (5)-ben a jobb oldal, és emiatt a bal oldal is a végétlenhez tart, azaz (1) valóban teljesül.

Megjegyzés: A bizonyításból az is leolvasható, hogy alkalmas $c'$ konstansssal minden elég nagy $n$ esetén fennáll

$$\sum_{p \leq n} \frac{1}{p} > c' \log \log n. \quad (5a)$$

Ugyanígy igazolható

$$\sum_{p \leq n} \frac{1}{p} < c'' \log \log n.$$

is, sőt a prímszámtétel (vagy az azzal ekvivalens T 5.4.2 Tétel) kicsit ügyesebb alkalmazásával

$$\sum_{p < \sqrt{n}} \frac{1}{p} \sim \log \log n.$$

következik. Ezeknél is élessebb becslést kapunk majd azonban az T 5.6.2 Tételben (ráadásul a prímszámtétel felhasználása nélkül), sőt már az T 5.6.1 Tételre adott harmadik bizonyítás (13) egyenlőtlensége is sokkal erősebb (5a)-nál.

 Második bizonyítás: Tegyük fel indirekt, hogy a prímek reciprokösszege konvergents. Ekkor létezik olyan $k$ , hogy
Rögzitsük le $k$ értékét, és osszuk a pozitív egészeket két csoportba: az első csoportba azok a számok kerülnek, amelyeknek van $p_k$-nál nagyobb prímosztója, a második csoportot pedig azok a számok alkotják, amelyeknek minden prímosztója kisebb vagy egyenlő, mint $p_k$.

Legyen $N$ (nagy) természetes szám, és tekintsük a $\mathcal{H} = \{1, 2, \ldots, N\}$ halmazt. Meg fogjuk mutatni, hogy elég nagy $N$-et választva, a $\mathcal{H}$ elemeinek kevesebb, mint a fele tartozik az első csoportba, és ugyancsak kevesebb, mint a fele tartozik a második csoportba, ami nyilvánvaló ellentmondás.

Vizsgáljuk először az első csoportot. Tetszőleges $\mathcal{P}$ prim esetén $\mathcal{H}$ -ban a $\mathcal{P}$ -vel osztható elemek száma $\lfloor \frac{N}{p} \rfloor$. Ebből az első csoportbeli elemek darabszámára a következő felső becslés adódik:

$$\sum_{p_k < p \leq N} \left\lfloor \frac{N}{p} \right\rfloor \leq \sum_{p_k < p \leq N} \frac{N}{p} < \sum_{j=1}^{\infty} \frac{1}{j} < \frac{N}{2}$$

(az utolsó lépésben (6)-ot használtuk fel). Ez azt jelenti, hogy $\mathcal{H}$ elemeinek kevesebb, mint a fele tartozik az első csoportba.

A második csoport vizsgálatához felhasználjuk, hogy minden pozitív egész (egyértelműen) előállítható egy négyzetes és egy négyzetmentes szám szorzataként. Ez a számelmélet alaptételéből következik: Válasszuk külön $n$ kanonikus alakjában a páros és páratlan kitevőket:

$$n = q_1^{2^{\alpha_1}} \cdots q_k^{2^{\alpha_k}} q_{r-1}^{2^{\beta_1}} \cdots q_s^{2^{\beta_s}} + 1$$

(ahol $r = 0$, illetve $r = s$ is megengedett), ekkor

$$n = \left( q_1^{\alpha_1} \cdots q_k^{\alpha_k} q_{r-1}^{\beta_1} \cdots q_s^{\beta_s} \right)^2 \cdot (q_{r+1} \cdots q_s)$$

adjá a kívánt előállítást.

Írjuk fel $\mathcal{H}$ -nak a második csoportba tartozó elemeit ilyen $a^2b$ alakban (ahol $b$ négyzetmentes). Ekkor $1 \leq a \leq \lfloor \sqrt{N} \rfloor$, továbbá $b$ a $q_1 \cdots q_k$ primek közül néhány különbözőnek (akár az összesnek) a szorzata (de $b$ lehet az üres szorzat is, ekkor $b = 1$).

Ebből következik, hogy az $a^2$ választására $\lfloor \sqrt{N} \rfloor$ lehetőség adódik, a $b$ választására pedig $2^k$ (ahány részhalmaz van a $\{q_1, \ldots, q_k\}$ halmaznak). Ennél foga az ilyen $a^2b$ szorzatok száma legfeljebb $\sqrt{N} \cdot 2^k$. Mivel $k$ rögzített, ezért elég nagy $N$ esetén $2^k < \sqrt{N}/2$, tehát $\sqrt{N} \cdot 2^k < N/2$. Ezzel igazoltuk, hogy $\mathcal{H}$ elemeinek kevesebb, mint a fele tartozik a második csoportba.

Harmadik bizonyítás: Felhasználjuk a következő (analízisbeli) tételeket:

(i) $\sum_{j=1}^{\infty} \frac{1}{j} > \log n$;

(ii) $\sum_{j=1}^{\infty} \frac{1}{j^2} < 2$;

(iii) $\log \left( \frac{1}{1-x} \right) = x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots \leq x + x^2$, ha $0 \leq x \leq \frac{1}{2}$.

Rátérve a tételünk bizonyítására, tekintsük a következő szorzatot:
PRÍMSZÁMOK

\[ A_n = \prod_{p \leq n} \left( 1 + \frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^n} \right), \]

ahol \( n > 1 \) egész és

\[ p^\nu_s \leq n < p^{\nu_s + 1}, \quad \text{és az} \quad \nu_p = \lfloor \log_p n \rfloor. \]

Megmutatjuk, hogy

\[ A_n > \sum_{j=1}^{\nu_s} \frac{1}{j}. \quad (7) \]

Legyen először \( n = 10 \), és írjuk ki az \( A_{10} \) tényezőit részletesen:

\[ A_{10} = \left( 1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} \right) \left( 1 + \frac{1}{3} + \frac{1}{3^2} \right) \left( 1 + \frac{1}{5} \right) \left( 1 + \frac{1}{7} \right). \]

Ha \( j \leq 10 \), akkor \( j \) kanonikus alakjában csak a 2, 3, 5, 7 prímek fordulhatnak elő, éspedig legfeljebb akkora kitevővel, mint amilyennel az \( A_{10} \) egyes tényezőiben szerepelnek. Ezért tetszőleges \( j \leq 10 \) előállítható (ráadásul egyértelműen) ezen primhatványok sorozataként. Ez azt jelenti, hogy ha elvégezzük a sorozást \( A_{10} \)-ben, akkor biztosan megkapjuk minden \( j \leq 10 \) szám reciprokát, és így \( A_{10} \geq \sum_{j=1}^{10} 1/j \).

Ugyanezt a megondolást a 10 helyett tetszőleges \( n \) -re végrehajtva a (7) egyenlőtlenséget nyerjük. Ebből (i) felhasználásával

\[ A_n > \log n \quad (8) \]

adódik.

Most felső becslést keresünk \( A_n \)-re. Az \( A_n \) tényezőiben szereplő mértani sorozatokat összegezve kapjuk, hogy

\[ A_n = \prod_{p \leq n} \frac{1 - \left(\frac{1}{p}\right)^{\nu_s+1}}{1 - \frac{1}{p}} < \prod_{p \leq n} \frac{1}{1 - \frac{1}{p}}. \quad (9) \]

A (8) és (9) egyenlőtlenségekből

\[ \log n < \sum_{p \leq n} \frac{1}{1 - \frac{1}{p}} \quad (10) \]

adódik. (10)-et logaritmálva a

\[ \log \log n < \sum_{p \leq n} \log \frac{1}{1 - \frac{1}{p}} \quad (11) \]

eyenlőtlenséget kapjuk. A (11) jobb oldalát (iii) szerint felülről becsülve

\[ \log \log n < \sum_{p \leq n} \frac{1}{p} + \sum_{p \leq n} \frac{1}{p^2} \quad (12) \]
adódik. Végül (ii) miatt a (12) jobb oldalán álló második összeg kisebb, mint 2, és így

\[ \sum_{p \leq \sqrt{n}} \frac{1}{p} \geq \log \log n - 2, \tag{13} \]

amiből a tétel állítása következik. □

A harmadik bizonyításból azt is megkaptuk, hogy az \( n \)-nél nem nagyobbnak primek reciprokösszege nem lehet lényegesen kisebb \( \log \log n \)-nél (lásd a (13) egyenlőtlenséget). A következőkben ezt tovább élesíjük, és azt igazoljuk, hogy ennek a reciprokösszegnek a \( \log \log n \)-től való eltérése korlátos:

### 5.6.2 Tétel

Létezik olyan \( c \) konstans, hogy minden \( n \geq 3 \) egész számra

\[ \sum_{p \leq \sqrt{n}} \frac{1}{p} - \log \log n < c. \tag{14} \]

**Bizonyítás:** A bizonyításhoz szükségünk lesz a \( \sum_{p \leq \sqrt{n}} \frac{1}{p} \) összeg becsélére:

### 5.6.3 Tétel

Létezik olyan \( c' \) konstans, hogy minden \( n \geq 2 \) egész számra

\[ \sum_{p \leq n} \frac{\log p}{p} - \log \log n < c'. \tag{15} \]

Az 5.6.3 Tétel bizonyítása: Induljunk ki az \( n! \) kanonikus alakjából (T 1.6.8 Tétel). Ezt logaritmálva

\[ \log n! = \sum_{p \leq \sqrt{n}} \log p \left( \frac{n}{p} \right) + \frac{n}{p^2} + \frac{n}{p^3} + \cdots \] \tag{16}

adódik. Meg fogjuk mutatni, hogy (16) bal oldala „körülbelül“ \( n \log \log n \), a jobb oldalon pedig a \( \log p \) szorzójában „az egészrész elhagyható és csak az első tag számít”, vagyis a jobb oldal „körülbelül”

\( n \sum_{p \leq n} \frac{1}{p} \). Innen \( n \)-nél való osztás után kapjuk a kivánt (15) egyenlőtlenséget.

Nézzük mindezt pontosan és részletesen. A (16) bal oldalán álló \( \log n! \) becséléshez használjuk fel, hogy \( n \geq 2 \) -re

\[ \left( \frac{n}{e} \right)^n < n! < n^n. \]

Itt a felső becslés nyilvánvaló, az alsó becslés pedig könnyen igazolható teljes indukcióval. Ezeket az egyenlőtlenségeket logaritmálva kapjuk, hogy

\[ n(\log n - 1) < \log n! < n \log n. \tag{17} \]

Az \( \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots \) összeget a következőképpen becsülnthetjük:

\[ \frac{n}{p} - 1 < \frac{n}{p} + \frac{n}{p^2} + \cdots < \frac{n}{p} + \frac{n}{p^2} + \cdots = \frac{n}{p(\sqrt{p} - 1)}. \tag{18} \]

Jelöljük (16) jobb oldalát \( J \)-vel. Ekkor (18) alapján \( J \) -re az alábbi becsléseket nyerünk:
Az L 5.4.5 Lemma alapján

\[ \sum_{p \leq a} \log p < \sum_{p \leq a} \frac{\log p}{p} < j < \sum_{p \leq a} \frac{\log p}{p} + \sum_{p \leq a} \frac{\log p}{p(p-1)} \tag{19} \]

továbbá

\[ \sum_{p \leq a} \frac{\log p}{p(p-1)} < \sum_{k=2}^{\infty} \frac{\log k}{k(k-1)} \tag{21} \]

ahol a (21) jobb oldalán álló végtelen sor konvergens, és az is megmutatható, hogy az összege kisebb, mint 4.

A (20) és (21) egyenlőtlenségek felhasználásával (19)-ből kapjuk, hogy

\[ \left| \frac{j}{n} - \sum_{p \leq a} \frac{\log p}{p} \right| < 4. \tag{22} \]

Ugyanakkor (16) alapján \( J = \log n! \), ezért (17)-ből

\[ \left| \frac{j}{n} - \log n \right| < 1 \tag{23} \]

döntően következik. Végül (22) és (23) miatt (15) is teljesül (például \( c' = 5 \) megfelel). □

Az T 5.6.2 Tétel bizonyításához kényelmesebb, ha az T 5.6.3 Tételt az egész \( n \) értékekről tetszőleges \( x \geq 2 \) valós számra is kiterjesztjük. Ehhez vegyük észre, hogy

\[ \sum_{p \leq x} \frac{\log p}{p} = \sum_{p \leq \lfloor x \rfloor} \frac{\log p}{p} \leq \frac{x}{\lfloor x \rfloor} < \log \frac{3}{2} \]

és így (15) alapján

\[ \left| \sum_{p \leq x} \frac{\log p}{p} - \log x \right| \leq \left| \sum_{p \leq \lfloor x \rfloor} \frac{\log p}{p} - \log \lfloor x \rfloor \right| + \left| \log \lfloor x \rfloor - \log x \right| < c' + \log \frac{3}{2}. \]

Ezzel megmutattuk, hogy tetszőleges \( x \geq 2 \) valós szám esetén

\[ \left| \sum_{p \leq x} \frac{\log p}{p} - \log x \right| < 6. \tag{24} \]

Vezessük még be a következő jelöléseket tetszőleges \( x \geq 2 \) valós számra:

\[ f(x) = \sum_{p \leq x} \frac{\log p}{p}, \quad g(x) = \frac{1}{\log x} \quad és \quad h(x) = f(x) - \log x. \tag{25} \]

Az \( f(x) \) és \( g(x) \) definiciója alapján \( f(2) g(2) = 1/2 \), továbbá bármely \( k \geq 3 \) egész szám esetén
PRÍMSZÁMOK

\[(f(k) - f(k - 1))g(k) = \begin{cases} \frac{1}{k}, & \text{ha } k \text{ prím;} \\ 0, & \text{ha } k \text{ nem prím.} \end{cases} \]

Ebből következik, hogy tetszőleges \( n \geq 3 \) egészre fennáll

\[
\sum_{j \leq n} \frac{1}{j} = f(2)g(2) + \sum_{k=1}^{n} (f(k) - f(k - 1))g(k). \tag{25}
\]

(26) jobb oldalát az ún. parciális összegezés (Abel-féle átrendezés) segítségével átalakítva kapjuk, hogy

\[
\sum_{j \leq n} \frac{1}{j} = f(2)(g(2) - g(3)) + f(3)(g(3) - g(4)) + \ldots
\]

\[
\ldots + f(n)(g(n) - g(n+1)) + f(n+1)g(n). \tag{27}
\]

Most megmutatjuk, hogy (27) jobb oldalán az összeg egy általános tagja (az utolsó kivételével)

\[
f(k)(g(k) - g(k + 1)) = - \int_{k}^{k+1} f'(t)g'(t)dt \tag{28}
\]

alakba írható. Ez azért igaz, mert a (balról zárt, jobbról nyílt) \([k, k + 1]\) intervallumon az \( f'(t) \)

függvény értéke a konstans \( f'(k) \), továbbá a Newton–Leibniz-szabály szerint

\[
\int_{k}^{k+1} f'(t)dt = g(k + 1) - g(k). \tag{28}
\]

(28) felhasználásával (27)-ből a következő egyenlőséget nyerjük:

\[
\sum_{j \leq n} \frac{1}{j} = f(n)g(n) - \int_{2}^{n} f(t)g'(t)dt. \tag{29}
\]

Most kiszámítjuk a (29) jobb oldalán szereplő integrált az

\[
f'(t) = \log t + i(t) \quad \text{és} \quad g'(t) = \left( \frac{1}{\log t} \right)' = -\frac{1}{(\log t)^2}
\]

összefüggések felhasználásával:

\[
- \int_{2}^{n} f'(t)g'(t)dt = \int_{2}^{n} \frac{dt}{i(t)} + \int_{2}^{n} \frac{l(t)dt}{(\log t)^2}. \tag{30}
\]

A (30) jobb oldalán szereplő első integrál

\[
\int_{2}^{n} \frac{dt}{i(t)} = \left[ \log \log t \right]_{2}^{n} = \log \log n - \log \log 2. \tag{31}
\]

A (30) jobb oldalán szereplő második integrál

\[
\int_{2}^{n} \frac{l(t)dt}{(\log t)^2} < 6 \int_{2}^{n} \frac{dt}{t(\log t)^2} = 6 \left[ \frac{1}{\log t} \right]_{2}^{n} = \frac{6}{\log 2} \tag{32}
\]

\[
- \frac{6}{\log n}.
\]
Most azt igazoljuk, hogy a (29) jobb oldalán álló \( f(n)g(n) \) szorzat is korlátos:

\[
|f(n)g(n)| = \left| \frac{\log n + h(n)}{\log n} \right| = \left| 1 + \frac{h(n)}{\log n} \right| < 1 + 6 = 7. \tag{34}
\]

Végül (29)-et (33)-mal és (34)-gyel összevetve kapjuk az T 5.6.2 Tétel állítását.

Megjegyzés: A (32) becslést helyett az intervallumra megismételve kiderül, hogy esetén a (30) jobb oldalán szereplő második integrálnak létezik határértéke, és az attól való eltérés abszolút értéke legfeljebb \( 6/\log n \). Ugyanez -re nyilvánvaló. Így létezik olyan \( c_1 \) és \( c_2 \) konstans, hogy minden \( n \geq 3 \) egészre

\[
\left| \sum_{\nu \leq n} \frac{1}{\nu} - \log \log n - c_1 \right| \leq \frac{c_2}{\log \log n}.
\]

Feladatok

5.6.1 (M [571]) Legyen \( \mathbb{L} \) rögzített pozitív egész. Tekintsük a pozitív egészek alábbi részsorozatait, és döntsük el, hogy az elemek reciprokainál álló végleten sorok konvergensek vagy divergensek-e:

(a) az \( \mathbb{L} \) -lel osztható számok;

(b) a teljes hatványok;

(c) a négyzetmentes számok;

(d) azok a számok, amelyeknek minden prímosztója kisebb, mint \( \mathbb{L} \); 

(e) azok a számok, amelyeknek minden prímosztója nagyobb, mint \( \mathbb{L} \); 

(f) azok a számok, amelyek kanonikus alakjában minden prímszám kitevője legalább 2 (ezeket négyzetmentes számoknak szokták hívni).

A (c) sorozat kivételével vizsgáljuk meg azt is, hogy nagy \( n \) esetén az egyes számsorozatoknak "körűbelül" hány elemük van \( n \) -ig; ez pontosabban azt jelenti, hogy ha az \( U = \{ u_1 < u_2 < \ldots \} \) sorozatról van szó, akkor az \( U(n) = \sum_{u_i \leq n} 1 \) függvényre keresünk aszimptotikát, illetve minél jobb becséléseket. (A négyzetmentes számokra vonatkozó eredményt lásd a 6.7.2 feladatban [211].)

5.6.2 Az T 5.6.1 Tételre adott első bizonyításban alkalmazott "integrálkritérium" segítségével döntsük el, hogy az alábbi végleten sorok konvergensek vagy divergensek-e:

(a) \( \sum_{n=1}^{\infty} \frac{1}{n^{3/2}} \); 

(b) \( \sum_{n=2}^{\infty} \frac{1}{n(\log n)^3} \); 

(c) \( \sum_{n=2}^{\infty} \frac{1}{n \log n \cdot \log \log n} \).
5.6.3 Az alábbi végleten sorokban az összegzés a prímek szerint történik. Vizsgáljuk meg a konvergencia, illetve divergencia kérdését:

(a) $\sum_{p \in \mathbb{P}} \frac{1}{p \log p}$ ;
(b) $\sum_{p \in \mathbb{P}} \frac{1}{p \log \log p}$ .

5.6.4 Tekintsük a pozitív egészek alábbi típusú $a_1 < a_2 < \ldots$ részsorozatait. Mit állíthatunk az elemek reciprokáiból álló végleten sorokról a konvergencia/divergencia szempontjából? (Lehetséges válaszok: biztosan konvergens — biztosan divergens — lehet konvergens, és lehet divergens is.)

(a) Az $a_n$ elemek páronként relatív prím összetett számok.
(b) Minden $n$-re az $a_n$ kanonikus alakjában a prímek kiveőinek az összege legalább $2 \log \frac{n}{2}$ .
(c) Minden $n$-re $a_{n+1} - a_n < 10^{1000}$ .
(d) Minden $n$-re $\frac{a_{n+1}}{a_n} < 1.00001$ .
(e) Az $a_n$ elemek között nincs két olyan, amelynek ugyanannnyi osztója lenne.

5.6.5 Ha az $A = \{a_1 < a_2 < \ldots\}$ pozitív egészekből álló számsorozatra $\sum_{n=1}^{\infty} \frac{1}{a_n} < \infty$ , akkor ez azt jelenti, hogy az $A$ „ritka”. Érdemes-e a ritkaság fogalmát aszerint finomítani, hogy mekkora a $\sum_{n=1}^{\infty} \frac{1}{a_n}$ összeg?

5.6.6 (M [575]) Tetszőleges $s > 1$ valós számra a Riemann-féle zétafüggvényt a következőképpen definiáljuk:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} , \quad (35)$$

Ismeretes (vagy az 5.6.2a feladat [148] mintájára igazolható), hogy a (35) jobb oldalán álló végleten sor ($s > 1$ esetén) konvergens. Például $\zeta(2) = \pi^2 / 6$ .

Most egy végleten szorzatot értelmezünk ($\mathbb{P}$ a primeken fut végig):

$$\prod_{p} \frac{1}{1 - \frac{1}{p^s}} = \lim_{n \to \infty} \prod_{p \leq n} \frac{1}{1 - \frac{1}{p^s}} . \quad (36)$$

Bizonyítsuk be, hogy $s > 1$ esetén a (36) jobb oldalán szereplő határérték létezik és egyenlő $\zeta(s)$ -sel.

5.6.7 Legyen $0 < a_j < 1 , \ j = 1, 2, \ldots$ és definiáljuk az alábbi végleten szorzatot:

$$\prod_{j=1}^{\infty} (1 - a_j) = \lim_{n \to \infty} \prod_{j=1}^{n} (1 - a_j) .$$

Bizonyítsuk be, hogy

$$\sum_{j=1}^{\infty} a_j = \infty \iff \prod_{j=1}^{\infty} (1 - a_j) = 0 .$$

Megjegyzés: Általában egy (nulla tényezőket nem tartalmazó) végleten szorzatot akkor nevezzük konvergensnek, ha a részletszorzatok sorozatának létezik véges és $0$-től különböző határértéke.
5.6.8 (*) Az 5.6.1 Tétel harmadik bizonyítása során megmutattuk (lásd a (10) egyenlőtlenséget), hogy

\[
\log n < \prod_{\nu \leq n} \frac{1}{1 - \frac{1}{\nu}}.
\]

Bizonyítsuk be, hogy érvényes az alábbi fordított irányú becslés is: létezik olyan \( c \) konstans, amelyre (minden \( n \geq 2 \) esetén)

\[
c^{\log n} \geq \prod_{\nu \leq n} \frac{1}{1 - \frac{1}{\nu}}.
\]

5.6.9 Legyen \( a > 1 \), és jelölje \( p_v(a) \), illetve \( P_v(a) \) az \( a \) legkisebb, illetve legnagyobb prímosztóját. Döntsük el, hogy az alábbi végleten sorok konvergensek vagy divergensek-e:

(a) \( \sum_{n=2}^{\infty} \frac{1}{n p_v(n)} \);

(b) \( \sum_{n=2}^{\infty} \frac{1}{a P_v(a)} \).

5.7 Prímtesztek

Könnyű-e meghatározni egy szám prímtényezős felbontását? Látszólag igen, hiszen csak meg kell nézni rendre, hogy osztható-e 2-vel, 3-mal, 5-tel stb. Ha találunk egy (prím)osztót, akkor a hányadost kell tovább bontani. Ha pedig a szám négyzetgyökéig elmenve egyáltalán nem találunk ilyen osztót, akkor a szám biztosan prím (lásd az 1.4.7a feladatot [18]).

Ily módon gyorsan fel tudjuk bontani például a 143-at, vagy be tudjuk látni, hogy a 197 prím (13-ig egyik prímszámmal sem osztható).

Nagy számoknál már nemigen tudjuk megvalósítani, hogy csak a primeket próbáljuk ki, osztják-e a számot, hiszen a primek nem állnak eleve rendelkezésünkre. Természetesen ekkor sem érdemes minden számot osztóként kipróbálni: nyilván elég, ha a vizsgált számot annyiszor osztjuk 2-vel, hogy páratlan számhoz jussunk, és ekkor már csak a páratlan számokkal való oszthatóságot kell tekinteni. Ezt a gondolatot tovább is fejleszthetjük: a 2 mellett (például) a 3 és az 5 hatványait is leválaszthatjuk ily módon, és ezután elég csak a 30-hoz relatív prim osztókat keresni.

Igazán nagy számok esetén azonban ezek a „próbaosztásos” módszerek a gyakorlatban teljesen használhatatlanok. A nehézséget az jelenti, hogy olyan sok próbálkozást kellene (számítógéppel) végrehajtani, amihez évmilliárdok sem elegendőik. Sőt, a próbaosztásos módszerek továbbfejlesztett változatai, illetve az eddig kidolgozott egyéb faktorizációs algoritmusok is reménytelenül „lassúak”. Egy 500-jegyű (összetett) számot, amelynek nincsenek kis prímosztói, vagy nincs valamilyen speciális tulajdonsága, a jelenlegi leggyorsabb számítógépek sem tudnának a Föld kihűlése előtt tényezőkre bontani.

Ily módon gyorsan fel tudjuk bontani például a 143-at (= 11 · 13), vagy be tudjuk látni, hogy a 197 prím (13-ig egyik prímszámmal sem osztható).

5.7 Prímtesztek

Könnyű-e meghatározni egy szám prímtényezős felbontását? Látszólag igen, hiszen csak meg kell nézni rendre, hogy osztható-e 2-vel, 3-mal, 5-tel stb. Ha találunk egy (prím)osztót, akkor a hányadost kell tovább bontani. Ha pedig a szám négyzetgyökéig elmenve egyáltalán nem találunk ilyen osztót, akkor a szám biztosan prím (lásd az 1.4.7a feladatot [18]).

Ily módon gyorsan fel tudjuk bontani például a 143-at (= 11 · 13), vagy be tudjuk látni, hogy a 197 prím (13-ig egyik prímszámmal sem osztható).

Nagy számoknál már nemigen tudjuk megvalósítani, hogy csak a primeket próbáljuk ki, osztják-e a számot, hiszen a primek nem állnak eleve rendelkezésünkre. Természetesen ekkor sem érdemes minden számot osztóként kipróbálni: nyilván elég, ha a vizsgált számot annyiszor osztjuk 2-vel, hogy páratlan számhoz jussunk, és ekkor már csak a páratlan számokkal való oszthatóságot kell tekinteni. Ezt a gondolatot tovább is fejleszthetjük: a 2 mellett (például) a 3 és az 5 hatványait is leválaszthatjuk ily módon, és ezután elég csak a 30-hoz relatív prim osztókat keresni.

Igazán nagy számok esetén azonban ezek a „próbaosztásos” módszerek a gyakorlatban teljesen használhatatlanok. A nehézséget az jelenti, hogy olyan sok próbálkozást kellene (számítógéppel) végrehajtani, amihez évmilliárdok sem elegendőik. Sőt, a próbaosztásos módszerek továbbfejlesztett változatai, illetve az eddig kidolgozott egyéb faktorizációs algoritmusok is reménytelenül „lassúak”. Egy 500-jegyű (összetett) számot, amelynek nincsenek kis prímosztói, vagy nincs valamilyen speciális tulajdonsága, a jelenlegi leggyorsabb számítógépek sem tudnának a Föld kihűlése előtt tényezőkre bontani.

Ugyanakkor léteznek olyan esetek azonban, amelyek (teljes vagy majdnem teljes biztonsággal) viszonylag gyorsan eldöntik, hogy egy nagy szám prím-e vagy összetett (azonban az utóbbi esetben nem tudják megadni a tényezőket). Az ilyen algoritmusokat nevezik primteszteknek.

A gyors prímszámok lelepteze első hallásra megépőnek tűnik, különösen azzal összehasonlítva, hogy egy nemtriviális osztó megkeresése (jelenlegi ismereteink szerint) jóval kilátástalanabb feladat, mint egy türe ráelélni a szénakazalban. Ezek az algoritmusok azonban nem osztót keresnek, hanem olyan, gyorsan ellenőrizhető feltételeket vizsgálnak, amelyeket a primek kielégítik, az összetett számok viszont gyakorlatilag nem. A „gyakorlatilag” azt jelenti, hogy a legtöbb módszernél az esetleges „igen ritka” kivételiek, és ezzel együtt a tévedés lehetőségének egy elenyészően csökély mértékű kockázatát meg kell engednünk.)
Speciális alakú számokra már látottunk prímteszteket, ilyen volt a Fermat-, illetve a Mersenne-számok tesztje (T 5.2.2, illetve T 5.2.4 Tétel).

Az általános prímtesztek tárgyalása előtt megmutatjuk, hogy néhány alapvető szárméleti feladat megoldására létezik gyors algoritmus.

5.7.1 Tétel. T 5.7.1

Legyenek \(a\), \(b\), \(c\) és \(m\) egészek, ahol \(b > 1\) és \(m > 0\). Ekkor

I. \(a^b\) maradéka modulo \(m\);

II. az \(a\) és \(b\) legnagyobb közös osztója;

III. (páratlan \(b\) és \((a, b) = 1\) esetén) az \(\left(\frac{a}{b}\right)\) Jacobi-szimbólum;

IV. az \(ax + by = c\) lineáris diofantikus egyenlet megoldásai és

V. az \(ax \equiv c \pmod{b}\) kongruencia megoldásai

kiszámíthatók legfeljebb \(5 \log_2 b\) lépésben, ahol egy lépés két egész szám összeadását, kivonását, szorzását vagy maradékos osztását jelenti.

A fentiak alapján egy 500-jegyű \(b\) szám esetén ezek a feladatok legfeljebb

\(5 \log_2 b \approx 2500 \log_2 10 < 9000\)

lépésben megoldhatók. Ezt egy gyors számítógép a másodperc töredéke alatt elvégzi, ráadásul a konkrét eljárásokat ügyesebb szervezéssel még gyorsabbná és automatikusabbná lehet tenni.

Bizonyítás: 1. Az \(a^b\) szám modulo \(m\) vett maradékát az ismételt négyzetre emelések segítségével és minden lépés után az eredményt modulo \(m\) redukálva érdemes végezni (ez a módszer szerepelt már a 3.2 pontbeli Példában modulo 59 vett maradékának a meghatározásánál, valamint a Fermat-számok tesztjénél, lásd az T 5.2.2 Tétel bizonyítása utáni megjegyzéseket).

Legyen \(t = \lfloor \log_2 b \rfloor\), és írjuk fel a \(b\) kitevőt kettes számrendszerben. A \(b\) a számítógépen valószínűleg eleve ebben az alakban van tárolva, de más alapú számrendszerből történő átszámítás is megvalósítható legfeljebb \(\log_2 b\) lépésben, hiszen az T 1.2.2 Tétel szerint a számjegyeket a 2-vel történő maradékos osztások sorozatával kapjuk meg.

\[ b = 2^{i_1} + 2^{i_2} + \cdots + 2^{i_t}, \quad \text{alci} \quad 0 \leq i_1 < i_2 < \cdots < i_t \leq t. \]

Ezután ismételt négyzetre emelesekkel (és mindig mod \(m\) redukálva) számoljuk ki

\[ a^2, a^4, a^a, \ldots, a^a \]

maradékát mod \(m\). Végül az

\[ a^b = a^{i_1} \cdot a^{i_2} \cdot \cdots \cdot a^{i_t}, \]

összefüggés alapján megkapjuk a keresett maradékot.

Például \(5^{10001}\) modulo \(m\) kiszámításához először meghatározzuk

\[ 5^2, 5^4, 5^8, \ldots, 5^{12} \]
maradékát modulo \( m \), majd ezek közül a megfelelőket összeszorozzuk (és továbbra is minden lépésben csak a szorzat maradékát vesszük modulo \( m \)):

\[
5^{1000} = 5^8 \cdot 5^{32} \cdot 5^{128} \cdot 5^{256} \cdot 5^{712}.
\]

Az \( a^b \) modulo \( m \) maradék meghatározásához \( t \) darab négyzetre emelést és legfeljebb \( t \) darab további szorzást (és modulo \( m \) redukciót) végezünk. Így összesen legfeljebb \( 2t \leq 2 \log_2 b \) ilyen szorzásra és redukcióra, azaz maradékos osztásra volt szükség. Ehhez hozzávéve a \( b \) kettes számrendszerbeli felírásának lépésszámát is, azt kaptuk, hogy \( a^b \) modulo \( m \) maradékát meg tudjuk kapni legfeljebb \( 5 \log_2 b \) lépésben (ahog egy lépés egy szorzást vagy egy maradékos osztást jelent).

II. A legnagyobb közös osztó kiszámításához a legkisebb abszolút értékű maradékokkal végzett euklideszi algoritmust alkalmazzuk (azaz, amikor a maradékos osztásoknál negatív maradéket is megengedünk, és a maradék abszolút értéke legfeljebb az osztó abszolút értékének a fele, lásd az T 1.2.1A Tételt):

\[
\begin{align*}
a &= b q_1 + r_1, & \text{ahol} & \quad |r_1| \leq \frac{b}{2}, \\
b &= r_1 q_2 + r_2, & \text{ahol} & \quad |r_2| \leq \frac{|r_1|}{2} \leq \frac{b}{4}, \\
r_1 &= r_2 q_3 + r_3, & \text{ahol} & \quad |r_3| \leq \frac{|r_2|}{2} \leq \frac{b}{8}, \\
& \vdots \\
r_{n-2} &= r_{n-1} q_n + r_n, & \text{ahol} & \quad |r_n| \leq \frac{|r_{n-1}|}{2} \leq \frac{b}{2^n}, \\
r_{n-1} &= r_n q_{n+1}.
\end{align*}
\]

Az euklideszi algoritmus ebben az esetben \( n + 1 \) lépésből áll. Mivel

\[
1 \leq |r_n| \leq \frac{b}{2^n},
\]

ezért

\[
2^n \leq b, \quad \text{azaz} \quad n \leq \log_2 b.
\]

Ezzel beláttuk, hogy az euklideszi algoritmus legfeljebb \( 1 + \log_2 b \) lépést igényel (ahog egy lépés egy maradékos osztást jelent).

Megjegyezzük, hogy a szokásos módon, a legkisebb nemnegatív maradékokkal végzett euklideszi algoritmus is legfeljebb konstansszor \( \log_2 b \) lépést igényel, lásd az 5.7.1 feladatot [159].

III. A T 4.3.2 Tétel alapján a Jacobi-szimbólum kiszámítását a „számlálóban” szereplő kettőhatványok leválasztásával és a reciprocitási tétel ismételt alkalmazásával végezhetjük, ami tulajdonképpen az előbbi euklideszi algoritmus egy variánsa (lásd a T 4.3.2 Tétel utáni Példát).

Nézzük mindezt részletesen. Az \( \left( \frac{a}{b} \right) \) számolásánál az \( a \cdot t \ b \) -vel maradékosan elosztva azt kapjuk, hogy

\[
\left( \frac{a}{b} \right) = \left( \frac{r}{t} \right), \quad \text{ahol} \quad |r| \leq \frac{b}{2^n},
\]

Szükség esetén \( \left( \frac{a}{b} \right) \) felhasználásával azt is elérhetjük, hogy \( r > 0 \) teljesüljön. Ha \( r \) páros, akkor a következő lépésben \( \left( \frac{a}{t} \right) \) kiemelése után a „számláló” ismét feleződik. Ha \( r \) páratlan, akkor a reciprocitási tétel alapján az \( r \) a „nevezőbe” kerül, az új „számláló” pedig \( b \cdot \text{nek} \) az \( r \) szerinti \( s \) maradéka, ahol \( |s| \leq r/2 \), és ismét elérhető, hogy \( s > 0 \) legyen. Ez azt jelenti, hogy a „számláló” minden lépésben legalábbis feleződik, és így a lépésszám most is legfeljebb \( \log_2 b \) . Ehhez hozzájön
még, hogy $\left( \frac{3}{5} \right)$ és $\left( \frac{5}{3} \right)$ kiszámításához szükség van a $\mathbb{U}$ -nek modulo 4, illetve modulo 8 maradéka, ez egy-egy maradékos osztással megkapható, illetve a $\mathbb{U}$ kettés számrendszerbeli alakjának utolsó két, illetve három jegyéből azonnal leolvasható. Hasonlóan egyszerű a „számláló” paritásának a megállapítása, illetve páros esetben a felelézése is.

Természetesen $\left( \frac{3}{5} \right)$ csak akkor értelmes, ha $b > 1$ páratlan szám és $\left( a,b \right) = 1$ . Ez utóbbi feltétel teljesülése az euklideszi algoritmus segítségével előre is ellenőrizhetjük, azonban erre nincs szükség.

Ha ugyanis $\left( u,v \right) = d > 1$, akkor a fenti eljárást végezve előbb-utóbb egy olyan helyzet adódik, ahol a számláló $d$, a nevező pedig többszöröse $d$ -nek (lásd az 5.7.2 feladatot [160]), és ít nyilvánvalóan elakadunk, tehát nem létezik az $\left( \frac{a}{d} \right)$ Jacobi-szimbólum. (Az $\left( u,v \right) = 1$ esetben ez nem fordulhat elő, akkor az utolsó lépésben egy $\left( \frac{1}{x} \right)$ vagy $\left( \frac{-1}{x} \right)$ Jacobi-szimbólumot kell kiszámolnunk.)

IV–V. A 2.5 pontban láttuk, hogy a két probléma ekvivalens. Továbbá az T 1.3.6 és T 1.3.5 (vagy a T 7.1.1) Tételek szerint az $u^2 + v^2 = r$ diofantikus egyenlet megoldásaival az euklideszi algoritmus segítségével állíthatjuk elő, és innen a kívánt lépesszámbevésle is leolvasható. $

Most rátérünk a prímtesztek tárgyalására. A legegyszerűbb általános prímteszt azonnal következik a kis Fermat-tételből:

Ha egy $u > 2$ számra $2^{u-1} \equiv 1 \pmod{u}$, akkor $u$ összetett.

Az T 5.7.1 Tétel alapján ez a feltétel valóban gyorsan ellenőrizhető.

Tisztáznunk kell azonban az alábbi fontos kérdést: milyen következtetést vonhatunk le $u$-ra, ha $2^{u-1} \equiv 1 \pmod{n}$ ?

Sajnos ekkor nem lehetünk teljesen biztosak abban, hogy az $u$ prim, ugyanis végletesen sok olyan $u$ összetett szám létezik, amelyre $2^{u-1} \equiv 1 \pmod{n}$ . Ezeket 2-es alapú álprimekn vagy pseuodprimeknak nevezzük (a legkisebb a 341).

Megmutatható azonban, hogy a 2-es alapú alprimek ritkák a primekhez képest: az $x$ -nél nem nagyobb alprimek számának és $\pi(x)$ -nek a hányadosa $x \rightarrow \infty$ mellett (nagyon erősen) 0-hoz tart. (Ezt illustrálandó egy konkrét számpélda is mutatunk: $19^{10}$ -ig a 2-es alapú alprimek száma 14887 , a primek száma pedig 4559529511 , az arányuk körülbelül egy a harmincezerhez.)

Mindezek alapján, ha egy nagy $u$ számról $2^{u-1} \equiv 1 \pmod{n}$ teljesül, akkor azt mondhatjuk, hogy az $u$ „nagy valószínűséggel prim”. Ezt a kijelentést úgy kell érteni, hogy ha a tesztet sok, véletlenszerűen választott $u$ -re alkalmazzuk, akkor csak igen ritkán (gyakorlati szempontból nézve szinte sohasem) fordulhat elő, hogy $2^{u-1}$ maradéka 1, és az $u$ mégis összetett.

Mindezek lényegét az alábbi tételben is összefoglaljuk:

5.7.2 Tétel. T 5.7.2

Legyen $u > 2$ . Ha $2^{u-1} \not\equiv 1 \pmod{n}$ , akkor $u$ biztosan összetett. Ha $2^{u-1} \equiv 1 \pmod{n}$ , akkor $u$ „majdnem biztosan” prim. A feltétel gyorsan ellenőrizhető, ha a hatványozást ismételt négyzetre emelések segítségével végezzük. $

A tesztet többféleképpen is továbbfejleszthetjük: $u^{v-1}$ maradékké modulo $n$ nemcsak az $a = 2$ értékére, hanem (mondjuk) az 1000-nél kisebb összes primszámról is kiszámítjuk; ha legalább egy $a$ -ra ez a maradék nem 1 (és $u > 1090$ ), akkor $n$ a kis Fermat-tétel szerint biztosan összetett. Még hatékonyabb, ha az első valahány prim helyett véletlenszerűen választott, $t$ -nel nem osztható számokat veszünk $a$ -nak (lásd az 5.7.13 feladatot [160]).
Ha mindegyik kipróbált \( a \) -ra \( a^{n-1} \equiv 1 \pmod{n} \), akkor \( n \) „még inkább majdnem biztosan” prim, azonban sajnos továbbra sem lehetünk ebben teljesen biztosak. Létezné ugyanis olyan összetett számok, amelyekre bármely \( \left( a, n \right) = 1 \) esetén \( a^{n-1} \equiv 1 \pmod{n} \), ilyen például az 1729 (lásd a 2.4.15c feladatot [48]). Az ilyen számokat univerzális álprimeknek vagy Carmichael-számoknak nevezzük.

Az álprimek „típusait” külön definícióban is összefoglaljuk:

5.7.3 Definíció . D 5.7.3

Ha egy \( n \) összetett számról \( n^{\frac{n-1}{2}} \equiv 1 \pmod{n} \) teljesül, akkor az \( n \) alapú álprimnek nevezzük.

Ha az \( n \) összetett számra a fenti kongruencia minden \( \left( a, n \right) = 1 \) esetén teljesül, akkor az \( n \) univerzális álprim vagy Carmichael-szám.

Minden esetben ugyanúgy használható az „álprim” helyett a „pszeudoprím” elnevezés is.

A Carmichael-számok ekvivalens karakterizációira nézve lásd az 5.7.7 feladatot [160].

Régóta ismert, hogy bármely \( a > 1 \) esetén végtelen sok \( a \) alapú álprim létezik (lásd az 5.7.5 feladatot [160]). Azt azonban csak 1992-ben sikerült igazolni, hogy az univerzális álprimek száma is végtelen.

Az alábbiakban két olyan prímtesztet tárgyalunk, amelyek már az álprimeket is „leleplezik”. Mindkettőben „véletlen” számokat használunk, amin (legalábbis elvileg) azt értjük, hogy egész számoknak egy „nagyméretű”, de véges halmazából egymás után „kiveszünk” elemeit úgy, hogy bármely elem kiválasztásának „úgy valószínűsege” (mintha egy urnából golyókat húznánk ki visszatevéssel). Például egy kettes számrendszerben 2000-jegyű véletlen számot úgy kaphatunk, hogy az első jegy 1-es, a többi számjegyet pedig 1999 egymás utáni pénzfeldobás eredményeként állapítjuk meg. A gyakorlatban természetesen a számítógép „dobálja a pénzérmét”, illetve valójában valamilyen véletlenszám-generátor használ (amely tulajdonképpen általaiban csak a véletlent nagyon jól „utánzó” ún. „álvéletlen” számsorozatokat produkál.)

5.7.4 Tétel (Solovay–Strassen-prímteszt) . T 5.7.4

(A) Legyen \( \alpha > 1 \) páratlan szám, és tekintsük az

\[
\alpha^{\frac{n-1}{2}} \equiv \left( \frac{\alpha}{n} \right) \pmod{n}
\]

kongruenciát, ahol \( \left( \frac{\alpha}{n} \right) \) a Jacobi-szimbólum.

Ha \( \alpha \) prim, akkor (1) minden \( a \not\equiv 0 \pmod{n} \) esetén teljesül.

Ha \( \alpha \) összetett, akkor (1) egy modulo \( n \) teljes maradékkrendszer elemeinek kevesebb, mint a felére teljesül.

(B) Az (A) kritérium alapján a következőképpen dönthetjük el egy nagy páratlan \( n \) -ről, hogy prim-e vagy összetett. Válasszunk (mondjuk) 1000 véletlen \( a \not\equiv 0 \pmod{n} \) értéket, és mindegyikre vizsgáljuk meg, hogy az (1) feltétel teljesül-e. Ha legalább egy esetben nem teljesül, akkor az \( n \) biztosan összetett. Ha mind az 1000 esetben teljesül, akkor \( 2^{1000} \) nél kisebb annak a valószínűsége, hogy az \( n \) összetett.

Megjegyzések: 1. Ha \( \left( \alpha, n \right) > 1 \), akkor az \( \left( \frac{\alpha}{n} \right) \) Jacobi-szimbólum nem értelmes, tehát (1) eleve nem teljesülhet.
2. Az T 5.7.1 Tétel alapján az (1) feltétel (akár ezer $a$-ra is) gyorsan ellenőrizhető.

3. A Solovay–Strassen-teszt is magában hordozza annak a lehetőségét, hogy egy összetett számot tévesen prímnek „nyilvánítunk”. Az T 5.7.2 Tétel teszthelyezé képest azonban mind elméleti, mind pedig gyakorlati szempontból óriási az előrelépés.

Az T 5.7.2 Tétel tesztnél a 2-es alapú álprímeket egyáltalán nem tudjuk leleplezni, az ilyen számokra a teszt $\text{el} \, \text{esőd}$ mond, vagyis egy konkrét álprím esetén „száz százalékosan” tévedünk, amikor a tesz alapján prímek véljük (csak szerencsére ritkán botlunk álprimekbe). Ugyanígy, egy nagy univerzális álprím tesztelésére a továbbfejlesztett változat sem alkalmas, hiába próbálunk ki akár egymillió $a$ értéket is; egy ilyen $a$-et ismét csak tévesen gondolunk prímnek (hacsak nem került véletlennel egy $a$-hez nem relatív prim az $a$-k közé, de ennek gyakorlatilag nulla az esélye).

Ugyanakkor a Solovay–Strassen-teszt elől egyetlen összetett szám sem „bújhat el”, erre nézve nincsenek „álprímek”; bár a Solovay–Strassen-teszt igazolja az $\eta$ összetettségét. Ez egyben azt is jelenti, hogy a tévedés valószínűségét (a tesztelt számot függetlenül) tetszőlegesen kicsire tudjuk lecsökkenteni, ha elég sok $a$ értéket próbálunk ki. (Ebből a szempontból az ezer próbánál adódó $2^{-1000}$-es hibalehetőség tökéletes biztonságot nyújt.)

Bizonyítás: A (B) rész az (A) rész közvetlen következménye, így elég csak az utóbbit igazolnunk.

Ha $\eta$ prim, akkor (1) azonnal adódik a T 4.1.2 Tételből és a Legendre-szimbólum definíciójából (lásd a D 4.1.3 Definíció utáni (2) képletet).

Legyen az $\eta$ összetett. Mivel (1) eleve csak az $a$-hez relatív prim $a$-ra teljesül, ezért elegendő azt megmutatni, hogy (1)-et egy modulo $\eta$ redukált maradékrendszer elemeinek lehetsége is.

Egy $\eta$-hez relatív prim $a$ számot nevezzünk $a$-tanúnak, ha (1) nem teljesül, és $cinkosnak$, ha (1) teljesül. Ezzel a terminológiával élve azt kell igazolnunk, hogy egy redukált maradékrendszer elemeinek legalább a fele tanú.

Először megmutatjuk, hogy minden páratlan összetett $\eta$-hez létezik tanú.

Vizsgáljuk először azt az esetet, amikor az $\eta$ nem négyzetmentes, tehát van olyan $q$ prim, amelyre $q^2 \mid \eta$. Jelölje az $\eta$ különböző prímosztóit $\eta = q_1 \cdot q_2 \cdot \cdots \cdot q_s$, legyen $\eta$ primitív gyök modulo $q^2$, és legyen $\nu$ az

$$x \equiv g \pmod{q^2}, \quad x \equiv 1 \pmod{q_i}, \quad 2 \leq i \leq s$$

szimultán kongruenciarendszer egy megoldása (ha $s = 1$, akkor legyen $\nu = \eta$ ). Megmutatjuk, hogy minden $\eta$-hez létezik tanú.

Mivel minden $i$-re $(\nu, q_i) = 1$, ezért $(\nu, q^2) = 1$. Tegyük fel indirekt, hogy

$$\nu^{q-1} = \left( \frac{\nu}{q} \right) \pmod{q}. \quad \text{(2)}$$

A (2) kongruenciát négyzetre emelve kapjuk, hogy

$$\nu^{q-1} = \left( \frac{\nu}{q} \right)^2 = 1 \pmod{q^2}. \quad \text{(3)}$$

Mivel $q^2 \mid \eta$, ezért a (3) kongruencia akkor is teljesül, ha az $\eta$ modulus helyett a $q^2$ modulusra nézzük; ekkor $\nu \equiv g \pmod{q^2}$-et is felhasználva

$$\nu^{q-1} = 1 \pmod{q^2}. \quad \text{(4)}$$
adódik. Mivel a \( g \) primitív gyök \( \mod q^2 \), azaz a rendje \( \varphi(q^2) = q(g - 1) \), ezért (4) alapján \( g(g - 1) \mod n - 1 \). Ugyanakkor \( q^2 \mod n \) is igaz, vagyis \( q \mod n \)-nek és az \( n - 1 \)-nek is osztója, ami ellentmondás.

Most nézzük azt az esetet, amikor az \( n \) négyzetmentes, azaz \( n = q_1 \cdot \ldots \cdot q_s \), ahol a \( q_i \)-k különböző prímek és \( s \geq 2 \).

Itt két alesetet különböztetünk meg aszerint, hogy

\[
\alpha z \equiv 1 \pmod n
\]

minden \( (a, n) = 1 \) esetén fennáll-e vagy sem.

Ha (5) minden \( (a, n) = 1 \)-re teljesül, akkor legyen \( h \) kvadratikus nemmaradék modulo \( Q \), és legyen \( u \) az

\[
x \equiv h \pmod{q_1}, \quad x \equiv 1 \pmod{q_i}, \quad 2 \leq i \leq s
\]

szimultán kongruenciarendszer egy megoldása. Ekkor \( u \) tanú, ugyanis \( (u, n) = 1 \), és így (5) szerint

\[
u^i \equiv 1 \pmod{q_i}, \quad 2 \leq i \leq s
\]

azaz

\[
\left( \frac{u}{q_i} \right) = \left( \frac{1}{q_i} \right) \ldots \left( \frac{1}{q_s} \right) = -1.
\]

Rátérve a másik alesetre, legyen \( (u, n) = 1 \) olyan szám, amelyre (5) nem igaz. Ekkor az \( n \) prímosztói között van (legalább egy) olyan, mondjuk \( Q \), amelyre

\[
a z \equiv 1 \pmod{n}.
\]

Legyen \( z \) az

\[
z \equiv e \pmod{q_1}, \quad z \equiv 1 \pmod{q_i}, \quad 2 \leq i \leq s
\]

szimultán kongruenciarendszer egy megoldása. Megmutatjuk, hogy \( z \) tanú. Egyrészt

\[
z \equiv a z \equiv a \cdot e \equiv e \pmod{q_1}, \quad \text{és így} \quad z \cdot z \equiv 1 \pmod{n},
\]

másrészt

\[
z \equiv 1 \pmod{q_1}, \quad \text{és így} \quad z \equiv 1 \pmod{n}.
\]

Ez azt jelenti, hogy

\[
z \equiv \pm 1 \pmod{n}, \quad \text{ugyanakkor} \quad \left( \frac{z}{n} \right) = \pm 1,
\]

tehát \( z \) valóban tanú.

Ezzel megmutattuk, hogy minden páratlan összetett \( n \)-hez létezik tanú.

Végül belátjuk, hogy egy redukált maradékkonkrans elemeinek legalább a fele tanú.

Legyen \( t \) egy tetszőleges tanú, és legyenek \( c_1, c_2, \ldots, c_k \) páronként inkongruens cinkosok. Belátjuk, hogy ekkor \( c_1 c_2 \cdot \ldots \cdot c_k \) páronként inkongruens tanúk.
Egyrészt \( (t, n) = (e_i, n) = 1 \) miatt \( (t, n) = 1 \) is teljesül, másrészt (ismét \( (t, n) = 1 \) -et is felhasználva kapjuk, hogy) a \( \ell e_i \) elemek is páronként inkongruensek modulo \( n \). Tegyük fel indirekt, hogy valamely \( i \)-re \( \ell e_i \), cinkos lenne, azaz

\[
(\ell e_i)^{\frac{\phi - 1}{2}} \equiv \left( \frac{\ell e_i}{n} \right) \pmod{n} \quad (7)
\]

teljesülne. Mivel \( G \) is cinkos, ezért

\[
c_i^{\frac{\phi - 1}{2}} \equiv \left( \frac{c_i}{n} \right) \pmod{n} \quad (8)
\]

is igaz. A (7) és (8) kongruenciákat összeszorozva azt kapjuk, hogy

\[
t^{\frac{\phi - 1}{2}} c_i^{\frac{\phi - 1}{2}} \equiv \left( \frac{t}{n} \right) \left( \frac{c_i}{n} \right)^2 \pmod{n} \quad (9)
\]

(8)-at négyzetre emelve

\[
c_i^{\phi - 1} = \left( \frac{c_i}{n} \right)^2 \equiv 1 \pmod{n}
\]

adódik, és ezt (9)-be beírva azt nyerjük, hogy

\[
t^{\frac{\phi - 1}{2}} c_i^{\frac{\phi - 1}{2}} \equiv \left( \frac{t}{n} \right) \pmod{n},
\]

vagyis \( t \) is cinkos, ami ellentmondás.

Ezzel beláttuk, hogy ha páronként inkongruens cinkosokat egy tanúval végigszorzunk, akkor páronként inkongruens tanúkat kapunk. Ez viszont azt jelenti, hogy egy redukált maradékrrendszer elemei között legalább annyi tanú van, mint cinkos, vagyis az elemekek legalább a fele tanú.

A következő prímteszt kiindulópontja a kis Fermat-tétel, valamint az, hogy ha \( p \) prim és \( a^2 \equiv 1 \pmod{p} \), akkor csak \( a = \pm 1 \pmod{p} \) lehetséges. Ennek megfelelően, ha \( p \nmid a \), akkor az

\[
a^{\frac{p-1}{2}}, a^{\frac{p+3}{2}}, a^{\frac{p-3}{2}}, \ldots
\]

számok modulo \( P \) vett legkisebb abszolút értékű maradékaiknak sorozata mindenképpen 1-gyel kezdődik és vagy végig 1, vagy pedig az első 1-től különböző maradék szükségképpen \( -1 \). Ugyanakkor megmutatjuk, hogy ha \( P \) helyett egy tetszőleges \( n \) összetett számot veszünk, akkor sok \( a \)-ra már nem ilyen maradéksorozatot kapunk. Ennek megfelelően a következő prímtesztet nyerjük (a fenti feltételt technikai okokból kissé módosított alakban, lényegében a „fordított” sorozatra adjuk meg):

5.7.5 Tétel (Miller–Lenstra–Rabin-prímteszt). T 5.7.5

Legyen \( n > 1 \) páratlan szám, \( n - 1 = 2^k r \), ahol \( r \) páratlan. Az

\[
a^{2^l} \equiv \begin{cases} a \pmod{n}, & \text{ha } l < \frac{k}{2} \text{ vagy } l = \frac{k}{2}, \\ a^{-1} \pmod{n}, & \text{ha } l > \frac{k}{2} \end{cases}
\]

számokat jó sorozatnak nevezzük, ha ezek modulo \( n \) vett legkisebb abszolút értékű maradéka között előfordul \( -1 \) vagy pedig \( a^r \) maradéka 1.
Ha \( \mu \) prim, akkor (10) minden \( a \neq 0 \pmod{n} \) esetén jó sorozat.

Ha \( \mu \) összetett, akkor (10) egy modulo \( n \) teljes maradékrangszer elemeinek kevesebb, mint a felére alakot jó sorozatot.

Ez a kritérium gyorsan ellenőrizhető: ismételt négyzetre emelésével kiszámítjuk \( a^\mu \) maradékát modulo \( n \), majd ebből a sorozat további elemei egy-egy újabb négyzetre emeléssel adódnak.

A kritérium alapján az T 5.7.4 Tétel (B) részéhez hasonlóan megfogalmazhatjuk magát a konkrét eljárást is.

A bizonyítás vázlata: Az T 5.7.4 Tétel bizonyításának menetét és (értelmszerűen módosított) tanú-cinkos szóhasználatát követjük.

Ha \( \mu \) prim, akkor az T 5.7.5 Tétel kimondása előtt vázoltuk, hogy minden \( P \neq \mu \) esetén jó sorozatot kapunk.

Ha \( \mu \) összetett és nem négyzetmentes, akkor ugyanúgy kaphatunk tanút, mint az T 5.7.4 Tétel bizonyításában.

Ha \( \mu \) összetett és négyzetmentes, akkor tekintsük azt a legnagyobb \( 0 \leq j \leq k - 1 \) számot, amelyhez van olyan \( (a, \mu) = 1 \), hogy

\[
a^{2j} \neq 1 \pmod{n}. \tag{11}
\]

Mivel van olyan \( j \) és \( a \), amelyre (11) teljesül, például \( j = 0 \) és \( a = -1 \) megfelel [hiszen \((-1)^r \neq 1 \pmod{n}\)], ezért a jelzett maximális \( j \) is valóban létezik.

A (11)-ből következik, hogy az \( \mu \) egyik prímosztójára, mondjuk \( \nu \)-re

\[
a^{2j} \neq 1 \pmod{\nu}. \tag{11'}
\]

Ekkor az T 5.7.4 Tétel bizonyításában a (6) kongruenciarendszer szerint gyártott \( z \) tanú, ugyanis az ottani gondolatmenethez hasonlóan kapjuk, hogy

\[
z^{2j} \neq \pm 1 \pmod{n},
\]

ugyanakkor \( j \) definíciója szerint (\( j < k - 1 \) esetén)

\[
z^{2j} = 1 \pmod{n}.
\]

Végül, ha \( z \neq 0 \) vagy a nem négyzetmentes esetben kapott \( v \neq 0 \) páronként inkongruens cinkosokkal megszorozzuk, akkor az T 5.7.4 Tétel bizonyításában látott módon páronként inkongruens tanukat kapunk (a \( z \) helyett tetszőleges tanút véve ez nem feltétlenül igaz). Ezzel megmutattuk, hogy összetett \( \mu \) esetén egy redukált maradékrangszer elemeinek legalább a fele tanú.

Megjegyzések:
1. A Miller–Lenstra–Rabin-teszt valójában az T 5.7.5 Tételben jelzett mértéknél is jóval hatékonyabb: finomabb módszerekkel az is megmutatható, hogy egy redukált maradékrangszer elemeinek több, mint a háromnegyezele tanú.

Az AKS-teszt nagy ötlete, hogy $f_c = g_c$ helyett csak azt ellenőrizzük, hogy $f_c$ és $g_c$ egy alkalmazott $\hat{u} \in \mathbb{Z}_n[x]$ polinommal osztva azonos maradékot ad-e. Ha $\hat{u}$ foka ($n$ -hez képest) elég alacsony, akkor ez a számolás már kivitelezhető, hiszen az ismételt négyzetre emeléseknél mindig redukálunk „mod $n$” is. Ez különösen kényelmes, ha $\hat{u} = x^n - 1$ alakú polinom, hiszen ekkor csak az $x$-hatványok kitevőit kell redukálni mod $\tau$ (vagyis $x^j$ helyére $x^{\tau^j}$-et írunk, amíg csak lehetséges).

Ha $\hat{u}$ prim, akkor természetesen $f_c = g_c$ miatt bármely $\hat{u}$ szerinti maradékuk is egyenlő. Az AKS-teszt lényege, hogy ha alkalmazott $\tau$-et választunk, akkor az összetett számok ezt nem teljesítik, vagyis minden összetett $n$-hez van olyan $c < K$ (ahol $K$ az $n$-hez képest „igen kicsi”), hogy $f_c$ és $g_c$ maradéka nem ugyanaz $x^n - 1$-gyel osztva.

A teszt algoritmusa ennek alapján a megfelelő $\tau$ kiválasztása után „végigpróbálja” $c = 1, 2, \ldots, K$ -ra, hogy $f_c = g_c \text{ (mod } x^n - 1)$ fennáll-e. Ha ez valamelyik $c$-re nem igaz, akkor $\tau$ biztosan összetett (ez már a kiinduló megmegondolásainkból következik), ha viszont mindegyik $c$-re igaz, akkor $\hat{u}$ biztosan prim (ennek belátása a teszt „nehéz” része).

Az $\tau$ –nek egy „nem túl nagy” és bizonyos tulajdonságokkal rendelkező prímszámot kell választani, ennek létezését egy mély számelméleti tétel biztosítja. Az, hogy ezen $\tau$-mel az összetett számok már „néhány” $c$-valamelyikénél is szükségképpen „telelésiödnek”, a véges testekre vonatkozó alapvető tételek felhasználásával igazolható.
képlete alapján a (c) részből következik, hogy a szokásos euklideszi algoritmus lépésszáma legfeljebb 
\[ \log_2 b + c \], ahol \( c = \frac{1 + \sqrt{5}}{2} \) és \( d \) alakmas konstans, és ez a becslés tovább már nem javítható.

5.7.2 Tekintsük az \( \left( \frac{b}{a} \right) \) Jacobi-szimbólum kiszámítására az T 5.7.1 Tétel bizonyításának III. pontjában látott eljárást. Mutassuk meg, hogy ha ezt \( \left( a, b \right) = d > 1 \) mellett alkalmazzuk, akkor végül egy olyan helyzethez jutunk, ahol a „számláló” \( d \), a „nevező” pedig többszöröse \( d \)-nek. (Ez azt jelenti, hogy ily módon is kiderül, ha a Jacobi-szimbólum nem értelmes, és így \( a \) és \( b \) relatív prímséget nem kell előre külön ellenőrizni.)

5.7.3 Mutassuk meg, hogy a 341 kettes alapú álprim, de nem hármas alapú álprim.

5.7.4 (M [575]) Bizonyítsuk be, hogy ha az \( n \) kettes alapú álprim, akkor \( 2^n - 1 \) is az.

5.7.5 Legyen \( a > 1 \). Bizonyítsuk be, hogy ha a \( p > 2 \) prim nem osztója \( a \equiv 1 \)-nek, akkor az

\[ n = \frac{a^{2p} - 1}{a^2 - 1} \]

szám \( a \) alapú álprim. (Az \( a = 2 \), \( p = 5 \) esetben \( n = 341 \).)

5.7.6 Igazoljuk, hogy az 561 univerzális álprim.

5.7.7 Bizonyítsuk be, hogy egy \( n \) összetett számra az alábbi három felétel bármelyike ekvivalens.

(a) Bármely \( \left( a, n \right) = 1 \) esetén \( a^{n-1} \equiv 1 \mod n \).

(b) Az \( n \) négyzetmentes, továbbá \( p \mid n = \Rightarrow p - 1 \mid n - 1 \).

(c) Bármely \( a \)-ra \( a^{n-1} \equiv a \mod n \).

Megjegyzés: Ennek alapján az univerzális álprim definíciójában (a) helyett a (c) [vagy a (b)] feltételt is választhatott volna.

5.7.8 Mutassuk meg, hogy egy univerzális álprimnek legalább három prímosztója van.

5.7.9 (a) A tárgyalt primteszteknél a feltétel ellenőrzése előtt nem szükséges külön megnézni, hogy a kipróbált \( a \) és a vizsgált \( n \) relatív prímek-e. Milyen előny származhat abból, ha mégis kiszámítjuk \( \left( a, n \right) \) értékét?

(b) Ha az \( n \) két szájegyű prim szorzata, akkor „nagyjából” mekkora a valószínűsége annak, hogy egy véletlenszerűen választott \( a \) szám az \( n \)-hez nem relatív prim?

5.7.10 Mutassuk meg, hogy ha \( a^2 \equiv 1 \mod n \), de \( a \neq \pm 1 \mod n \), akkor az \( n \)-nek gyorsan meg tudjuk határozni egy nemtriviális osztóját.

5.7.11 (*) Bizonyítsuk be, hogy ha \( n \)-en kívül ismerjük a \( \kappa(n) \) egy (nemnulla) többszörösségét is, akkor gyorsan elő tudjuk állítani az \( n \) kanonikus alakját. (Pontosabban, az eljárásban elvileg fennáll annak a lehetősége, hogy mégsem sikerül az \( n \)-et primitívnyelvőkre bontani, de gyakorlatilag ez sohasem fordulhat elő.)

5.7.12 Vizsgáljuk meg, alkalmazás-prímprozolók a Wilson-tétel és megfordítása, azaz ha azt ellenőrizzük, hogy \( n \) osztója-e \( (n - 1)! + 1 \)-nek.

5.7.13 (a) Mutassuk meg, hogy ha az \( n \) összetett szám nem univerzális álprim, akkor \( \kappa^{\nu - 1} \equiv 1 \mod n \) egy modulo \( n \) teljes maradéksrendszer elemeinek kevesebb, mint a felére teljesül.
(b) Írjuk le az (a) részen alapuló konkrét prímtesztet.

5.7.14 Mutassuk meg, hogy az alábbi prímteszt gyors, és a tévedés lehetősége akármilyen pici (előre megadott) korlát alá szorítható.

Az \( n > 1 \) páratlan számról akarjuk eldönteni, hogy prim-e. Adott darabszámú (de elég sok) véletlen \( n \parallel a \) -ra megnézzük \( a^{(n-1)/2} \) maradékát modulo \( n \). Az \( n \) -et akkor „nyilvánjuk” prímnek, ha az összes vizsgált \( a \)-ra a maradék \( \pm 1 \), de van köztük \(-1\) is.

5.7.15 Legyen \( u = 2^k r + 1 \), ahol \( k \geq 1 \), \( r \) páratlan és \( 0 < r < 2^k \). Tegyük fel, hogy egy \( a \) egész száma

\[
a^{\frac{n-1}{2}} \equiv -1 \pmod{n}.
\]

Lássuk be, hogy ekkor \( n \) prim.

5.7.16 Legyen \( n > 2 \). Mutassuk meg, hogy az alábbi feltételek bármelyikéből következik, hogy az \( n \) prim.

(a) Van olyan \( a \) egész szám, amelyre \( a^{n-1} \equiv 1 \pmod{n} \), és az \( n - 1 \) bármely \( p_i \) primosztójára

\[
a^{\frac{n-1}{p_i}} \not\equiv 1 \pmod{n}.
\]

(b) * Az \( n - 1 \) bármely \( p_i \) primosztójához van olyan \( a_i \) egész szám, amelyre

\[
a_i^{n-1} \equiv 1 \pmod{n} \quad \text{és} \quad a_i^{\frac{n-1}{p_i}} \not\equiv 1 \pmod{n}.
\]

(c) * Létezik az \( n - 1 \)-nek egy \( \sqrt{n} \)-nél nagyobb \( c \) osztója a következő tulajdonsággal: a \( c \) bármely \( p_i \) primosztójához van olyan \( a_i \) egész szám, amelyre

\[
a_i^{n-1} \equiv 1 \pmod{n} \quad \text{és} \quad \left(c_i^{\frac{n-1}{p_i}} - 1, n\right) = 1.
\]

5.7.17 (M [576]*) Mutassuk meg, hogy a Miller–Lenstra–Rabin-teszt hatékonyabb a Solovay–Strassen-tesztnél az alábbi értelmenben. Ha egy adott \( n \) -re az \( a \) tanú a Solovay–Strassen-tesztnél, akkor ugyanez az \( a \) tanú a Miller–Lenstra–Rabin-tesztnél is; vagyis, ha egy \( a \) -ra az T 5.7.4 Tételnél szereplő (1) feltétel nem teljesül, akkor erre az \( a \) -ra az T 5.7.5 Tételnél megadott (10) számhalmaz nem alkotható jó sorozatot.

5.8 Titkosírás

A klasszikus titkosírási sémaikban \( A \) és \( B \) előre megegyeznek egy \( T \) titkosító kulcsban (például minden betű helyett az ábécé rákövetkező betűjét írják), amelynek az inverze az \( M \) megfejtő kulcs (az előző esetben ez minden betű helyett az azt megelőzőt jelenti). Ekkor \( A \) az üzenet helyett annak \( T \) szerint titkosított változatát küldi el \( B \)-nek, aki azt az \( M \) segítségével fejti meg.

Ezek a kulcsok nemsak betűkre, hanem hosszú betűsorozatokra is vonatkozhatnak, és rendkívül bonyolultak is lehetnek. Ezekben a ma már csak számítógéppel kezelhető hatalmas rendszerekben a gép a kulcsok szabályai szerint végzi a titkosítást, illetve a megfejtést, és az üzennettovábbítás is futár helyett elektronikus úton történik.

Ezek a sémaik kielégítik azt a két alapkövetelményt, hogy \( A \) üzenetét csak \( B \) érti meg, továbbá egy harmadik fél nem tud hamis üzenetet küldeni \( A \) nevében \( B \)-nek. Hátrányt jelent azonban, hogy
nehézkes (és veszélyes) a kulcs előzetes egyeztetése, valamint nem dönthetők el az $A$ és $B$ között esetleg felmerülő viták, hiszen a közös $T$ és $M$ kulcsok birtokában akármelyikük képes a másik nevében „hamis” üzenetet gyártani.


Ez első hallásra képtelen ötletnek hangzik, hiszen ha az egyik irányban ismeri valaki az eljárást, akkor a másik irányban is meg tudja adni. Valóban, legyenek a $T$ és $M$ függvények (amelyek egymás inverzei) például az $\{1,2,\ldots,N\}$ halmaz bijekciói (látni fogjuk, hogy ez az általánosság megszoritása nélkül mindig feltehető). Ha meg akarjuk határozní (mondjuk) $M(5)$ -öt, akkor a nyilvános $T$ kulcs segítségével sorban kiszámítjuk a $T(1), T(2), \ldots$ értékeket, amíg az 5-öt meg nem kapjuk; az $M(5)$ függvényérték az a $k$ lesz, amelyre $T(k) = 5$.

Ez elven szépen hangzik, azonban ha $N$ mondjuk egy 500-jegyű szám, akkor ez az út a gyakoralathan már nem járható. Eckor ugyanis bármely számítógép évmilliárdok alatt is a $T(1), T(2), \ldots$ értékeket csak egy elenyésző töredéként tudna meghatározni, vagyis majdnem biztos, hogy $M(5)$ -öt sohasem találna meg. (A helyzetet megróbáljuk az alábbi hasonlattal érzékelteni. Egy angol-magyar szótár elven használható magyar-angol szótárként is: ha például az „ablak“ szó angol megfelelőjét keressük, akkor sorra nézzük az angol-magyar szótár (általánosan szereplő) angol szavait, amíg a magyar jelentések között az „ablak“ fel nem bukkan. Ezt a „window“-nél be is következik. Nem valószínű, hogy ezek után bárkinek is eszébe jutna, hogy elég csak az angol-magyar szótárt megvenni.)

Mindezek alapján nem elképzelhetetlen, hogy a $T$ kulcs nyilvános ismerete mellett is az $M$ kulcs egyedüll az illetékes személy titka maradjon. Nézzük, hogyan működik az ezen az elven alapuló űn. nyilvános jelkulcsú titkosírás.

Minden szereplő elkészít magának egy $T, M$ kulcs párat, amelyek egyes inverzei, a $T$ kulcsot nyilvánosságra hozza, az $M$ kulcsot viszont titokban tartja. Legyen az $A$ kulcspára $T_A, M_A$, a $B$ kulcspája pedig $T_B, M_B$ . Ekkor $A$ az $u$ üzenet helyett a $v = T_B(M_A(u))$ értéket küldi el $B$ -nek, aki ezt a következőképpen fejti meg: $u = T_A^{-1}(M_B(v))$ . Ez valóban igaz, hiszen

$$T_A(M_B(v)) = T_A[M_B(T_B(M_A(u)))] = T_A(M_A(u)) = u.$$

(Az $A$ a $v$ készítéséhez szükséges $M_A$ függvényt ismeri, a nyilvános $T_A$ függvényt pedig kikeresi a teletitok–könyvből, a $B$ -nél hasonló a helyzet $M_B$ -vel és $T_A$ -val.)

Most is teljesül az a két alapkövetelmény, hogy $A$ üzenetét csak $B$ érti meg, hiszen senki más nem ismeri a megfejtéshez szükséges $M_B$ -t, továbbá egy harmadik fél nem tud hamis üzenetet küldeni $A$ nevében $B$ -nek, hiszen csak $A$ ismeri a kódoláshoz szükséges $M_A$ -t.

Emellett nincs szükség előzetes kulcserejetteségre, és mindenki használhatja ugyanezeket a kulcsait másokkal történő levelezésben is. Végül $A$ és $B$ között sem merülhet fel vita az üzenetről, mert a hamisíthatatlan „elektronikus aláírásként” működő $M_A$ akár bíróság előtt is egyértelműen bizonyítja a levél valódiságát.

A rendszer megvalósításához tehát olyan $T, M$ kulcs párokat van szükség, hogy a kulcslajdodonos egy alkalmas, csak az ő rendelkezésére álló információ alapján mindkét kulcsot ismerje, azonban mások még a nyilvánosságra hozott $T$ birtokában sem legyenek képesek $M$ -et meghatározni.

Korábban láttuk, hogy ilyen „magántitok” például egy nagy szám primitényezős felbontása, amelyet csak az ismer, aki ezeket a primitényezőket összeszorozta. Ezt használta fel Rivest, Shamir és
Adleman 1976-ban a Diffie–Hellman-féle elv egy konkrét megvalósításához, amelyet ma RSA-sémának nevezünk. (Az elnevezés a felfedezők (vagy feltalálók?) nevének kezdőbetűiből származik.) Az RSA-séma ismertetése előtt megmutatjuk, hogy tetszőleges titkosírási rendszer visszavezethető arra az esetre, amikor a \( T \) és \( M \) függvények az \( \{1, 2, \ldots, N\} \) halmaz bijekciói (vagyis permutációi), ahol az \( N \) egy tetszőleges nagy egész szám. Ennek érdekében a betüket és egyéb jelkeket (egy mindenki által ismert módon) számokként kell alkalmaznunk. Majd az üzenetből ily módon gyártott számsorozatot adott méretű blokkokra vágjuk szét, és az egyes blokkokat (természetes módon) egyszerű (nagy) számokká tekintjük. Az így keletkező számok alkotják majd a \( T \) és \( M \) függvények értelmezési tartományát és értékkészletét.

A betűknek és jeleknek például az alábbi módon feleltethetünk meg kétjegyű (tizes számrendszerbeli) számokat: A \( \longmapsto 01 \), Á \( \longmapsto 02 \), B \( \longmapsto 03 \), ..., Z \( \longmapsto 35 \), „pont” \( \longmapsto 36 \) stb., és (mondjuk) négy ilyen kétjegyű szám alkossan egy blokkot. Ezzel az üzenetet nyolcjegyű, azaz \( 1 \) és \( 10^8 - 1 \) közé eső számokká alakítjuk, vagyis ekkor \( N \) vehető \( 10^8 - 1 \)-nek.

Nézzük meg, mit kapunk ily módon a „számmelélet” szóból. Az S-nek megfelel a 25, az Z-nek a 35, az Á-nak a 02 stb., és (mondjuk) négy ilyen kétjegyű szám alkosson egy blokkot. Ezzel az üzenetet nyolcjegyű, azaz \( 1 \) és \( 10^8 - 1 \) közé eső számokká alakítjuk, vagyis ekkor a

\[
\begin{align*}
25350216 & |06151607|150626
\end{align*}
\]

számsorozat keletkezik. Ez a 25350216, 06151607, 15062600 blokkot jelenti (az utolsó csonka blokkot nullákkal egészítettük ki). Ig így a titkosírás \( T \) (illetve \( M \)) kulcsát rendre erre a három számra kell alkalmaznunk. (Még egyszer hangsúlyozzuk, hogy a szövegenek ez a számokká konvertálási módja mindenként számára ismert, és csak arra szolgál, hogy a titkosírásban szereplő \( T \) és \( M \) függvényeket egységesen és kényelmesebben lehessen majd megadni.) Most rátérünk az RSA-séma szerinti \( T, M \) külcspar konstrukciójára.

Legyen \( N = pq \), ahol \( p \) és \( q \) két nagy prímszám, amelyeket a kulcstulajdonos titokban tart, ugyanakkor \( N \)-et teljes nyugalommal nyilvánosságra hozza. Választ továbbá egy olyan \( t > 1 \) egészt, amelyre \( \left(\frac{t}{N}\right) = 1 \), és nyilvánosságra hozza, hogy az \( t \) kulcsa a következő:

\[
T(r) = r^t \mod N, \quad r = 1, 2, \ldots, N. \tag{1}
\]

Hogyan lehet \( M = T^{-1} \) -et megkapni? Keressük \( M \) -et hasonló alakban:

\[
M(s) = s^w \mod N, \quad s = 1, 2, \ldots, N. \tag{2}
\]

Ez akkor lesz megfelelő, ha minden \( r \)-re

\[
\begin{align*}
\tau &= TM(r) = MT(r) = r^w \mod N,
\end{align*}
\]

azaz, ha minden \( \tau \)-re

\[
\tau^t = \tau \mod N. \tag{3}
\]

A \( P \) és \( Q \) primekre a kis Fermat-tételt felhasználva könnyen következik, hogy tetszőleges \( k \) -val

\[
\begin{align*}
\tau^{1+k\varphi(N)} &= \tau \mod N
\end{align*}
\]

minden \( \tau \)-re teljesül (lásd az 5.8.3a feladatot [164]). A (4) alapján (3)-ban (és így (2)-ben is) megfelelő \( \mu \) -hez jutunk, ha megoldjuk az

\[
\begin{align*}
\tau^t &= 1 + k\varphi(N)
\end{align*}
\]
lineáris diofantikus egyenletet \( mx - re \) -es \( k -ra\). Mivel \( (r; \varphi(N)) = 1 \), ezért van megoldás, és az euklideszi algoritmus segítségével gyorsan megkapható.

Mindezt azonban csak a kulcskezdések tulajdonosa tudja megcsinálni, mert más nem ismeri \( \varphi(N) \) értékét, hiszen ahhoz tudnia kellene, mik az \( N \) prímtényezői.

A kulcskezdések az eljárás alapját képező \( P \) és \( Q \) prímeket a következőképpen generálja. Sorra választ (mondjuk 250, illetve 300-jegyű páratlan véletlen számokat, és (például az 5.7 pontban tárgyalt prímtesztek valamelyikévékel) ellenőrzi, hogy prím-e. Ezt addig csinálja, amíg egy-egy prímet nem talál. Mivel egyrészt a prímteszt gyors, másrészt „elég sok” 250, illetve 300-jegyű prim van (a prímszámtétel szerint körülbelül minden \( \log(10^{300})/2 \approx 345 \)-ódik 300-jegyű páratlan szám prim), ezért \( P \) és \( Q \) hamar kiválasztható.

Végül, (1) és (2) alapján mind a \( T(r) \), mind pedig az \( M(s) \) függvényértékeket az ismételt négyzetre emelés módszerével gyorsan kiszámolhatók (persze ez utóbbiakat csak a kulcskezdések tulajdonosa meghatározni).

A \( P \), \( Q \) és \( t \) kiválasztásánál néhány biztonsági szabályt is figyelembe kell venni. Ha például \( P \) és \( Q \) túl közel lenne egymáshoz, akkor könnyebben lenne az \( N \) et faktorizálni, ezért kellett a \( P \) és \( Q \) választásánál különböző nagyságú véletlen számokat tesztelni. Hasonló okokból szükséges az is, hogy \( P - 1 \) -nek és \( Q - 1 \) -nek legyenek nagy prímtényezői stb. Ezekkel a technikai részletekkel nem foglalkozunk.

Mennyire biztonságos ez az eljárás? Úgy tűnik, hogy (az óvatossági rendszabályok maximális betartása esetén) nincs okunk aggodalomra. Nincs azonban kizárva, hogy valaki talál egy olyan módszert, amellyel gyorsan tud nagy számokat is prímtényezőkre bontani, és akkor hozzáfér az \( M \) kulcshez. Az is elképzelhető, hogy valamilyen egészen másféle formában képes előállítani az \( M \) függvényt. Mindez azonban meglehetősen valószínűség.

Az RSA-séma lényegét az alábbi tételben foglaljuk össze:

**5.8.1 Tétel (RSA-séma).**

Legyen \( P \), \( Q \) két nagy prim, \( N = PQ \) és \( (r; \varphi(N)) = 1 \). Defináljuk a \( T, M \) kulcspárt (1), illetve (2) alapján, ahol \( m \) -re teljesül (5). Nyilvános: \( N \), \( t \) és \( T \), titkos: \( P \), \( Q \), \( \varphi(N) \), \( m \) és \( M \). Ekkor \( M = T^{-1} \) és \( M \) a \( T \) ismeretében sem határozható meg.

A \( P \) és \( Q \) prímeket a kulcskezdések véletlen számok prímtesztelésével nyeri, ezek segítségével \( m \) -et gyorsan meg tudja határozni. Az \( M(s) \) függvényértékeit a kulcskezdések, a \( T(r) \) függvényértékeket pedig bárki gyorsan ki tudja számítani.

### Feladatok

**5.8.1** Milyen problémát jelenthet, ha a Diffie–Hellman-sémben az \( A \) az \( u \) üzenet helyett nem a \( v = T_D(M_A(u)) \), hanem csak a \( v' = T_D(u) \) értéket küldi el \( D \)-nek?

**5.8.2** Bizonyítsuk be, hogy az (1) által definiált \( T \) függvénynek akkor és csak akkor létezik inverze, ha \( (r; \varphi(N)) = 1 \).

**5.8.3** Legyen \( N = pq \), ahol \( p \) és \( q \) különböző prímek.

(a) Bizonyítsuk be, hogy \( r^{k \cdot \varphi(N)} \equiv r \pmod{N} \) minden \( r \)-re teljesül.
(b) Adjuk meg az összes olyan \( \sigma > 0 \) egész, amelytel\( \tau^x = \tau \left( u^{-1} \right) \) minden \( \tau \)-re teljesül.

5.8.4 Tegyük fel, hogy az RSA-sémához (a prímtesztelés tökéletlensége folytán) olyan \( P \) számot használunk fel, amely nem prim, hanem univerzális álprim (és ezt persze nem is tudjuk). Gondot okoz-e ez az RSA-sémában?

5.8.5 (*) Mutassuk meg, hogy az RSA-séma nem biztonságos, ha olyan \( t \) kitevőt választunk, amelynek a modulo \( \varphi(N) \) vett rendje kicsi.

5.8.6 Legyen \( P \) nagy prim és \( g \) egy primitív gyök modulo \( P \). Jelenlegi tudásunk szerint a \( g \) alapú diszkret logaritmus, vagyis \( g^i \mod P \) meghatározása reménytelen feladat, erre nem ismerünk gyors algoritmust. Ez azt jelenti, hogy bármely \( k \)-ra a \( g^k \mod P \) vett \( a \) maradékát gyorsan ki tudjuk számítani, azonban \( a \)-ből \( k \) értékét más nem tudja előállítani.

Az \( A \) és \( B \) választ egy-egy ilyen \( k_A \), illetve \( k_B \) kitevőt, amelyet titokban tartanak, azonban \( g^{k_A} \), illetve \( g^{k_B} \) modulo \( P \) maradékát nyilvánosságra hozzák. Mutassuk meg, hogy ekkor a \( g^{k_A k_B} \) szám modulo \( P \) maradékát mind \( A \), mind pedig \( B \) ki tudja számítani, rajtuk kívül más azonban (remélhetőleg) nem. (Ez azt jelenti, hogy ily módon \( A \) és \( B \) külön egyeztetés nélkül meg tudnak állapodni egy közös jelszóban vagy számkukban, anélkül hogy a titkos \( k_A \), illetve \( k_B \) értéküket egymás tudomására kellene hozniuk).

5.8.7 Hosszú ideig úgy tűnt, hogy az alább ismertett sémá, az ún. moduláris háttárés- vagy részösszegprobléma is felhasználható nyilvános jelkulcsú titkosításra, később azonban kiderült, hogy ez nem biztonságos.

(a) A pozitív egészombbál álló \( C = \{c_0, c_1, \ldots, c_{n-1} \} \) sorozatot nevezzük (házi használatra) összegjektívnek, ha a különböző \( c_i \)-kból képzett akárhány tagú összegek mind különbözök.

Bizonyítsuk be, hogy ha a \( C \) sorozat „szupernövekedő”, azaz

\[
c_i > \sum_{j=0}^{i-1} c_j, \quad i = 1, 2, \ldots, k - 1, \tag{6}
\]

akkor \( C \) összegjektív.

(b) Legyen \( C \) összegjektív, \( m > \sum_{i=0}^{k-1} c_i \) és \( \left( r, m \right) = 1 \), továbbá

\[
d_i = r_i \mod \text{ legkisebb pozitív maradéka (mod } m), \quad i = 0, 1, \ldots, k - 1. \tag{7}
\]

Mutassuk meg, hogy ekkor a \( d_0, \ldots, d_{k-1} \) sorozat is összegjektív.

(c) Legyen \( 0 \leq u < 2^k \), és írjuk fel az \( u \) számot kettes számrendszerben:

\[
u = \sum_{i=0}^{k-1} \delta_i 2^i, \quad \text{ahol} \quad \delta_i = 0 \text{ vagy } 1, \quad i = 0, 1, \ldots, k - 1.
\]

Bizonyítsuk be, hogy ha \( H \) összegjektív, akkor a

\[
u = \sum_{i=0}^{k-1} \delta_i h_i
\]

szám ismeretében \( u \) elvileg meghatározható.
(d) Mutassuk meg, hogy a (6) és a belőle gyártott (7) típusú sorozatokra az $u$-t $v$-ből gyakorlatilag is gyorsan meghatározható.

Mindezek alapján vegyünk egy (6) típusú $C$ sorozatot, és készítsünk ebből egy (7) típusú $D$ sorozatot. Magát a $D$-t hozzuk nyilvánosságra, azonban a $G_i$, $m$ és $r$ értékeket tartsuk titokban. Ekkor bárki gyorsan ki tudja számítani az $u$-ból a $v$-t, és mi ezt $C$, $m$ és $r$ ismeretében visszafelé is meg tudjuk csinálni. Mivel egy általános összeginjektív sorozat esetén a $v$-ből az $u$ konkrét előállítása igen nehéz, ezért úgy tűnt, hogy a (7) típusú sorozatoknál is ez a helyzet, ha valaki nem ismeri a $G_i$, $m$ és $r$ értékeket. Mint említettük, ez a vélekedés tévesnek bizonyult.
6. fejezet - SZÁMELMÉLETI FÜGGVÉNYEK

Számelméleti függvényen a pozitív egészeken értelmezett komplex értékű függvényt értünk. Ezek közül elsősorban azok lesznek érdekesek számunkra, amelyek a pozitív egészek valamilyen aritmetikai tulajdonságával kapcsolatosak. Ilyen például az \( n \) pozitív osztóinak számát jelölı \( d(n) \) és a kongruenciáknál nélkülözhetetlen Euler-féle \( \varphi(n) \) , amelyekkel már az 1., illetve 2. fejezetben találkoztunk. További fontos példák az \( n \) pozitív osztóinak összegét jelent\( \sigma(n) \), amely a tőkéletes számokhoz is kapcsolódik, valamint a \( \mu(n) \) Möbius-függvény, amely az összegzési és megfordítási függvényénél játszik alapvető szerepet. A \( \varphi(n) \) példáján keresztül bemutatjuk azt a sok számelméleti függvényre jellemző kétarcúsát, amely egyfelől a függvényértékek szeszélyes ingadozását, másfelől az „átlagos” értelmenben vett szabályos viselkedést jelenti. Az átlagértékek vizsgálatát a konvolúció felhasználásával kiterjeszthetjük a \( \sigma(n) \)-re és a \( \varphi(n) \)-re is. Ez utóbbi eredmény egyúttal megadja, mi a (pontosan definiálható értelmen vett) valószínűsége annak, hogy két szám relatív prim. (Ez a valószínűség meglepően nagynak bizonyul: \( 6/\pi^2 \approx 0,61 \).) Különösen érdekes az \( n \) különböző (pozitív) primosztóinak számát jelent\( \lambda(n) \) függvény vizsgálata, amelyről kiderül, hogy (ellentétben például a \( d(n) \) -nel) legtöbbször az átlagértékéhez közeli függvényértékeket vesz fel. Hardy és Ramanujan ezen híres tétele értéke Turán Pál adott egyszerű bizonyítást, amely később a valószínűségi számelmélet kiindulópontjává vált. Végül abból a Erdős által elindított témakörből adunk izelítőt, amely azt vizsgálja, milyen feltételekkel karakterizálható az additív függvények közül a logaritmusfüggvény.

6.1 Multiplikativitás, additivitás

6.1.1 Definíció . D 6.1.1

Számelméleti függvényeknek a pozitív egészeken értelmezett komplex értékű függvényeknek nevezzük.

Példák: \( d(n) \) az \( n \) pozitív osztóinak a száma (lásd az T 1.6.3 Tételt);

az Euler-féle \( \varphi \) -függvény (lásd a D 2.2.7 Definíciót és a T 2.3.1 Tételt); \( f(n) = (-1)^n \), \( \varphi(n) = \sqrt{n^2 + 3} + isint \) stb.

Néhány fontos számelméleti függvényt a 6.2 pontban fogunk ismertetni.

A számelméleti függvények vizsgálatánál gyakran lényeges szerepet játszanak az alábbi tulajdonságok:

6.1.2 Definíció . D 6.1.2

Az \( f \) számelméleti függvény multiplikatív, ha bármely \( (a, b) = 1 \) esetén \( f(ab) = f(a)f(b) \) teljesül.

6.1.3 Definíció . D 6.1.3

Az \( f \) számelméleti függvény teljesen multiplikatív (vagy totálisan multiplikatív), ha minden \( a, b \) esetén \( f(ab) = f(a)f(b) \) teljesül.

Példák:
Az Euler-féle \( \varphi \) -függvény multiplikatív (ezt a T 2.3.1 Tétel első bizonyításában igazoltuk), de nem teljesen multiplikatív, mert például \( \varphi(5) \neq \varphi(2)\varphi(4) \). Hasonló a helyzet a \( d(n) \)-nel (lásd a 6.1.1 feladatot [169]).

Az \( f(n) = n^\alpha \) függvény, ahol \( \alpha \) rögzített valós szám, teljesen multiplikatív (és így multiplikatív is).

\[ g(n) = 3n - 2 \] függvény nem multiplikatív, mert például \( (2, 3) = 1 \), de \( g(6) \neq g(2)g(3) \).

Ha a függvényértékek szorzata helyett az összegükre követelünk meg a fentiekhez hasonló feltételeket, akkor az additív, illetve teljesen additív függvény fogalmához jutunk:

6.1.4 Definíció . D 6.1.4

Az \( f \) szármelméleti függvény additív, ha bármely \((a, b)\) esetén \( f(ab) = f(a) + f(b) \) teljesül.

6.1.5 Definíció . D 6.1.5

Az \( f \) szármelméleti függvény teljesen additív (vagy totálisan additív), ha minden \( a, b \) esetén \( f(ab) = f(a) + f(b) \) teljesül.

Külön is felhívjuk a figyelmet arra, hogy a feltétel az additív, illetve teljesen additív függvény definíciójában is \( \varphi \)-függvényre vonatkozik.

Példák:

A (bármilyen alapú) logaritmusfüggvény teljesen additív.

\[ f(a) = 1 + (-1)^a \] additív, de nem teljesen additív.

\[ g(a) = 1 + \log_2 a \] nem additív (és így nem lehet teljesen additív sem).

Az \( f = 0 \) (azaz az azonosan nulla) függvény mind teljesen multiplikatív, mind pedig teljesen additív, de más függvény nem lehet egyszerre multiplikatív és additív (ez leolvasható például a T 6.1.6 Tételből).

Először megmutatjuk, hogy egy additív, illetve egy \( \neq 0 \) multiplikatív függvény az 1 helyen csak speciális értéket vehet fel:

6.1.6 Tétel . T 6.1.6

Ha \( f \) multiplikatív és \( f \neq 0 \), akkor \( f(1) = 1 \).

Ha \( g \) additív, akkor \( g(1) = 0 \).

Bizonyítás: Legyen \( a \) olyan pozitív egész, amelyre \( f(a) \neq 0 \). Ekkor \( (a, 1) = 1 \) miatt \( f(a) = f(a \cdot 1) = f(a)f(1) \), ahonnan \( f(a) \neq 0 \)-val történő egyszerűsítés után \( 1 = f(1) \) adódik.

A másik állítás is hasonlóan bizonyítható.

A T 6.1.6 Tétel tehát az additivitásnak, illetve multiplikativitásnak egy szükséges (de nem elégséges) feltételét adja.

Az additivitás, illetve multiplikativitás definíciójából azonnal következik, hogy egy additív, illetve \( \neq 0 \) multiplikatív függvényt a primhatvány helyeken felvett értékei már egyértelműen meghatároznak:
6.1.7 Tétel. \( T \) 6.1.7

Legyen \( f \) multiplikatív, \( g \) additív és \( n > 1 \) kanonikus alakja \( n = p_1^{a_1} \cdots p_r^{a_r} \). Ekkor

\[
f(n) = f(p_1^{a_1}) \cdots f(p_r^{a_r}) \quad \text{és} \quad g(n) = g(p_1^{a_1}) + \cdots + g(p_r^{a_r}).
\]

Ezt a tényt használtuk fel a \( f(n) \) képletének levezetésekor is (a \( T \) 2.3.1 Tétel első bizonyításában).

A teljesen additív, illetve \( (\neq 0) \) teljesen multiplikatív esetben a függvényt már a prim helyeken felvett értékei is egyértelműen meghatározzák:

6.1.8 Tétel. \( T \) 6.1.8

Legyen \( f \) teljesen multiplikatív, \( g \) teljesen additív és \( n > 1 \) kanonikus alakja \( n = p_1^{a_1} \cdots p_r^{a_r} \). Ekkor

\[
f(n) = f(p_1^{a_1}) \cdots f(p_r^{a_r}) \quad \text{és} \quad g(n) = \alpha_1 g(p_1) + \cdots + \alpha_r g(p_r).
\]

A \( T \) 6.1.7 Tételt kiegészíthetjük azzal, hogy a primhatvány helyeken felvett értékekre a multiplikativitás, illetve additivitás már semmilyen megszorítást sem jelent, ezek „szabadon megválaszthatók”. Ezen pontosan a következőt kell érteni: akárhogyan írjuk elő a primhatvány helyeken felvendő értékeket, biztosan létezik olyan multiplikatív, illetve additív függvény, amely ezen a helyeken az előírt értékeket veszi fel. A teljesen multiplicitív, illetve teljesen additív esetben hasonló értelmutáció érvényes a primhatványok helyett a primekre. (Minderre vonatkozólag lásd a 6.1.4 feladatot [169].)

Feladatok

6.1.1 Mutassuk meg, hogy a \( d(n) \) függvény multiplikatív, de nem teljesen multiplikatív.

6.1.2 Az alábbi függvények közül melyek multiplikatívak, illetve teljesen multiplikatívak, és melyek additívak, illetve teljesen additívak?

(a) \[ f(n) = \begin{cases} 0, & \text{l.a. } 6 \mid n; \\ 1, & \text{l.a. } 6 \nmid n. \end{cases} \]

(b) \[ g(n) = \begin{cases} 0, & \text{l.a. } 3 \mid n; \\ 1, & \text{l.a. } 3 \nmid n. \end{cases} \]

(c) \[ h(n) = \begin{cases} 0, & \text{l.a. } 3 \mid n; \\ 2, & \text{l.a. } 3 \nmid n. \end{cases} \]

(d) \[ k(n) = \begin{cases} 2, & \text{l.a. } 3 \mid n; \\ 0, & \text{l.a. } 3 \nmid n. \end{cases} \]

6.1.3 Van-e olyan \( h \) additív, illetve multiplikatív függvény, amelyre \( h(6) = 0 \), \( h(10) = 1 \) és \( h(15) = 3 \)?

6.1.4 Legyen \( \varphi_1, \varphi_2, \cdots = 2, 3, 5, 7, \cdots \) a primszámok, \( \varphi_1, \varphi_2, \cdots = 2, 3, 4, 5, 7, 8, 9, 11, \cdots \) pedig a primhatványok sorozata, és legyenek \( \varphi_1, \varphi_2, \cdots \) tetszőleges komplex számok.
(a) Bizonyítsuk be, hogy pontosan egy olyan \( f \neq 0 \) multiplikatív, illetve \( g \) additív függvény létezik, amelyre
\[
f(q_i) = g(q_i) = c_i, \quad i = 1, 2, \ldots
\]

(b) Bizonyítsuk be, hogy pontosan egy olyan \( s \neq 0 \) teljesen multiplikatív, illetve \( t \) teljesen additív függvény létezik, amelyre
\[
s(p_i) = t(p_i) = c_i, \quad i = 1, 2, \ldots
\]

6.1.5 Ha \( g \) csak pozitív egész értékeket vesz fel, akkor tetszőleges \( f \) -re definiálhatjuk a \( h(u) = (f \circ g)(u) - f(g(u)) \) összetétet függvényt. Melyek igazak az alábbi állítások közül?

(a) Ha \( f \) és \( g \) teljesen multiplikatív, akkor \( h \) is teljesen multiplikatív.

(b) Ha \( f \) és \( g \) teljesen additív, akkor \( h \) is teljesen additív.

(c) Ha \( f \) multiplikatív és \( g \) teljesen multiplikatív, akkor \( h \) is multiplikatív.

(d) Ha \( f \) teljesen multiplikatív és \( g \) multiplikatív, akkor \( h \) is multiplikatív.

6.1.6 (a) Legyen \( f \) teljesen additív. Melyek azok a pozitív egészek, amelyekre a \( g(n) = f(kn) \) függvény is teljesen additív?

(b) Oldjuk meg a feladatot arra az esetre is, ha a teljes additivitás helyett (mind \( f \) -re, mind pedig \( g \) -re) csak additivitást követelünk meg.

(c) Vizsgáljuk meg a kérdés teljesen multiplikatív, illetve multiplikatív változatát is.

6.1.7 (M \[577\]) (a) Bizonyítsuk be, hogy ha \( f \) teljesen additív, akkor
\[
\text{minden } a, b\text{-re } f(a) + f(b) = f(a+b).
\]

(b) Mutassuk meg, hogy \( (\nabla) \) akkor is érvényes, ha \( f \) -ről csak additivitást teszünk fel.

(c) \( * \) Adj meg az összes olyan \( f \) -et, amelyre \( (\nabla) \) fennáll.

(d) \( * \) Vizsgáljuk meg a problémakörnek az \( f(a)f(b) = f((a, b)) \) egyenlőségre vonatkozó megfelelőjét is.

6.1.8 Legyen \( f \) valós értékű és \( \overline{g(n)} = 2f(a) \). Mutassuk meg, hogy \( g \) akkor és csak akkor multiplikatív, ha \( f \) additív.

Megjegyzés: Ennek alapján a valós értékű additív függvények és a pozitív értékű multiplikatív függvények vizsgálata kölcsönösen visszavezethető egymásra.

6.1.9 (a) Bizonyítsuk be, hogy két additív, illetve két teljesen additív függvény összege és különbsége is additív, illetve teljesen additív.

(b) Bizonyítsuk be, hogy két teljesen additív függvény szorzata sohasem teljesen additív, kivéve azt a triviális esetet, amikor a két függvény közül legalább az egyik a 0 függvény.

(c) Mutassunk olyan példát, amikor két \( \neq 0 \) additív függvény szorzata is additív, és olyat is, amikor a szorzatuk nem additív.
(d) - (M [579]) Adjuk meg az összes olyan additív függvénypárt, amelyek szorzata is additív.

(e) Mutassuk meg, hogy két multiplikatív, illetve két teljesen multiplikatív függvény szorzata is multiplikatív, illetve teljesen multiplikatív.

(f) Bizonyítsuk be, hogy két különböző ≠ 0 multiplikatív függvény összege, illetve különbsége sohasem multiplikatív.

6.1.10 (a) Bizonyítsuk be, hogy két additív, illetve két teljesen additív függvény számával középe is additív, illetve teljesen additív.

(b) Bizonyítsuk be, hogy ha két teljesen multiplikatív függvény számával középe is teljesen multiplikatív, akkor a két függvény egyenlő. Mi a helyzet, ha (mindhárom függvényre) a teljes multiplikativitás helyett csak multiplikativitást követelünk meg?

6.1.11 Tegyük fel, hogy \( f \) multiplikatív, \( g \) additív és \( f + g \) konstans. Mutassuk meg, hogy ekkor \( f^{[100]} + g^{[100]} \) multiplikatív és \( f^{[100]}g^{[100]} \) additív.

6.1.12 (*) (a) Tegyük fel, hogy a \( h \) additív függvény előáll két multiplikatív függvény különbségeként. Bizonyítsuk be, hogy ha \( a, b \) és \( c \) páronként relatív primérek, akkor \( h(a)h(b)h(c) = 0 \).

(b) Tegyük fel, hogy a \( h \) additív függvény a triviális \( h \equiv b \) előállításon kívül másképp is felírható egy multiplikatív és egy additív függvény szorzataként. Bizonyítsuk be, hogy ha \( a, b \) és \( c \) páronként relatív primérek, akkor \( h(a)h(b)h(c) = 0 \).

6.1.13 (a) (M [581]) Tegyük fel, hogy egy additív függvény értékkészlete csak véges sok számból áll. Igazoljuk, hogy akkor ezen értékek mindegyikét a függvénynek végétlen sok helyen kell felvennie.

(b) Mutassunk példát arra, hogy az (a) rész állítása multiplikatív függvényekre általában nem igaz.

(c) Tegyük fel, hogy egy \( f \) multiplikatív függvény értékkészlete csak véges sok számból áll, és van olyan érték, amelyet a függvény csak véges sokszor vesz fel. Bizonyítsuk be, hogy ekkor létezik olyan \( K \), hogy ha \( n \) -nak van \( K \) -nál nagyobb prímosztója, akkor \( f(n) = 0 \).

6.1.14 Melyek igazak az alábbi állítások közül?

(a) Ha \( f \) additív, és van olyan \( a \), \( b \) számpár, amelyre \((a, b) \neq 1 \) és \( f(ab) = f(a) + f(b) \), akkor \( f \) teljesen additív.

(b) Ha \( f \) additív, és van olyan \( a \), \( b \) számpár, amelyre \((a, b) \neq 1 \) és \( f(ab) = f(a) + f(b) \), akkor végétlen sok ilyen számpár is létezik.

(c) Ha \( f \) additív, de nem teljesen additív, akkor \((a, b) \neq 1 \) -ből következik, hogy \( f(ab) \neq f(a) + f(b) \).

(d) Ha \( f \) additív, de nem teljesen additív, akkor végétlen sok olyan \( a \), \( b \) számpár létezik, amelyre \( f(ab) \neq f(a) + f(b) \).

(e) Ha \( f \) multiplikatív, de nem teljesen multiplikatív, akkor végétlen sok olyan \( a \), \( b \) számpár létezik, amelyre \( f(ab) \neq f(a)f(b) \).

6.1.15 (M [582]*) Jelölje \( \varphi(n) \) az \( 1, 2, \ldots, n \) számok közül azoknak az \( i \) -nél az \( i \) -knek a számát, amelyekre \( (i, n) = (i + 1, n) = 1 \). Adjunk képletet \( \varphi(n) \) -re az \( n \) kanonikus alakjának alapján.
6.1.16 (*) Bizonyítsuk be:

\[ \sum_{1 \leq k \leq n, \frac{k}{n} = 1} (k - 1, n) = \varphi(n)d(n). \]

6.2 Nevezetes függvények

Ebben a pontban néhány fontos számelméleti függvényt vezetünk be, ezek a \( \sigma(n), \mu(n), \omega(n), \Omega(n) \) és \( d_k(n) \).

6.2.1 Definíció. \( \text{D 6.2.1} \)

\( \sigma(n) \) az \( n \) pozitív osztóinak az összege. ♦

Példa: \( \sigma(1) = 1 \), \( \sigma(10) = 18 \), \( \sigma(n) = n + 1 \iff n \) prim.

Oszton a fejezet további részében mindig pozitív osztót fogunk érteni.

6.2.2 Tétel. \( \text{T 6.2.2} \)

Ha az \( n \) kanonikus alakja \( n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \), akkor

\[ \sigma(n) = \prod_{i=1}^{r} (1 + p_i^{\alpha_i} + p_i^{2\alpha_i} + \cdots + p_i^{\alpha_i}) = \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}. \]

Bizonyítás: Ugyanazt a gondolatmenetet követjük, amelyet a \( d_k(n) \) képletének levezetésénél használtunk (T 1.6.3 Tétel).

Az T 1.6.2 Tétel szerint az \( n \) összes (pozitív) osztóját úgy kapjuk meg, ha a

\[ d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r} \tag{1} \]

kifejezésben a \( \beta_1, \beta_2, \cdots, \beta_r \), kitevők egymástól függetlenül végigfutnak a

\[ \beta_1 = 0, 1, \ldots, \alpha_1, \quad \beta_2 = 0, 1, \ldots, \alpha_2, \ldots, \quad \beta_r = 0, 1, \ldots, \alpha_r, \]

értékeken, továbbá az \( n \) minden osztója csak egyféleképpen áll elő a fenti alakban. Ennek megfelelően a \( \sigma(n) \) az összes ilyen \( d \) összege.

Másrészt nyilván ugyanezt az összeget kapjuk, ha a

\[ \prod_{i=1}^{r} (1 + p_i^{\alpha_i} + p_i^{2\alpha_i} + \cdots + p_i^{\alpha_i}) \tag{2} \]

szorzást elvégezzük; az (1) szorzat akkor keletkezik, amikor (2) első tényezőjéből a \( p_1^{\alpha_1} \) tagot, a második tényezőből \( p_2^{\alpha_2} \) tagot stb. szorozzuk össze.

Ezzel beláttuk a tétel állításában szereplő első egyenlőséget.

A második egyenlőség a véges mértani sorozatok jól ismert összegképletéből adódik. ♦
A T 6.2.2 Tétel egy másik lehetséges bizonyítására nézve lásd a 6.2.1 feladatot [176].

6.2.3 Definíció . D 6.2.3

A \( \mu(n) \) Möbius-függvényt a következő módon értelmezzük:

\[
\mu(n) = \begin{cases} 
1, & \text{ha } n = 1; \\
(-1)^x, & \text{ha } n = p_1 \ldots p_x, \text{ akkor } p_1 \ldots p_x \text{ különböző prímek;} \\
0, & \text{ha van olyan } p \text{ prím, amelyre } p^2 \mid n. 
\end{cases}
\]

Példa: \( \mu(10) = 1 \), \( \mu(20) = 0 \), \( \mu(30) = -1 \).

A \( \mu \) -függvény későbbi fontos szerepe elsősorban az alábbi egyszerű tulajdonságán múlik:

6.2.4 Tétel . T 6.2.4

\[
\sum_{d \mid n} \mu(d) = \begin{cases} 
1, & \text{ha } n = 1; \\
0, & \text{ha } n > 1. 
\end{cases}
\]

Bizonyítás: Ha \( n = 1 \), akkor \( \sum_{d \mid 1} \mu(d) = \mu(1) = 1 \).

Ha \( n > 1 \), akkor legyen az \( n \) kanonikus alakja \( n = p_1^{\alpha_1} \ldots p_r^{\alpha_r} \). Mivel a nem négyzetmentes számokra a \( \mu \)-függvény értéke 0, ezért elég az összegzést az \( n \) -négyzetmentes osztóira elvégezni. Ennélfogva

\[
\sum_{d \mid n} \mu(d) = \mu(1) + \mu(p_1) + \cdots + \mu(p_r) + \\
+ \mu(p_1p_2) + \mu(p_1p_3) + \cdots + \mu(p_{r-1}p_r) + \cdots + \mu(p_1p_2 \ldots p_r) = \\
= 1 - r + \binom{r}{2} - \binom{r}{3} + \cdots + (-1)^r \binom{r}{r} = (1 - 1)^r = 0. \]

6.2.5 Definíció . D 6.2.5

\( \omega(n) \) az \( n \) különböző ( pozitív) prímosztóinak a száma.

\( \Omega(n) \) az \( n \) „összes” ( pozitív) prímosztóinak a száma, tehát amikor a primeket a kanonikus alakban szereplő kitevő szerinti multiplicitással számoljuk.

Képlettel: \( \omega(1) = \Omega(1) = 0 \), és ha az \( n \) kanonikus alakja

\( n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \) (ahol minden \( \alpha_i > 0 \)),

akkor

\( \omega(n) = r \) és \( \Omega(n) = \alpha_1 + \cdots + \alpha_r. \)

Példa: \( \omega(50) = 2 \), \( \Omega(50) = 5 \), \( \omega(n) = \Omega(n) \iff n \text{ négyzetmentes.} \)

6.2.6 Definíció . D 6.2.6

Legyen \( k \) rögzített pozitív egész. Ekkor \( d_k(n) \) az \( n = x_1^{\alpha_1} \cdots x_k^{\alpha_k} \) egyenlet pozitív egész megoldásainak a számát jelenti, ahol két megoldást akkor is különbözőnek tekintünk, ha csak a tényezők sorrendjében térnek el egymástól.
Nyilván $d_1(n) = 1$, $d_k(1) = 1$, továbbá $d_k(n) = d(n)$ (a $d_k(n)$ függvény tehát a $d(n)$ általánosításának tekinthető).

6.2.7 Tétel. T 6.2.7

Ha az $n$ kanonikus alakja $n = p_1^{a_1} \cdots p_r^{a_r}$, akkor

$$d_k(n) = \prod_{i=1}^{r} \left( \frac{\alpha_i - k - 1}{k - 1} \right).$$

Bizonyítás: Az $\omega_i$ számok primosztói is a $p_1 \cdots p_r$ prímek közül kerülnek ki, ezért az $\omega_i$ számok kanonikus alakja

$$\omega_1 = p_1^{\delta_1} \cdots p_r^{\delta_r}, \quad \ldots, \quad \omega_k = p_1^{\delta_{r+1}} \cdots p_r^{\delta_{r+k}},$$

ahol

$$0 \leq \delta_{ij} \leq a_i, \quad i = 1, 2, \ldots, r, \quad j = 1, 2, \ldots, k.$$

(A kitevők az első index a prim, a második index pedig az ismeretlen sorszámát jelenti.)

Ekkor az $\omega = \omega_1 \omega_2 \cdots \omega_k$ egyenlet pontosan akkor teljesül, ha

$$\alpha_1 = \beta_{11} + \beta_{12} + \cdots + \beta_{1k}, \quad \ldots, \quad \alpha_k = \beta_{r1} + \beta_{r2} + \cdots + \beta_{rk}. \quad (3)$$

A (3) egyenletrendszer $r$ darab

$$\alpha = y_1 + y_2 + \cdots + y_k, \quad y_i \geq 0 \text{ egész} \quad (4)$$

típusú egyenletet tartalmaz.

Vizsgáljuk meg, hogy egy ilyen egyenletnek hány megoldása van.

Más megfogalmazásban (4) megoldásszáma azt jelenti, hányféleképpen lehet az $\omega$ számot $k$ darab nemnegatív egész összegeként előállítani, ha az összeadandók sorrendje is számít, vagyis ha két előállítást akkor is különbözőnek tekintünk, ha csak az összeadandók sorrendjében térnek el egymástól.

Vegyük egy $\alpha$ hosszúságú szakaszt, és mérjük fel rá sorban az $y_1, \ldots, y_k$ hosszúságú szakaszokat (beleértve a 0 hosszúságúakat is). Ezt úgy is interpretálhatjuk, hogy leírunk $\omega$ darab 1-est, majd egy * jellet jelezzük, hogy ennek a szakasznak vége, ezután leírunk $\omega_2$ darab 1-est, amelyet ismét egy * elválasztójel követ stb., végül $\omega_k$ darab 1-es zárja a sort.

Például, ha $\alpha = 7$ és $k = 4$, akkor a $\omega = 7 + 4 + 0 + 1 + 2$ előállításnak az $1111 * 11$ elsőjel esetén a $1111 * 111$ jelsorozat felel meg. Megfordítva a $1111 * 1111$ jelsorozat a $7 = 0 + 4 + 3 + 0$ előállításból származott.

Ennek megfelelően a (4) egyenlet megoldásszáma megegyezik az ilyen jelsorozatok számával.

Egy jelsorozat $\alpha$ darab 1-est és $k - 1$ darab * elválasztójéjelet tartalmaz, tetszőleges sorrendben. Ennél fogva az ilyen jelsorozatok száma

$$\binom{\alpha + k - 1}{k - 1}. \quad (5)$$
Az (5) képlet alapján a (3)-ban szereplő egyenletek megoldásszáma rendre

\[
\left( \alpha_1 + \frac{k - 1}{k - 1} \right), \left( \alpha_2 + \frac{k - 1}{k - 1} \right), \ldots, \left( \alpha_r + \frac{k - 1}{k - 1} \right). \tag{6}
\]

Mivel az egyes egyenletek egymástól teljesen függetlenek, ezért a (3) rendszer megoldásszámát az egyes egyenletek megoldásszámainak, azaz a (6)-ban felsorolt számoknak a szorzata adja. □

Megjegyezzük, hogy a \( \sigma(n), \Omega(n), d_k(n) \) (és így speciálisan \( d(n) \)) függvényekre adott képlet akkor is igaz marad, ha megengedjük, hogy az \( n \) kanonikus alakjában az \( \alpha_i \) kivevő között a nulla is előforduljon, azonban \( \varphi(n) \) és \( \omega(n) \) képlete csak úgy érvényes, ha a kanonikus alakban minden kivevő valóban pozitív.

Végül megvizsgáljuk a megismert függvényeket multiplikativitás, illetve additivitás szempontjából.

### 6.2.8 Tétel

\( \varphi(n), \sigma(n), \mu(n) \) és \( d_k(n) \) multiplikatív, de nem teljesen multiplikatív (a \( d_1(n) = 1 \) triviális esetnél eltekintve).

\( \omega(n) \) additív, de nem teljesen additív.

\( \Omega(n) \) teljesen additív. □

**Bizonyítás:** \( \varphi(n) \) multiplikativitása szerepelt a T 2.3.1 Tétel első bizonyításában (valamint a 2.2.14 [41] és 2.6.10 feladatokban [61] is). Továbbá például

\[ 6 = \varphi(2) \neq \varphi(3) \varphi(3) = 4, \]

tehát \( \varphi(n) \) nem teljesen multiplikatív. (Sőt, \( (a, b) \neq 1 \) esetén \( \varphi(ab) = \varphi(a) \varphi(b) \) sohasem teljesül, lásd a 2.3.10a feladatot [45].)

A \( \sigma(n) \) multiplikativitásához a T 6.2.2 Tételben bizonyított képletet használjuk fel (egy másik bizonyítást kaphatunk az 1.6.5a-b feladat [28] alapján, lásd a 6.2.1 feladatot [176]).

Ha \( a = 1 \) vagy \( b = 1 \), akkor \( \sigma(ab) = \sigma(a)\sigma(b) \) nyilván teljesül.

Ha \( (a, b) = 1 \) és a kanonikus alakjuk

\[ a = p_1^{a_1} \cdots p_r^{a_r}, \quad b = q_1^{b_1} \cdots q_s^{b_s}, \]

ahol a relatív prím ség miatt \( p_i \neq q_j \), akkor \( ab \) kanonikus alakja

\[ ab = p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s}, \]

és így a \( \sigma \) képletét \( a \)-ra, \( b \)-re és \( ab \)-re alkalmazva kapjuk, hogy

\[ \sigma(a)\sigma(b) = p_1^{a_1+1} - 1 \cdots , p_r^{a_r+1} - 1 , q_1^{b_1+1} - 1 \cdots , q_s^{b_s+1} - 1 , a_1 - 1 \cdots , a_s - 1 = \sigma(ab). \]

Továbbá például

\[ 3\delta - \sigma(2)\sigma(3) \neq \sigma(12) = 28, \]
tehát $\sigma(n)$ nem teljesen multiplikatív. (Sőt, $(a, b) \neq 1$ esetén $\sigma(ab) = \sigma(a)\sigma(b)$ sohasem teljesül, lásd a 6.2.2 feladatot [176].)

A $\mu(n)$ multiplikativitását a függvény D 6.2.3 Definíciója alapján igazoljuk. Ha $x = 1$ vagy $b = 1$, akkor $\mu(ab) = \mu(a)\mu(b)$ nyilván teljesül. Ha $x$ és $b$ közül legalább az egyik nem négyzetmentes, akkor a szorzatuk sem az, és így $\mu(ab) = \mu(a)\mu(b) = 0$. Végül, ha mindkettő négyzetmentesek és $(a, b) = 1$, akkor a szorzatuk is négyzetmentes;

\[ a = p_1 \ldots p_x, \quad b = q_1 \ldots q_y, \quad ab = p_1 \ldots p_x q_1 \ldots q_y, \]

és így

\[ \mu(a)\mu(b) = (-1)^x(-1)^y = (-1)^{x+y} = \mu(ab). \]

Továbbá például

\[ -1 = \mu(5)\mu(15) \neq \mu(75) = 0, \]

tehát $\mu(n)$ nem teljesen multiplikatív.

(Megjegyezzük, hogy a $i(\mu(n))$ esetében — szemben a $d(\varphi(n))$, $\varphi(n)$ és $\sigma(n)$ függvényeknél tapasztaltakkal — olyan $a$, $b$ számpárokból is végzeten sok van, amelyekre $(a, b) \neq 1$ és mégis $\mu(a)\mu(b) = \mu(ab)$; legyen például $a = 4$ és $b$ tetszőleges páros szám.)

A $d_\kappa(n)$ -re vonatkozó állítást a $\sigma(n)$ -nél láttottakhoz hasonlóan igazolhatjuk.

Végül, az $\varphi(n)$ -re és $\Omega(n)$ -re vonatkozó állítás azonnal következik a függvények D 6.2.5 Definíciójából. □

Feladatok

6.2.1 Bizonyítsuk be a $\sigma(n)$ multiplikativitását az 1.6.5a-b feladat [28] felhasználásával, majd ennek alapján vezessük le a $\sigma(n)$ képletét.

6.2.2 Mutassuk meg, hogy ha $(a, b) \neq 1$, akkor $\sigma(ab) < \sigma(a)\sigma(b)$, továbbá $k > 1$ esetén $d_k(ab) < d_k(a)d_k(b)$.

6.2.3 Tegyük fel, hogy $m;\sigma(n)\sigma(n)$ nem osztható 3-mal. Bizonyítsuk be, hogy ekkor $n$ négyzetszám.

6.2.4 Bizonyítsuk be, hogy minden $n$ -hez végzeten sok olyan $k$ létezik, amelyre $\sigma(n)/\sigma(n;k)$.

6.2.5 Egy $\Omega$ szám (pozitív) osztóinak az összegét elosztjuk az $\Omega$ (pozitív) osztói reciprokainak az összegével. Mit kapunk eredményül?

6.2.6 Határozzuk meg az összes olyan $\Omega$ -et, amelyre $\sigma(\Omega)$

(a) páratlan; (b) kettőhatvány.

6.2.7 (M [583]*) Bizonyítsuk be, hogy a $\sigma(\Omega)$ függvény értékkészletéből végzeten sok természetes szám kimarad.
6.2.8  (M [585]*) Határozzuk meg az összes olyan $n$ pozitív egészt, amelyhez létezik olyan $k$, hogy $\sigma(n^k) = k!$.

6.2.9  Mutassuk meg, hogy bármely $n$ összetett számra $\sigma(n) \geq n + \sqrt{n} + 1$. Mikor áll egyenlőség?

6.2.10  Tekintsük a $\sigma(n) = n + c$ egyenletet, ahol az $n$ az ismeretlen és a $c$ rögzített pozitív egész.
(a) Oldjuk meg az egyenletet, ha $c$ értéke
(a1) 1;
(a2) 5;
(a3) 8;
(a4) 11.
(b) Mely $c$ értékek esetén van az egyenletnek végletes sok megoldása?

(c) Tegyük fel, hogy a páros Goldbach-sejtés abban a kicsit erősebb értelmen igaz, hogy minden $6$-nál nagyobb páros szám előáll két különböző prímszám összegeként. Mutassuk meg, hogy ekkor a fenti egyenletnek minden $c \neq 5$ páratlan szám esetén létezik megoldása.

Megjegyzés: Sokáig megoldatlan probléma volt, hogy végletes sok olyan $c$ pozitív egész létezik-e, amelyre egyáltalán nincs megoldás. Erdős megmutatta, hogy valóban végletes sok ilyen (páros) $c$ van.

6.2.11  Tekintsük a $\sigma(n) - \varphi(n) = c$ egyenletet, ahol az $n$ az ismeretlen és a $c$ rögzített pozitív egész.
(a) Oldjuk meg az egyenletet, ha $c$ értéke
(a1) 2;
(a2) 4;
(a3) 5;
(a4) 10.
(b) Mely $c$ értékek esetén van az egyenletnek végletes sok megoldása?
(c) Tegyük fel, hogy a páros Goldbach-sejtés abban a kicsit erősebb értelmen igaz, hogy minden $6$-nál nagyobb páros szám előáll két különböző prímszám összegeként. Adjunk meg ennek alapján végletes sok olyan $c$ értéket, amelyre a fenti egyenletnek létezik megoldása.

6.2.12  Hány olyan $a \neq b$ számpár létezik, ahol $a$ és $b$ is összetett és
(a) $a + \varphi(b) = b + \varphi(a)$;
(b) $a + \sigma(b) = b + \sigma(a)$?

6.2.13  Bizonyítsuk be, hogy az alábbi egyenlőtlenségek minden $n$-re teljesülnek, és határozzuk meg, mikor áll egyenlőség.
(a) $\sigma(n) \leq \frac{(n+1)d(n)}{2}$;
(b) $\sigma(\tau) \leq \frac{n\tau}{2} + 1$;
(c) \( \sigma(n) \geq n + 2d(n) - 3. \)

6.2.14 (*) Oldjuk meg a \( 2\sigma(n) = nd(n) \) egyenletet.

6.2.15 (a) Bizonyítsuk be, hogy az alábbi egyenlőtlenségek minden \( n > 1 \) számra teljesülnek, és határozzuk meg, mikor áll egyenlőség.

(a1) \( \sigma(n)\varphi(n) \leq n^2 - 1 \); (a2) \( \sigma(n) + \varphi(n) \geq 2n \).

(b) Igazoljuk, hogy

(b1) \( \sigma(n)\varphi(n) > \frac{n^2}{2} \); (b2) \( \inf \frac{\sigma(n)\varphi(n)}{n^2} = \frac{\alpha}{\pi^2} \).

6.2.16 (*) Bizonyítsuk be:

\[ \varphi(n) \mid n\sigma(n) - 2 \iff n \text{ prím vagy } n = 1, 4, 6, 22. \]

6.2.17 Milyen értékeket vesznek fel az alábbi függvények?

(a) \( f(n) = \mu(n) + \mu(2n) + \mu(5n) + \mu(10n) \);

(b) \( (M\ [585]) \ g(n) = \sum_{k|n} \mu(k) \).

6.2.18 (a) Hány olyan egymást követő szám adható meg, hogy \( \mu(n) \) azok egyikén sem nulla?

(b) Hány olyan egymást követő szám adható meg, hogy \( \mu(n) \) azok mindegyikén nulla?

6.2.19 (*) Igazoljuk, hogy a primitív komplex \( n \) -edik egységgyökök összege \( \mu(n) \).

6.2.20 Adjuk meg egyszerűbb alakban a \( \mu(n)\left(\Omega(n) - \omega(n)\right) \) függvényt.

6.2.21 (a) Bizonyítsuk be, hogy

\[ \Omega(n) \leq d(n) \leq \Omega(n) \]

minden \( n \) -re teljesül. Mikor áll egyenlőség?

(b) Hogyan általánosítható az (a) rész \( d(n) \) -ről \( d_k(n) \) -re?

6.2.22 Melyek igazak az alábbi állítások közül?

(a) Ha \( n \) négyzetszám, akkor \( d(n) \mid d_s(n) \).

(b) Ha \( d(n) \mid d_s(n) \), akkor \( n \) négyzetszám.

6.2.23 Legyen \( \nu \) tetszőleges valós szám és definiáljuk a \( \sigma_\nu(n) \) függvényt, mint az \( n \) pozitív osztói \( \nu \) -edik hatványainak az összegét:

\[ \sigma_\nu(n) = \sum_{d|n} d^\nu. \]

Speciálisan: \( \sigma_1(n) = \sigma(n) \) és \( \sigma_0(n) = d(n) \).

Adjunk képletet \( \sigma_\nu(n) \) -re, és lássuk be, hogy \( \sigma_\nu(n) \) multiplikatív.
6.3 Tökéletes számok

A régi görögök számmisztikájának fontos eleme, hogy egy szám osztóját (kivéve magát a számot) a szám részének tekintették, és tökéletesnek nevezték azokat a számokat, amelyek a „réseikből összeállnak”. Ilyen például a $6 = 1 + 2 + 3$ és a $28 = 1 + 2 + 4 + 7 + 14$. Euklídész Elemek című könyvében szerepel az alábbi általános konstrukció is (bizonyítással együtt!):

„Ha az egységtől kezdve kétszeres arányban képezünk egy mértani sorozatot, amíg a sorösszeg prim nem lesz, és az összeggel megszorozzuk az utolsó tagot, akkor a szorzat tökéletes szám lesz.”

Mai terminológiával a tökéletes számok éppen azok, amelyekre ($\sigma(n)$ hiszen magát az $n$ -et is az osztók közé számítjuk), és Euklídész tétele szerint az

$$(1 + 2 + 2^2 + \cdots + 2^k)2^k = (2^{k+1} - 1)2^k$$

szám tökéletes, ha $2^{k+1} - 1$ prim. $A \ k = 1$ és $k = 2$ esetekben éppen a 6-ot és a 28-at kapjuk.

A $2^n$ alakú prímek a Mersenne-prímek (lásd az 5.2 pontot), és tudjuk, hogy ekkor $n$ is szükségképpen prim. Mint az 5.2 pontban már említettük, Merseennes (másokhoz hasonlóan) éppen a minél nagyobb tökéletes számok előállítása céljából foglalkozott az ilyen alakú prímekkel.


Most megismételjük a tökéletes szám definícióját, és bebizonyítjuk a páros tökéletes számok leírását megadó Euklídész–Euler-tételt.

6.3.1 Definíció .  D 6.3.1

Az $n$ pozitív egész tökéletes szám, ha $\sigma(n) = 2n$.  

6.3.2 Tétel .  T 6.3.2

Egy $n$ páros szám akkor és csak akkor tökéletes, ha $n = 2^{p-1}(2^p - 1)$ alakú, ahol $2^p - 1$ (Mersenne-prím) (és így $P$ is szükségképpen prim).  

Bizonyítás: Először megmutatjuk, hogy az ilyen alakú számok valóban tökéletesek. Mivel $2^n - 1$ prim, ezért a megadott alak egyben az $n$ kanonikus alakja, és így a T 6.2.2 Tétel szerint kapjuk, hogy

$$\sigma(n) = (1 + 2 + \cdots + 2^{p-1})(1 + (2^p - 1)) = (2^p - 1)2^p = 2n.$$

A megfordításhoz tegyük fel, hogy $n$ páros és tökéletes, azaz

$$n = 2^k t, \ \text{ahol} \ k \geq 1 \ \text{és} \ t \ \text{páratlan, továbbá} \ \sigma(n) = 2n. \hspace{1cm} (1)$$

Mivel $(2^k, t) = 1$, ezért a $\sigma$ -függvény multiplikativitását és a $\sigma(2^k)$ -ra vonatkozó képleteket felhasználva (1)-ből

$$2^{k+1} t = 2n = \sigma(n) = \sigma(2^k)\sigma(t) = (2^{k+1} - 1)\sigma(t). \hspace{1cm} (2)$$
adódik.

Vonjuk ki (2)-ből (pontosabban az egyenlőségsor első és utolsó tagjából) a \((2^{k+1} - 1)^t\) értéket, ekkor a \(t\) számot szorzattá tudjuk bontani:

\[
l = (2^{k+1} - 1)(\sigma(t) - t).
\]  

(3)

A (3)-ból következik, hogy a \(t\) osztói között szerepel a \(\sigma(t) - t\). Emellett \(k \geq 1\) miatt \(2^{k-1} - 1 > 1\) , ezért (3) alapján \(\sigma(t) - t \neq l\).

Mivel \(\sigma(t) - t\) és \(t\) különböző osztói \(-\)nek, továbbá ezek összege egyenlő \(\sigma(t)\) -vel, vagyis a \(t\) összes osztójának az összegével, ezért a \(t\) -nek nem lehet több osztója. Ez azt jelenti, hogy \(t\) prim, és így \(\sigma(t) - t = 1\).

Ezt (3)-ba, majd (1)-be visszahelyettesítve kapjuk, hogy

\[
n = 2^k(2^{k+1} - 1), \text{ ahol } 2^{k-1} - 1 \text{ prím},
\]

ami a \(p = k + 1\) helyettesítés után éppen az \(n\) keresett előállítását adja. 

**Feladatok**

6.3.1 Mutassuk meg, hogy minden páros tökéletes szám utolsó számjegye 6 vagy 8 (a tízes számrendszerben).

6.3.2 Bizonyítsuk be, hogy ha létezik egy páratlan \(n\) tökéletes szám, akkor szükségképpen

(a) \(n = s^2p\), ahol \(p\) egy \(4^k + 1\) alakú prim;

(b) \(n \equiv 1 \pmod{12}\) vagy \(n \equiv 9 \pmod{36}\).

6.3.3 Egy természetes számot a régi görögök nyomán **hiányosnak** nevezünk, ha nagyobb, mint a nála kisebb pozitív osztóinak az összege (azaz „a részei együttesen kevesebbet tesznek ki nála”). **Bővelkedő** egy szám, ha ez az összeg nagyobb magánál a számnál (azaz „a részei együttesen többet tesznek ki nála”). Például a 10 hiányos, mert \(1 + 2 + 5 < 10\), a 12 viszont bővelkedő, mert \(1 + 2 + 3 + 4 + 6 > 12\).

Igazoljuk az alábbi állításokat.

(a) Minden primhatvány hiányos szám.

(b) Ha egy \(n\) páratlan számnak csak két különböző prímosztója van, akkor \(n\) hiányos.

(c) Minden \(k \geq 3\) esetén végtelen sok olyan páratlan bővelkedő szám és végtelen sok olyan páratlan hiányos szám létezik, amelynek pontosan \(k\) különböző prímosztója van.

(d) Egy bővelkedő szám minden többszöröse is bővelkedő.

(e) Bármely hiányos számnak végtelen sok bővelkedő többszöröse és végtelen sok hiányos többszöröse van.

6.3.4 (*) Ha az osztók közül magán a számon kívül az 1-et is kihagytuk, és a többi osztóból akarjuk a számot összeállítani, akkor a \(\sigma(n) = 2n + 1\) feltételhez jutunk. Bizonyítsuk be, hogy egy ilyen tulajdonságú szám szükségképpen egy páratlan szám négyzete.
Megjegyzés: Ezeket a számokat kvázitökéletes számoknak nevezzük. Megoldatlan probléma, hogy egyáltalán létezik-e kvázitökéletes szám.

6.3.5 (M [585]*) Az $\sigma$ pozitív egész szupertökéletesnek nevezzük, ha $\sigma(\sigma(n)) = 2n$. Bizonyítsuk be az alábbi állításokat.

(a) Egy $n$ páros szám akkor és csak akkor szupertökéletes, ha $n = 2^v - 1$ alakú, ahol $2^v - 1$ (Mersenne-)prim.

(b) Egy páratlan szupertökéletes szám szükségképpen négyzetszám.

(c) Egy páratlan primszám hatványa nem lehet szupertökéletes.

Megjegyzés: Az (a) rész szerint a páros szupertökéletes számok száma megegyezik a Mersenne-primek számával, és így megoldatlan, hogy végig sokáig páros szupertökéletes szám létezik-e. Szintén megoldatlan, hogy a páratlan számok között található-e egyáltalán szupertökéletes szám.

6.3.6 Az $\sigma$ pozitív egész harminkus számnak (vagy Ore-számnak) nevezzük, ha a pozitív osztóinak a harmonikus közepe egész szám. Bizonyítsuk be az alábbi állításokat.

(a) Az $\sigma$ akkor és csak akkor harmonikus, ha $\sigma(n) = n\sigma(\sigma(n))$.

(b) Minden tökéletes szám egyben harmonikus is.

(c) Egy primhatvány nem lehet harmonikus.

(d) A négyzetmentes számok közül egyedül a 6 harmonikus.

Megjegyzés: Léteznek a tökéletes számokon kívül is harmonikus számok, ilyen például az 1 és a 140. Megoldatlan probléma, hogy végig sok harmonikus szám van-e, és hogy az 1-nél nagyobb páratlan számok között található-e egyáltalán harmonikus szám.

6.3.7 Az $a \neq b$ pozitív egészek barátságos számpárt alkotnak, ha $\sigma(a) = \sigma(b) = a + b$. Ilyen számpár például a 220 és a 284.

(a) Mutassuk meg, hogy egy barátságos számpár egyik tagja hiányos, a másik tagja pedig bövelkedő szám (a definíciókat lásd a 6.3.3 feladatban [180]).

(b) Igazoljuk, hogy egy barátságos számpár egyik eleme sem lehet kettőhatvány.

Megjegyzés: A barátságos számok fogalma is a régi görögöktől ered: „az egyik szám részeiből, azaz nála kisebb pozitív osztóiból éppen összeáll a másik szám, és viszont”. Megoldatlan probléma, hogy létezik-e végig sok barátságos számpár, továbbá, hogy létezik-e egyáltalán olyan barátságos számpár, amelynek elemei relatív prímek, illetve ellenkező paritásúak.

6.4 A $d(n)$ függvény vizsgálata

Először megmutatjuk, hogy a $d(n)$ függvény értékei szeszélyesen ingadoznak, a függvény „grafikonjában” tetszőlegesen mély „völgyek” és tetszőlegesen magas „hegyek” találhatók.

6.4.1 Tétel (Völgytétel).

Tetszőleges $K$ pozitív egészhez végig sok olyan $n$ található, amelyre

$$d(n - 1) - d(n) \geq K \quad \text{és} \quad d(n + 1) - d(n) \geq K$$

egyidejűleg teljesül. ♠
**Bizonyítás:** Az \( n \)-et alkalmas prímszámoknak fogjuk választani, ekkor \( d(n) = 2^r \).

Az (1) feltétel így azt jelenti, hogy \( r - 1 \) -nek és \( n + 1 \) -nek is legalább \( K + 3 \) osztója van. Ez biztosan teljesül, ha például \( 2K + 2 \mid n - 1 \) és \( 3K + 2 \mid n + 1 \), azaz ha az \( n \) megoldása az

\[
x \equiv 1 \pmod{2K + 2}, \quad x \equiv -1 \pmod{3K + 2}
\]

szimultan kongruenciarendszernek.

A (2) rendszer \((2K + 2, 3K + 2) = 1\) miatt biztosan megoldható, és az összes (positív) megoldás

\[
x \equiv x_0 \pmod{6K + 2}
\]

az alakra írható.

Azt kell még igazolnunk, hogy a (3) számtani sorozatban végiglen sok prim található. Ez Dirichlet tétele (5.3.1 Tétel) szerint akkor teljesül, ha \( (x_0, 6K + 2) = 1 \). Mivel \( x_0 \) kielégiti (2)-t, ezért \( x_0 \) relatív prim a 2-höz és a 3-hoz, és így \( 6K + 2 \)-höz is.

6.4.2 Tétel (Hegytétel).

Tetszőleges \( K \) pozitív egészhez végiglen sok olyan \( n \) található, amelyre

\[
d(n) - d(n - 1) > K \quad \forall n \quad d(n) - d(n + 1) > K
\]

egyidejűleg teljesül. ◆

**Bizonyítás:** Az \( n \).-et az első \( r \) prímszám szorzatának fogjuk választani:

\[
u = p_1 \cdots p_r, \quad \text{ekkora} \quad d(n) = 2^r.
\]

Meg fogjuk mutatni, hogy

\[
d(n - 1) \leq 2^{r - 1} \quad \forall n \quad d(n + 1) \leq 2^{r - 1}.
\]

Így (5)-ből és (6)-ból már következik, hogy

\[
d(n) - d(n - 1) \geq 2^{r - 1} \quad \forall n \quad d(n) - d(n + 1) \geq 2^{r - 1},
\]

azaz \( 2^{r - 1} > K \) esetén (4) is teljesül.

A (6)-beli egyenlőtlenségek közül a \( d(n + 1) \) -re vonatkozó bizonyítjuk, a másik igazolása ugyanúgy történhet.

Írjuk fel \( n + 1 \) -et prímek szorzataként: \( n + 1 = q_1 \cdots q_s \) (itt \( Q_1 \equiv Q_s \) is előfordulhat). Mivel \( n \) az első \( r \) prímszám szorzata és \( (n + 1, n) = 1 \), ezért bármely \( i \) esetén \( Q_i > p_i \) (ahol \( p_i \) az \( r \)-edik prímszám).

Az \( n + 1 \) összes osztóját úgy kapjuk meg, hogy valahány \( Q_j \)-t válasszuk, és ezeket összeszorozzuk (például az 1, illetve az \( n + 1 \) akkor adódik, ha egyetlen \( Q_i \)-t sem válasszunk, illetve az összes \( Q_j \)-t vesszük). Ha a \( Q_j \)-k nem mind különbözők, akkor ugyanaz az osztót többféleképpen is megkapjuk. Ennek alapján \( d(n + 1) \leq 2^s \). A (6)-beli \( d(n + 1) \leq 2^{r - 1} \) egyenlőtlenségehez így elég azt megmutatnunk, hogy \( s \leq r - 1 \).
Tegyük fel indirekt, hogy $s \geq r$. Ekkor ($r \geq 2$ esetén) az alábbi módon jutunk ellentmondásra:

$$a + 1 = q_1 \cdots q_s \geq q_1 \cdots q_r \geq p_r + 1 \geq p_1 \cdots p_r + 2 = a + 2.$$  

Az imént bizonyított hegy- és völgytétel is illusztrálja, hogy a $d(n)$ függvény igen szabálytalanul viselkedik. A következőkben az első $n$ helyen felvett függvényértékek átlagát fogjuk vizsgálni, és kiderül, hogy ez az átlagértékfüggvény (vagy középértékfüggvény) már igen „szép” képet mutat.

### 6.4.3 Tétel

Legyen

$$D(n) = \sum_{i=1}^{n} d(i).$$

Ekkor bármely $n$ -re

$$\left| \frac{D(n)}{\log n} - 1 \right| \leq 1.$$  

**Bizonyítás:** Fel fogjuk használni, hogy bármely $n$ -re

$$\log n < \sum_{j=1}^{\lfloor \frac{n}{j} \rfloor} \frac{1}{j} \leq 1 + \log n.$$  

(A (8) egyenlőtlenség az T 5.6.1 Tétel első bizonyításában alkalmazott integrálos terület-összehasonlítás segítségével igazolható.)

Készítsünk egy $u \times n$ -es táblázatot (mátrixot), amelyben az $i$ -edik sor $j$ -edik eleme, $a_{ij}$ aszerint 1 vagy 0, hogy a $i$-osztója-e az $j$ -nek vagy sem:

$$a_{ij} = \begin{cases} 1, & \text{ha } j \mid i; \\ 0, & \text{ha } j \nmid i. \end{cases}$$

Például $u = 6$ -ra a következő táblázatot kapjuk:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

A bizonyítás alapgondolata, hogy kétféleképpen is meghatározzuk a táblázat összes elemének az összegét (vagyis a táblázatban szereplő 1-esek számát).

Az $i$ -edik sorban annyi 1-es szerepel, ahányoszor $j \mid i$ teljesül, vagyis az $i$ -edik sor elemeinek az összege $d(i)$. Innen soronkénti összegzéssel azt kapjuk, hogy a táblázat elemeinek az összege

$$D(n) = \sum_{i=1}^{n} d(i).$$  

A $j$ -edik oszlopban pontosan a...
számú helyeken áll 1-es, tehát a \( \frac{\tau_j}{j} \)-edik oszlop elemeinek az összege \( \frac{n}{j} \). Innen oszloponként összegezéssel az adódik, hogy a táblázat elemeinek az összege

\[
\sum_{j=1}^{n} \left\lfloor \frac{n}{j} \right\rfloor.
\]

Mivel (9) és (10) is a táblázat elemeinek az összege, ezért

\[
D(n) = \sum_{j=1}^{n} \left\lfloor \frac{n}{j} \right\rfloor.
\]

Az

\[
\frac{n}{\tau_j} - 1 < \left\lfloor \frac{n}{\tau_j} \right\rfloor < \frac{n}{\tau_j}
\]
egyenlőtlenség és (8) felhasználásával (11)-ből egyrészt

\[
D(n) \leq \sum_{j=1}^{n} \left( \frac{n}{\tau_j} - 1 \right) = n \sum_{j=1}^{n} \frac{1}{j} - n(1 + \log n)
\]
másrészt

\[
D(n) > \sum_{j=1}^{n} \left( \frac{n}{\tau_j} - 1 \right) = n \sum_{j=1}^{n} \frac{1}{j} - n > n(-1 + \log n)
\]
adódik. A (12a) és (12b) egyenlőtlenségeket \( n \)-nel osztova éppen a bizonyítandó (7) egyenlőtlenséget kapjuk. ■

A T 6.4.3 Tétel állítását \( D(n) - \tau_n \log n \) \( \leq \tau_n \) alakba is írhatjuk. Az alábbi tételeben a \( D(n) \) és az \( \tau_n \log n \) függvények eltéréserére (azaz a „hibaakra”) ennél erősebb becselést adunk.

Ehhez szükségünk lesz a \( \sum_{j=1}^{n} \frac{1}{j} \) összegnek a (8)-nál pontosabb, következő becslésére is: A \( \sum_{j=1}^{n} \frac{1}{j} - \log n \) sorozat konvergens, a határértéke \( \gamma = 0.577 \ldots \) az ún. Euler-konstans, és bármely \( n \)-re

\[
\sum_{j=1}^{n} \frac{1}{j} - \log n - \gamma \leq \frac{10}{n}.
\]

6.4.4 Tétel. T 6.4.4

Létezik olyan \( c \) konstans, hogy bármely \( n \)-re

\[
|D(n) - \tau_n \log n - (2\gamma - 1)\tau_n| < c\sqrt{n}.
\]

Bizonyítás: A \( d(i) \) azoknak az \( x, y \) pozitív egész számpárokak a száma, amelyekre \( xy = i \) (az \( x \) és \( y \) sorrendje is számít). Ennélfogva \( D(n) = \sum_{i=1}^{n} d(i) \) azoknak az \( x, y \) pozitív egész számpároknak a száma, amelyekre \( xy \leq n \).

184
Ez azt jelenti, hogy $D(n)$ a síkon akkor az $(x,y)$ egész koordinátájú pontoknak, azaz rácspontoknak a száma, amelyek az első síknegyedben az $xy = n$ hiperbola és a koordinátatengelyek közé esnek, beleértve a hiperbolán levő rácspontokat, de nem számítva a koordinátatengelyek rácspontjait. Most megszámoljuk ezeket a rácspontokat.

Legyen $A(n)$ azoknak az $(x,y)$ rácspontoknak a száma, amelyekre $x \leq \sqrt{n}$ . Mivel a rácspontok elhelyezkedése szimmetrikus az $y = x$ egyenesre nézve, ezért azoknak a rácspontoknak a száma is $A(n)$ , amelyekre $y \leq \sqrt{n}$ . Ezzel minden rácspontot figyelembe vettük, de kétszer számoltuk azokat a rácspontokat, amelyekre $x \leq \sqrt{n}$ és $y \leq \sqrt{n}$ is teljesül. Ezek éppen annak a négyzetnek a rácspontjai, amelynek egyik átlója az origót és a $(\sqrt{n}, \sqrt{n})$ pontot összekötő szakasz. Így ezeknek a rácspontoknak a száma $[\sqrt{n}]^2$ .

Ez azt jelenti, hogy az összes rácspontok száma

$$D(n) = 2A(n) - [\sqrt{n}]^2.$$  \hspace{1cm} (15)

Most meghatározzuk $A(n)$ -et. Mivel a $j$ abszisszázú rácspontok száma $\lfloor n/j \rfloor$ , ezért

$$A(n) = \sum_{j=1}^{\lfloor \sqrt{n} \rfloor} \lfloor n/j \rfloor.$$  \hspace{1cm} (16)

A (16) jobb oldalán álló összeget a T 6.4.3 Tétel bizonyításából látott módon becsülve azt kapjuk, hogy

$$A(n) = n \sum_{j=1}^{\lfloor \sqrt{n} \rfloor} \frac{1}{j} + f(\lfloor n/j \rfloor), \quad \text{ahol} \ |f(\lfloor n/j \rfloor)| < \sqrt{n}. \hspace{1cm} (17)$$

Alkalmazzuk most a (17)-beli összegre (13)-at:

$$\sum_{j=1}^{\lfloor \sqrt{n} \rfloor} \frac{1}{j} \log \lfloor \sqrt{n} \rfloor + \gamma - g(\lfloor n/j \rfloor), \quad \text{ahol} \ |g(\lfloor n/j \rfloor)| \leq \frac{10}{\lfloor \sqrt{n} \rfloor}. \hspace{1cm} (18)$$

Ezt (17)-be beírva azt kapjuk, hogy

$$A(n) \approx n \log \lfloor \sqrt{n} \rfloor + \gamma n + l(\lfloor n/j \rfloor), \hspace{1cm} \text{(13a)}$$

ahol

$$|l(\lfloor n/j \rfloor)| = \left| ng(\lfloor n/j \rfloor) + f(\lfloor n/j \rfloor)\right| < \frac{10n}{\lfloor \sqrt{n} \rfloor} + \sqrt{n} < \frac{10n}{\sqrt{n}} + \sqrt{n} = 21\sqrt{n}. \hspace{1cm} (19a)$$

Most (19a) további átalakításához megbecsüljük a $\frac{\log a}{a} - \log \lfloor \sqrt{n} \rfloor$ különbséget.

Mivel $(\log a)' = 1/a$ , ezért a Lagrange-féle középértéktétel szerint bármely $c > 1$ -hez létezik olyan $u$ , amelyre $a - 1 < u < c$ és

$$\log a - \log (a - 1) = \frac{\log a - \log (a - 1)}{a - (c - 1)} = \frac{1}{u} < \frac{1}{a - 1}.$$ 

Ennél főgva $n \geq 4$ -re
A (20) alapján (19a) és (19b) átírható a következő alakba:

\[ A(n) = \frac{n \log n}{2} + \gamma n + k(n), \quad \text{ahol} \quad |k(n)| < 23 \sqrt{n}. \quad (21) \]

Szükségünk lesz még \( n - \sqrt[n]{n} \) becslésére:

\[
0 \leq n - \sqrt[n]{n} = (\sqrt[n]{n})^2 - (\sqrt[n]{n})^2 - \sqrt[n]{n}^2 < 1(\sqrt[n]{n} + \sqrt[n]{n}) = 2\sqrt[n]{n}. \quad (22)
\]

Végül (21)-et és (22)-t (15)-be beírva azt kapjuk, hogy

\[ D(n) = n \log n + (2\gamma - 1)n + \ell(n), \text{ ahol} \quad |\ell(n)| < 48\sqrt[n]{n}. \]

Megjegyzések: 1. A számelmélet egyik sokat vizsgált és nehéz problémája, hogy a T 6.4.4 Tételben a hibatagra adott (14) becslés mennyire javítható. Bebizonyították, hogy az állítás akkor is érvényes, ha helyére \( n \) -t írunk, azonban \( n \) -nél már nem marad igaz.

2. Mivel

\[ \log 1 + \log 2 + \cdots + \log n \sim n \log n \]

(a két függvény aszimptotikusan egyenlő, azaz a hanyadosuk 1-hez tart), ezért a T 6.4.3 (vagy T 6.4.4) Tételből az is következik, hogy

\[ \delta(1) + \delta(2) + \cdots + \delta(n) \sim \log 1 + \log 2 + \cdots + \log n. \quad (23) \]

A (23) összefüggés úgy értelmezhető, hogy a \( d(n) \) függvény „átlagos nagyságrendje” \( \log n \).

Ez azonban nem jelenti azt, hogy egy „tipikus” \( n \) -nek „körülbelüli” \( \log n \) osztója lenne; a 6.7 pontban bebizonyítjuk (lásd a 6.7.6 feladatot [211]), hogy az osztók száma általában ennél kevesebb, a „legtöbb” \( n \) -re \( d(n) \) értéke „körülbelül”

\[ (\log n)^{1.02} = (\log n)^{0.69}. \]

A \( \log n \) -es átlag a ritkán előforduló, de kirívóan sok osztóval rendelkező számoknak köszönhető.

Végül a \( d(n) \) függvény értékkészletének néhány további tulajdonságát vizsgáljuk.

A \( d(n) \) függvény minden \( k \geq 2 \) egész számot végzen sokszor felvesz, hiszen bármely \( p \) primre \( d(p^{k-1}) = k \).

Az 1.6.11 feladatban [28] több egyszerű felső becslést adjunk \( d(n) \) -re az \( n \) függvényében. Az alábbi tételben ezeket élesítjük:

6.4.5 Tétel. \quad T 6.4.5

Bármely rögzített \( \delta > 0 \) esetén

\[ \lim_{n \to \infty} \frac{d(n)}{n^\delta} = 0. \]
A bizonyításhoz az alábbi segítdételt használjuk fel:

6.4.6 Tétel. T 6.4.6

Legyen \[ \{ q_1 < q_2 < \ldots \} = \{ 2, 3, 4, 5, 7, 8, 9, 11, \ldots \} \]
a primhatványok sorozata és \( f \) egy tetszőleges multiplikatív számelméleti függvény. Ekkor
\[ \lim_{j \to \infty} f(q_j) = 0 \quad \iff \quad \lim_{n \to \infty} f(n) = 0. \]

\[ \text{A T 6.4.6 Tétel bizonyítása: A feltétel szerint van olyan } H \text{ és } k, \text{ hogy } \]
\[ \left| f(q_j) \right| \leq H \text{ minden } j \text{-név, } \iff \left| f(q_j) \right| \leq 1, \text{ ha } j > k. \quad (24) \]

Először megmutatjuk, hogy bármely \( n \) -re
\[ |f(\alpha^n)| \leq H^k. \quad (25) \]

Ha \( n \) kanonikus alakja \( \alpha^n = \prod_{i=1}^{r} p_i^{a_i} \), akkor az \( f \) multiplikativitása miatt
\[ |f(\alpha^n)| = \prod_{i=1}^{r} |f(p_i^{a_i})|. \quad (26) \]

A (26) jobb oldalán szereplő tényezők közül (24) szerint legfeljebb \( k \) darab nagyobb, mint 1, és ezek értéke is legfeljebb \( H \), azaz (25) valóban teljesül.

Legyen \( \varepsilon > 0 \) tetszőleges. Be kell látni, hogy létezik olyan \( q_0 = q_0(\varepsilon) \), hogy minden \( n > q_0 \) esetén \( |f(n)| < \varepsilon \).

A feltétel szerint létezik olyan \( s = s(\varepsilon) \), hogy
\[ |f(q_j)| < \frac{\varepsilon}{H^{k}}, \quad \text{ha } j > s. \quad (27) \]

Megmutatjuk, hogy \( q_1 \cdots q_s \) megfelel \( q_0 \) -nak.

Ha \( n > q_1 \cdots q_s \), akkor az \( n \) kanonikus alakjában szerepelnie kell egy \( p_i \)-nél nagyobb \( q_j \) primhatványnak: \( n = q_j^{a_j} \), ahol \( (q_j, q_1) = 1 \).

Ekkor (27) alapján \( |f(q_j)| < \varepsilon / H^k \), továbbá (25) alapján \( |f(n)| \leq H^k \), és így
\[ |f(\alpha^n)| = |f(q_j)| \cdot |f(\alpha^n)| < \frac{\varepsilon}{H^{\kappa}} \cdot H^k = \varepsilon. \]

\[ \text{A T 6.4.5 Tétel bizonyítása: A T 6.4.6 Tételt az } \]
\[ f(\alpha^n) = \frac{d(\alpha^n)}{\varepsilon^{\kappa}} \]
függvényre fogjuk alkalmazni. Ehhez azt kell megmutatni, hogy
\[ \lim_{j \to \infty} \frac{d(q_j)}{q_j^{\kappa}} = 0. \quad (28) \]
Legyen $q_i = p^\alpha$ (ahol $p$ prim). Ekkor

$$d(q_i) = d(p^\alpha) = \alpha + 1 \leq 2\alpha = \frac{2\log(p^\alpha)}{\log p} \leq \frac{2\log q_i}{\log 2},$$

tehát

$$\frac{d(q_i)}{q_i^\delta} \leq \frac{2}{\log 2} \cdot \frac{\log q_i}{q_i^\delta}, \quad (\forall \delta)$$

Mivel

$$\lim_{x \to \infty} \frac{\log x}{x^\delta} = 0,$$

ezért (29)-ben a jobb oldal, és így a bal oldal is 0-hoz tart. ■

*Megjegyzés:* Megmutatható, hogy a $d(n)$ függvény „maximális” nagyságrendje körülbelül

$$\frac{\log n}{n^{\frac{1-\varepsilon}{\log \log n}}}.$$

Ez pontosan a következőket jelenti:

(i) Bármely $\varepsilon > 0$-hoz létezik olyan $n_0 = n_0(\varepsilon)$, hogy minden $n > n_0$ esetén

$$d(n) < n^{\frac{1+\varepsilon}{\log \log n}}.$$

(ii) Bármely $\varepsilon > 0$-hoz végtelen sok olyan $n$ létezik, amelyre

$$d(n) > n^{\frac{1-\varepsilon}{\log \log n}}.$$

A (ii) állítás bizonyítását a 6.4.3b feladatban [188] tűztük ki.

**Feladatok**

6.4.1 (*) Mutassuk meg, hogy a T 6.4.1 és T 6.4.2 Tételek állítása a $d(n)$ helyett a $\sigma(n)$, $\varphi(n)$, $\Omega(n)$, $\omega(n)$ és $k > 1$ esetén a $d_k(n)$ függvényekre is érvényes.

6.4.2 Bizonyítsuk be, hogy bármely rögzített $\delta > 0$ és $k$ pozitív egész esetén

$$\lim_{n \to \infty} \frac{d_k(n)}{n^{\frac{\delta}{\log n}}} = 0.$$

6.4.3 Legyen $\varepsilon > 0$ tetszőleges. Mutassuk meg, hogy végtelen sok olyan $n$ létezik, amelyre

(a) $d(n) > (\log n)^{100};$

(b) $\sigma d(n) > n^{\frac{1-\varepsilon}{\log \log n}}.$

6.4.4 Mutassuk meg, hogy bármely $n$-re $\Omega(n) \leq \log_2 n$. Mikor áll egyenlőség?

6.4.5 (*) Legyen $\varepsilon > 0$ tetszőleges. Igazoljuk az alábbi állításokat.
(a) Minden elég nagy $n$-re
\[ \omega(n) < \frac{(1 + \varepsilon) \log n}{\log \log n}, \]
(b) Végtelen sok $n$-re
\[ \omega(n) > \frac{(1 - \varepsilon) \log n}{\log \log n}, \]

**6.4.6** Bizonyítsuk be, hogy minden elég nagy $n$ esetén

(a) $\varphi(n) > n^{0.99}$
(b) $\varphi(n) > \frac{n}{2 \log n}$
(c) $\varphi(n) > \frac{n}{\log n \log \log n}$ és
(d) $\sigma(n) < n^{1.01}$
(e) $\sigma(n) < 2n \log n$
(f) $\sigma(n) < C n \log \log n$

(ahol a (c) és (f) részben $C$ egy alkalmas abszolút konstans).

**6.4.7** Igazoljuk az alábbi állításokat.

(a) A $\varphi(n)/n$ függvény értékkészlete mindenütt sűrű a $[0, 1]$ intervallumban.

(b) A $\sigma(n)/n$ függvény értékkészlete mindenütt sűrű $[1, \infty]$-ben.

**6.4.8** (*) A Dirichlet-tétel azt mondja ki, hogy ha az $a$ és $d$ pozitív egészek relatív prímek, akkor az $a + kd$, $k = 0, 1, 2, \ldots$ számok sorozat végtelen sok prímet tartalmaz. Ez a tétel jelentősen élesíthető:

(i) Ezeknek a prímeknek a reciprokösszege divergens.

(ii) Az $a$-nél kisebb ilyen prímek száma rögzített $d$ mellett $n \to \infty$-re
\[ \sim \frac{n}{\varphi(d) \log n}. \]

Ezek az eredmények az T 5.6.1, illetve T 5.4.1 Tételek általánosításai.

(a) Legyen $k$ tetszőleges, rögzített pozitív egész. Mutassuk meg (i) felhasználásával, hogy $k \mid \varphi(n)$ majdnem minden $n$-re teljesül. Ez pontosan a következőt jelenti. Legyen $P(N)$ azoknak az $x \leq N$ egészeknek a száma, amelyekre $k \mid \varphi(x)$. Ekkor $\lim_{N \to \infty} P(N)/N = 1$.

(b) (M [587]) Bizonyítsuk be, hogy a $\varphi$-függvény értékkészletéből majdnem minden pozitív egész hiányzik. (Az előzőhöz hasonlóan ezen a következőt kell érteni. Legyen $C(N)$ azoknak az $n \leq N$ értékeknek a száma, amelyek előfordulnak a $\varphi$-függvény értékkészletében. Ekkor $\lim_{N \to \infty} G(N)/N = 0$.)
6.4.9 (*) Mutassuk meg, hogy az előző feladat állításai a \( \varphi \) helyett a \( \sigma \) -függvényre is érvényesek.

### 6.5 Összegzési és megfordítási függvény

#### 6.5.1 Definíció

Az \( f \) számelméleti függvény osztókra vonatkozó összegzési függvényén az

\[
f^+(n) = \sum_{d|n} f(d)
\]

függvényt értjük. ◆

Példák:

Az \( f(n) = 1 \) függvény összegzési függvénye \( f^+(n) = \delta(n) \), a \( g(n) = n \) függvényé pedig \( g^+(n) = \sigma(n) \).

A 2.3.14 feladat [45] szerint \( \rho^+(n) = n \), a T 6.2.4 Tétel alapján \( \nu^+(n) = \nu(n) \), ahol

\[
\nu(n) = \begin{cases} 
1, & \text{ha } n = 1; \\
0, & \text{ha } n > 1. 
\end{cases} \tag{1}
\]

#### 6.5.2 Tétel

Bármely \( f \) számelméleti függvényhez pontosan egy olyan függvény található, amelynek az összegzési függvénye \( f \). Ezt az egyértelműen meghatározott függvényt az \( f \) megfordítási függvényének nevezzük, és \( \tilde{f} \)-mal jelöljük. ◆

Bizonyítás: Írjuk fel minden \( n \)-re a megfordítási függvénytől megkövetelt

\[
f(n) = \sum_{d|n} \tilde{f}(d)
\]
egyenlőséget:

\[
\begin{align*}
f(1) &= \tilde{f}(1) \\
f(2) &= \tilde{f}(1) + \tilde{f}(2) \\
f(3) &= \tilde{f}(1) + \tilde{f}(3) \\
f(4) &= \tilde{f}(1) + \tilde{f}(2) + \tilde{f}(4) \\
f(5) &= \tilde{f}(1) + \tilde{f}(5) \\
f(6) &= \tilde{f}(1) + \tilde{f}(2) + \tilde{f}(3) + \tilde{f}(6) \\
&\vdots
\end{align*}
\]

Azt kell belátni, hogy ez a végtelen sok egyenletből álló és a végtelen sok \( \tilde{f}(1), \tilde{f}(2), \ldots \) ismeretlenre vonatkozó „egyenletrendszer” egyértelműen megoldható.

Az első egyenlet pontosan akkor teljesül, ha
\[ \tilde{f}(1) = f(1). \]

Az első és második egyenlet együttesen pontosan akkor teljesül, ha \( \tilde{f}(1) \) az első egyenletből kapott érték és

\[ \tilde{f}(2) = f(2) - \tilde{f}(1). \]

Ugyanígy haladhatunk tovább indukcióval. Tegyük fel, hogy az első \( m - 1 \) egyenletből álló egyenletrendszerek pontosan egy \( \tilde{f}(1), \ldots, \tilde{f}(m - 1) \) megoldása van, és tekintsük most az első \( m \) egyenletből álló rendszert. Mivel az \( \tilde{f}(m) \) „ismeretlen” először az \( m \)-edik egyenletben fordul elő, így az első \( m \) egyenlet együttesen pontosan akkor teljesül, ha \( \tilde{f}(1), \ldots, \tilde{f}(m - 1) \) az első \( m - 1 \) egyenletből (az indukció szerint) egyértelműen adódó érték és

\[ f(m) = \sum_{d \mid m} \tilde{f}(d). \quad (2) \]

Ezzel az \( \tilde{f} \) függvény létezését és egyértelműségét beláttuk. (A (2) képlet az \( \tilde{f} \) függvény értékeinek egy rekurzív előállítását jelenti.)

**Példák:** A D 6.5.1 Definíció utáni példákat „visszafelé olvasva” (és az ottani jelöléseket használva) azt kapjuk, hogy

\[ \tilde{d}(n) = 1; \quad \tilde{\sigma}(n) = n; \quad \tilde{g}(n) = \varphi(n); \quad \tilde{e}(n) = \mu(n). \]

Az alábbiakban a megfordítási függvényt „képlet” alakban is előállítjuk:

**6.5.3 Tétel (Möbius-féle megfordítási formula)**. \hspace{1cm} T 6.5.3

\[ \tilde{f}(n) = \sum_{d \mid n} \mu(d) f\left(\frac{n}{d}\right). \quad \blacklozenge \]

**Bizonyítás:** Mivel a T 6.5.2 Tétel szerint \( \tilde{f} \) egyértelműen létezik, így elég megmutatni, hogy a (3) jobb oldalán megadott függvény összegzési függvénye éppen \( \tilde{f}(n) \). Ezt a szereplő összegek megfelelő átrendezésével és (1) felhasználásával igazolhatjuk:

\[ \tilde{h}^{+}(n) = \sum_{d \mid n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu(d) f(c) \]

függvény \( \tilde{h}^{+}(n) \) összegzési függvénye éppen \( \tilde{f}(n) \). Ezt a szereplő összegek megfelelő átrendezésével és (1) felhasználásával igazolhatjuk:

\[ \tilde{h}^{+}(n) = \sum_{d \mid n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu(d) f(c) - \sum_{e \mid n} \mu(e) f\left(\frac{n}{e}\right) = \sum_{c \mid n} \tilde{f}(c) \left( \sum_{d \mid \frac{n}{c}} \mu(d) \right) - \sum_{c \mid n} \tilde{f}(c) \mu\left(\frac{n}{c}\right) = \sum_{c \mid n} \tilde{f}(c) \mu\left(\frac{n}{c}\right) - \sum_{c \mid n} \tilde{f}(c) \mu\left(\frac{n}{c}\right) = f(n). \blacklozenge \]

Végül a megfordítási függvény egy érdekes alkalmazását, az ún. Smith-féle determinánsot mutatjuk be:

**6.5.4 Tétel**. \hspace{1cm} T 6.5.4

Legyen \( \tilde{f} \) tetszőleges számelméleti függvény, és képezzük az \( n \times n \)-es
mátrixot, ahol \((i, j)\) az \(i\) és \(j\) számok legnagyobb közös osztóját jelenti. Ekkor az \(A\) mátrix determinánsa

\[
\det A = f(1)f(2)\ldots f(n).
\]

Bizonyítás: Tekintsük azt az \(n \times n\) -es \(B\), illetve \(C\) mátrixot, amelyben az \(i\) -edik sor \(j\) -edik eleme \(b_{ij}\), illetve \(c_{ij}\), ahol

\[
b_{ij} = \begin{cases} 1, & \text{ha } j \, | \, i; \\ 0, & \text{ha } j \, \nmid \, i, \end{cases}
\]

és

\[
c_{ij} = b_{ij}f(j), \quad \text{azaz} \quad c_{ij} = \begin{cases} f(j), & \text{ha } j \, | \, i; \\ 0, & \text{ha } j \, \nmid \, i. \end{cases}
\]

Mindkét mátrixban a főátló fölött csupa 0 áll, tehát a determinánsuk a főátlóbeli elemek szorzata. A \(D\) mátrix főátlójában minden elem 1-es, a \(C\) mátrix főátlójában pedig az \(f(1), \ldots, f(n)\) elemek szerepelnek, ezért

\[
\det B = 1 \quad \text{és} \quad \det C = f(1)f(2)\ldots f(n). \quad (4)
\]

Most vizsgáljuk meg a \(D = BC^T\) szorzatmátrixot, ahol \(C^T\) a \(C\) mátrix transzponáltját jelöli. Ekkor \(D\) -ben az \(i\) -edik sor \(j\) -edik eleme

\[
d_{ij} = b_{i1}c_{j1} + b_{i2}c_{j2} + \cdots + b_{in}c_{jn} = b_{i1}b_{j1}f(1) + b_{i2}b_{j2}f(2) + \cdots + b_{in}b_{jn}f(n). \quad (5)
\]

Itt

\[
b_{ik}b_{jk}f(k) = \begin{cases} f(k), & \text{ha } k \, | \, i \, \& \, j; \\ 0, & \text{egyéb kérést.} \end{cases}
\]

azaz

\[
b_{ik}b_{jk}f(k) = \begin{cases} f(k), & \text{ha } k \, | \, (i, j); \\ 0, & \text{ha } k \, \nmid \, (i, j). \end{cases} \quad (6)
\]

A (6)-ot (5)-be beírva és \(\tilde{f}\) definícióját felhasználva azt kapjuk, hogy

\[
d_{ij} = \sum_{k|(i,j)} f(k) = f((i, j))
\]

tehát \(D = A\).
Végül a determinánsok szorzástétele és (4) alapján
\[ \det A = \det D = (\det B)(\det C) = \tilde{f}(1)\tilde{f}(2) \ldots \tilde{f}(n). \]

Feladatok

6.5.1 Mutassuk meg, hogy \( d_k(n) = d_{k-1}(n) \).

6.5.2 Bizonyítsuk be az alábbi állításokat:

(a) \( f \) multiplikatív \( \iff \) \( f^+ \) multiplikatív.
(b) \( f \) multiplikatív \( \iff \) \( \tilde{f} \) multiplikatív.

Megjegyzés: A 6.5.2 feladatból [193] azonnal következik például a \( d(n) \), \( \sigma(n) \), illetve \( \varphi(n) \) függvények multiplikativitása.

6.5.3 (a) Melyek azok a teljesen multiplikatív függvények, amelyeknek az összegzési függvénye is teljesen multiplikatív?
(b) Melyek azok az additív függvények, amelyeknek az összegzési függvénye is additív?

6.5.4 Legyen \( n \) kanonikus alakja \( n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \). Bizonyítsuk be az alábbi állításokat.

(a) Ha \( f \) multiplikatív és \( f \neq 0 \), akkor
\[ f^+(n) = \prod_{i=1}^{r} \left( 1 + f(p_i^1) + f(p_i^2) + \cdots + f(p_i^{\alpha_i}) \right) \]
és
\[ \tilde{f}(n) = \prod_{i=1}^{r} \left( f(p_i^{\alpha_i} - 1) \right). \]
(b) Ha \( f \) teljesen multiplikatív, és egyetlen prim helyen sem veszi fel a 0 vagy 1 értéket, akkor
\[ f^+(n) = \prod_{i=1}^{r} \frac{f(p_i^{\alpha_i} - 1)}{f(p_i)} \]
e és \[ \tilde{f}(n) = \tilde{f}(1) \prod_{i=1}^{r} \left( 1 - \frac{1}{f(p_i)} \right). \]

Mely függvények képlete adódik az \( f(n) = n \) speciális esetben?

6.5.5 Adjuk meg az alábbi függvények megfordítási függvényét:

(a) \( f(n) = \pi \) (konstans függvény);
(b) \( g(n) = \frac{(-1)^n + 1}{2} \);
(c) \( \Omega(n) \);
(d) \( \omega(n) \).

6.5.6 Bizonyítsuk be, hogy ha \( f \) additív és \( \omega(n) \geq 2 \), akkor \( \tilde{f}(n) = 0 \).
6.5.7 Adjuk meg egyszerűbb alakban a
\[ \sum_{d|\sigma-a} \sigma(a) \mu(b) \]
összeget.

6.5.8 Bizonyítsuk be, hogy
\[ \sum \frac{\mu(d)}{d} = \frac{\varphi(n)}{n}. \]

6.5.9 Igazoljuk az alábbi állításokat.

(a) A primitív komplex \( n \)-edik egységgyökök összege \( \mu(n) \).

(b) A primitív komplex \( n \)-edik egységgyökök \( k \)-adik hatványainak összege
\[ \frac{\mu(n') \rho(n)}{\rho(n')} , \quad \text{ahol} \quad n' = \frac{n}{(n, k)}. \]

(c) Ha \( P \) prim, akkor a modulo \( P \) páronként inkongruens primitív gyökök összege \( \mu(P - 1) \)-gyel kongruens modulo \( P \).

6.5.10 Számítsuk ki azokat az \( a \times n \)-es determinánsokat, ahol az \( i \)-edik sor \( j \)-edik eleme

(a) \( \{i, i\} \);

(b) \( \sigma\{i, j\} \);

(c) \( d\{i, j\} \);

(d) \( \mu\{i, j\} \).

6.5.11 Legyenek \( s_1, \ldots, s_n \) tetszőleges olyan különböző pozitív egészek, amelyekre minden \( s_i \) -nek minden osztója is szerepel az \( s_j \)-k között. Mutassuk meg, hogy a T. 6.5.4 Tétel megfelelője akkor is érvényben marad, ha az \( 1, 2, \ldots, n \) számok helyére mindenhol az \( s_1, \ldots, s_n \) számokat írjuk.

6.6 Konvolúció

6.6.1 Definíció

Az \( f \) és \( g \) számelméleti függvények konvolúcióján az
\[ (f \ast g)(vi) = \sum_{d|vi} f(d) g(vi/d) = \sum_{vi=d} f(d) g(vi) \]
függvényt értjük. ◆

Az összegzési, illetve megfordítási függvény képzése a konvolúció speciális esete: \( f^+ \) definíció szerint az \( f \) és a konstans 1 függvény konvolúciója, \( \bar{f} \) pedig a Möbius-féle megfordítási formula alapján az \( f \) és \( \mu \) konvolúciója, azaz
Most megvizsgáljuk a konvolúció művelet tulajdonságait.

6.6.2 Tétel. T 6.6.2

A konvolúció asszociatív és kommutatív, az egységelem

\[ \varepsilon(n) = \begin{cases} 1, & \text{ha } n = 1; \\ 0, & \text{ha } n > 1, \end{cases} \]

és pontosan azoknak az \( f \)-eknek létezik inverze, amelyekre \( f(1) \neq 0 \).

Bizonyítás: Kommutativitás: közvetlenül következik a definícióból.

Asszociativitás:

\[ (f * (g * h))(n) = \sum_{l+n} f(l) \left( \sum_{d=l} g(d) h(d) \right) = \sum_{l+n} f(l) g(d) h(d), \]

és ugyanerre az alakra hozható \((f * g) * h\) is.

Egységelem:

\[ (\varepsilon * f)(n) = \sum_{q+n} \varepsilon(q) f(n) = 1 \cdot f(n) + \sum_{1 < d | n} 0 \cdot f(n) = f(n). \]

Inverz: A T 6.5.2 Tétel bizonyításához hasonlóan járhatunk el. Az \( \hat{f} \) függvény \( g \) inverzének az

\[ \nu = \hat{f} \times g \]

feltételt, vagyis az alábbi egyenlőségeket kell kielégítenie:

\[ 1 = \nu(1) = f(1)g(1) \]
\[ 0 = \nu(n) = f(1)g(n) + f(n)g(1) \]
\[ 0 = \nu(2) = f(1)g(2) + f(2)g(1) \]
\[ 0 = \nu(3) = f(1)g(3) + f(3)g(1) \]
\[ 0 = \nu(4) = f(1)g(4) + f(2)g(2) + f(4)g(1) \]
\[ 0 = \nu(5) = f(1)g(5) + f(5)g(1) \]
\[ 0 = \nu(6) = f(1)g(6) + f(2)g(3) + f(3)g(2) + f(6)g(1) \]
\[ \vdots \]

Ebben a végfel t ten sok egyenletből álló egyenletrendszerben \( g(1), g(2), \ldots \) az ismeretlenek. Az első \( n \)

eyenletben csak a \( g(1), \ldots, g(n) \) ismeretlenek szerepelnek, a \( g(n) \) először az \( n \)-edik egyenletben

fordul elő.

Ha \( f(1) = 0 \), akkor az első egyenlet nem oldható meg, tehát \( f(1) \neq 0 \) az inverz létezésének

szükséges feltétele. Az elégőségességhez azt kell megmutatni, hogy \( f(1) \neq 0 \) esetén az

eyenletrendszer (egyértelműen) megoldható.

Az első egyenlet pontosan akkor teljesül, ha

\[ g(1) = \frac{1}{\hat{f}(1)}. \]

Az első és második egyenlet együttesen pontosan akkor teljesül, ha \( g(1) \) az első egyenletből

eyenletűen adódó érték és
\[ g(2) = \frac{-f(2)g(1)}{f(1)}. \]

Ugyanígy haladhatunk tovább indukcióval. Tegyük fel, hogy az első \( m - 1 \) egyenletből álló egyenletrrendszernek pontosan egy \( g(1), \ldots, g(m - 1) \) megoldása van, és tekintsük most az első \( m \) egyenletből álló rendszert. Mivel a \( g(n) \) „ismeretlen” először az \( m \) -edik egyenletben fordul elő, így az első \( m \) egyenlet együttesen pontosan akkor teljesül, ha \( g(1), \ldots, g(m - 1) \) az első \( m - 1 \) egyenletből (az indukció szerint) egyértelműen adódó érték és

\[ g(m) = -\frac{1}{f(1)} \sum_{d \mid m} g(d) \frac{f(n)}{d}. \]

A \( G \) függvények ezzel a rekurzív definíciójával megadtuk az \( f \) invértét. □

Most a konvolúció segítségével egy egyszerű bizonyítást adunk a Möbius-féle megfordítási formulára, és ebből együttal az is világosabban válik, mi az „oka” a \( \mu \) függvény kitüntetett szerepének.

A megfordítási függvény definícióját a konvolúció segítségével az

\[ \tilde{f} \ast 1 = \tilde{f} \] (1)

eyenlőséggel írhatjuk fel, és ebből kell \( \tilde{f} \) -ot kifejezni. Jelöljük az 1 függvény inverzét \( g \)-vel, és „szorozzuk be” (1)-et \( g \)-vel (azaz vegyük mindkét oldalnak a \( g \)-vel való konvolúcióját). Ekkor (a konvolúció műveleti tulajdonságait is felhasználva) kapjuk, hogy

\[ \tilde{f} = f \ast g. \] (2)

Itt a \( g \) az 1 függvény inverze, ami azt jelenti, hogy \( \tilde{1} = g = e \), azaz \( g^{-1} = e \), vagy más szóval \( g = \tilde{e} = t \). Ezt (2)-be beírva

\[ \tilde{f} = f \ast \mu \]

adódik, ami éppen a Möbius-féle megfordítási formula.

A számelméleti függvények vizsgálatánál igen fontos szerepet játszik a függvényekhez rendelt Dirichlet-sor:

6.6.3 Definíció . △ 6.6.3

Legyen \( \tilde{f} \) számelméleti függvény és \( \mathcal{S} \) azoknak az \( s \) valós számoknak a halmaza, amelyekre a

\[ \sum_{n=1}^{\infty} \frac{\tilde{f}(n)}{n^s} \]

végteken konvergens. Ekkor az \( \tilde{F} \)-hez tartozó Dirichlet-sor

\[ \tilde{F}(s) = \sum_{n=1}^{\infty} \frac{\tilde{f}(n)}{n^s} \]

végteken sorral értelmezett \( \tilde{F} : \mathcal{S} \rightarrow \mathbb{C} \) függvényt értjük. ★
Az $\mathcal{F}$ függvény ételmezési tartománya tehát azoknak az $s$ valós számoknak a halmaza, amelyekre a (3) végétlen sor konvergens.

Könnyen adódik (lásd a 6.6.6 feladatot [198]), hogy ha (3) egy $\omega_0$ helyen konvergens, akkor minden $s > \omega_0 + 1$ helyen abszolút konvergens. A továbbiakban az $\mathcal{F}(s)$ függvényt csak olyan $s$ helyeken fogjuk tekinteni, amelyekre a (3) sor abszolút konvergens. Ennek az lesz az előnye, hogy felhasználhatjuk az abszolút konvergens sorokra vonatkozó tételeket, amelyeket úgy foglalhatunk össze, hogy abszolút konvergens sorokkal „ugyanúgy” számlálhatunk, mint a véges sok tagból álló összegekkel. Ez többek között azt jelenti, hogy egy abszolút konvergens sor tagjait tetszôlegesen átrendezve és csoportosítva ismét abszolút konvergens sort kapunk, amelynek az összege megegyezik az eredeti sor összegével, és két abszolút konvergens sort a „minden tagot minden taggal” „szabály” szerint összeszorozva (és az így keletkezô szorzatokat tetszôlegesen átrendezve és csoportosítva) egy olyan abszolút konvergens sort kapunk, amelynek az összege az eredeti két sor összegének a szorzata.

Megjegyezzük, hogy a Dirichlet-sor lehet (valós helyett) komplex változós függvényként, illetve a konvergenciát egy általánosított nem vizsgáló „formális sorként” is tekinteni, ezzel azonban nem foglalkozunk.

Az egyik legfontosabb Dirichlet-sor az $\mathcal{F} = 1$ függvényhez tartozó Riemann-féle zétafüggvény:  

$$\zeta(s) = \sum_{\nu=1}^{\infty} \frac{1}{\nu^s}, \quad (4)$$

amelyet már az 5.6.6 feladatban [149] definiáltunk. A (4) sor $s > 1$-re abszolút konvergens, és az 5.6.6 feladat [149] szerint felírható az alábbi végtelen szorzatként is:

$$\zeta(s) = \prod_{\nu=1}^{\infty} \frac{1}{1 - \frac{1}{\nu^s}} = \lim_{r \to \infty} \prod_{\nu \leq r} \frac{1}{1 - \frac{1}{\nu^s}}. \quad (5)$$

Az Eulertől származó (5) összefüggés alapján nem meglepô, hogy a prímszámok eloszlásának vizsgálatát szoros kapcsolatba hozható a $\zeta$ -függvény viselkedésével. Így például a prímszámokra vonatkozóan különösen fontos tételeket nyerhetünk, ha beigazolódna a híres Riemann-sejtés, amely azt állítja, hogy a komplex változóra megfelelôen kiterjesztett $\zeta$ -függvény bármely valós gyökének a valós része 1/2.

Az alábbi tétel a Dirichlet-sor és a konvolúció kapcsolatáról szól:

6.6.4 Tétel . T 6.6.4

Jelölje az $f, g$, illetve $h$ számfolyos függvényekhez tartozó Dirichlet-sorokat $F(s), G(s)$, illetve $H(s)$, és tegyük fel, hogy ezek abszolút konvergensek, továbbá $h = f * g$. Ekkor $H(s) = F(s)G(s)$.

Bizonyítás: Az abszolút konvergens sorok szorzásának tulajdonságait felhasználva

$$F(k)G(s) = \left( \sum_{\nu=1}^{\infty} \frac{f(n)}{\nu^s} \right) \left( \sum_{m=1}^{\infty} \frac{g(m)}{m^s} \right) = \sum_{k=1}^{\infty} \sum_{\nu \in \mathbb{N}} \frac{f(k)g(m)}{(kn)^s} = \sum_{\nu=1}^{\infty} \sum_{k=1}^{\infty} \frac{f(k)g(m)\mu(n)}{\nu^s} = \frac{\zeta(s)}{\nu^s} = H(s).$$

A T 6.6.4 Tétel alapján könnyen meghatározhatjuk például a Möbius-függvény

$$M(s) = \sum_{\nu=1}^{\infty} \frac{\mu(n)}{\nu^s}.$$
Dirichlet-sorát. Ez a sor \( |\mu(n)| \leq 1 \) miatt \( s > 1 \)-re abszolút konvergens. Mivel \( \mu * 1 = \delta \), ezért

\[
M(s) \zeta(s) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{1^s} + \sum_{n=2}^{\infty} \frac{0}{n^s} = 1,
\]

tehát

\[
M(s) = \frac{1}{\zeta(s)} \quad \text{azaz} \quad \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\sum_{n=1}^{\infty} \frac{1}{n^s}}.
\]

Speciálisan \( s = 2 \)-re ebből azt kapjuk, hogy

\[
\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} = \frac{6}{\pi^2}.
\]

Feladatok

6.6.1 Melyik (ismert) függvényt kapjuk, ha az \( f = 1 \) függvénynek a konvolúció szerinti \( k \)-adik hatványát (azaz a \( k \)-tényezős \( 1 * 1 * \cdots * 1 \) konvolúciót) képezzük?

6.6.2 Bizonyítsuk be, hogy a számelméleti függvények az összeadás és a konvolúció műveletére kommutatív, nullosztómentes, egységelemes gyűrűt alkotnak.

6.6.3 Legyen \( f \) olyan (komplex értékű) számelméleti függvény, amelyre \( f(1) \neq 0 \). Hány \( k \)-adik gyöke van \( f \)-nek a konvolúcióra nézve?

6.6.4 (a) Bizonyítsuk be, hogy két multiplikatív függvény konvolúciója is multiplikatív.

(b) Legyen \( f \) és \( g \) teljesen multiplikatív. Mutassuk meg, hogy \( f \times g \) akkor és csak akkor teljesen multiplikatív, ha minden \( n > 1 \)-re \( (fg)(n) = 0 \).

6.6.5 Igazoljuk, hogy

\[
\sum_{d|n} \sigma(d) \varphi\left(\frac{n}{d}\right) = \varphi(n).
\]

6.6.6 Bizonyítsuk be, hogy ha a

\[
\sum_{n=1}^{\infty} \frac{f(n)}{n^s}
\]

végtelen sor \( s = s_0 \)-ra konvergens, akkor minden \( s > s_0 + 1 \)-etén abszolút konvergens.

6.6.7 Jelölje az \( f, f^+ \), illetve \( \tilde{f} \) számelméleti függvényekhez tartozó Dirichlet-sorokat rendre \( F(s), F^+(s) \), illetve \( \tilde{F}(s) \). Bizonyítsuk be, hogy abszolút konvergencia és \( s > 1 \) esetén

\[
F^+(s) = \tilde{f}(s)\zeta(s) \quad \text{és} \quad \tilde{F}(s) = \frac{\tilde{F}(s)}{\zeta(s)}.
\]

6.6.8 Bizonyítsuk be, hogy \( s > 1 \) esetén
SZÁMELMÉLETI FÜGGVÉNYEK

(a) \( \sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \zeta'(s) \);

(b) \( \sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \zeta'(s) \).

6.6.9 Bizonyítsuk be, hogy \( s > 2 \) esetén

(a) \( \sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \zeta'(s) \zeta(s-1) ; \)

(b) \( \sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \zeta'(s-1) \zeta(s) . \)

6.6.10 Ebben a feladatban a \( \zeta \)-függvényre adott sorzat-előállítást általánosítsuk multiplikatív, illetve teljesen multiplikatív függvényekre. A prímek szerint vett végtermészetes sorzatot az 5.6.6 feladatban [149] (illetve az ebben a pontban az (5) képletben) látott módon értelmezzük, és feltesszük, hogy valamennyi végtelen sor abszolút konvergencs.

(a) Bizonyítsuk be, hogy ha \( f \) multiplikatív, akkor

\[ \sum_{n=1}^{\infty} f(n) \zeta(n) = \prod_{p} \left( \sum_{k=0}^{\infty} f(p^k) \right). \]

(b) Mutassuk meg, hogy ha \( f \neq 0 \), \( f \) teljesen multiplikatív és bármely \( P \) prímre \( |f(p)| < p^s \), akkor

\[ \sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p} \frac{1}{1 - f(p)/p^s } . \]

6.6.11 Bizonyítsuk be, hogy \( s > 1 \) esetén

\[ \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \prod_{p} \left( 1 - \frac{1}{p^s} \right) . \]

6.6.12 (M [588]) Számítsuk ki az alábbi végtelen sorok összegét:

(a) \( \sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} ; \)

(b) \( \sum_{n=1}^{\infty} \left( \frac{\varphi(n)}{n} \right)^2 . \)

6.6.13 (*) Határozzuk meg a négyzetmentes számok reciprokainak négyzetösszegét.

6.6.14 (a) Bizonyítsuk be, hogy ha \( |\omega| < 1 \) és a

\[ \sum_{n=1}^{\infty} \frac{f(\omega^n)}{1 - x^n} \]

eyenlőség két oldalán szereplő végtermészetes sorok abszolút konvergensek, akkor az egyenlőség teljesül.

(b) Számítsuk ki az alábbi végtelen sorok összegét:

(b1) \( \sum_{n=1}^{\infty} \frac{\varphi(n)}{2^n - 1} ; \)

(b2) \( \sum_{n=1}^{\infty} \frac{\varphi(n)}{2^n - 1} . \)
6.7 Átlagérték

A 6.4 pontban bebizonyítottuk, hogy noha a $d(n)$ függvény értékei igen erős ingadozást mutatnak, az első $n$ helyen felvett függvényértékek átlaga már kiegyenlítette viselkedik. Ebben a pontban más nevezetes függvények, a $\sigma$, $\varphi$ és $\omega$ átlagértékfüggvényeit fogjuk vizsgálni.

6.7.1 Definíció . D 6.7.1

Legyen $f$ számelméleti függvény és $F(n) = f(1) + f(2) + \cdots + f(n)$. Az $f$ függvény átlagértékfüggvényén vagy középértékfüggvényén az

$$\frac{F(n)}{n} = \frac{f(1) + f(2) + \cdots + f(n)}{n}$$

függvényt értjük. ♠

Az átlagértékfüggvény kiszámításánál többször szükségünk lesz az alábbi tételekre:

6.7.2 Tétel . T 6.7.2

Ha $f = g \ast h$, akkor

$$F(n) = \sum_{i=1}^{n} f(i) = \sum_{i=1}^{n} g(i) \left( \sum_{k=1}^{\lfloor n/i \rfloor} h(k) \right).$$

Bizonyítás: A konvolúció definíciójának alapján

$$\sum_{i=1}^{n} f(i) = \sum_{i=1}^{n} g(i) h(i) = \sum_{i=1}^{n} g(i) \left( \sum_{k=1}^{\lfloor n/i \rfloor} h(k) \right).$$

A T 6.7.2 Tétel legegyszerűbb speciális esete, ha $f = g^+ = g \ast 1$. Ekkor

$$\sum_{i=1}^{n} f(i) = \sum_{i=1}^{n} g(j) \left( \sum_{k=1}^{\lfloor n/j \rfloor} 1 \right) = \sum_{i=1}^{n} g(j) \left\lfloor \frac{n}{j} \right\rfloor.$$

Az $f(n) = d(n)$ esetben $g = 1$, és így (2) a

$$D(n) = \sum_{j=1}^{n} \left\lfloor \frac{n}{j} \right\rfloor$$
alakot ölti, ami megegyezik a T 6.4.3 Tétel bizonyításában szereplő (11) egyenlőséggel.

Elsőként a $\sigma$ átlagértékfüggvényével foglalkozunk.

6.7.3 Tétel . T 6.7.3

Legyen $\Sigma(n) = \sigma(1) + \sigma(2) + \cdots + \sigma(n)$. Ekkor

$$\Sigma(n) \sim \frac{\pi^2}{12} n^2,$$

ahol $\sim$ az aszimptotikus egyenlőséget jelöli.
A (3) összefüggés két másik ekvivalens alakja

\[
\frac{\gamma}{n} \sim \frac{\pi^2}{12} n, \quad (4)
\]

illetve

\[
\sigma(1) + \sigma(2) + \cdots + \sigma(n) \sim \frac{\pi^2}{6} \cdot 1 + \frac{\pi^2}{6} \cdot 2 + \cdots + \frac{\pi^2}{6} n. \quad (5)
\]

(4) azt jelenti, hogy a \( \sigma \) középértékfüggvénye jól közelíthető az \( \pi^2/12 \) függvényvel, (5)-őt pedig úgy értelmezhetjük, hogy a \( \sigma \) átlagos nagyságrendje \( \pi^2/6 \).

Bizonyítás: Próbálkozzunk először a \( d(n) \)-nél használt módszer értelmszerű módosításával. Mint az imént láttuk, ez tulajdonképpen a T 6.7.2 Tétel következményeként kapott (2) egyenlőség alkalmazását jelenti. Ennek megfelelően a \( v^i(n) = n \) jelöléssel \( \sigma = v^+ = v + 1 \), és így

\[
\Sigma(n) = \sum_{i=1}^{n} \sigma(i) = \sum_{j=1}^{n} \left[ \frac{n}{j} \right], \quad (6)
\]

(6) jobb oldalát a szokásos módon \( u - 1 < [u] \leq u \) felhasználásával becsülve

\[
u^2 - \frac{n^2 + 1}{2} < \Sigma(n) \leq u^2
\]

adódik, amiből nem kapunk aszimptotikát \( \Sigma(n) \)-re.

Ezen úgy segíthetünk, ha a T 6.7.2 Tételt a \( \sigma = 1 \times v \) konvolúcióra, azaz \( \eta = 1 \) és \( \tilde{u} = v \) szereposztással alkalmazzuk (ahol \( v^i(n) = n \));

\[
\Sigma(n) = \sum_{j=1}^{n} \sum_{k=1}^{\left\lfloor \frac{n}{j} \right\rfloor} k = \sum_{j=1}^{n} \frac{\left\lfloor \frac{n}{j} \right\rfloor \left( \frac{n}{j} \right) - 1}{2}, \quad (7)
\]

(7) jobb oldalának becsüléséhez használjuk fel, hogy \( u > 0 \) esetén

\[
u^2 - u = (v - 1)u < [u]([u] + 1) \leq u(a + 1) = u^2 + u,
\]

és így

\[
[u]([u] + 1) - u^2 \leq u. \quad (8)
\]

(8)-at \( u = n/\tilde{n} \)-re alkalmazva (7)-ből azt kapjuk, hogy

\[
\left| \Sigma(n) - \sum_{j=1}^{n} \frac{n^2}{2j^2} \right| \leq \sum_{j=1}^{n} \frac{n^2}{2j^2} \leq \frac{n(1 + \log n)}{2},
\]

azaz \( u \geq 3 \)-ra

\[
\Sigma(n) = \frac{n^2}{2} \sum_{j=1}^{n} \frac{1}{j^2} + U(n), \quad \text{ahol} \quad U(n) \leq n \log n. \quad (9)
\]
adódik. Ha \( n \to \infty \), akkor (10) jobb oldalán az első tag határértéke
\[
\frac{1}{2} \sum_{j=1}^{\infty} \frac{1}{j^2} = \frac{\pi^2}{12},
\]
és a második tag pedig 0-hoz tart, vagyis
\[
\lim_{n \to \infty} \frac{\Sigma(n)}{n^2} = \frac{\pi^2}{12}.
\]
Ez ekvivalens a bizonyítandó (3) állítással. 

Hasonló módszerekkel kezelhető a \( \rho \) középértékfüggvénye is:

### 6.7.4 Tétel .  T 6.7.4

Legyen \( \Phi(n) = \varphi(1) + \varphi(2) + \cdots + \varphi(n) \). Ekkor
\[
\Phi(n) \sim \frac{3}{\pi^2} n^2,
\]
ahol \( \sim \) az aszimptotikus egyenlőséget jelöli.

A (11) összefüggés két másik ekvivalens alakja
\[
\frac{\Phi(n)}{n^2} \sim \frac{6}{\pi^2},
\]
illetve
\[
\rho(1) + \rho(2) + \cdots + \rho(n) \sim \frac{6}{\pi^2} \cdot 1 + \frac{6}{\pi^2} \cdot 2 + \cdots + \frac{6}{\pi^2} \cdot n. \tag{13}
\]

(12) azt jelenti, hogy a \( \rho \) középértékfüggvénye jól közelíthető az \( \frac{3n^2}{\pi^2} \) függvényel, (13)-at pedig úgy értelmezhetjük, hogy a \( \rho \) átlagos nagyságrendje \( 6n^2/\pi^2 \).

**Bizonyítás:** A T 6.7.2 Tételt most a \( \phi = \mu \ast \psi \) konvolúcióra, azaz \( g = \mu \) és \( h = \psi \) szereposztással alkalmazzuk (ahol \( \psi(n) = \tau_n \)):

\[
\Phi(n) = \mu(\varnothing) \sum_{k=1}^{n} \frac{|\mu(\varnothing)|}{k} + \sum_{j=1}^{n} \mu(j) \frac{1}{j^2} \left( \frac{1}{j} \right) + 1. \tag{14}
\]

A további lépések teljesen a T 6.7.3 Tétel bizonyításának mintájára végzhetők (a hibatag becslésénél \( |\mu(\varnothing)| \leq 1 \) -et kell felhasználnunk). Végül a (10)-nek megfelelő
\[
\frac{\Phi(n)}{n^2} = \frac{1}{2} \sum_{j=1}^{n} \mu(j) \frac{U(n)}{n^2} \tag{15}
\]
becsléshez jutunk. Ha \( n \to \infty \), akkor (15) jobb oldalán a második tag 0-hoz tart, az első tag határértéke pedig
Mivel a T 6.6.4 Tétel utáni (7) képlet szerint
\[ \frac{1}{2} \sum_{j=1}^{\infty} \frac{\mu(j)}{j^2} = \frac{6}{\pi^2}, \]
ezért
\[ \lim_{n \to \infty} \frac{\mathcal{Q}(n)}{n^\beta} = \frac{3}{\pi^2}. \]

A T 6.6.4 Tétel alapján egyúttal arra is választhatunk kaphatunk, mennyi annak a valószínűsége, hogy két szám relatív prim. Más megfogalmazásban ez azt jelenti, hogy milyen valószínűséggel látszik egy P ráccspont az origóból (hiszen pontosan akkor nem esik az origót -vel összekötő szakasz belsejébe további ráccspont, ha P koordinátái relatív prímek). Először a fenti valószínűség pontos értelmezésére van szükség. Megvizsgáljuk, hogy mennyi a relatív prímek arányának a szorzatban két, amelyek mindkét eleme pozitív és \( \leq n \), majd vesszük ennek az arányának a határértékét, ha \( n \to \infty \):
\[ \lim_{n \to \infty} \frac{H(n)}{n^\beta}, \text{ ahol } H(n) = \sum_{\substack{1 \leq a \leq n, 1 \leq b \leq n \atop (a,b)=1}} 1. \quad (15) \]

Meg fogjuk mutatni, hogy ez a határérték valóban létezik, és ezt a határértéket nevezzük a szóban forgó valószínűségnek.

A ráccspontos megfogalmazásban ez a következő: az első síknegyedben vesszük azt az \( n \) oldalhosszúságu \( Q_n \) négyzetet, amelynek egyik csúcsa az origó és két oldala a koordinátatengelyekre esik, és megvizsgáljuk, hogy \( Q_n \) ráccspontjai között (a tengelyeken levő pontokat nem számítva) mennyi az origóból láthatók arányának a \( Q_n \) négyzet oldalhosszával a végleten tartva tekintjük ennek az arányának a határértékét.

6.7.5 Tétel. T 6.7.5

Két szám relatív prímének a valószínűsége (a (16)-beli értelemben) \( 6/\pi^2 \). ☐

A tétel állításának természetesen az is része, hogy ez a valószínűség, vagyis a (16)-beli határérték egyáltalán létezik.

Mint jeleztük, ez a valószínűség szoros kapcsolatban van a \( \varphi \) átlagértékefüggvényével. Ennek alapján a T 6.7.5 Tétel azonnal következne fog a T 6.7.4 Tételből. A T 6.7.5 Tételre egy másik bizonyítást is adunk a logikai szitaformula segítségével (és ebből tulajdonképpen a T 6.7.4 Tételre is egy újabb bizonyítást nyerünk).

Első bizonyítás: Megmutatjuk, hogy
\[ \Phi(n) = \sum_{i=1}^{n} \varphi(i) \approx H(n) = \sum_{\substack{1 \leq a \leq n, 1 \leq b \leq n \atop (a,b)=1}} 1 \]
között az alábbi összefüggés érvényes:

203
SZÁMELMÉLETI FÜGGVÉNYEK

\[ H(n) = 2\Phi(n) - 1. \]  \hfill (17)

Ennek igazolásához tekintsük a T 6.7.5 Tétel kimondása előtt definiált \( Q_u \) négyzetet, és bontsuk ezt az origóból kiinduló átlója segítségével két háromszögbe. \( H(n) \) éppen azoknak a \( Q_u \)-beli rácsponkoknak a száma (a tengelyeken levő pontokat nem számítva), amelyekben a két koordináta relatív prím. Ezek a rácsponkok az origóból kiinduló átlóra nézve simmetrikusak helyezkednek el. Az átló alatti háromszögben az \( k \) abszcisszájú pontok közül azok a rácsponkok felek meg, amelyek \( f \) ordinátájára \( 1 \leq t \leq i \) és \( (i, t) = 1 \) teljesül. Az illyen rácsponkok száma \( \varphi(i) \), és így az alsó háromszögben a keresett rácsponkok száma

\[
\sum_{i=1}^{\kappa} \varphi(i) = \Phi(n).
\]

A szimmetria miatt ugyanennyi rácspon teljesíti a feltételeit a felső háromszögben is. Ekkor két számból számoltuk az átlón levő rácsponkot, magán az átlón azonban csak egyetlen ilyen rácspon, az \( (1, 1) \) található. Ennek megfelelően az origóból látható rácsponkok száma valóban \( 2\Phi(n) - 1 \).

A (17) egyenlőségből a T 6.7.4 Tétel alapján kapjuk, hogy

\[
\lim_{\kappa \to \infty} \frac{H(n)}{\pi^2} = \Phi(n) \lim_{\kappa \to \infty} \frac{\Phi(n)}{\pi^2} = \frac{6}{\pi^2} - 1.
\]

Második bizonyítás: \( H(n) \)-et a logikai szitaformula segítségével fogjuk meghatározni.

Az \( \{(a, b) \mid 1 \leq a \leq \kappa, 1 \leq b \leq \kappa\} \) rendezett számpárok közül azoknak a számát kell meghatározni, amelyekre \( a \) és \( b \) relatív prím.

Ehhez „ki kell szitálni a rossz tulajdonságúakat”, vagyis azokat, amelyekre \( a \)-nak és \( b \)-nek van (egy vagy több) közös prímosztója.

Tekintsük először azokat a számpárokat, amelyek mindkét koordinátája osztható egy adott \( p \) prímmel (függetlenül attól, hogy van-e további közös prímosztójuk vagy sem). Ezeknek a számpároknak a száma nyilván \( \lceil \kappa/p \rceil^2 \).

Most nézzük azokat a számpárokat, amelyek koordinátái több, előre megadott \( P \) prímmel oszthatók (ismét nem törödve azzal, oszthatók-e további primekkel vagy sem). Egy egész akkor és csak akkor osztható adott primek mindegyikével, ha osztható ezen primek szorzatával. Ennél fogva például

\[
\left\lceil \frac{n}{p_1p_2} \right\rceil^2
\]

azoknak a számpároknak a száma, amelyek mindkét koordinátája osztható \( P \)-gyel és \( P \)-vel is, ahol \( \kappa < n \) különböző primek stb.

Így a logikai szitaformula szerint

\[
H(n) = n^2 - \sum_{i=1}^{\kappa} \left\lceil \frac{n}{i} \right\rceil^2 + \sum_{1 \leq i \leq \kappa, \text{prím}} \left\lceil \frac{n}{p_1p_2} \right\rceil^2 + \ldots \]  \hfill (18)

Vegyük észre, hogy (18) jobb oldalán éppen a

\[
\mu(j) \left\lceil \frac{n}{j} \right\rceil^2, \quad j = 1, 2, \ldots, \kappa
\]
alakú tagok összege áll, azaz
\[
H(n) = \sum_{j=1}^{n} \mu(j) \left\lfloor \frac{n}{j} \right\rfloor^2.
\]
(19)

(19) jobb oldalának becsléséhez használjuk fel, hogy \( a > 0 \) esetén

\[
0 \leq a^2 - |a|^2 = (a - |a|)(a + |a|) < 2a,
\]
és így

\[
|a|^2 - c^2 < 2a.
\]

Alkalmazzuk (20)-at \( a = n/j \) -re, ekkor \( |\mu(j)| \leq 1 \) -et is figyelembe véve (19)-ből azt kapjuk, hogy

\[
\left| H(n) - \sum_{j=1}^{n} \mu(j) \left\lfloor \frac{n}{j} \right\rfloor^2 \right| < 2 \sum_{j=1}^{n} \frac{n}{j}^2 < 2n(1 + \log n),
\]

azaz \( n \geq 3 \) -ra

\[
H(n) = \sum_{j=1}^{n} \frac{j\mu(j)}{j^2} + V(n), \quad \text{ahol} \quad |V(n)| < 4n \log n. \quad (21)
\]

(21)-et \( n^2 \) -tel osztva a

\[
\frac{H(n)}{n^2} = \sum_{j=1}^{n} \frac{\mu(j)}{j^2} + \frac{V(n)}{n^2},
\]

becsléshez jutunk, ahonnan a T 6.7.4 Tétel bizonyításának végéhez hasonló módon

\[
\lim_{n \to \infty} \frac{H(n)}{n^2} = \sum_{j=1}^{\infty} \frac{\mu(j)}{j^2} = \frac{6}{\pi^2}
\]

adódik. \( \blacksquare \)

Most rátérünk az \( \omega \) középértékfüggvényének a vizsgálatára:

6.7.6 Tétel. T 6.7.6

Az \( \omega \) középértékfüggvényének a \( \log \log n \) függvénytől való eltérése korlátos. Más szóval, ha \( z(n) = \omega(1) + \omega(2) + \cdots + \omega(n) \), akkor létezik olyan \( C \) konstans, hogy minden \( n \geq 3 \) egész számra

\[
\left| \frac{z(n)}{n} - \log \log n \right| < C. \quad \blacklozenge
\]

Bizonyítás: Alkalmazzuk a T 6.7.2 Tételt az \( \omega = \tilde{\omega} \ast 1 \) konvolúcióra (ekkor \( g = \tilde{\omega} \) és \( \mu = 1 \)):

\[
z(n) = \sum_{i=1}^{n} \omega(i) = \sum_{j=1}^{n} \tilde{\omega}(j) \left\lfloor \frac{n}{j} \right\rfloor. \quad (22)
\]

Könnyen ellenőrizhető (lásd például a 6.5.5d feladatot [193]), hogy
$$\omega(j) = \begin{cases} 1, & \text{ha } j \text{ prím;} \\ 0, & \text{egyébként.} \end{cases} \quad (23)$$

A (23)-at (22)-be beírva

$$\varphi(n) = \sum_{\nu \leq n} \frac{\nu}{\nu^s}, \quad (24)$$

adódik. Az

$$a - 1 < [a] \leq a$$

eyenlőtlenséget $a = n/p$-re felhasználva (24)-ből a szokásos módon azt kapjuk, hogy

$$\varphi(n) = n \sum_{\nu \leq n} \frac{1}{\nu} W(\nu), \quad \text{sőt,} \quad |W(\nu)| \leq r(n) \sim n,$$

azaz

$$\left| \frac{\varphi(n)}{n} - \sum_{\nu \leq n} \frac{1}{\nu^s} \right| < 1. \quad (25)$$

Mivel az T 5.6.2 Tétel szerint ($n \geq 3$-ra)

$$\sum_{\nu \leq n} \frac{1}{\nu} - \log \log n$$

korlátos, ezért (25)-ből következik az állítás. ■

Könnyen igazolható, hogy

$$\sum_{\nu \leq n} \log \log \nu \sim n \log \log n,$$

ezért a T 6.7.6 Tételből az is következik, hogy

$$\omega(2) + \cdots + \omega(n) \sim \log \log 2 + \log \log 3 + \cdots + \log \log n. \quad (26)$$

A (26) összefüggést úgy értelmezhetjük, hogy az $\omega$ átlagos nagyságrendje is $\log \log n$.

Általában nem igaz, hogy egy számelméleti függvény a legtöbbször a középértéke vagy az átlagos nagyságrendje körüli értékeket vesz fel. Legyen például

$$f(\tau i) = \begin{cases} \tau, & \text{ha } \tau \text{ nögyészlet;} \\ 0, & \text{egyébként.} \end{cases}$$

Ekkor

$$f(n) - \sum_{i=-1}^{n} f(i) = \sum_{k \leq \sqrt{n}} k^2 \sim \frac{n^{3/2}}{3},$$

ahonnan azt kapjuk, hogy $f$ középértékfüggvénye
\[ \frac{F(n)}{n^\delta} \sim \sqrt{n} / 3, \]

és az is könnyen adódik, hogy \( f(n) \) átlagos nagyságrendje \( \sqrt{n}/2 \). Ugyanakkor \( f(n) \) értéke majdnem minden \( n \)-re 0.

Hardy és Ramanujan nevezetes tétele azt mondja ki, hogy az \( \omega \) függvény a legtöbbször a középtőkfüggvényéhez közeli értéket vesz fel, azaz a legtöbb \( n \)-re az \( n \) számnak körülbelül \( \log \log n \) különböző prímosztója van. A tételre Turán Pál bizonyítását közöljük, amely kiindulópontja lett a valószínűségszámítás számelméleti alkalmazásainak.

**6.7.7 Tétel (Hardy–Ramanujan-tétel)**. T 6.7.7

Legyen \( \delta > 1/2 \) tetszőleges rögzített valós szám, \( n \geq 3 \), és jelöljük \( k(n) \)-nel azoknak az \( i \) egészeknek a számát, amelyekre \( 3 \leq i \leq n \) és

\[ \left| \omega(i) - \log \log i \right| < \left( \log \log i \right)^\delta . \]

Ekkor

\[ \lim_{n \to \infty} \frac{k(n)}{n^\delta} = 1. \]

Mivel \( \delta < 1 \)-re

\[ \lim_{n \to \infty} \left( \frac{\log \log i}{\log \log \frac{n}{i}} \right)^\delta = 0, \]

ezért a T 6.7.7 Tételből következik, hogy egy „ritka” részsorozattól eltekintve

\[ \omega(i) \sim \log \log i. \]

A T 6.7.7 Tételt az alábbi véges változatából fogjuk levezetni:

**6.7.7A Tétel**. T 6.7.7A

Bármely \( \varepsilon > 0 \)-hoz léteznek olyan (az \( \varepsilon \)-tól függő) \( T \), hogy tetszőleges \( n \geq 3 \) esetén az \( 1, 2, \ldots, n \) számok között legalább \( (1 - \varepsilon)n \) darab olyan \( i \) található, amelyre

\[ \left| \omega(i) - \log \log n \right| < T \sqrt{\log \log n}. \]

Felhívjuk a figyelmet arra az eltéréssre, hogy a \( \log \log \) függvénynek (27)-ben az \( i \) helyen, (28)-ban pedig az \( n \) helyen felvett helyettesítési értéke szerepel. Mivel azonban a \( \log \log \) függvény igen lassan változik, ezért a legtöbbször \( i \)-re ez alig jelent különbséget (lásd majd a (41) képletet).

Először a T 6.7.7A Tételt bizonyítjuk, és utána megmutatjuk, hogyan következik ebből a T 6.7.7 Tétel.

**A T 6.7.7A Tétel bizonyítása:** A bizonyítás alapján tartjuk a következő: belátjuk, hogy az

\[ U = \sum_{i=1}^{n} \left( \omega(i) - \log \log n \right)^2 \]

négyzetösszeg „viszonylag kicsi”, és így a tagok nemnegatívává miatt csak kevés \( i \)-re lehet \( \omega(i) - \log \log n \) „nagy”.

207
Nézzük mindezt részletesen. Megmutatjuk, hogy alkalmas $c$ konstansal bármely $n \geq 3$-ra fennáll
\[
U = \sum_{i=1}^{n} \left( \omega(i) - \log \log n \right)^2 < cn \log \log n.
\]  
(30)

Ehhez fel fogjuk használni, hogy a T 6.7.6 Tétel szerint ($n \geq 3$-ra)
\[
\sum_{i=1}^{n} \omega(i) = n \log \log n + nA(n), \quad \text{ahol } A(n) \text{ korlátos},
\]  
(31)

továbbá az T 5.6.2 Tétel szerint ($n \geq 3$-ra)
\[
\sum_{\nu < n}^{\frac{1}{p}} = \log \log n + B(n), \quad \text{ahol } B(n) \text{ korlátos}.
\]  
(32)

Végezzük el (29)-ben a négyzetre emeléseket:
\[
U = \sum_{i=1}^{n} \omega^2(i) - 2 \log \log n \sum_{i=1}^{n} \omega(i) + n(\log \log n)^2.
\]

Innen (31) alapján azt nyerjük, hogy
\[
U = \sum_{i=1}^{n} \omega^2(i) - 2 \log \log n \left( n \log \log n + nA(n) \right) + n(\log \log n)^2 =
\]
\[
= \sum_{i=1}^{n} \omega^2(i) - n(\log \log n)^2 - 2nA(n) \log \log n.
\]  
(33)

Az $U$ felső becsléséhez így a
\[
V = \sum_{i=1}^{n} \omega^2(i)
\]  
(34)
özseget kell felülről becsülnünk.

Az $\omega(i)$ definícióját (részben) beirva a szokásos összegáterezés után
\[
V = \sum_{i=1}^{n} \omega^2(i) = \sum_{i=1}^{n} \omega(i) \sum_{\nu | i} 1 = \sum_{\nu \leq n} \sum_{k=1}^{\left[ \frac{n}{\nu} \right]} \omega(\nu k)
\]  
(35)

adódik. Mivel
\[
\omega(\nu k) = \begin{cases} 
\omega(k), & \text{ha } p \mid k; \\
1 + \omega(k), & \text{ha } p \nmid k,
\end{cases}
\]
ezért (35)-ből azt kapjuk, hogy
\[
V \leq \sum_{\nu \leq n} \sum_{k=1}^{\left[ \frac{n}{\nu} \right]} \left(1 + \omega(k)\right) = \sum_{\nu \leq n} \left[ \frac{n}{\nu} \right] \frac{\mu}{\nu} + \sum_{\nu \leq n} \sum_{k=1}^{\left[ \frac{n}{\nu} \right]} \omega(k).
\]  
(36)

Jelöljük a (36) jobb oldalán szereplő első összeget $K$-val, a második, kettős összeget pedig $L$-lel.

Ekkor $K$-ra (32) alapján a következő felső becsést nyerjük:
Az $L$ felső becsleséhez beírjuk $\omega(k)$ definícióját és a szokásos összegátrendezést alkalmazzuk (itt $p'$-re)$ aszt jelzi, hogy az összegzés prímekre történik, majd felhasználjuk (32)-t:

$$L = \sum_{i \leq \pi} \sum_{x \leq \pi'} \frac{1}{\pi' x} \leq n \sum_{p \leq \pi} \frac{1}{\log p} = n \left( \log \log n + \mathcal{B}(\pi) \right).$$

(37)

A (37) és (38) becsléseket (36)-ba beírva azt kapjuk, hogy

$$V \leq n \left( \log \log n + \mathcal{B}(\pi) \right) + \pi \left( \log \log n + B(n) \right)^2.$$

(38)

Végül, ha a $V = \sum_{i = 1}^{\pi} \omega(i)^2$ -re ily módon nyert (39) becslést (33)-ba behelyettesítjük, akkor az $n \left( \log \log n \right)^2$ tagok kiejtik egymást, és

$$U \leq \left( 1 + 2B(n) - 2\lambda(\pi) \right) \pi \log \log n + \left( B(n) + B^2(n) \right) n < cn \log \log n$$

adódik, amivel (30)-at bebizonyítottuk.

Most már csak a bizonyítás elején jelzett gondolatmenetnek azt a részét kell pontosítani, hogy ha a (29) négyzetösszeg „kicsi”, akkor ebben csak kevés „nagy” tag szerepelhet.

Jelöljük $s$ -el a (28)-at nem teljesítő (azaz „rossz”) $1 \leq i \leq \pi$ számoknak a számát. A tétel állítását kicsit átfogalmazva, azt kell belátnunk, hogy bármely $\epsilon > 0$ -hoz található olyan $T$, amelyre $s < \epsilon n$ teljesül.

Csökkentsük (30) bal oldalát úgy, hogy írjunk $\left( \omega(i)^2 - \log \log n \right)^2$ helyére ennél az $s$ darab „rossz” $i$ -nél $T^2 \log \log n$ -et, a többi $i$ -nél pedig 0-t. Ekkor (30) alapján azt kapjuk, hogy

$$sT^2 \log \log n \leq cn \log \log n, \text{ azaz } s \leq \frac{c}{T^2} n.$$

(40)

Ha most $T$ értékét a

$$\frac{c}{T^2} \leq \epsilon$$

feltételnek megfelelően választjuk, akkor éppen a kivánt $s < \epsilon n$ becslés adódik. □

A T 6.7.7 Tétel bizonyítása: Azt kell igazolni, hogy bármely $\epsilon > 0$ -hoz létezik olyan (az $c$ -től függő) $T_0$, hogy minden $n > T_0$ esetén a $3, 4, \ldots, n$ számok között legfeljebb $\epsilon n$ darab olyan $i$ található, amelyre (27) nem teljesül.

Amint korábban is jelezdtük, a már bizonyított T 6.7.7A Tétel esetén a (28) képletben $\log \log n$ szerepel, míg a bizonyítandó T 6.7.7 Tétel esetén a (27) képletben $\log \log i$ -ről van szó. A bizonyításhoz tulajdonképpen ezt az eltérést kell áthidalni.

A bizonyítás lényege az alábbi észrevétel: a $\log \log n$ függvény olyan lassan változik, hogy $\sqrt{n}$ és $n$ között „majdnem” konstansnak tekinthető, a $\sqrt{n}$-nél kisebb $i$ értékek pedig olyan kevesen vannak, hogy az belefér a megengedett kivételek halmazába.
Nézzük mindezt részletesen. Alkalmazzuk a T 6.7.7A Tételt \( \varepsilon \) helyett \( \varepsilon / 2 \)-re. Ekkor a \( \sqrt{n} \) és \( n \) közé eső számok között legfeljebb \( \varepsilon n / 2 \) olyan \( i \) van, amelyre (28) nem teljesül. Mivel \( \sqrt{n} \leq i \leq n \) esetén
\[
\log \log n - \log 2 = \log \log \sqrt{n} \leq \log \log i \leq \log \log n,
\]
ezért az előbbi kijelentés akkor is igaz marad, ha (28)-ban a \( \log \log n \) helyett mindkétszer \( \log \log i \) szerepel, ehhez csak \( T \) értékét kell (a (40)-ben előírt) megfelelően nagyobbra választani. Ha \( n \) eléggé nagy, akkor a \( \sqrt{n} \) -nél kisebb \( i \) értékek száma kevesebb, mint \( \varepsilon n / 2 \), vagyis azt kaptuk, hogy alkalmas \( T \) és eléggé nagy \( n \) esetén a \( 3, 4, \ldots, n \) számok között legalább \( (1 - \varepsilon)n \) darab olyan \( i \) található, amelyre
\[
|\omega(i) - \log \log i| < T \sqrt{\log \log i}.
\]
Mivel \( \delta > 1 / 2 \), ezért minden, a \( T \)-től és \( \delta \)-tól függően eléggé nagy \( n \) -re
\[
T \sqrt{\log \log i} < (\log \log i)^\delta,
\]
es így (42)-ből következik a T 6.7.7 Tétel állítása.

Megjegyzés: A T 6.7.7A Tétel bizonyításának a valószínűségszámítási tartalma a következő. Legyen \( \eta \) rögzített, és tekintsük az \( \omega \)-t valószínűségi változónak, amely egyforma, azaz \( 1/\eta \) valószínűséggel veszi fel az \( \omega(1), \omega(2), \ldots, \omega(n) \) értékeket. Ennek a valószínűségi változónak az \( E \) várható értéke definíció szerint az \( \omega \) középértékfüggvényének az \( \eta \) helyen felvett értéke, ami körülbelül \( \log \log n \) . A (29)-ben megadott \( U \) pedig körülbelül \( n D^2 \), ahol \( D \) az \( \omega \) szórása. A T 6.7.7A Tétel állítása ezután a \( D \)-re adott felső becsülésből (lásd (30)) és a
\[
P(|\omega - E| > r D) < \frac{1}{r^3}
\]
Csebisev-egyenlőtlenségből következett (ahol \( P \) az esemény valószínűségét jelöli).

A T 6.7.6, T 6.7.7 és T 6.7.7A Tételek az \( \omega \) helyett a \( \Omega \) függvényre is igazak, lásd a 6.7.5b feladatot [211]. Ezekből a
\[
2^{\mu(a)} \leq d(\tau) \leq 2^\Omega(a)
\]
eyenlőtlenség segítségével igazolható az a 6.4 pontban már jelzett érdekeség is, hogy a legtöbb \( n \) esetén a \( d(\tau) \) függvény értéke „körülbelül”
\[
(\log \tau)^{1.052} = (\log \tau)^{0.69...},
\]
ami lényegesen kisebb, mint a \( d(\tau) \) középértékének megfelelő \( \log \tau \) -es nagyságrend (lásd a 6.7.6 feladatot [211]).

**Feladatok**

6.7.1 Számítsuk ki a
\[
\sum_{j=1}^{n} \mu(j) \left\lfloor \frac{n}{j} \right\rfloor
\]
összeget.

6.7.2 Mi a valószínűsége annak, hogy egy pozitív egész szám négyzetmentes legyen?

6.7.3 (*) Bizonyítsuk be az alábbi aszimptotikus egyenlőségeket a $d_4(n)$ függvény, illetve rögzített $\nu > 0$ esetén a 6.2.23 feladatban [178] definiált $\sigma_\nu(n)$ függvény középértékfüggvényére:

$$\frac{D_4(n)}{n} = \frac{d_4(1)+d_4(2)+\cdots+d_4(n)}{n} \sim \frac{\log^2(n)}{\nu^2};$$

$$\frac{E_\nu(n)}{n} = \frac{e_\nu(1)+e_\nu(2)+\cdots+e_\nu(n)}{n} \sim \nu^{\nu+1}.$$

6.7.4 (M [589]*) Igazoljuk, hogy bármely $k$ esetén léteznak olyan $\nu_1, \ldots, \nu_k$ különböző egész számok, amelyekre $\sigma(\nu_1) = \cdots = \sigma(\nu_k)$.

6.7.5 (a) Bizonyítsuk be, hogy

$$0 < \sum_{i=1}^{n} \left( \Omega(i) - \omega(i) \right) < n.$$

(b) Mutassuk meg, hogy a T 6.7.6, T 6.7.7 és T 6.7.7A Tételek állításai az $\omega$ helyett a $\Omega$ függvényre is igazak.

6.7.6 Mutassuk meg, hogy a legtöbb $\nu$-re az $\nu$ számok körülbelül

$$(\log \nu)^{\log 2}$$
osztója van a következő értelenben. Legyen $\varepsilon > 0$ tetszőleges, és jelöljük $k(\nu)$ -nel azoknak az $1 \leq i \leq n$ számoknak a számát, amelyekre

$$(\log n)^{\omega 2 - \varepsilon} < d(i) < (\log n)^{\omega 2 + \varepsilon}.$$  

Ekkor

$$\lim_{\nu \to \infty} \frac{k(\nu)}{\nu} = 1.$$  

6.7.7 (*) Jelölje $\overline{h}(\nu)$ azoknak az $1 \leq i \leq n$ számoknak a számát, amelyek felirhatók két $\sqrt{\nu}$ -nél kisebb pozitív egész szorzataként. Számítsuk ki a

$$\lim_{\nu \to \infty} \frac{h(\nu)}{\nu};$$

határértéket.

6.7.8 Fogalmazzuk meg pontosan és bizonyítsuk be a Hardy–Ramanujan-tétel következő általánosítását:

Tegyük fel, hogy az $f$ valós értékű additív függvény rendelkezik az alábbi tulajdonságokkal.

(i) Létezik olyan $K$, hogy minden $p$ prímre $0 \leq f(p) \leq K$.

(ii) Minden $p$ prímre és $\alpha > 0$ esetére $f(p^\alpha) = f(p)$.
(iii) $\sum f(p)/p$ végahlen sor divergens.

Ekkor majdnem minden $n$-re

$$f(n) \sim \sum_{p \leq n} \frac{f(p)}{p}.$$ 

## 6.8 Additív függvények karakterizációja

Láttuk, hogy a legtöbb szármelméleti függvényre a függvényértékek ingadozása jellemző. Az alábbi, Erdős Páltól származó tétel azt mutatja, hogy az additív függvények körében ez alól teljes mértékben csak a logaritmusfüggvény jelent kivételt:

### 6.8.1 Tétel

**T 6.8.1**

Legyen $f$ valós értékű additív függvény, és tegyük fel, hogy

(i) $f(n)$ monoton,

vagy

(ii) $f(n+1) - f(n) \to 0$, ha $n \to \infty$.

Ekkor alkalmas $c$ konstanssal $f(n) = c \log n$.

**Bizonyítás:** Azt a kicsit erősebb eredményt fogjuk igazolni, hogy ha egy $f$ valós értékű additív függvényre a

$$\lim_{n \to \infty} \inf \{ f(n+1) - f(n) \} \geq 0 \tag{1}$$

feltétel teljesül, akkor $f(n) = c \log n$.

Ebből a T 6.8.1 Tétel valóban következik: ha $f$ a (ii) tulajdonsággal rendelkezik, vagy $f$ monoton növekszik, akkor $f$ nyilván kielégíti (1)-et, ha pedig $f$ monoton fogyó, akkor $f$ helyett $-f$ teljesíti (1)-et, és így $(-f)(n) = c \log n$, azaz $f(n) = -c \log n$ adódik.

A bizonyítás alapgondolata a következő. Legyen $k > 1$ rögzített egész, és írjunk fel egy tetszőleges $n$-et $k$ alapú számrendszerben:

$$n = a_1 k^s + \cdots + a_s k + a_0, \quad s = \lfloor \log_k n \rfloor. \tag{2}$$

Az $n$ utolsó számjegyét elhagya és az utolsó előtti számjegyet alkalmazan megváltoztatva, az $n$-hez „viszonylag közel” találunk egy olyan

$$n' = a_1 k^s + \cdots + a_2 k^2 + a_0 \tag{3}$$

számot, amelyre $(a_1, k) = 1$. Ekkor a feltételek alapján $f(n)$ „nem sokkal tér el” az

$$f(n') = f(k) + f(a_1 k^{s-1} + \cdots + a_2 k + a_0) \tag{4}$$

függvényértéktől. Az eljárást a (4) jobb oldalán levő második tagra megismételve stb. végül azt kapjuk, hogy
Nézzük mindezt pontosan és részletesen. Legyen $\varepsilon > 0$ tetszőleges. Ekkor az (1) feltétel szerint van olyan (az $\varepsilon$ -tól függő) $u_0$, hogy minden $u > u_0$ esetén

$$f(u + 1) - f(u) \geq -\varepsilon,$$

azaz

$$f'(u) \leq f(u + 1) + \varepsilon.$$  \hfill (5)

(A technikai lépések kényelmesebb leírása érdekében feltesszük, hogy $u_0 > k^2$.)

Ha (5)-ben $n$ helyére rendre az $u = n + 1, n + 2, \ldots, n + t - 1$ értékeket írjuk, akkor

$$f(n + 1) \leq f(n + 2) + \varepsilon, f(n + 2) \leq f(n + 3) + \varepsilon, \ldots, f(n + t - 1) \leq f(n + t) + \varepsilon,$$

és így

$$f(n) \leq f(n + 1) + \varepsilon \leq f(n + 2) + 2\varepsilon \leq \cdots \leq f(n + t) + t\varepsilon$$ \hfill (6)

adódik.

Legyen $n$, „sokkal nagyobb” $u_0$ -nál, és tekintsük (rögzített $k > 1$ mellett) a (2) előállítást. Válasszuk a (3)-nak megfelelő legkisebb olyan $n'$ számot, amelyre $u' > n$ és $(u_1, k) = 1$. Ez azt jelenti, hogy $n$ utolsó számjegyét elhagyjuk, és az utolsó előtti $\Theta$ számjegy helyett egy nála nagyobb $a_1$ -t veszünk (esetleg $a_1 = k + 1$ is előfordulhat). Jelöljük az $n'$ és $n$ különbségét $t$ -vel:

$$t = n' - n = (a_1' - a_1)k - u_0.$$  \hfill (7)

Ha $a_1 = 0$, akkor $a_1' = 1$, ha pedig $a_1 \geq 1$, akkor $1 \leq a_1 < a_1' \leq k + 1$, ezért (7) alapján mindenképpen

$$0 < t \leq k^2$$  \hfill (8)

teljesül. Rendre a (6), majd a (7) és (8), végül a (4) összefüggéseket alkalmazva, azt kapjuk, hogy

$$u > u_0$$

és így

$$f(n) \leq f(n + 1) + t\varepsilon \leq f(n + 2) + k^2\varepsilon = f(k) + f(a_k k^{n-1} + \cdots + a_2 k + a_1') + k^2\varepsilon.$$  \hfill (9)

Tekintsük most a (9) jobb oldalán szereplő középső tagban előforduló

$$n_k = a_k k^{n-1} + \cdots + a_2 k + a_1'$$

számot. Ha ebben $a_1' = k + 1$, akkor írjuk át $n_k$ -et a szokásos számrendszeres alakba (ahol tehát minden $k$ -hatvány együttthatoja $k$ -nál kisebb; ekkor az utolsó számjegy 1-es lesz, az utolsó előtti 1-gyel nő, illetve ha az $k - 1$ volt, akkor további változások is történhetnek).

Most ismételjük meg az egész eddigi eljárást $n_n$ helyett $n_k$ -re. Ekkor azt kapjuk, hogy

$$f(a_k k^{n-1} + \cdots + a_2 k + a_1') = f(n_k) \leq f(k) + f(a_k k^{n-2} + \cdots + a_2 + a_1') + k^2\varepsilon,$$

amit (9)-be beírva

$$f(n) \leq f(n + 1) + t\varepsilon \leq f(n + 2) + k^2\varepsilon = f(k) + f(a_k k^{n-1} + \cdots + a_2 k + a_1') + k^2\varepsilon,$$

amit (9)-be beírva

$$f(n) \leq f(n + 1) + t\varepsilon \leq f(n + 2) + k^2\varepsilon = f(k) + f(a_k k^{n-1} + \cdots + a_2 k + a_1') + k^2\varepsilon.$$
adódik. Hasonlóan haladhatunk tovább mindaddig, amíg \( n_0 \)-nál nagyobb helyeken felvett függvényértékek keletkeznek. Végül azt nyerjük, hogy

\[ f(n) \leq (s - s_0) f(k) + (s - s_0) k^2 \varepsilon - M_0, \]

ahol \( s - s_0 \) a lépések száma és \( M_0 \) az \( n_0 \)-ig terjedő függvényértékek maximuma. Itt \( M_0 \) csak \( \varepsilon \)-tól, \( s_0 \) pedig \( \varepsilon \)-től és (a rögzített) \( k \)-tól függ, ezért (10) átírható az

\[ f(n) \leq s f(k) + s k^2 \varepsilon + M_1 \]

alakba, ahol \( M_1 \) az \( \varepsilon \)-től és \( k \)-től függő konstans.

Hasonlóan nyerhetünk alsó becslést is \( f(n) \)-re. Ehhez \( \alpha' \)-t most is az \( n \)-hez közel és az \( (a' : k) = 1 \) feltételnél megfelelően kell választanunk, azonban most a minimális \( u' > r \) helyett a maximális \( u' < r \) követelményt írjuk elő (most \( a' = -1 \) is lehet). A felső becslés lépésein csak annyiban kell módosítani, hogy a \( t \)-értékét \( n - u' \)-nek vesszük, és (6) helyett az

\[ f(n) \geq f(n - t) - t \varepsilon \]

eyenlőtlen séget alkalmazzuk. Ekkor az előzőkhöz teljesen hasonlóan az adódik, hogy alkalmas \( M_2 \)

vel

\[ f(n) \geq s f(k) - s k^2 \varepsilon - M_2 \]

teljesül.

A (11) és (12) egyenlőtlen ségekből \( s = \log_{\alpha} n \) -nel történő osztás után azt kapjuk, hogy

\[ \left| \frac{f(n)}{\log_{\alpha} n} - f(k) \right| \leq k^2 \varepsilon + \frac{M}{\log_{\alpha} n}. \]

Ha \( n \to \infty \), akkor (13) jobb oldala \( k^2 \varepsilon \) -hoz tart. Mivel azonban \( \varepsilon \) tetszőleges volt, ezzel beláttuk, hogy

\[ \lim_{n \to \infty} \frac{f(n)}{\log_{\alpha} n} = f(k). \]

A (14)-ből nyilván következik, hogy

\[ \lim_{n \to \infty} \frac{f(n)}{\log_{\alpha} n} = f(k), \]

azaz

\[ \lim_{n \to \infty} \frac{f(n)}{\log_{\alpha} n} = \frac{f(k)}{\log_{\alpha} k}. \]

Jelöljük a (15)-beli határértéket \( c \)-vel; mivel \( c \) nem függ a (jobb oldalon szereplő) \( k \)-tól, ez éppen azt jelenti, hogy bármely \( k > 1 \)-re

\[ \frac{f(k)}{\log_{\alpha} k} = c, \]
azaz

\[ f(k) = c \log k. \] (15)

Végül, mivel \( f(1) = \log 1 = 0 \), ezért (16) teljesül \( k = 1 \) -re is.

**Feladatok**

**6.8.1** Bizonyítsuk be, hogy ha egy \( f \) komplex értékű teljesen additív függvény korlátos, akkor \( f = 0 \).

**6.8.2** Mutassuk meg, hogy ha egy \( f \) komplex értékű additív függvényre az \( f(n) \) függvényértékek sorozata konvergens, akkor \( f = 0 \).

**6.8.3** Melyek a valós értékű monoton multiplikatív függvények?

**6.8.4** Bizonyítsuk be, hogy ha egy \( f \) valós értékű additív függvényre

\[
\limsup_{n \to \infty} \left( f(n) - f(n-1) \right) \leq 0,
\]

akkor \( f(n) = c \log n \).

**6.8.5** Mutassuk meg, hogy ha egy komplex értékű \( f \) additív függvényre

\[
\lim_{n \to \infty} \left( f(n) - f(n-1) \right) = 0,
\]

akkor \( f(n) = c \log n \), ahol \( c \) alkalmas komplex konstans.

**6.8.6** Bizonyítsuk be az alábbi állításokat.

(a) Létezik a természetes számoknak akármilyen ritka olyan \( a_n \) részsorozata, hogy ha egy \( f \) valós értékű additív függvényre \( f(a_n) \) monoton, akkor \( f(n) = c \log n \).

(b) Létezik a természetes számoknak akármilyen ritka olyan \( a_n \) részsorozata, hogy ha egy \( f \) valós értékű additív függvényre

\[
\lim_{n \to \infty} \left( f(a_n) - f(a_{n-1}) \right) = 0,
\]

akkor \( f = 0 \).

(Az akármilyen ritka azt jelenti, hogy bármilyen előre megadott \( b_n \) sorozathoz található olyan \( c_{a_n} \) sorozat, amely rendelkezik az előírt tulajdonsággal, és \( a_n > b_n \).)
7. fejezet - DIOFANTIKUS EGYENLETEK

Diofantikus (vagy diofantoszi) egyenletnek általában olyan egész együtttható algebrai egyenletet nevezünk, melynek a megoldásait is az egész (esetenként a racionális) számok körében keresünk. Diophantosz görög matematikus az i.sz. III. században élt Alexandriában, és sokféle ilyen egyenlettel foglalkozott. (Akkoriban teljesen természetes volt, hogy egész, illetve racionális megoldásokat kerestek, hiszen az irracionalis számok annak ellenére sem nyertek igazán polgárigot, hogy a görögök bebizonyították ezek létezését.) A diofantikus egyenletek története egyébként még annál is sokkal régebbre nyúlik vissza; közel négyezer éves kötből tanúsága szerint már a babilonaiak is ismerték az ún. pitagorasi számhármasok előállítási módját.

A diofantikus egyenletek megoldása igen változatos módszereket igényel, univerzális megoldási módszer nem létezik (sőt, mint az 5.1 pontban már említettük, annak az egyszerűbb kérdésnek a megválaszolására sem létezik általános algoritmus, hogy egy tetszőlegesen adott diofantikus egyenletnek egyáltalán van-e megoldása vagy sem). Egy-egy konkrét egyenlet esetén is gyakran igen nehéz eldönteni a megoldhatóságot, a megoldásszámról, illetve az összes megoldás meghatározásáról nem is beszéle. Ez a témakör is bővelkedik híres megoldatlan problémákban.

A már az 1. fejezetben is szerepelt lineáris diofantikus egyenletek részletes tárgyalása után a pitagorasi számhármasokkal foglalkozunk, majd néhány jól használható elemi módszert mutatunk be diofantikus egyenletek megoldására. A továbbiakban olyan diofantikus problémák következnek, amelyek kezeléséhez látszólag egészen más jellegű matematikai eszközöket érdemes bevetni: a két négyzetsszám összegéből történő előállíthatósághoz a Gauss-egészeket, a Fermat-sejtés köbsszámokra vonatkozó speciális eseténél az Euler-egészeket és a Pell-egyenletnél a diofantikus approximációkat. Ezeknek a „segédeszközöknél” a kialakulását és önálló elméletét terebélyesedést éppen a diofantikus egyenleteknél való alkalmazhatóságuk segítette elő. Az ezekből kifejlődött területeknek a részletes bemutatására a 8–11. fejezetek kerül majd sor. Végül, a jelen fejezet utolsó pontjában a fenti fromtól mind a probléma jellegében, mind pedig a megoldási módszerekben alapvetően eltérő partíció kérdéseket tárgyalunk.

7.1 Lineáris diofantikus egyenlet

Először az \( ax + by = c \) kétismeretlen lineáris diofantikus egyenlettel foglalkozunk. Itt \( a, b, c \) rögzített egész számok, ahol az \( a = b = 0 \) esetet eleve kizárjuk, és megoldáson \( x, y \) egész számokból álló számpár értünk.

A megoldhatóság szükséges és elégséges feltételét az T 1.3.6 Tételben, az egyenletek a lineáris kongruenciákkal való kapcsolatát a T 2.5.3 Tétel bizonyítása során tárgyaljuk. Az T 1.3.6 Tétel bizonyításából azt is leolvastuk, hogy az egyenlet egy megoldását az euklideszi algoritmus segítségével kaphatjuk meg. Ebből az T 5.7.1 Tétel szerint következett, hogy az egyenlet egy megoldását nagy számok esetén is „gyorsan” meg tudjuk határozni; ezt a tényt az RSA-sémán (T 5.8.1 Tétel) is felhasználtuk.

Most megadjuk a megoldásszámot és az összes megoldás leírását. A teljesség kedvéért a tétel állításában a megoldhatóságról és a megoldási módszerről korábban bizonyított állításokat is összefoglaljuk.

7.1.1 Tétel . \( T \ 7.1.1 \)

Legyenek \( a, b \) és \( c \) rögzített egész számok, ahol \( a \) és \( b \) közül legalább az egyik nem nulla, és tekintsük az \( ax + by = c \) diofantikus egyenletet.

(i) Az egyenlet akkor és csak akkor oldható meg, ha \((a, b) | c\).
(ii) Megoldhatóság esetén végigelen sok megoldás van. Ha \( x_0, y_0 \) (egy rögzített) megoldás, akkor az összes \( x', y' \) megoldást az alábbi képlet szolgáltatja:

\[
x' = x_0 + t \cdot \frac{b}{(a,b)}, \quad y' = y_0 - \frac{a}{(a,b)} \cdot t, \quad \text{ahol} \quad t = 0, \pm 1, \pm 2, \ldots \tag{1}
\]

(iii) Az egyenlet egy megoldását az euklideszi algoritmus segítségével kaphatjuk meg.

*Bizonyítás:* Mint már említettük, (i)-et és (iii)-at az T 1.3.6 Tételben igazoltuk.

Rátérve (ii)-re, először azt mutatjuk meg, hogy az (1)-ben megadott \( x', y' \) számok valóban az egyenlet egy megoldását szolgáltatják. Mivel \( x_0, y_0 \) megoldás, azaz \( ax_0 + by_0 = c \), így

\[
a x_0 + b y_0 = c \tag{2}
\]

A megfordításhoz tegyük fel, hogy \( x', y' \) egy tetszőleges megoldás, és belátjuk, hogy \( x' \) és \( y' \) a kívánt alakú.

A feltétel szerint

\[
a x_0 + b y_0 = c \quad \text{és} \quad a x' + b y' = c.
\]

A két egyenlőséget egymásból kivonva

\[
a (x' - x_0) + b (y' - y_0) = 0
\]

adódik. Rendezés és \((a, b)\)-vel történő osztás után azt kapjuk, hogy

\[
\frac{a}{(a, b)} (x' - x_0) = \frac{b}{(a, b)} (y_0 - y'), \tag{2}
\]

Mivel

\[
\frac{b}{(a, b)} = \frac{a}{(a, b)} = 1,
\]

ezért (2)-ből

\[
\frac{b}{(a, b)} | x' - x_0,
\]

azaz alkalmas \( t \) egésszel

\[
x' = x_0 + t \cdot \frac{b}{(a, b)} \tag{3}
\]

következik. A (3)-at (2)-be visszahelyettesítve kapjuk, hogy

\[
y' = y_0 - \frac{a}{(a, b)}.
\]

Ezzel megmutattuk, hogy \( x' \) és \( y' \) valóban az (1)-ben előírt alakú.
A diofantikus egyenletek tényleges megoldásakor az euklideszi algoritmusnak egy olyan variánsát érdemes alkalmazni, amelynek segítségével (nemcsak egy megoldáshoz jutunk el, hanem) egyszerre tudjuk az összes megoldást (paraméteres alakban) előállítani. Ezt az eljárást egy konkrét példán keresztül mutatjuk be.

Példa: Oldjuk meg a \( 43x + 25y = 98 \) diofantikus egyenletet.

Fejezzük ki az egyenletből azt az ismeretlen, amelynek az együtthatója kisebb abszolút értékű, és a törtből válasszunk le olyan részeket, amelyek biztosan egész értékűek:

\[ y = \frac{38 - 43x}{25} = 1 - 2x + \frac{7x - 2}{25}. \quad \langle A1 \rangle \]

Ekkor az (A1) jobb oldalán álló \( \frac{7x - 2}{25} \) tört is egész szám kell hogy legyen, jelöljük ezt \( x \) -val. Innen \( 7x - 2 = 25n \). Ez egy hasonló diofantikus egyenlet, mint az eredeti, csak itt az \( x \) együthatójának kisebb az abszolút értéke, mint az eredeti egyenletben \( y \) együtthatójáé volt.

Ismételjük meg most az előző eljárást a \( 7x - 2 = 25n \) egyenletre, fejezzük ki \( x \) -et, és válasszuk le a garantáltan egész értékű kifejezéseket:

\[ x = \frac{25n + 2}{7} = 4n + \frac{2 - 3n}{7}. \quad \langle A2 \rangle \]

Az (A2) jobb oldalán szereplő \( \frac{2 - 3n}{7} \) tört egész szám kell hogy legyen, jelöljük \( u \) -vel, ekkor \( 2 - 3u = 7v \). Hasonlóan tovább haladva kapjuk, hogy

\[ u = \frac{2 - 7v}{3} = -2v + \frac{2 - 2v}{3}. \quad \langle A3 \rangle \]

A \( \frac{2 - 2v}{3} \) egész számot \( v \) -vel jelölve \( 2 - v = 3w \), azaz

\[ v = 2 - 3w. \quad \langle A4 \rangle \]

Mivel (A4)-ben már nem szerepel tört, most elindulunk „visszafelé”, és rendre (A3), (A2) és (A1) felhasználásával \( u \), \( x \) és \( y \) értékét kifejezünk a \( v \) paraméter segítségével:

\[ u = -2v + w = -2(2 - 3w) + w = -4 + 7w; \quad \langle B3 \rangle \]
\[ x = 4n + v = 4(-4 + 7w) + (2 - 3w) = -14 + 25w; \quad \langle B2 \rangle \]
\[ y = 4 - 2x + u = 4 - 2(-14 + 25w) + (-4 + 7w) = 28 - 43w. \quad \langle B1 \rangle \]

A módszertől világos, hogy a (B2)-(B1) képletén a \( 48x + 25y = 98 \) diofantikus egyenlet összes megoldását, ahol a \( v \) paraméter tetszőleges egész szám. Ugyanis egyrésztt, ha egy \( x, y \) egész számpár megoldás, akkor az (A1)-(A3) lépésekben végighaladva eljutunk \( v \) -hez, majd ennek segítségével \( x \) -re és \( y \) -ra a (B2)-(B1) képletén adódik, másrészt tetszőleges egész \( v \)-re az így képzett \( x \) és \( y \) számok egész leeresznek és kielégítik az egyenletet.

Megjegyzések: 1. Nézzük az eljárás lépései során keletkező együtthatópárokat:

\[ \{43, 25\}; \quad \{25, 7\}; \quad \{7, 3\}; \quad \{3, 1\}. \]

Ezek rendre úgy keletkeztek, hogy a 43-at a 25-tel osztva \( -7 \) volt a (legkisebb abszolút értékű) maradék, a 25-öt a 7-tel osztva \( -3 \) stb. Ez azt jelenti, hogy itt valóban az euklideszi algoritmus egy variánsáról van szó, és ebből az is következik, hogy a diofantikus egyenlet megoldásait így módon „gyorsan“ meg tudjuk határozni.
2. A fenti módszer lényege, hogy az ismeretlenek együtthatóinak az abszolút értékeit megfelelően csökkentve végül a törteket teljesen kiküszöböljük. Ebből a szempontból mellékes, hogy a „konstans” tag abszolút értékét csökkentjük-e vagy sem. Akár végrehajtjunk ilyen átalakítást (mint a fenti példában), akár nem, ez az eljárás lépészámait nem befolyásolja, legfeljebb „kényelmesebb”, ha kisebb számmokkal dolgozunk.

3. Nem szükséges a megoldhatóság feltételét előre külön ellenőrizni, az eljárásból is automatikusan kiderül, ha nincs megoldás: ekkor egy olyan törthöz jutunk, amelyben már nem szerepel ismeretlen, azonban a tört értéke nem egész szám.

4. A (B2)–(B1) képlet összhangban van a T 7.1.1 Tételnek az összes megoldást leíró (1) előállításával: most \(x_1 = -14\), \(y_1 = 28\), és a \(l\) szerepét \(n\) játsza. Ez az észrevétel esetleges számolási hibák kiszűrésére is alkalmas: a végeredményként kapott képletet mindig érdemes ilyen szempontból (1)-gyel összevetni.

Kettőnél több ismeretlenes lineáris diofantikus egyenletekre is a kétismeretlenes esethez hasonló állítások érvényesek. Ezeket az alábbi tételben foglaljuk össze, a bizonyításokat a 7.1.8 feladatban [220] tűzük ki.

7.1.2 Tétel. T 7.1.2

Legyen \(k \geq 2\), \(a_1, \ldots, a_k\) nem csupa 0 egész számok, \(e\) tetszőleges egész, és tekintsük az

\[ a_1x_1 + \cdots + a_kx_k = e \]

diofantikus egyenletet (azaz megoldáson egy egészre ből álló \(x_1, \ldots, x_k\) szám- \(k\)-ast érünk).

(i) Az egyenlet akkor és csak akkor oldható meg, ha \(\left\langle a_1, \ldots, a_k \right\rangle \mid e\).

(ii) Megoldhatóság esetén végtermek megoldás van. Az összes megoldás \(k - 1\) egész paraméter segítségével adható meg. A megoldások meghatározása a két ismeretlen esetén látott módszer értelemeszerű általánosításával történik.

Feladatok

7.1.1 Bolondóciában csak 47 és 79 forintos bankjegyek léteznek. Hányféleképpen lehet pontosan 1000 forintot kifizetni?

7.1.2 Egy szigeten 7- és 11-fejű sárkányok élnek. Hány sárkány él a szigeten, ha összesen 118 fejük van?

7.1.3 Egy üzletben háromféle csokoládé kapható, 70, 130, illetve 150 forintos egységárban. Hányféleképpen lehet (pontosan) 5000 forintért pontosan 50 darab csokoládét vásárolni?

7.1.4 (M [590]) Valamikor a huszadik században az 99 évnel nem idősebb és különböző korú Alexander és Bernát mindkettő éppen annyi idősek, mint annyiből a születési évszámukban a számjegyek összege. Hány év közöttük a korkülönbség?

7.1.5 Mutassuk meg, hogy a T 7.1.1 Tétel (ii) állítása a T 2.5.4 Tételből (illetve az arra adott bizonyításból) is következik.

7.1.6 A síkon hány rácspon tot tartalmazhat egy

(a) racionális;

(b) irracionális

meredekségű egyenes?
7.1.7 Adjuk meg a $6x + 10y + 15z = 7$ diofantikus egyenlet összes megoldását.

7.1.8 Igazoljuk a T 7.1.2 Tétel állításait.

7.1.9 Bizonyítsuk be, hogy az $a_1x_1 + \cdots + a_kx_k = c$ diofantikus egyenletnek akkor és csak akkor létezik megoldása, ha minden $m$ pozitív egész esetén megoldható az $a_1x_1 + \cdots + a_kx_k = c \pmod{m}$ kongruencia.

7.1.10 (*) Mely $a_1, \ldots, a_k$ egészek esetén igaz, hogy az $a_1x_1 + \cdots + a_kx_k = c$ diofantikus egyenletnek minden elég nagy $c$ esetén létezik pozitív egészekben megoldása?

7.1.11 (*) Legyenek $a$ és $b$ rögzített, relatív prim, 1-nél nagyobb egészek. Nevezzünk (házi használatra) egy $c$ pozitív egészét ($a$ -ból és $b$ -ből) „osszerakhatónak”, ha $c$ felírható $c = ax + by$ alakban, ahol $x$ és $y$ nemnegatív egészek.

(a) Mutassuk meg, hogy ha $c > ab - a - b$, akkor $c$ összerakható, azonban $c = ab - a - b$ nem összerakható.

(b) Hány nem összerakható pozitív egész létezik?

Megjegyzés: A feladat (a) részét több változóra a következőképpen általánosíthatjuk. Legyenek $a_1, \ldots, a_k$ relatív prim, 1-nél nagyobb egészek. Keressük azt a maximális $F = F(a_1, \ldots, a_k)$ egészit, amelyre az $a_1x_1 + \cdots + a_kx_k = F$ diofantikus egyenlet nem oldható meg nemnegatív egészekben. Ezt a kérdést Frobenius-problémának nevezzük. A $k > 2$ eset vizsgálata igen nehéz.

7.1.12 (*) (a) Mutassuk meg, hogy minden elég nagy $n$ esetén létezik $n$ darab olyan (nem feltétlenül egybevágó) kocka, amelyekből (mindegyiket egyszer felhasználva) összeállítható egy (nagyobb) kocka.

(b) Igazoljuk ugyanezit minden $n \geq 4 \cdot 5$-ra.

Megjegyzés: Megoldatlan probléma, hogy az állítás igaz-e $n = 47$ -tel is.

7.2 Pitagorasi számhármasok

Pitagorasi számhármasoknak az $x^2 + y^2 = z^2$ egyenlet pozitív egész megoldásait nevezzük. Geometriai megfogalmazásban a pitagorasi számhármasok azoknak a derékszögű háromszögeknek az oldalhosszait jelentik, amelyekben mindhárom oldal hossza egész szám.

Azonnal látszik, hogy az egyenlet megoldható (például a $3, 4, 5$ számhármas megoldás), sőt egy $x, y, z$ megoldást tetszőleges $d$ pozitív egészel beszorozva a kapott $dx, dy, dz$ számhármas is nyilván megoldás. Ezért külön érdemes azokat a megoldásokat vizsgálni, ahol $(x, y, z) = 1$, ezeket alapmegoldásoknak vagy primitív pitagorasi számhármasoknak nevezzük.

Megmutatjuk, hogy alapmegoldásból is végelen sok van, sőt elő tudjuk állítani az összes alapmegoldást és így az összes megoldást is alkalmas paraméterek segítségével:

7.2.1 Tétel. T 7.2.1

(i) Az

$$x^2 + y^2 = z^2 \quad (1)$$

egyenletnek az
feltételt kielégítő összes pozitív egész megoldását (azaz az alapmegoldásokat, vagy más néven a primitív pitagoraszi számhármasokat) a következő képlet szolgáltatja (itt az $x$ és $y$ felcseréléséből adódó megoldásokat azonosnak tekintjük):

$$x = 2mn, \quad y = m^2 - n^2, \quad z = m^2 + n^2,$$  \hspace{1cm} (3)

ahol az $m$ és $n$ paraméterek tetszőleges olyan pozitív egészek, amelyekre

$$m \text{ és } n \text{ kül/állózó paritású, } \quad m > n \quad \text{és} \quad (m, n) = 1.$$  \hspace{1cm} (4)

(ii) Az (1) egyenlet összes pozitív egész megoldását (azaz az összes pitagoraszi számhármast) az alapmegoldások többszöröseiként kapjuk meg, tehát

$$x = 2mn \cdot d, \quad y = (m^2 - n^2) \cdot d, \quad z = (m^2 + n^2) \cdot d,$$  \hspace{1cm} (5)

ahol $d$ tetszőleges pozitív egész, az $m$ és $n$ pozitív egészekre pedig teljesül (4).

$\blacklozenge$

\textit{Bizonyítás:} Végig valamennyi változó pozitív egész jelöl.

(i) Először azt mutatjuk meg, hogy ha $x$, $y$, $z$ alapmegoldás (azaz eleget tesz (1)-nek és (2)-nek), akkor $x$, $y$ és $z$ szükségképpen a (3)-ban és (4)-ben előírt alakban.

Első lépésként belátjuk, hogy $x$, $y$ és $z$ páronként is relatív primek. Nézzük például $\{x, z\}$ = 1-et, a másik két eset ugyanúgy igazolható. Tegyük fel indirekt, hogy egy $P$ prímre $P \mid x$ és $P \mid z$ fennáll. Ekkor ebből $P \mid \frac{x^2 - z^2}{y^2}$ és így $P$ prim volta miatt $P \nmid y$ következik. Ez azt jelenti, hogy $P$ közös osztója az $x$, $y$ és $z$ számoknak, ami ellentmond (2)-nek.

Most megmutatjuk, hogy $x$, $y$ és $z$ közül az egyik páros, a másik páratlan. Mindkettő nem lehet páros, hiszen $\{x, y\}$ = 1 . Ha mindkettő páratlan, akkor a négyzetük 1 maradékot ad 4-gyel osztva, vagyis $x^2 + y^2 = z^2$ bal oldala 2 maradékot ad 4-gyel osztva, a jobb oldal viszont 0-t vagy 1-et, ami ellentmondás.

Feltehetjük, hogy $x$ páros és $y$ páratlan. Ekkor (1)-et átrendezve, 4-gyel elosztva és szorzattá bontva az

$$\left( \frac{x}{2} \right)^2 - \frac{y}{2} \cdot \frac{z}{2} = \frac{z - y}{2},$$  \hspace{1cm} (6)

alakhoz jutunk.

Belátjuk, hogy a (6) jobb oldalán szereplő két ténylegő relatív prim. Tegyük fel, hogy $k$ közös osztója $(z + y)/2$-nek és $(z - y)/2$-nek. Ekkor

$$k \mid \frac{z + y}{2} = \frac{z - y}{2} = z \quad \text{és} \quad k \mid \frac{z + y}{2} = \frac{z - y}{2} = y.$$  \hspace{1cm} (7)

Mivel $\{y, z\} = 1$, ezért $k \mid 1$, tehát valóban

$$\left( \frac{z + y}{2} , \frac{z - y}{2} \right) = 1.$$  \hspace{1cm} (7)

221
Az 1.6.2a feladat [27] alapján (6)-ból és (7)-ből következik, hogy a (6) jobb oldalán szereplő két pozitív tényező külön-külön is négyzetszám, azaz alkalmas \( m \) és \( n \) pozitív egéssel

\[
\frac{z + y}{2} = mn^2 \quad \text{és} \quad \frac{z - y}{2} = n^2. \tag{8}
\]

A (8) egyenlőségeket összeadva, illetve kivonva, valamint (6)-ba visszahelyettesítve éppen a kívánt (3) előállítást kapjuk \( z \)-re, \( y \)-ra és \( x \)-re.

A (4) feltételek is teljesülnek; ezek rendre \( z \) (vagy \( y \)) páratlanságából, \( y > 0 \)-ból, illetve (7)-ből következnek.

Rátérve a megfordításra, most azt igazoljuk, hogy a (3)–(4) képlet mindig primitív pitagoraszi számhármast definiál.

Az így megadott \( x \), \( y \) és \( z \) számok az \( m > n > 0 \) feltétel miatt pozitív egészek, és egyszerű behelyettesítéssel ellenőrizhető, hogy kielégítik az (1) egyenletet.

Azt kell még megmutatni, hogy \( (x, y, z) = 1 \). Ehhez elég belátni, hogy (például) \( y \) és \( z \) relativ primek.

Tegyük fel indirekt, hogy van olyan \( p \) prim, amelyre \( p \mid y \) és \( p \mid z \). Ekkor \( p \mid z + y \) és \( p \mid z - y \) is teljesül, azaz

\[
p \mid (m^2 + n^2) + (m^2 - n^2) = 2m^2 \quad \text{és} \quad p \mid (m^2 + n^2) - (m^2 - n^2) = 2n^2. \tag{9}
\]

Mivel \( p \) prim, ezért (9)-ból következik, hogy \( p = 2 \), vagy \( p \mid m^2 \) és \( p \mid n^2 \).

A \( p = 2 \) eset nem lehetséges, mert \( m \) és \( n \) ellenkező paritása miatt \( z = m^2 - n^2 \) páratlan.

A másik esetben pedig (ismét felhasználva, hogy \( p \) prim) azt kapjuk, hogy \( p \mid mn \) és \( p \mid n \), ami ellentmond az \( (m, n) = 1 \) feltételnek.

(ii) Mint már említettük, egy alapmegoldást (vagy bármilyen megoldást) \( d \) -vel végigsorozva nyílvan ismét megoldást kapunk. Megfordítva, egy tetszőleges \( x, y, z \) megoldás előáll az \( x/d, y/d, z/d \) alapmegoldás \( d \) -szereseként, ahol \( d = (x, y, z) \).

Feladatok

7.2.1 Mutassuk meg, hogy ha egy derékszögű háromszög oldalai egész számok, akkor az oldalhosszak szorzata osztható 60-nal.

7.2.2 Számítsuk ki a derékszögű háromszög oldalait, ha tudjuk, hogy az oldalak egész számok és a háromszög területe 60.

7.2.3 Adjuk meg az összes olyan derékszögű háromszögöt, amelynek az oldalai egész számok és a kerület és terület mérőszáma megegyezik.

7.2.4 Mely \( k \) egészekre létezik olyan egész oldalú derékszögű háromszög, amelynek az egyik oldala \( k \)?

7.2.5 Mutassuk meg, hogy végten sok olyan háromtagú számjegy sorozat létezik, amelynek tagjai relatív primek és mindhárom elem négyzetszám.
7.3 Néhány elemi módszer

Az alábbiakban néhány tipikus módszert mutatunk be, amelyek gyakran alkalmazhatók diofantikus egyenletek vizsgálatánál.

1. „Szorzat = szám”

A 7.2.2 [222] és 7.2.3 feladatokhoz [222] fűzött két-két útmutatás mindegyikében a megoldás kulcsát egy-egy olyan diofantikus egyenlet szolgáltatta, ahol az egyik oldalon egy \( c \neq 0 \) egész szám, a másik oldalon pedig egy szorzat állt:

\[
d^2 : mn(m - n)(m + n) = 0, \quad (x - 4)(y - 4) = 8 \quad \text{stb.}
\]

Ilyen típusú szorzatú bontás segítségével most azt a problémát vizsgáljuk meg, hogy mely pozitív egészek állnak elő és hányféleképpen két négyzetszám különbségésként.

7.3.1 Tétel. \( T \) 7.3.1

Tekintsük az \( \omega^2 - \eta^2 = \nu \) diofantikus egyenletet, ahol \( \nu \) rögzített pozitív egész.

(i) Az egyenlet akkor és csak akkor oldható meg, ha \( \nu \equiv 2 \ (\text{mod} \ 4) \).

(ii) A megoldásszám \( 2d(\nu) \), ha \( \nu \) páratlan, és \( 2d(\nu) \), ha \( \nu \) páros, és \( 4 | \nu \) (ahol \( d(\nu) \) a \( \nu \) pozitív osztóinak a száma).

Bizonyítás: Az \( (x + y)(x - y) = \omega^2 \) egyenlőség pontosan akkor teljesül, ha \( x + y \) és \( x - y \) az \( \nu \) két komplementer osztója, azaz

\[
x + y = d_1, \quad x - y = d_2, \quad \text{ahol} \quad d_1d_2 = \nu. \quad \{1\}
\]

Az (1) egyenletrendszert megoldva

\[
x = \frac{d_1 + d_2}{2}, \quad y = \frac{d_1 - d_2}{2}
\]

adódik. Itt \( x \) -re és \( y \) -ra pontosan akkor kapunk egész értéket, ha \( d_1 \) és \( d_2 \) azonos paritású.

Ennek megfelelően az \( \omega^2 - \eta^2 = \nu \) diofantikus egyenlet akkor és csak akkor oldható meg, ha az \( \nu \) felirható két azonos paritású osztója szorzataként, a megoldások száma pedig az ilyen azonos paritású osztópárok száma (ahol a két osztó sorrendje is számít és a negatív osztókat is figyelembe kell venni).

Ha \( \nu \) páratlan, akkor minden osztója is páratlan, tehát minden osztópár megfelel. Ennek megfelelően (az egyenlet megoldható és) a megoldások száma az \( \nu \) összes (pozitív és negatív) osztóinak a száma, vagyis \( 2d(\nu) \).

Ha \( \nu \) páros, de nem osztható 4-gyel, akkor \( \nu \) nem írható fel két azonos paritású szám szorzataként, hiszen két páratlan szám szorzata páratlan, két páros szám szorzata pedig osztható 4-gyel. Ez azt jelenti, hogy az egyenlet ilyen \( \nu \) -ekre nem oldható meg.

Ha \( 4 | \nu \), akkor azok az osztópárok felelnek meg, amelyekben mindkét osztó páros szám:

\( \nu = (2k_1)(2k_2) \). Mivel ez ekvivalens az \( \nu/4 = k_1k_2 \) feltétellel, ezért (az egyenlet megoldható és) a megoldásszám az \( \nu/4 \) összes (pozitív és negatív) osztóinak a száma, vagyis \( 2d(\nu/4) \).
II. „Szorzat = hatvány”

A számelmélet alaptételéből következik, hogy ha egy \( k \)-adik hatvány két relatív prim tényező szorzata, akkor egységszorzóktól eltekintve a tényezők maguk is \( k \)-adik hatványok (lásd az 1.6.2 feladatot [27]). Ez a tény fontos szerepet játszott a T 7.2.1 Tétel bizonyításánál (lásd az ottani (6), (7) és (8) képleteket), valamint az 1.6.3 feladat [27] megoldásánál. A következő példával azt illusztráljuk, hogy ilyen típusú megondolások gyakran akkor is alkalmazhatók, ha a tényezők nem feltétlenül relatív primek.

Példa: Oldjuk meg az \( x^6 - 7x = y^3 \) diofantikus egyenletet.

Az \( x = y = 0 \) nyilván megoldás, továbbá ha \( x, y \) megoldás, akkor \( x, -y \) is az, ezért a továbbiakban feltehetjük, hogy \( x \) (és így \( y \)) pozitív.

Az egyenlet bal oldalát bontsuk szorzattá:

\[
x(x^2 + 7) = y^3,
\]

és vizsgáljuk meg a két tényező legnagyobb közös osztójának lehetséges értékeit. Legyen \( d = (x, x^2 + 7) \), ekkor

\[
d | (x^2 + 7) \cdot x = 7,
\]

azaz csak \( d - 1 \) és \( d = 7 \) jöhet szóba.

Ha \( d = 1 \), akkor \( x \) és \( x^2 + 7 \) külön-külön is köbszámok, azaz alkalmas \( u \) és \( v \) (pozitív) egészekkel

\[
x = u^3 \quad \text{és} \quad x^2 + 7 = v^3.
\]

A második egyenlőségben \( x \) helyére \( u^3 \)-t beírva

\[
v^3 - u^3 = 7
\]

adódik. Két pozitív köbszám különböse csak a \((8, 1)\) pár esetén lehet 7: ha \( a > b > 0 \), akkor

\[
u^3 - b^3 \geq (b - 1)^3 - b^3 = 3b^2 + 3b + 1 \geq 7,
\]

és egyenlőség csak a \( b = 1 \), \( a = b + 1 = 2 \) értékekre áll fenn. ( Másik indoklást: a

\[
7 = e^3 - b^3 = (e - b)(e^2 + eb + b^2)
\]

szorzat-előállításban a tényezők eleve csak \( \pm 1 \) és \( \pm 7 \) lehetnek megfelelő párosításban.)

(3) és (4) alapján így az \( x = 1 \), \( y = 2 \) megoldást kapjuk.

Nézzük most a \( d = 7 \) esetet. Ekkor \( 7 \mid x \) és \( x^3 \) alapján \( 7 \mid y^3 \), és így a 7 prim volta miatt \( 7 \mid y \) következik. Vizsgáljuk meg, hogy a 7 hányadik hatványával osztható (2) jobb oldala, illetve a bal oldal két tényezője. A jobb oldalon \( y^3 \)-ban a 7 kitevője legalább 3, ugyanakkor a bal oldal második tényezőjére (\( 7^2 \mid x^2 \) miatt) \( 7^2 \mid x^2 + 7 \). Ennél fogy a bal oldal első tényezőjében a 7 kitevője legalább 3 - 1 = 2, azaz szükségképpen \( 7^2 \mid x \).

A fentiekből adódó \( x = 7^2 \) és \( y = 7^6 \) összefüggéseket (2)-be beírva és \( 7^4 \)-nal egyszerűsíte azt kapjuk, hogy
Az (5) bal oldalán álló két tényező relatív prim, tehát külön-külön is köbszámok:

\[ r = u^3 \quad \text{és} \quad \tau^3 r^2 + 1 = \tau^3 u^6 + 1 - z^3. \]

Az utolsó egyenlőség szerint \( \tau^3 - (7\tau^2)^3 = 1 \), ez azonban nemnulla köbszámok esetén nem lehetséges.

Ez azt jelenti, hogy a \( d = 7 \) eset nem valósulhat meg.

Összefoglalva, az egyenletnek három megoldása van:

\[ x = y = 0; \quad x = 1, y = 2; \quad x = -1, y = -2. \]

Ugyanennél az egyenletnél egy másik eljárás is célhoz vezet, lásd alább a IV. módszert.

III. Megoldhatatlanság bizonyítása kongruencia segítségével

Ha egy diofantikus egyenlet esetén az egyenlet két oldala valamely alkalmaz modulus szerint sohasem lehet kongruens egymással, akkor az egyenlőség biztosan nem teljesülhet (ez fordított irányban nem igaz!).

Példa: Oldjuk meg az \( x^4 + 5y^4 = 4z^4 \) diofantikus egyenletet.

Az egyenletnek nyílván megoldása \( x = y = z = 0 \) . Megmutatjuk, hogy más megoldás nincs.

Tegyük fel indirekt, hogy létezik olyan megoldás, ahol \( x, y, z \) nem mindegyike 0. Ekkor azt is feltehetjük, hogy \( x = y = z = 0 \), és \( x, y, z \) relatív primek. Ha ugyanis \( \{x, y, z\} = d > 1 \), akkor az egyenlet \( d^4 \) -nel elosztva kapjuk, hogy \( x/d, y/d, z/d \) is megoldás, és ez a három szám már relatív prim is.

Mivel \( x^4 + 5y^4 = 4z^4 \), ezért

\[ x^4 + 5y^4 \equiv 4z^4 \pmod{5} \]  

is teljesül. A kis Fermat-tétel szerint bármely \( a \) egész számra

\[ a^4 = \begin{cases} 1 \pmod{5}, & \text{ha } 5 \nmid a; \\ 0 \pmod{5}, & \text{ha } 5 \mid a. \end{cases} \]

Ha \( 5 \nmid x \), akkor (7) alapján (6) bal oldala 1-gyel, a jobb oldal viszont 0-val vagy 4-gyel kongruens modulo 5, ami lehetetlen. Az \( 5 \nmid z \) eset ugyanígy ellentmondásra vezet. Ebből következik, hogy \( 5 \mid x \) és \( 5 \nmid z \).

Legyen \( x = 5x_1 \), \( z = 5z_1 \), ezt az eredeti egyenletbe beírva

\[ 5^4 x_1^4 + 5^4 y_1^4 = 4 \cdot 5^4 x_1^4, \quad \text{száz} \quad 5^5 x_1^4 + y_1^4 = 4 \cdot 5^3 z_1^4 \]

adódik. Ennél fogva \( 5 \nmid y_1 \), és így az 5 prim volta miatt \( 5 \nmid y_1 \) is teljesül. Ez azonban ellentmond az \( \{x, y, z\} = 1 \) feltételnek.

Megjegyzések: 1. A fenti egyenletet modulo 5 helyett modulo 16 vizsgálva is hasonló módon ellentmondásra juthatunk.
2. Általában olyan modulussal érdemes próbálkozni, amely osztója az egyenlet valamelyik együtthatójának vagy amelyre nézve az egyenletben előforduló hatványok kevés maradékosztályba eshetnek csak. Például a négyzeteszámok 8-cal osztva csak 0, 1 vagy 4, a negyedik hatványok 16-tal osztva csak 0 vagy 1 maradékon adhatnak, ezért gyakran érdemes modulusrnak a 8-at, illetve a 16-at választani.

3. Ha valamilyen modulus esetén nem jutunk ellentmondásra, ez csak annyit jelent, hogy a megfelelő kongruencia megoldható, ebből azonban nem következik, hogy az egyenletnek is van megoldása (és persze az sem következik, hogy az egyenletnek nincs megoldása). Például a fenti egyenletnél az \( m = 3 \) vagy az \( m = 7 \) modulus nem segített volna, hiszen az \( x^4 + 5y^4 \equiv 4z^4 \pmod{3} \), illetve \( (m \equiv 7 \pmod{7}) \) kongruenciának létezik nemtrivialis megoldása:

\[(\pm 1)^4 + 5(\pm 1)^4 \equiv 4 \cdot 3^4 \pmod{3}, \quad \text{és} \quad (\pm 1)^4 + 5(\pm 2)^4 \equiv 4 \cdot 1^4 \pmod{7}.
\]

4. Még egyszer hangsúlyozzuk, hogy ez a módszer lényegében csak akkor vezethet (önmagában) eredményre, ha a diofantikus egyenletnek nincs megoldása, illetve csak „trivialis” megoldása van (mint a fenti egyenletnél \( x = y = z = 0 \)). Ha ugyanis létezik az egyenletnek (nemtrivialis) megoldása, akkor az tetszőleges \( m \) modulus esetén kielégíti a megfelelő kongruenciát is, tehát egyetlen modulussal sem jutunk ellentmondásra. (Az természetesen igaz, hogy az ilyen jellegű kongruenciás megfontolások bármely diofantikus egyenlet esetén segíthetnünk bizonyos típusú megoldások kizárásában.)

5. A diofantikus egyenlet megoldhatatlansága esetén sem biztos, hogy ez a módszer célhoz vezet. Egyrészt nem biztos, hogy rátalálunk egy olyan modulusra, amely kihozza a keresett ellentmondást, másrészt lehet, hogy nincs is ilyen modulus: a 4.2.8 feladatban [109] láttuk, hogy van olyan egyenlet, amelynek nincs egész vagy racionális megoldása, ugyanakkor a megfelelő kongruencia bármely \( m \) modulus esetén megoldható.

IV. Egyenlőtlenségek alkalmazása

Tekintsünk egy \( f(x) = x^k \) típusú diofantikus egyenletet. Ha van olyan \( c \), hogy minden \( c \)-nél nagyobb abszolút értékű \( x \) egész számra az \( f(x) \) két egymást követő \( k \)-adik hatvány közé esik (az egyenlőséget nem megengedve), akkor világos, hogy csak olyan megoldások jöhetnek szóba, ahol \( |x| \leq c \). Az így megmaradt véges sok \( x \)-et végigpróbálva megkaphatjuk az egyenlet összes megoldását.

Az eljárást a (II. módszerrel már vizsgált) \( x^3 + 7x = y^4 \) diofantikus egyenleten mutatjuk be.

Mint láttuk, elegendő az \( x > 0 \) esetre szorítkozni, továbbá \( x = 1 \), \( y = 2 \) megoldás.

Egyszerű számolással adódik, hogy ha \( x > 1 \), akkor

\[x^3 < x^5 + 7x < (x + 1)^3,
\]

teját \( x > 1 \) esetén \( x^3 + 7x \) nem lehet köbszám.

Mindezek alapján az egyenlet összes megoldása a II. módszernél megadott három számpár.

Feladatok

7.3.1 Legyen \( n \) rögzített pozitív egész. Hány „lényegesen különböző módon” írható fel az \( n \) két négyzeteszám különbségéként, azaz hány megoldása van az \( x^2 - y^2 = n \) egyenletnek a nemnegatív egészek körében?
7.3.2 Egy háziasszony egy tepsi süteményt úgy akar (egyforma téglalap alakú darabokra) felvágni,
hogy ugyanannyi „égett”, azaz a tepsi falával legalább egy oldalon érintkező, mint „nem égett”, azaz
a tepsi falával nem érintkező szelet keletkezzen. Hogyan végezze a szeletelést?

7.3.3 Ottlik Géza, a kiváló prózairó, matematikai tanulmányokat is folytatott. Ezzel kapcsolatos
visszaemlékezéseiben szerepel az alábbi feladat: Bizonyítsuk be, hogy bármely \( p > 2 \) prim esetén a
\( \frac{2}{p} \) szám pontosan egyféle példája van, amely egyszerűen írható fel két különböző pozitív egész reciprokának összegeként.
(Az összeadandók sorrendjére nem vagyunk tekintettel.)

7.3.4 (*) Mely 4 számlálójú törteket írható fel két természetes szám reciprokának az összegeként?

7.3.5 Mutassuk meg, hogy ha az \( n \) pozitív egész nem \( 24k + 1 \) alakú, akkor \( \frac{n}{n} \) felírható három
természetes szám reciprokának az összegeként.

Megjegyzés: Erdős és Straus egy nevezetes, máig bizonyítatlan sejtése szerint minden \( n \) pozitív egészendelkezik a fenti tulajdonsággal.

7.3.6 Bizonyítsuk be, hogy minden pozitív racionális szám végten sokféle képen áll elő véges sok
különböző pozitív egész reciprokának az összegeként.

Megjegyzés: A pozitív egészket reciprokait, azaz az \( 1 \) számú törtöket és \( \frac{1}{n} \) törtéket
egyiptomi törtnek nevezzük, mert az ókori Egyiptomban a racionális számokat általában ilyen tört
összegeként írták fel.

7.3.7 Van-e olyan negyedik hatvány, amely 4-gyel nagyobb egy ötödik hatványnál?

7.3.8 (M [591]) Adjuk meg az alábbi egyenletrendszer összes olyan megoldását, ahol \( x, y, z, s \)
ezt \( t \) racionális számok:

\[
t^2 + (s + z)^2 = s^2 + y^2 = (y + t)^2 + x^2.
\]

7.3.9 Bizonyítsuk be, hogy 99 egymást követő négyzetes szám összege nem lehet teljes hatvány.

7.3.10 (M [591]) Adjuk meg az összes olyan egész számot, amelynek a köbe előáll nyolc
szomszédos egész szám köbének az összegeként.

7.3.11 (*) Bizonyítsuk be, hogy 6 egymást követő természetes szám nem osztható két (diszjunkt)
csoportba úgy, hogy az egyik csoport elemeinek a szorzata megegyezzen a másik csoport elemeinek
a szorzatával. Igazoljuk ugyanezt az állítást 6 helyett 106-ra is.

7.3.12 Adott \( n \) pozitív egészhez adjuk meg az összes olyan \( n, n, \cdots, n \) pozitív egész, amelyre

\[
(t_1, m_1) = 1 \quad \text{és} \quad (x^2 - y^2)^m = (x^2)^n.
\]

7.3.13 Adjuk meg a következő diofantikus egyenleteket:

(a) \( xy + 3x + 5y = 7 \);

(b) \( x^2 - 2y^2 + 363z^2 = 77 \);

(c) \( 2x^2 + 3y^2 = z^2 \);

(d) \( x^2 - 230y^2 = 7z^2 \);

(e) \( x^5 + 3y^5 = 5z^5 \);

(f) \( (x^2 - 7)(y^2 + 7) = z^3 \).
7.3.14 Milyen alapú számrendszerekben igaz, hogy az alábbi alakú számok négyzetszámok?
(a) 111;
(b) 11111;
(c) 111111.
(A „kimaradt” 1111-re vonatkozóan lásd a 7.7.7 feladatot [256].)

7.4 Gauss-egészek

A T 7.3.1 Tételben pontos választ adtunk arra, mely pozitív egészek állnak elő és hányféleképpen két négyzetszám különségévéként. Most azt a rokon kérdést vetjük fel, hogy mi a helyzet különség helyett összegre, azaz mely pozitív egészek állnak elő és hányféleképpen két négyzetszám összegeként.

Az diofantikus egyenlet megoldásánál a bal oldal szorzattá bontása volt a kulcslépés. Az \( z^2 - y^2 = n \) esetben ilyen szorzattá bontás az egész (vagy akár valós) számok keretén belül maradva nem létezik, azonban a komplex számok körében már igen: \( \sqrt[2]{a} + \sqrt[2]{b} \) komplex számok szármelletének a kiépítése, ahol \( a \) és \( b \) egész számok. Az ilyen komplex számokat nevezzük Gauss-egészeknek.

Az egész számok mintájára a Gauss-egészek körében is definiáljuk a megfelelő számelméleti fogalmakat (oszthatóság, egység, legnagyobb közös osztó, felbonthatlan, prim), majd megmutatjuk, hogy a Gauss-egészekre is érvényes a számelmélet alaptétele, ezután pedig az összes Gauss-felbonthatlan „áttekinthetése” következik. Mindezek birtokában a következő pontban visszatérünk majd a kiindulási problémánkról, az \( z^2 + y^2 = n \) diofantikus egyenletre.

7.4.1 Definíció .

Gauss-egészeknek azokat az \( \alpha = a + bi \) komplex számokat nevezzük, ahol \( a \) és \( b \) egész szám. ♠

Az egyértelmű megkülönböztetés érdekében ebben a pontban az egész számokat latin betűkkel, míg a Gauss-egészeket görög betűkkel jelöljük.

A Gauss-egészek a komplex számok összeadására és szorzására kommutatív, egységelemes, nullosztómentes gyűrűt alkotnak.

A Gauss-egészek szármelletévi vizsgálatánál kulcsszerepet játszik a norma fogalma:

7.4.2 Definíció .

Az \( \alpha = a + bi \) Gauss-egész normájának nevezzük és \( N(\alpha) \)-val jelöljük az \( \alpha \) abszolút értékének négyzetét:

\[
N(\alpha) = |\alpha|^2 = a^2 + b^2. ♠
\]

A Gauss-egészek definiciójából és a komplex számok abszolút értékének tulajdonságaiiból azonnal adódnak az alábbi egyszerű, de fontos állítások:
7.4.3 Tétel. T 7.4.3
Tetszőleges $\alpha$, $\beta$ Gauss-egészek esetén

(i) $N(\alpha^2)$ nemnegatív egész szám;
(ii) $N(\alpha) = 0 \iff \alpha = 0$,
(iii) $N(\alpha\beta) = N(\alpha)N(\beta)$.

A Gauss-egészek szármeléletének kiépítéséhez az egész számokra az 1. fejezetben látott utat követjük: a fogalmak definiálása és a szármelélet alapfeltételeinek bizonyítása az ottani mintára történik. Egyedül a maradékos osztás tételének a Gauss-egészekre vonatkozó megfelelője (7.4.8 Tétel) mutat komolyabb formai eltérést, ettől eltekintve szinte „lemásoljuk” az egész számoknál szereplő felépítést.

7.4.4 Definíció. D 7.4.4
A $\beta$ Gauss-egész az $\alpha$ Gauss-egész osztójának nevezzük, ha létezik olyan $\gamma$ Gauss-egész, amelyre $\alpha = \beta \gamma$.

Akárcsak az egész számoknál, ugyanazt jelenti az „$\alpha$ osztható $\beta$-val”, illetve az „$\alpha$ többszöröse a $\beta$-nak” kifejezés is, és a Gauss-egészeknél is a $\beta | \alpha$ jelölést használjuk.

7.4.5 Tétel. T 7.4.5
Ha $\beta | \alpha$ (a Gauss-egészek körében), akkor $N(\beta) | N(\alpha)$ (az egész számok körében).

Bizonyítás: Az állítás a D 7.4.4 Definícióból és a T 7.4.3/(iii) Tételből következik.

A T 7.4.5 Tétel megfordítása nem igaz, amint azt a tétel fölött megadott második példa is mutatja.

7.4.6 Definíció. D 7.4.6
Az $\varepsilon$ Gauss-egész egység, ha minden Gauss-egésznek osztója.

Az egységek sokféle ekvivalens jellemzéséről szól a következő tétel:

7.4.7 Tétel. T 7.4.7
Egy $\varepsilon$ Gauss-egészre az alábbi feltételek ekvivalensek:

(i) $\varepsilon$ egység.
(ii) $\varepsilon | 1$.
(iii) \( N(\varepsilon) = 1 \).

(iv) \( \varepsilon = 1, -1, i \) vagy \( -i \).

\textbf{Bizonyítás:} (i) \( \implies \) (ii): Ha \( \varepsilon \) minden Gauss-egésznek osztója, akkor speciálisan az 1-nek is osztója.

(ii) \( \implies \) (iii): A T 7.4.5 Tételből következik.

(iii) \( \implies \) (iv): A \( N(a + bi) = a^2 + b^2 = 1 \) egyenlőség egész \( \alpha \), \( \beta \) mellett csak \( a = \pm 1, b = 0 \), illetve \( a = 0, b = \pm 1 \) esetén teljesülhet.

(iv) \( \implies \) (i): Bármely \( \alpha \) Gauss-egészre

\[ \alpha = 1\alpha - (1)(-\varepsilon) = i(-i\alpha) = (-i)(i\alpha). \]

Most rátérünk a maradékos osztás Gauss-egészekbeli megfelelőjére:

\textbf{7.4.8 Tétel}.

Tetszőleges \( \alpha \) és \( \beta \neq 0 \) Gauss-egészekhez léteznek olyan \( \gamma \) és \( \ell \) Gauss-egészek, melyekre

\[ \alpha = \beta \gamma + \varrho \quad \text{és} \quad N(\varrho) < N(\beta). \]  

(1)

\textbf{Bizonyítás:} Az (1) feltétel ekvivalens

\[ \frac{\alpha}{\beta} - \gamma = \frac{\varrho}{\beta} \quad \text{és} \quad |\varrho| < |\beta|, \quad \text{azaz} \quad |\varrho| < 1 \]

teljesülésével. Ez azt jelenti, hogy olyan \( \gamma \) Gauss-egész kell keressi, amelyre

\[ \left| \frac{\alpha}{\beta} - \gamma \right| < 1. \]  

(2)

A Gauss-egészek a komplex számsikon a szokásos egyséngyűjthetőségek esetében is teljesülnek. A (2) feltétel így megfelel \( \gamma \) és \( \ell \) Gauss-egészekhez léteznek olyan \( \gamma \) és \( \ell \) Gauss-egészek, melyekre

\[ \alpha = \beta \gamma + \varrho \quad \text{és} \quad N(\varrho) < N(\beta). \]

(1)

\textbf{Bizonyítás:} Az (1) feltétel ekvivalens

\[ \frac{\alpha}{\beta} - \gamma = \frac{\varrho}{\beta} \quad \text{és} \quad |\varrho| < |\beta|, \quad \text{azaz} \quad |\varrho| < 1 \]

teljesülésével. Ez azt jelenti, hogy olyan \( \gamma \) Gauss-egész kell keressi, amelyre

\[ \left| \frac{\alpha}{\beta} - \gamma \right| < 1. \]  

(2)

A Gauss-egészek a komplex számsikon a szokásos egyséngyűjthetőségek esetében is teljesülnek. A (2) feltétel így megfelel \( \gamma \) és \( \ell \) Gauss-egészekhez léteznek olyan \( \gamma \) és \( \ell \) Gauss-egészek, melyekre

\[ \alpha = \beta \gamma + \varrho \quad \text{és} \quad N(\varrho) < N(\beta). \]

(1)

\textbf{Bizonyítás:} Az (1) feltétel ekvivalens

\[ \frac{\alpha}{\beta} - \gamma = \frac{\varrho}{\beta} \quad \text{és} \quad |\varrho| < |\beta|, \quad \text{azaz} \quad |\varrho| < 1 \]

teljesülésével. Ez azt jelenti, hogy olyan \( \gamma \) Gauss-egész kell keressi, amelyre

\[ \left| \frac{\alpha}{\beta} - \gamma \right| < 1. \]  

(2)

A Gauss-egészek a komplex számsikon a szokásos egyséngyűjthetőségek esetében is teljesülnek. A (2) feltétel így megfelel \( \gamma \) és \( \ell \) Gauss-egészekhez léteznek olyan \( \gamma \) és \( \ell \) Gauss-egészek, melyekre

\[ \alpha = \beta \gamma + \varrho \quad \text{és} \quad N(\varrho) < N(\beta). \]

(1)

\textbf{Bizonyítás:} Az (1) feltétel ekvivalens

\[ \frac{\alpha}{\beta} - \gamma = \frac{\varrho}{\beta} \quad \text{és} \quad |\varrho| < |\beta|, \quad \text{azaz} \quad |\varrho| < 1 \]

teljesülésével. Ez azt jelenti, hogy olyan \( \gamma \) Gauss-egész kell keressi, amelyre

\[ \left| \frac{\alpha}{\beta} - \gamma \right| < 1. \]  

(2)

A Gauss-egészek a komplex számsikon a szokásos egyséngyűjthetőségek esetében is teljesülnek. A (2) feltétel így megfelel \( \gamma \) és \( \ell \) Gauss-egészekhez léteznek olyan \( \gamma \) és \( \ell \) Gauss-egészek, melyekre

\[ \alpha = \beta \gamma + \varrho \quad \text{és} \quad N(\varrho) < N(\beta). \]

(1)

\textbf{Bizonyítás:} Az (1) feltétel ekvivalens

\[ \frac{\alpha}{\beta} - \gamma = \frac{\varrho}{\beta} \quad \text{és} \quad |\varrho| < |\beta|, \quad \text{azaz} \quad |\varrho| < 1 \]

teljesülésével. Ez azt jelenti, hogy olyan \( \gamma \) Gauss-egész kell keressi, amelyre

\[ \left| \frac{\alpha}{\beta} - \gamma \right| < 1. \]  

(2)
A Gauss-egészeknél a legnagyobb közös osztó fogalmát eleve a kitüntetett közös osztó mintájára értelmezzük: olyan közös osztó, amely minden közös osztónak többszöröse.

7.4.9 Definíció . D 7.4.9

Az $\alpha$ és $\beta$ Gauss-egészek legnagyobb közös osztója $\delta$, ha

(i) $\delta \mid \alpha \beta$ ; és

(ii) ha egy $\gamma$ -ra $\gamma \mid \alpha \beta$ teljesül, akkor $\gamma \mid \delta$.♦

Most is feltesszük, hogy $\alpha$ és $\beta$ közül legalább az egyik nem nulla.

A legnagyobb közös osztó létezése az T 1.3.3 Tétel bizonyításához hasonlóan az euklideszi algoritmustól következik (az eljárás a Gauss-egészeknél is véges sok lépésben befejeződik, hiszen a maradékok normái nemnegatív egészek és szigorúan csökkenő sorozatot alkotnak). Az euklideszi algoritmus a legnagyobb közös osztó gyakorlati meghatározására is alkalmas.

A legnagyobb közös egységszerestől eltekintve egyértelmű, azaz ha $\delta$ az $\alpha$ és $\beta$ Gauss-egészek egyik legnagyobb közös osztója, akkor az összes legnagyobb közös osztót a $\delta$ egységszeresei adják. (Ez a legnagyobb közös osztó definíciójából következik.)

Mindezek alapján bármely két Gauss-egésznak (amelyek közül legalább az egyik nem nulla) pontosan négy legnagyobb közös osztója van. Mivel ezek oszthatósági szempontból teljesen egyformán viselkednek, valamint egyikük előtérbe helyezését sem támasztja alá olyan természetes kiválasztási elv, mint az egész számoknál a pozitivitás, ezért közöttük semmilyen formában nem teszünk különbséget, és az $\{\alpha, \beta\}$ jelölés közülük akármelyiket jelentheti.

A legnagyobb közös osztóra vonatkozó, az 1.3 pontban szereplő további tételek és definíciók megfelelői a Gauss-egészek körében is ugyanúgy érvényesek.

Most a Gauss-felbonthatatlan és a Gauss-prím fogalmát definiáljuk az D 1.4.1, illetve D 1.4.2 Definíciók mintájára.

7.4.10 Definíció . D 7.4.10

A $\pi$ egységtől (és nullától) különböző Gauss-egészt Gauss-felbonthatatlannak nevezzük, ha csak úgy bontható fel két Gauss-egész szorzatára, hogy valamelyik tényező egység. Azaz

$$\pi = \alpha \beta \implies \alpha \text{ vagy } \beta \text{ egység.}$$

7.4.11 Definíció . D 7.4.11

A $\pi$ egységtől és nullától különböző Gauss-egészt Gauss-prímnak nevezzük, ha úgy lehet osztója két Gauss-egész szorzatának, hogy legalább az egyik tényezőnek osztója. Azaz

$$\pi \mid \alpha \beta \implies \pi \mid \alpha \text{ vagy } \pi \mid \beta.$$

A Gauss-egészek körében is érvényes az T 1.4.3 Tétel megfelelője, és az arra adott bizonyítás is szó szerint átvihető:

7.4.12 Tétel . T 7.4.12

Egy Gauss-egész pontosan akkor Gauss-prím, ha Gauss-felbonthatatlan.
A továbbiakban ennek megfelelően általában a Gauss-felbonthatatlan helyett is a (rövidebb) Gauss-prím elnevezést fogjuk használni.

Most már minden készen áll az T 1.5.1 Tétel megfelelőjének a kimondásához és bizonyításához:

**7.4.13 Tétel (A szákmelélet alaptétele)**  

Minden, a 0-tól és egységektől különböző Gauss-egész felbontható véges sok Gauss-felbonthatatlan szorzatára, és ez a felbontás a tényezők sorrendjétől és egységszeresektől eltekintve egyértelmű. 

**Bizonyítás:** Az egyértelműségre az egész számoknál adott első bizonyítás szó szerint átvihető a Gauss-egészekre is (a második bizonyítás megfelelőjére nézve lásd a 7.4.11 feladatot [235]).

A felbonthatóság bizonyításához is lényegében az egész számoknál szereplő gondolatmenetet alkalmazhatjuk, azzal a két apró módosítással, hogy „a legkisebb pozitív nemtriviális osztója” helyett „a(kármelyik) legkisebb normájú nemtriviális osztója”, illetve \(a_i\) helyett \(N(a_i)\) veendő. A részletek végigondolását az Olvasóra bízzuk. 

**Megjegyzés:** Összefoglalva megállapíthatjuk, hogy az egész számoknál és a Gauss-egészeknél szinte azonos módon jutottunk el a szákmelélet alaptételéhez. A felbonthatóság bizonyítása mindkét számkörben közvetlenül történt (hasonló gondolatmenettel), az egyértelműség bizonyításához vezető út lépései pedig a következők voltak:

Maradékos osztás \(\Rightarrow\) létezik legnagyobb közös osztó (a „kitüntetett” értelemben) \(\Rightarrow\) minden felbonthatatlan egyben prim is \(\Rightarrow\) a szákmelélet alaptételének az egyértelműségi része.

Később megmutatjuk, hogy a (megfelelő értelemben vett) maradékos osztás elvégezhetőségéből mindig következik a szákmelélet alaptétele, de ez fordítva nem igaz (lásd a 11.3 pontot).

A továbbiakban célunk az összes Gauss-prím jellemzése, áttekintése. Ennek előkészítéseként kapcsolatot keresünk a Gauss-prímek és a (\(\mathbb{Z}\)-beli) prímszámok között:

**7.4.14 Tétel**  

(i) Minden \(\pi\) Gauss-prímhez pontosan egy olyan \(P\) pozitív prímszám létezik, amelyre \(\pi \mid P\).

(ii) Minden \(P\) pozitív prímszám vagy maga is Gauss-prím, vagy pedig pontosan két Gauss-prímnek a szorzata, amelyek normája \(P\), és amelyek egymás konjugáltjai.

**Bizonyítás:** (i) Mivel \(\pi \neq 0\) és \(\pi\) nem egység, ezért \(N(\pi) > 1\), és így \(N(\pi)\) felbontható pozitív prímszámok szorzatára: \(N(\pi) = p_1 p_2 \cdots p_r\). Ekkor \(\pi \mid \pi \pi = N(\pi) = p_1 p_2 \cdots p_r\), továbbá \(\pi\) Gauss-prím, tehát \(\pi\) szükségképpen osztója valamelyik \(P_i\)-nek is.

Az egyértelműség igazolásához tegyük fel indirekt, hogy \(\varpi \neq \varrho\) olyan pozitív prímszámok, amelyekre \(\pi \mid \varpi\) és \(\pi \mid \varrho\). Mivel \(P\) és \(Q\) (az egész számok körében) relatív primek, ezért alkalmas \(\mu\) és \(\nu\) egész számmakat \(1 = \varpi \mu + \varrho \nu\) teljesül. Ekkor \(\pi \mid \varpi\) és \(\pi \mid \varrho\) miatt \(\pi \mid \varpi \mu + \varrho \nu\), azaz \(\pi \mid 1\) is fennáll, ami ellentmondás.

(ii) Ha a \(P > 0\) prímszám nem Gauss-prím, akkor (a szákmelélet alaptétele szerint) felírható legalább két Gauss-prím szorzataként:

\[
p = \pi_1 \cdots \pi_t, \quad \text{ahol} \quad t \geq 2.
\]
A normákra áttérve, (3)-ból
\[ p^2 = N(p) = N(\pi_1) \cdots N(\pi_s) \]
következik. Mivel \( \pi_i \) nem egység, ezért \( N(\pi_i) > 1 \). A \( p^2 \) azonban csak egyféleképpen bontható 1-nél nagyobb egész számok szorzatára: \( p^2 = p \cdot p \). Ebből következik, hogy (4), és így (3) jobb oldalán is csak két tényező szerepelhet:
\[ p = \pi_1 \pi_2, \quad \text{ahol} \quad N(\pi_1) = N(\pi_2) = p. \]
Végül a
\[ p = \pi_1 \pi_2 \quad \text{és} \quad p = N(\pi_1) = \pi_1 \pi_1 \]
egyenlőségekből kapjuk, hogy \( \pi_2 = \overline{\pi_1} \).

És most lássuk a Gauss-prímek „listáját”:

7.4.15 Tétel

Az alábbi Gauss-egészek adják az összes Gauss-prímet (c tetszőleges egységet jelöl):

(A) \( \varepsilon(1 + i) \);

(B) \( \varepsilon q \), ahol \( q \) pozitív \( 4k - 1 \) alakú prímszám;

(C) \( \pi \), ahol \( N(\pi) \) egy pozitív \( 4k + 1 \) alakú prímszám; minden ilyen prímszámhoz egység szerinti eltekintve két Gauss-prím tartozik, amelyek egymás konjugáltai, de nem egymás egység szeresei.

Példák:

A \( 1 + i = \varepsilon(1 + i) \) és \( -7i \) Gauss-primek.

Szintén Gauss-prím a \( 2 - 5i \), mert \( (2 - 5i)(2 + 5i) = 29 \), és a 29 egy \( 4k + 1 \) alakú pozitív prímszám.

A \( 2 + 5i \) is Gauss-prím, amely nem egység szerese a \( 2 - 5i \)-nek.

A \( 29 = (5 - 2i)(5 + 2i) \) felbontás tényezői viszont (a számlítmény alaptétele szerint) már csak az előzők egység szeresei lehetnek, és valóban \( 5 - 2i = \varepsilon(2 + 5i) \), illetve \( 5 - 2i = -\varepsilon(2 - 5i) \).

Nem Gauss-prím a \( -37 \), mert a 37 (ugyan prímszám, de) nem \( 4k - 1 \) alakú.

A \( 9 + 2i \) sem Gauss-prím, mert \( (9 + 2i)(9 - 2i) = 85 \) nem prímszám.

Bizonyítás: A T 7.4.14 Tétel szerint az összes Gauss-prímet a pozitív prímszámoknak a Gauss-prímek szorzatára történő felbontásaiból kaphatjuk meg. Más és más típusú felbontást kapunk attól függően, hogy ez a pozitív prímszám (A) a 2; (B) \( 4k - 1 \) alakú; illetve (C) \( 4k + 1 \) alakú.

(A) Mivel \( 2 - (1 + i)(1 - i) = -(\varepsilon(1 + i))^2 \), ezért a 2-nek egység szerestől eltekintve egyetlen Gauss-prím osztója van, az \( 1 + i \).

(B) Legyen \( q \) pozitív \( 4k - 1 \) alakú prímszám. Tegyük fel indirekt, hogy \( q \) nem Gauss-prím. Ekkor a T 7.4.14 Tétel (ii) állítása szerint van olyan \( \pi = a + bi \) Gauss-prím, amelyre \( q = N(\pi) = a^2 + b^2 \).

Ez azonban lehetetlen, mert két négyzetszám összege nem lehet \( 4k - 1 \) alakú.
(C) Legyen \( P \) pozitív \( 4k + 1 \) alakú primszám. Először azt igazoljuk, hogy \( P \) nem Gauss-prím.

A T 4.1.4 Tétel szerint az \( x^2 \equiv -1 \ (\text{mod } P) \) kongruencia megoldható, azaz létezik olyan \( c \) egész szám, amelyre \( P \mid c^2 + 1 \). Ennek megfelelően a \( P \) a Gauss-egészek körében osztója a \((c + i)(c - i)\) szorzatnak. Ugyanakkor

\[
\frac{c \pm i}{P} = \frac{c \pm \frac{1}{P} \cdot i}{P}
\]

nem Gauss-egészek (mert például a képzetes részük nem egész szám), tehát a \( c + i \) és \( c - i \) tényezők egyike sem osztható \( P \) -vel. Ebből (a Gauss-prím definíciója szerint) következik, hogy a \( P \) nem Gauss-prím.

A T 7.4.14 Tétel alapján ekkor \( P = \pi \mathfrak{P} \), ahol \( \pi \) és \( \mathfrak{P} \) Gauss-primek. A szármetszet alaptétele szerint a \( P \) -nek egységszeresektől eltekintve ez az egyetlen felbontása Gauss-primek szorzatára, így már csak azt kell igazolnunk, hogy \( \pi \neq \mathfrak{P} \), ahol \( \varepsilon \) egység. Ez egyszerű számolással adódik a \( \pi = c + b\mathfrak{P} \) alakból az \( \varepsilon = 1 \), \(-1\), \( i \) és \(-i\) esetek végigpróbálásával (valamint következik a 7.4.3 feladatból [234] is). 

**Feladatok**

( \( \alpha, \beta, c + b\mathfrak{P} \) stb. végig Gauss-egész jelölnek.)

7.4.1 Mely Gauss-egészek oszthatók \( 1 \rightarrow i \)-vel?

7.4.2 Igazoljuk az alábbi állításokat:

(a) \( \gamma \mid \alpha \iff \gamma \mid \bar{\alpha} \);

(b) \( (\alpha, \gamma) = (\bar{\alpha}, \gamma) \);

(c) \( \alpha \) Gauss-prím \( \iff \bar{\alpha} \) Gauss-prím.

7.4.3 Legyen \( \alpha = a + b\mathfrak{P} \). Mutassuk meg, hogy

\[
\alpha \mid \bar{\alpha} \iff |a| = |b| \text{ vagy } ab = 0.
\]

7.4.4 Ha \( a \) és \( b \neq 0 \) két egész szám, akkor a \( b \mid c \) oszthatóságánál, illetve az \( (a, b) \) legnagyobb közös osztónál tulajdonképpen meg kellene mondani, hogy \( a \cdot t \) és \( b \cdot t \) most egész számoknak vagy pedig Gauss-egészeknek tekintjük. Bizonyítsuk be, hogy ez a megkülönböztetés fölösleges:

(a) \( b \mid c \) pontosan akkor igaz a Gauss-egészek körében, ha \( \mathbb{Z} \)-ben igaz;

(b) az \( a \) és \( b \) számok \( \mathbb{Z} \)-beli legnagyobb közös osztója (egységszerestől eltekintve) megegyezik a Gauss-egészek körében vett legnagyobb közös osztóval.

7.4.5 Melyek igazak az alábbi állítások közül?

(a) \( (N(\alpha), N(\beta)) = 1 \implies (\alpha, \beta) = 1 \).

(b) \( (\alpha, \beta) = 1 \implies (N(\alpha), N(\beta)) = 1 \).

(c) \( (\alpha, \beta) = (\alpha, \beta) = 1 \implies (N(\alpha), N(\beta)) = 1 \).
7.4.6 Számítsuk ki $\alpha$ és $\beta$ legnagyobb közös osztóját, ahol

(a) $\alpha = 8 + i$ és $\beta = 11 - 3i$ ;

(b) $\alpha = 3(1 - i)^3$ és $\beta = 6(2 + i)^3$ ;

(c) $\alpha = (4 + i)^{10} + (2 + i)^{11}$ és $\beta = (4 + i)^{10} - (2 + i)^{11}$ .

7.4.7 Legyen $\alpha = a + bi$ .

(a) Melyek igazak az alábbi állítások közül?

(a1) $\langle a, b \rangle = 1 \implies (a, b) = 1$.

(a2) $\langle a, b \rangle = 1 \implies (\alpha, \overline{\alpha}) = 1$.

(b) Milyen kapcsolatban áll egyegyással általában $\langle \alpha, \beta \rangle$ és $(a, b)$ ?

7.4.8 Nevezzük az $\alpha$ és $\beta$ Gauss-egészeket barátoknak, ha relatív primek, és egy („közönséges”) egész szám pontosan akkor többszöröse $\alpha$ -nak, amikor $\beta$ -nak.

(a) Bizonyítsuk be, hogy $a + bi$ -nek akkor és csak akkor létezik barátja, ha $(a, b) = 1$ és $a \neq b \mod 2$ .

(b) Hány barátja van $a + bi$ -nek ebben az esetben?

7.4.9 Bontsuk fel a $270 + 2513i$ Gauss-egész Gauss-prímek szorzatára.

7.4.10 Melyek igazak az alábbi állítások közül?

(a) Ha $\alpha$ Gauss-prím, akkor $N(\alpha)$ prímszám.

(b) Ha $N(\alpha)$ prímszám, akkor $\alpha$ Gauss-prím.

(c) Ha $\alpha$ egy Gauss-egész köbe, akkor $N(\alpha)$ egy nemnegatív egész szám köbe.

(d) Ha $N(\alpha)$ egy nemnegatív egész szám köbe, akkor $\alpha$ egy Gauss-egész köbe.

(e) Ha $\alpha \mid \alpha^2$ , akkor $N(\alpha)$ négyzetszám vagy egy négyzeteszám kétszerese.

(f) Ha $N(\alpha)$ négyzetszám vagy egy négyzeteszám kétszerese, akkor $\alpha \mid \alpha^2$ .

7.4.11 (*) Bizonyítsuk be a számelmélet alaptételének egyértelműségi részét az T 1.5.1 Tételben láttott második bizonyítás mintájára.

7.5 Számok előállítása négyzetösszegként

Ebben a pontban azt vizsgáljuk meg, hogy mely pozitív egészek állnak elő két, három, illetve négy négyzetszám összegeként (összeadandóként a 0-t is megengedve).

7.5.1 Tétel (Két-négyzetszám-tétel) . T 7.5.1

Legyen az $u$ pozitív egész kanonikus alakja
ahol a $p_{i}$ primok $4k + 1$, a $q_{i}$ primok $4k - 1$ alakúak, és a szereplő $\alpha$, $\beta_{\mu}$, $\gamma_{\nu}$ kitevők nemnegatív egészek.

Az

$$x^2 + y^2 = n$$

(2)

diofantikus egyenlet akkor és csak akkor oldható meg, ha minden $\gamma_{\nu}$ páros, és ebben az esetben a megoldásszám

$$4 \prod_{\mu=1}^{\nu} (\beta_{\mu} + 1).$$

A T 7.3.1 Tételhez hasonlóan, a csak az előjelben eltérő megoldásokat is külön megoldásoknak tekintjük. Ebből most is könnyen megkaphatjuk a „lényegesen különböző” megoldások számát, lád a 7.5.1 feladatot [240].

Példa: Legyen $n = 4050$. A 4050 kanonikus alakja $2 \cdot 3^4 \cdot 5^2$. Itt a 3 kitevője páros, tehát van megoldás, és a megoldásszám az 5 kitevőjéből $4(2 + 1) = 12$. A megoldások:

$$4050 = (\pm 45)^2 + (\pm 45)^2 = (\pm 9)^2 + (\pm 63)^2 = (\pm 9)^2 + (\pm 9)^2.$$

Bizonyítás: Az $x^2 + y^2 = n$ egyenlet átírható az

$$(x + yi)(x - yi) = n$$

(3)
alakba. Ennek megfelelően azt kell megállapítani, hogy mely $n$-ek és hányféleképpen írhatók fel két olyan Gauss-egész szorzataként, amelyek egymás konjugáltjai.

Ehhez először meghatározzuk az $n$ „kanonikus alakját” a Gauss-egészek körében. Ezen olyan

$$\varepsilon \zeta_{1}^{\alpha_{1}} \cdots \zeta_{i}^{\alpha_{i}}$$
előállítást értünk, ahol a szereplő $\zeta_{i}$ Gauss-primek közül semelyik kettő sem egységszerese egymáshoz és $\varepsilon$ egység. Például a 4 kanonikus alaka $(-1)(1 + \sqrt{-1})$ vagy $(-1)(1 - \sqrt{-1})$ stb. (A „külön” egységtényezőre az egész számok körében is szükség lehet, ha a kanonikus alakot a negatív egészekre is ki akarjuk terjeszteni: például $-9$ csak $(-1)3^2$ vagy $(-1)(-3)^2$ alakban írható fel ily módon.)

A T 7.4.15 Tétel alapján az $n$ (egyik) kanonikus alaka a Gauss-egészek körében

$$n = (-i)^{\nu}(1 + i)^{2\alpha_{1}} \tau_{1}^{\beta_{1}} \cdots \tau_{\nu}^{\beta_{\nu}} q_{1}^{\gamma_{1}} \cdots q_{m}^{\gamma_{m}},$$

(4)
ahol $\tau_{\mu} \overline{\tau_{\mu}} = p_{\mu}$. (A 4 (jobb) oldalán szereplő Gauss-primek közül semelyik kettő sem egységszerese egymáshoz egymáshoz.)

Mivel $x + yi \mid n^{\nu}$, ezért (a számmelémet alaptétele szerint) $x + yi$ kanonikus alaka

$$x + yi = \varepsilon (1 + i)^{\alpha_{i}} \prod_{\mu=1}^{\nu} \left( \tau_{\mu}^{\beta_{\mu}} \overline{\tau_{\mu}}^{\beta_{\mu}} \right) \prod_{\nu=1}^{\nu} q_{\nu}^{\gamma_{\nu}},$$

(5)
ahol $\varepsilon$ egység és minden Gauss-prim kitevője legfeljebb akkora, mint (4)-ben.
Az (5) egyenlőség konjugálásával és \( 1 - \xi = (-\xi)(1 + \xi) \) felhasználásával \( x - y\xi \)-ra az alábbi kanonikus alakot kapjuk:

\[
x - y\xi = (\xi(-\zeta)^{2\alpha})(1 - \xi)\prod_{\mu=1}^{r}\left(\prod_{\nu=1}^{s_{\mu}}\frac{\alpha_{\mu}}{\beta_{\mu}^{\nu}}\right)\prod_{\nu=1}^{s}q_{\nu}^{\nu}.
\]

(6)

A számmelmélet alapétele szerint (3) pontosan akkor teljesül, ha (4)-ben minden Gauss-prím kitevője megegyezik az (5)-és (6)-beli megfelelő kitevők összegével, továbbá a (4)-beli „külön” egységtenyező egyenlő az (5)-és (6)-beli ilyen egységtenyezők szorzatával.

Ez az alábbi egyenlőségek teljesülését jelenti:

1 + \xi kitevője  
\[ 2\alpha = \alpha' + \alpha' ', \quad (7a) \]

\( \pi_{\mu} \) kitevője  
\[ \beta_{\mu} = \beta_{\mu}' + \beta_{\mu}' ', \quad (7b) \]

\( \beta_{\mu} ' \) kitevője  
\[ \gamma_{\nu} = \gamma_{\nu}' + \gamma_{\nu}' ', \quad (7c) \]

\( q_{\nu} \) kitevője  
\[ \xi^{2} = \xi^{2} ' + \xi^{2} ' ', \quad (7d) \]

Ez az (7a) egyenlőségből kapjuk, hogy \( \alpha' = \alpha \) és ekkor (7e) is automatikusan teljesül tetszőleges \( \xi \) esetén. A (7b) és (7c) ugyanazt jelentik, és pontosan akkor állnak fenn, ha

\[ \beta_{\mu} = 0, 1, \ldots, \beta_{\mu}' \quad \text{és} \quad \beta_{\mu}' = \beta_{\mu} - \beta_{\mu}', \quad \mu = 1, 2, \ldots, r. \]

Végül (7d) akkor és csak akkor elégtethető ki, ha \( \gamma_{\nu} \) páros, és ekkor \( \gamma_{\nu}' = \gamma_{\nu}/2 \).

A fentiekből következik, hogy (2) akkor és csak akkor oldható meg, ha mindegyik \( \gamma_{\nu} \) páros.

A megoldásszám azoknak a lehetőségeknek a száma, ahányféleképpen az \( \xi \) esetén. A (7b) és (7c) ugyanazt jelentik, és pontosan akkor állnak fenn, ha

\[ \beta_{\mu} = 0, 1, \ldots, \beta_{\mu}' \quad \text{és} \quad \beta_{\mu}' = \beta_{\mu} - \beta_{\mu}', \quad \mu = 1, 2, \ldots, r. \]

Bizonyítás: Az állításnak csak azt a könnyebben adódó részét igazoljuk, hogy a (8)-beli számok nem állnak elő három négyzetszám összegeként, a másik irány igazolása jóval nehezebb.

A szerinti teljes indukcióval bizonyítunk.

A \( k = 0 \) esetben azt kell megmutatni, hogy a \( 8m + 7 \) alakú számok nem írhatók fel három négyzetsszám összegeként. Ez abból következik, hogy egy négyzetszám 0, 1 vagy 4 maradékot ad \( 8 \)-cal osztva, és három ilyen maradék összegeként sohasem kaphatunk 7 maradékot.

Tegyük most fel, hogy az állítás valamely \( k \)-ra igaz, és lássuk be, hogy ekkor \( k + 1 \)-re is teljesül. Indirekt felteszük, hogy léteznek olyan \( a, b \) és \( c \) egész számok, amelyekre

\[ a^{k+1} + (8m + 7) = a^{2} + b^{2} + c^{2}. \]

A (9) bal oldala osztható 4-gyel. Egy négyzetszám 4-gyel osztva 0-t vagy 1-et ad maradékkal, attól függően, hogy páros, illetve páratlan számot emeltünk négyzetre. Ezért a jobb oldal csak úgy lehet
osztható 4-gyel, ha \(a\), \(b\) és \(c\) mindegyike páros, tehát \(a/2\), \(b/2\) és \(c/2\) egész számok. Így (9)-et 4-gyel elosztva

\[
4^k(\text{sm} + 7) = (\frac{a}{2})^2 + (\frac{b}{2})^2 + (\frac{c}{2})^2
\]

adódik, ami ellentmond az indukciós feltevésnek. 

7.5.3 Tétel (Négy-négyzetszám-tétel) . T 7.5.3

Mindenn pozitív egész felírható négy négyzetszám összegeként. ☞

Bizonyítás: Szükségünk lesz az alábbi két segédtételre:

7.5.4 Lemma . L 7.5.4

Ha két szám felírható négy négyzetszám összegeként, akkor a szorzatuk is, nevezetesen

7.5.5 Lemma . L 7.5.5

Az

\[
1 + x^2 + y^2 \equiv 0 \pmod{p}
\]

kongruencia bármely \(P\) primre megoldható. ☞

A L 7.5.4 Lemma bizonyítása: A (10) azonosság egyszerű számolással ellenőrizhető. 

Megjegyezzük, hogy (10) „természetes” módon adódik a kvaterniók felhasználásával: ha az \(a\) és \(b\) kvaterniók

\[
a = a_1 + a_2i + a_3j + a_4k \quad \text{és} \quad b = b_1 + b_2i + b_3j + b_4k,
\]

akkor (10) éppen a (kvaternió)nomorákra vonatkozó \(N(a)N(b) = N(a\beta)\) azonosság kifejtett alakja.

(Természetesen \(N(a), N(b) = N(a\beta)\) is alkalmas lett volna a L 7.5.4 Lemma „szöveges” részének az igazolására, azonban ekkor (10) helyett egy másik azonosságot kaptunk volna, ugyanakkor a T 7.5.3 Tétel bizonyításában magára a (10) képletre is szükségünk lesz.)

A L 7.5.5 Lemma bizonyítása: Az állítás \(p = 2\) -re nyilvánvaló.

Tegyük fel indirekt, hogy valamely \(p > 2\) primre a (11) kongruenciának nincs megoldása, azaz bármely \(x\) és \(y\) egész esetén

\[
x^2 \not\equiv -1 - y^2 \pmod{p}.
\]

Ha \(x\) végigfut egy modulo \(P\) teljes maradékrrendszer elemein, akkor az \(x^2\) értékek a modulo \(P\) kvadratikus maradékokat és a 0 maradékosztály egy reprezentánsát adják. A T 4.1.2 Tétel alapján így

\[
x^2 \pmod{p} = \frac{\sqrt{\phi} - 1}{2} \quad \text{és} \quad \frac{\sqrt{\phi} + 1}{2}
\]
páronként inkongruens értéket kapunk.

Ugyanez érvényes $y^2$-re, és így $1 - y^2$-re is. Ebből (12) alapján az következik, hogy megadható $\frac{2x^2 + 1}{2} = p + 1$ olyan szám, amelyek páronként inkongruensek modulo $P$, ami nyilvánvaló ellentmondás.

Megjegyezzük, hogy a L 7.5.5 Lemma Chevalley tételéből (T 3.6.1 Tétel), illetve a 3.6.2 feladatból [94] is könnyen levezethető (lásd a 7.5.19 feladatot [242]).

Rátérünk a T 7.5.3 Tétel bizonyítására. Nevezzünk a rövidség kedvéért egy pozitív egészit „szép”-nek, ha felírható négyzetösszám összegként.

Mivel az 1 és a 2 nyilván szép, ezért a L 7.5.4 Lemma alapján elég azt megmutatni, hogy minden $p > 2$ prim is szép.

A $P$-nek létezik szép többszöröse, például a $4p^2$. Vegyük a legkisebb pozitív $m$-et, amelyre $mp$ szép, legyen

$$mp = a_1^2 + a_2^2 + a_3^2 + a_4^2,$$

(13)

Azt kell igazolnunk, hogy $m = 1$. Meg fogjuk mutatni, hogy $m > 1$ esetén létezik olyan $m_1$, amelyre $0 < m_1 < m$, és $m_1p$ is szép. Ez azonban ellentmond $m$ minimalitásának, és így valóban $m = 1$.

Először azt bizonyítjuk be, hogy $m < P$, azaz a $P$-nek létezik $y^2$-nél kisebb szép többszöröse. A L 7.5.5 Lemma alapján a (11) kongruencia megoldható, és a modulo $P$ legkisebb abszolút értékű maradékok rendszerét véve olyan $x$, $y$ megoldást kapunk, amelyre $|y| < \frac{m}{2}$ és $|x| < \frac{m}{2}$. Ekkor

$$x = 1^2 + x^2 + y^2 + 0 \text{ szép},$$

Most belátjuk, hogy $m$ szükségképpen páratlan. Ellenkező esetben (13)-ból következik, hogy két-két $a_1$, $a_2$, $a_3$, $a_4$ azonos paritású. Ekkor

$$(\frac{m}{2})^2 = \left(\frac{a_1 + a_2}{2}\right)^2 + \left(\frac{a_1 - a_2}{2}\right)^2 + \left(\frac{a_3 + a_4}{2}\right)^2 + \left(\frac{a_3 - a_4}{2}\right)^2,$$

ami ellentmond $m$ minimalitásának.

A (13) egyenlőséget most modulo $m$ fogjuk tekinteni. Legyen $b_1, b_2, b_3, b_4$ rendre az $a_1, a_2, a_3, a_4$ számok modulo $m$ szerinti legkisebb abszolút értékű maradéka, azaz

$$b_\nu \equiv a_\nu \pmod{m}, \quad |b_\nu| \leq \frac{m - 1}{2}, \quad \nu = 1, 2, 3, 4.$$

Ekkor

$$b_1^2 + b_2^2 + b_3^2 + b_4^2 = a_1^2 - a_2^2 + a_3^2 + a_4^2 = 0 \pmod{m},$$

azaz alkalmas $m_1$ egésszel

$$\nu m_1 = b_1^2 + b_2^2 + b_3^2 + b_4^2$$

teljesül. Megmutatjuk, hogy (15)-ben $0 < m_1 < m$.

Ha $m_1 = 0$, akkor mindegyik $b_\nu = 0$, azaz mindegyik $a_\nu$ osztható $m_1$-mel. Ebből következik, hogy
\[
7n^2 = a_1^2 + a_2^2 + a_3^2 + a_4^2 = mnp, \quad \text{tel.:} \quad m \mid \varrho,
\]
ami \(1 < m_0 < \varrho\) miatt lehetetlen.

Az \(\gamma_1 < \gamma\) egyenlőtlenség az
\[
m_{m1} = \sum_{\nu=1}^{1} b_{\nu}^2 \leq 4 \left(\frac{\gamma - 1}{2}\right)^2 < 4 \left(\frac{\gamma}{2}\right)^2 = m^2
\]
összefüggésből következik.

A (13) és (15) egyenlőségeket összeszorozva és (10)-et felhasználva azt kapjuk, hogy
\[
\gamma^2 m_{1} \varrho = c_1^2 + c_2^2 + c_3^2 + c_4^2,
\]
ahol a \(c_{\nu}\) számok (10)-ből olvashatók le.

Belátjuk, hogy mindegyik \(c_{\nu}\) osztható \(n\)-mel. Mivel \(b_{\nu} \equiv c_{\nu} \mod (m)\), ezért
\[
c_1 = a_1 b_1 + a_2 b_2 + a_3 b_3 + a_4 b_4 \equiv a_1^2 + a_2^2 + a_3^2 + a_4^2 = mnp \equiv 0 \mod (m),
\]
ez hasonlóan adódik az \(n\)-mel való oszthatóság a többi \(c_{\nu}\)-re is.

Így (16)-ot \(m^2\)-tel elosztra azt nyerjük, hogy \(m_{1}\varrho\) is felírható négy négyzetszám összegeként, ami \(0 < \gamma_1 < m_0\) miatt ellentmond \(m\) minimalitásának. 

Megjegyzés: A bizonyítás során használt módszer az ún. végtesen leszállás egyik változata volt. Az elnevezés magyarázata világosabban válik a gondolatmenetünk alábbi átfogalmazásából: Ha maga a \(\varrho\) nem szép, akkor tekintve a \(\varrho\)-nek egy szép \(m_1\varrho\) (pozitív) többszöröse, találunk egy másik szép \(m_2\varrho\) többszöröse, ahol \(0 < m_1 < m\), majd ugyanígy ehhez is találunk egy szép \(m_2\varrho\) többszöröse, ahol \(0 < m_2 < m_1\) stb. Ez azt jelenti, hogy pozitív egészekből egy végtesen, szigorúan monoton fogyó sorozatot kapunk (vagyis a pozitív egészek körében egy „végtesen leszállást” hajtunk végre), ami nyilván lehetetlen.

A végtesen leszállás a pozitív egészekre nézve leginkább egy indirekt teljes indukciós bizonyításhoz hasonlít. Az T 1.5.1 Tételnél az egyértelműségi rész második bizonyítása is tulajdonképpen egy végtesen leszállást takart.

A teljes indukcióval való rokonsága ellenére a végtesen leszállás más elven alapul: az ún. jölrendezési tulajdonságot használja fel, vagyis azt, hogy bármely részhalmaznak van minimális eleme, tehát nem képezhető végtesen leszálló sorozat. Így ha valamilyen tulajdonság ilyen végtesen leszállással öröklődik, akkor egy jölrendezett halmaz egyetlen eleme sem rendelkezhet ezzel a tulajdonsággal.

Mivel a kiválasztási axiomából következik, hogy bármely halmaz jölrendezhető, ezért a végtesen leszállás a halmazok jóval szélesebb körében alkalmazható, mint a teljes indukció.

**Feladatok**

7.5.1 Hány „lényegesen különböző módon” állítható elő egy adott pozitív egész két négyzetszám összegeként? (A T 7.5.1 Tétel utáni példában szereplő 4050 kétféleképpen: \(4\sqrt{50} = 45^2 + 45^2 = 9^2 + 63^2\).)

7.5.2 Hány olyan Gauss-egész létezik, amelynek a normája 98000?

7.5.3 Melyik az a legnagyobb \(r\), amelyre igaz, hogy végtesen sokszor előfordul \(r\) egymást követő szám, amelyek mindegyike felírható két négyzetszám összegeként vagy különbségeként?
7.5.4 Adjunk új bizonyítást a 4.1.5 feladat [102] állítására.

7.5.5 Mely \( \mu \)-ekre oldható meg és hány megoldása van az \( x^2 + 4y^2 = \mu \) diofantikus egyenletnek?

7.5.6 (*) Mely pozitív egészek írhatók fel és hányféleképpen két \textit{relatív prim} szám négyzetének az összegeként?

7.5.7 (*) (a) Hány olyan (páronként nem egybevágó) derékszögű háromszög létezik, amelynek az oldalai egész számok és az egyik oldal hossza \( k \)?

(b) Mi a válasz akkor, ha még azt is feltesszük, hogy az oldalhosszak relatív prímek?

7.5.8 Mutassuk meg, hogy az \( x^2 + y^2 = \mu \) diofantikus egyenlet megoldásszáma \( 4d'(\mu) - 4d''(\mu) \), ahol \( d'(\mu) \), illetve \( d''(\mu) \) az \( \mu \) pozitív egész \( 4k + 1 \), illetve \( 4k - 1 \) alakú pozitív osztóinak a számát jelöli.

7.5.9 (*) Átlagosan hányféleképpen írható fel egy pozitív egész két egész szám négyzetének az összegeként? Más megfogalmazásban ez az

\[
\frac{\tau(1) + \tau(2) + \cdots + \tau(n)}{\mu}
\]

középértékfüggvény viselkedését jelenti „nagy” \( \mu \) esetén, ahol \( \tau(n) \) az \( x^2 + y^2 = \mu \) diofantikus egyenlet megoldásszáma.

7.5.10 (M [593]*) Oldjuk meg az \( x^2 + 4y^2 = \mu \) diofantikus egyenletet.

7.5.11 (M [594]*) Mely Gauss-egészek írhatók fel két Gauss-egész négyzetének az összegeként?

7.5.12 A T 7.5.1 Tétel bizonyítása során Gauss-egészekre is definiáltunk kanonikus alakot, és láttuk, hogy egy Gauss-egésznek több kanonikus alakja is lehet. Mutassuk meg, hogy bármely, 0-tól és egységektől különböző Gauss-egész kanonikus alakainak a száma a 4-nek pozitív egész kitevős hatvánnyal. (Két kanonikus alakot azonosnak tekintünk, ha csak a tényezők sorrendjében térnek el, és természetesen kizárjuk, hogy a kanonikus alakban egy Gauss-prím nulladik hatványon forduljon elő.)

7.5.13 Melyek igazak az alábbi állítások közül?

(a) Ha két pozitív egész felírható két négyszám összegeként, akkor a szorzatuk is ilyen tulajdonságú.

(b) Ha két pozitív egész szorzata felírható két négyszám összegeként, akkor külön-külön a két tényező is ilyen tulajdonságú.

(c) Ha két pozitív egész szorzata és az egyik tényező felírható két négyszám összegeként, akkor a másik tényező is ilyen tulajdonságú.

(d) Ha két pozitív egész felírható három négyszám összegeként, akkor a szorzatuk is ilyen tulajdonságú.

7.5.14 (*) Mi a valószínűsége annak, hogy egy pozitív egész előáll három négyszám összegeként?

7.5.15 Melyik az a legkisebb \( r \), amelyre igaz, hogy minden \( \mu \)-elégy pozitív egész felírható legfeljebb \( r \) darab páratlan négyszám összegeként?

7.5.16 Vezessük le a három-négyzetszám-tételből a négy-négyzetszám-tételt.

7.5.17 (M [595]) Mely pozitív egészek állnak elő négy négyszám összegeként úgy, hogy az összeadandók között van (legalább) két azonos?

7.5.18 Megoldható-e az \( x^2 + 9y^2 + z^2 + 6t^2 - 10^{11} + 23 \) diofantikus egyenlet?
7.5.19 Igazoljuk a L 7.5.5 Lemmát Chevalley tétele (T 3.6.1 Tétel), illetve a 3.6.2 feladat [94] felhasználásával.

7.5.20 A T 7.5.1 Tételből következik, hogy minden $4k+1$ alakú pozitív prim felírható két négyzetszám összegeként. Adjunk erre a tényre új bizonyítást a T 7.5.3 Tételnél látott gondolatmenet alapján.

7.5.21 (*) A feladat célja a négy-négyszétszám-tétel egy másik bizonyításának a bemutatása. Ennél is felhasználjuk a L 7.5.4 és L 7.5.5 Lemmákat, de a végtelen leszállás helyett az alábbi (a) részben szereplő állítás segítségével kapjuk meg a $P$ prímmnek egy „kicsi” szép többszöröseit.

(a) Thue-lemma. Két egész koordinátájú $k$ -dimenziós vektort akkor nevezünk kongruensnek modulo egy $P$ prímszám, ha a megfelelő koordinátáik kongruensek modulo $P$ . Legyen $C$ tetszőleges $k \times k$ -as egész elemű mátrix és $u_1, \ldots, u_k, v_1, \ldots, v_k$ olyan pozitív egészek, amelyekre

$$u_1 \ldots u_k v_1 \ldots v_k > p^k.$$  

Ekkor léteznek olyan $x = \left( \begin{array}{c} x_1 \\ \vdots \\ x_h \end{array} \right) \neq 0$ és $z = \left( \begin{array}{c} z_1 \\ \vdots \\ z_h \end{array} \right)$ egész elemű vektorok, amelyekre

$$Cz \equiv z \pmod{p^k} \quad \text{és} \quad |z_1| < u_1, |z_i| < v_i, i = 1, 2, \ldots, k.$$  

(b) Az (a) rész (alkalmazás $k = 2$ speciális esete) és a L 7.5.5 Lemma segítségével mutassuk meg, hogy tetszőleges $P$ prímnak létezik $4P$ -nél kisebb szép pozitív többszöröse.

(c) Végül igazoljuk, hogy ha egy $P > 3$ primre $2P$ vagy $3P$ szép, akkor $P$ is az.

7.6 A Waring-problémakör

A négyzetek után a magasabb hatványok összegeként történő előállítással foglalkozunk. Ebben a pontban $k$ -végig 1-nél nagyobb pozitív egész jelöl, és $k$ -adik hatványon nemnegatív egész számok $k$ -adik hatványát fogjuk érteni.

Waring 1770-ben azt állította, hogy „minden szám felírható 4 négyzetszám, 9 köbszám, 19 negyedik hatvány stb. összegeként”. A nagyvonalúan odavetett „stb.” szócska két súlyos problémát is takar. Egyrésztt a 4, 9, 19 számokról nemigen látszik valami jól folytható szabályszerűség, másrésztt az sem világos, hogy ez a számsor egyáltalán folytható a végtelenségig. Ez utóbbihoz a következőt kell megmutatni: Bármely $k$ -hoz létezik olyan, csak a $k$ -től függő $r$ , hogy minden pozitív egész felírható $r$ darab $k$ -adik hatvány összegeként. Ezt az állítást először Hilbert igazolta 1909-ben.

Ma már (később részletszerű) minimalis bizonytalanságtól eltekintve) tudjuk, hogy folytatódik a Waring-féle számsor. Érdemes módon a 19 negyedik hatvány problémája állt ellen legtovább az ostromnak, ennek helyességét csak 1986-ban sikerült bizonyítani.

Mivel bármely szám $k$ -adik hatványok összegeként történő előállítását kiegészíthetjük tetszőleges számú $0^k$ taggal, ezért a legkisebb olyan darabszámot akarjuk meghatározni, hogy annyi $k$ -adik hatvány már minden pozitív egész előállításához elegendő legyen:

7.6.1 Definíció . D 7.6.1

Legyen $k > 1$ . Ekkor $g(k)$ a legkisebb olyan $r$ , hogy minden pozitív egész felírható $r$ darab nemnegatív egész szám $k$ -adik hatványának összegeként.
Példa: \( g(2) = 4 \), ugyanis egyrészt a négy-négyzetszám-tétel szerint minden pozitív egész négy négyzetszám összege, másrészt van olyan szám, például a 7, amelynek az előállításához három négyzetszám nem elegendő.

7.6.2 Tétel .  

\[ g(k) \geq 2^k - \left\lfloor \frac{3}{2} \right\rfloor - 2. \tag{1} \]

Bizonyítás: A \( g(k) \)-ra vonatkozó alsó becsléshez elég egyetlen olyan \( n \) pozitív egész találni, amelynek az előállításához „sok” \( k \)-adik hatványra van szükség.

Legyen \( n \) a legnagyobb olyan \( t2^k - 1 \) alakú szám, amely kisebb, mint \( 3^k \). Ekkor \( n \) felírásához csak \( (0^k,) \) \( 1^k \) és \( 2^k \) tagok állnak rendelkezésre, és ezekből nyílván az

\[ n = t2^k - 1 = 2^k + \cdots + 2^k + 1^k + \cdots + 1^k \]

előállítás használja fel a legkevesebbet. Innen azt kapjuk, hogy

\[ g(k) \geq 2^k + t - 2. \]

Így már csak azt kell igazolni, hogy \( t = \left\lfloor \left( \frac{3}{2} \right)^k \right\rfloor \). Ez abból következik, hogy

\[ t2^k - 1 < 3^k \iff t2^k \leq 3^k \iff t \leq \left( \frac{3}{2} \right)^k, \tag{2} \]

továbbá \( t \) a (2)-t kielégítő legnagyobb egész szám.

A \( g(\tilde{k}) \)-ra vonatkozó legfontosabb eredmény az, hogy (1)-ben általában egyenlőség teljesül: csak véges sok olyan \( \tilde{k} \)-létezhet, amelyre \( g(\tilde{k}) \) nagyobb az (1) jobb oldalán megadott értéknél. Ez csak olyan \( \tilde{k} \)-esetén következhet be, amikor \( (3/2)^{\tilde{k}} \) (egy pontosan felírható egyenlőtlenséget kielégítve) „abnormálisan” közel esik a felső egészszámhoz. A 99999000-nél kisebb számok között egyetlenegy sem teljesíti ezt a feltételt, és csaknem biztosra vehető, hogy nincsenek ilyen kivételek, azaz minden \( \tilde{k} \)-ra

\[ g(\tilde{k}) = 2^\tilde{k} + \left\lfloor \frac{3}{2} \right\rfloor - 2. \]

Ennek megfelelően (1) jobb oldala jelenti a Waring-féle számsor folytatását (speciálisan a \( \tilde{k} = 2 \), 3 és 4 esetben rendre a 4, 9, illetve 19 értékeket kapjuk).

A T 7.6.2 Tétel azt mutatja, hogy egyes „kis” \( n \)-ek előállítása igen sok \( k \)-adik hatványt igényel. Ezért érdemes azt is megvizsgálni, hogy minimálisan hány \( k \)-adik hatvány szükséges minden \( \tilde{k} \)-nel felírásához:

7.6.3 Definíció .  

Legyen \( \tilde{k} > 1 \). Ekkor \( G(\tilde{k}) \) a legkisebb olyan \( s \), hogy minden \( \tilde{k} \)-adik hatványt igényel.

Példa: \( G(2) = 4 \), ugyanis egyrészt nyilván \( G(2) \leq g(2) = 4 \), másrészt a három-négyzetszám-tétel szerint végletes szám 4 legkisebb szám létezik, amelynek az előállításához három négyzetszám nem elegendő.
Az alábbi táblázatban bemutatjuk a \( g(k) \) -ra és \( G(k) \) -ra vonatkozó eredményeket néhány kis \( k \) esetén:

<table>
<thead>
<tr>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>9</td>
<td>19</td>
<td>37</td>
<td>73</td>
<td>143</td>
<td>279</td>
</tr>
</tbody>
</table>

A táblázat jól érzékelheti, hogy már kis \( k \) esetén is igen nagy a bizonytalanság a \( G(k) \) pontos értékét illetően (például \( G(3) \) -nál a 4–7 jelölés azt jelenti, hogy \( G(3) \) -ra csak a 4 ≤ \( G(3) \) ≤ 7 becslés ismert). A \( G(k) \) pontos értékét eddig csak a \( k = 2 \) és 4 esetekben sikerült meghatározni.

Az viszont kiderült, hogy nagy \( k \) esetén \( G(k) \) értéke jóval kisebb \( g(k) \) -nál: például minden \( k > 1 \) -re fennáll \( G(k) < \frac{1}{6} k \log k \). (A jelenlegi legjobb eredmény szerint bármely \( \varepsilon > 0 \) -hoz létezik olyan \( k_0 = k_0(\varepsilon) \), hogy minden \( k > k_0 \) esetén \( G(k) < (1 + \varepsilon)k \log k \).) Így az exponenciális nagyságrendű \( g(k) \) -val szemben \( G(k) \) „csaknem” lineáris.

Az alábbiakban alsó becsléseket adunk \( G(k) \) -ra.

7.6.4 Tétel. T 7.6.4

Minden \( k > 1 \) esetén \( G(k) \geq k + 1 \). ●

Bizonyítás: Tegyük fel indirekt, hogy valamely \( k \) -ra \( G(k) \leq k \). Ekkor létezik olyan \( n_0 \), hogy minden \( n \geq n_0 \) egész szám felírható \( k \) darab \( k \)-adik hatvány összegeként, azaz

\[ n = x_1^k + x_2^k + \cdots + x_k^k. \quad (3) \]

Tekintsünk egy tetszőleges \( M \) („nagy”) pozitív egész, és jelöljük \( f(M) \) -mel azoknak az \( n \) -eknek a számát, amelyekre

\[ 0 \leq n \leq M, \quad (4) \]

és \( n \) előáll \( k \) darab \( k \)-adik hatvány összegeként. Az indirekt feltevés szerint

\[ f(M) \geq M - n_0. \quad (5) \]

Most felső becslést keresünk \( f(M) \) -re. A (4)-beli \( n \) -eket tekintve, ezek (3) előállításában csak olyan \( x_i \) számnok szerepelhetnek, amelyekre

\[ 0 \leq x_i \leq \sqrt[k]{i} \leq \sqrt[k]{M}, \quad i = 1, 2, \ldots, k. \]

Ez azt jelenti, hogy minden \( x_i \) értéke csak

\[ 0, 1, \ldots, \left\lfloor \sqrt[k]{M} \right\rfloor \quad (3) \]

lehet.

Mindebből következik, hogy a \( 0, 1, \ldots, \sqrt[k]{M} \) egészek közül legfeljebb annyit írható fel \( k \) darab \( k \)-adik hatvány összegeként, ahányféle lépésen az (5)-beli elemek közül \( k \) darabot ki tudunk választani úgy, hogy egy elemet többször is kiválaszthatunk, és a kiválasztás sorrendjére nem vagyunk tekintettel (ugyanis (3)-ban az összeadandók között lehetnek azonosak is, továbbá a tagok permutálása esetén az összeg ugyanazt az \( n \) -et állítja elő).
Az ilyen típusú kiválasztás az ismétléses kombináció, tehát a jelzett kiválasztások száma az (5)-beli elemek \( k \)-adosztályú ismétléses kombinációinak a száma, azaz
\[
\binom{k}{k-1} = \frac{(k-1)!}{1!(k-1-1)!} = \frac{(k-1)!}{1!(k-2)!} = \frac{(k-1)!}{(k-2)!}.
\]

Mindezeket összefoglalva, azt igazoltuk, hogy
\[
f(M) \leq \binom{k + \left\lfloor \sqrt{M} \right\rfloor}{k}.
\]
Az (5) és (6) egyenlőtlenségekből
\[
M - c_0 \leq \binom{k + \left\lfloor \sqrt{M} \right\rfloor}{k},
\]
következik. Írjuk be (7) jobb oldala helyett az
\[
\frac{1}{k!} (k + \left\lfloor \sqrt{M} \right\rfloor) (k - 1 + \left\lfloor \sqrt{M} \right\rfloor) \ldots (1 + \left\lfloor \sqrt{M} \right\rfloor)
\]
képletet, hagyjuk el az egészrész jeleket (ezzel (7) jobb oldalát nem csökkentettük), majd osszuk el mindkét oldalt \( M \)-mel oly módon, hogy az \( \frac{1}{k!} \) tényezők mindegyikét \( \sqrt{M} \)-mel osztjuk. Ekkor az
\[
1 - \frac{c_0}{M} \leq \frac{1}{k!} \left(1 + \frac{k}{\sqrt{M}}\right) \left(1 + \frac{k - 1}{\sqrt{M}}\right) \ldots \left(1 + \frac{1}{\sqrt{M}}\right)
\]
egyenlőtlenséghez jutunk. Ha \( M \to \infty \), akkor (8) bal oldalára 1-hez, jobb oldal pedig \( \frac{1}{k!} \) -hoz tart, ami \( k > 1 \) miatt ellentmondás.

Megjegyzés: A bizonyításból az is kiderült, hogy „nagyon sok” olyan \( n \) van, amely nem írható fel \( k \)- darab \( k \)-adik hatvány összegeként (például már \( k = 5 \) esetén is a számok „legalább \( \frac{2^{k-1}}{k} = \frac{119}{120} \)-ad része”, azaz „több, mint 99 százaléka” ilyen). Ugyanakkor a bizonyítás nem volt „konstruktív”: egyetlen „konkrét” \( n \) -ről sem mutatta ki, hogy \( n \) nem áll elő a kívánt alakban.

Most megmutatjuk, hogy a T 7.6.4 Tétel becslése például \( k = 6 \) esetén javítható:

7.6.5 Tétel. T 7.6.5.
\( G(6) \geq 9 \).

Bizonyítás: Felhasználjuk, hogy bármely \( a \) egészre
\[
a^6 = \begin{cases} 1 \mod 9, & \text{ha } 3 \nmid a; \\ 0 \mod 9, & \text{ha } 3 \mid a. \end{cases}
\]
A \( 3 \nmid a \) eset az Euler–Fermat-tételből következik, a \( 3 \mid a \) esetben pedig \( a^6 \) nemcsak 9-cell, hanem \( 3^6 \)-mal is osztható.

A T 7.6.5 Tétel állításához azt kell igazolnunk, hogy végig sok olyan \( n \) létezik, amely nem írható fel 8 darab hatodik hatvány összegeként. Megmutatjuk, hogy például az \( n = 27^k + 9 \) alakú számok ilyenek.

Tegyük fel indirekt, hogy
(10)

\[ \nu = x_1^6 + \cdots + x_k^6. \]

Tekintsük (10)-et modulo 9, ekkor (9) alapján azt kapjuk, hogy

\[ 0 = x_1 + \cdots + x_k \quad (\text{mod} \ 9), \quad \text{ahol} \quad \nu = 0 \quad \text{vagy} \quad 1, \quad i = 1, 2, \ldots, 8. \]

(11)

A (11) kongruencia nyilván csak úgy teljesülhet, ha minden \( x_i \) -re \( x_i = 0 \). Ez azt jelenti, hogy mindegyik \( x_i \) osztható 3-mal. Ekkor azonban (10) alapján \( 3^6 \mid \nu \), ami ellentmondás.

\[ \square \]

A \( G_{(k)} \) -ra vonatkozó további alsó becslések szerepelnek a 7.6.2 feladatban [246].

### Feladatok

7.6.1 Mutassuk meg, hogy \( G_{(200)} \leq G_{(600)} \).

7.6.2 (*) (a) Igazoljuk a \( G_{(k)} \) -ra vonatkozó alábbi alsó becsléseket:

\[ \begin{align*}
  (a1) & \quad G_{(4)} \geq 16; \\
  (a2) & \quad G_{(8)} \geq 32; \\
  (a3) & \quad G_{(24)} \geq 32; \\
  (a4) & \quad G_{(100)} \geq 125; \\
  (a5) & \quad G_{(250)} \geq 312. \\
\end{align*} \]

(b) Mely \( k \) értékekre általánosíthatók az (a)-beli becslések?

7.6.3 Legyen \( k > 1 \) tetszőleges. Bizonyítsuk be, hogy van olyan \( \nu \) pozitív egész, amely legalább 1000 („lényegesen”) különböző módon felírható \( k + 1 \) darab \( k \) -adik hatvány összegeként.

7.6.4 (a) Igazoljuk az alábbi azonosságot (\( a_1, a_2, a_3, a_4 \) tetszőleges komplex számok):

\[ \sum_{1 \leq i < j \leq 4} \left( (a_i + a_j)^4 + (a_i - a_j)^4 \right) = 6(a_1^4 + a_2^4 + a_3^4 + a_4^4). \]

(b) Bizonyítsuk be, hogy \( g(4) \leq 53 \).

7.6.5 Ha a számokat \( k \) -adik hatványok előjelés összegeként állítjuk elő, akkor általában \( g_{(k)} \) -nál, illetve \( G_{(k)} \) -nál kevesebb számú tag is elegendő. Mutassuk meg, hogy \( k = 2 \) esetén a minimális darabszám 3, ráadásul az \( z^2 + y^2 - z^2 = \nu \) és \( z^2 + y^2 - z^2 = \nu \) diofantikus egyenleteknek bármely \( \nu \) pozitív egész esetén végteken sok megoldása van.

### 7.7 A Fermat-sejtés

A 7.2 pontban láttuk, hogy az \( x^2 + y^2 = z^2 \) pitagorasi egyenletnek végteken sok pozitív egész megoldása van (és az összes megoldás leírható három paraméter segítségével). Fermat-nak a közelmúltban igazolt híres sejtése szerint magasabb hatványokra alapvetően más a helyzet:

7.7.1 Tétel (Fermat-sejtés, Wiles tétele) .

\[ \square \]

246
Ha $k > 2$ egész szám, akkor az $a^k + b^k = c^k$ egyenlet nem oldható meg pozitív (vagy ami ezzel ekvivalens, nullától különböző) egészekben.

A sejtés története 1637-ben kezdődött, amikor Diophantosz könyvének 1621-es kiadását olvasgatva, a pitagorasi számhármaskról szóló résznel Fermat a következő bejegyzést tette: „Két köbszám összege sohasem lehet köbszám, két negyedik hatvány összege sohasem lehet negyedik hatvány stb. Erre egy csodálatos bizonyítást találtam, sajnos a margón kevés a hely ahhoz, hogy leírhamass.”

Ez a néhány sor három és fél évszázadon keresztül matematikusok és laikusok egész seregét tartotta izgalomban. Mivel maga a rendkívül egyszerűen hangzó probléma minden matematikai előkészületének nélkül is megérthető, ezért igen sok műkedvelő is próbálkozott a megoldással, mindhiába. Nem ment sokkal jobban a dolog a „profit” matematikusoknak sem.

Könnyen adódik (lásd a 7.7.1 feladatot [256]), hogy ha a sejtés igaz egy adott $k$ kitevőre, akkor a $k$ minden többszörössére is igaz, ennélfogva elég a $k = 4$ és $k = p$ prim eseteket tisztáznii. Fermat-nál (valóban) megtalálható a $k = 4$ eset bizonyítása, majd jó száz éven később Euler a $k = 3$ kitevővel is boldogult. A 19. század első felében további néhány konkrét $k$ értékére sikertelen megoldani a problémát, majd a század közepén lényeges áttörést hozott az „ideális számok”, mai szóhasználattól az ideálok bevezetése, amelyekről a 11. fejezetben lesz részletesen szó. Ezt továbbfejlesztve számos olyan kritériumot dolgoztak ki, amelyek teljesülése esetén a Fermat-sejtés arra az adott $k$ (prim) kitevőre igaz. Ezek a kritériumok (elvileg) bármely konkrét $k$ értékére numerikusan ellenőrizhetőek, és ez az ellenőrzés szorgalmasan folyt is (az utóbbi évtizedekben már számítógépek segítségével).

Mindezek ellenére a 20. század hetvenes éveiben is csak véges sok prim kitevőre nyert bizonyítást a sejtés. Közben rengeteg még általánosabb sejtés született, mert várható volt, hogy a megoldás a Fermat-egyenletén általánosabb problémára vonatkozó tételből következik majd.

Óriási szenzációt jelentett 1983-ban Gerd Faltings eredménye: a Fermat-egyenletnek bármely $k$ kitevő esetén csak véges sok primitív (azaz $(x:y:z) = 1$ típusú) megoldása lehet.

Az igazi szenzációt azonban Andrew Wiles okozta 1993-ban, aki sokéves titokban végzett kutatás után a probléma végleges megoldásával rukkolt elő. Később kiderült, hogy a bizonyítás egy lényeges ponton hiába, de a hibát Wilesnak (Richard Taylor segítségével) 1994-ben sikerült kijavítania.

Így a Fermat-sejtés mára lekerült a híres megoldatlan problémák listájáról. Wiles sok száz oldalas bizonyítása a matematikusok csak egy igen szűk csoportja számára érthető, de remélhetőleg később születnek majd egyszerűbb bizonyítások is.

Ami Fermat „csodálatos bizonyítását” illeti, az minden bizonnyal csak vagy egy végig nem gondolt ötlet lehetett, vagy pedig egy hibás gondolatmenet volt, amely tulajdonképpen a számmelmélet alaptételeinek érvényességét olyan számkörben is feltételezte, ahol ez nem teljesül (lásd bővebben a 11.2 pontban). Továbbra is gyakorlatilag kizárható, hogy a Fermat-sejtésre valaki egy „igazi elemi” bizonyítást találjon.

A Fermat-sejtés több évszázados kutatása során a matematikusok számos hatékony, új elméletet dolgoztak ki a probléma kezelésére, amelyek a sejtés szempontjából ugyan csak részleges sikert hoztak, a matematika más területein azonban nélkülözhetetlennek váltak. Ez is jól mutatja, hogy egy adott probléma vizsgálatára gyakran ilyen közvetett módon megfelelő megoldások is kereshetőek.

A Fermat-sejtés több évszázados kutatása során a matematikusok számos hatékony, új elméletet dolgoztak ki a probléma kezelésére, amelyek a sejtés szempontjából ugyan csak részleges sikert hoztak, a matematika más területein azonban nélkülözhetetlennek váltak. Ez is jól mutatja, hogy egy adott probléma vizsgálatára gyakran ilyen közvetett módon megfelelő megoldások is kereshetőek.

Mindkét esetben valamivel erősebb eredményt igazolunk, mégpedig azért, mert valójában az eredeti kérdés megoldásához is csak ilyen (vagy hasonló) erősebb tételeknek a bizonyításával tudunk eljutni.

A Fermat-sejtés $k = 4$ kitevős esete nyilván következik az alábbi tételekből:

7.7.2 Tétel. T 7.7.2
Az \( x^4 + y^2 = z^4 \) egyenletnek nem létezik pozitív egész megoldása.

**Bizonyítás:** Az alábbi, önmagában is érdekes lemmát használjuk fel:

### 7.7.3 Lemma. L 7.7.3

Két (nemnulla) négyzetszám összege és különbsége nem lehet egyszerre négyzetszám. 📜

**A lemma bizonyítása:** A végletes leszállás módszerét használjuk (lásd a T 7.5.3 Tétel utáni megjegyzést).

Tekintsük az

\[
\begin{align*}
x^2 + y^2 &= z^2 \quad (1a) \\
x^2 - y^2 &= u^2 \quad (1b)
\end{align*}
\]

eyenletrendszert. A bizonyítás során megoldáson mindig pozitív egész megoldást fogunk érteni. Legyen \( x_0, y_0, z_0, u_0 \) egy olyan megoldás, ahol \( z_0 \) értéke a lehető legkisebb. Megmutatjuk, hogy ekkor létezik olyan \( x_1, y_1, z_1, u_1 \) megoldás, ahol \( 0 < z_1 < z_0 \), ami nyilvánvalóan ellentmond \( z_0 \) minimalitásának.

Feltételezzük, hogy \( (x_0, y_0, z_0, u_0) = 1 \). Ha ugyanis egy \( p \)-prim osztója \( z_0 \)-nak és \( u_0 \)-nak, akkor (1a)-ből a pitagorasi számhármasoknál látott módon következik, hogy \( p \mid y_0 \), majd ugyanily (1b)-ből kapjuk, hogy \( p \nmid u_0 \), és ekkor az \( x_0/p \), \( y_0/p \), \( z_0/p \), \( u_0/p \) számnégyes olyan megoldás, ahol \( z_0/p < z_0 \), ami ellentmond \( z_0 \) minimalitásának.

Az (1a) és (1b) egyenletekre az \( x_0, y_0, z_0, u_0 \) megoldást behelyettesítve és a két egyenlőséget összeadva, illetve kivonva

\[ 2x_0^2 = z_0^2 + u_0^2 \] (2a)

és

\[ 2y_0^2 = z_0^2 - u_0^2 \] (2b)

adódik. (2a)-ból (is) látszik, hogy \( z_0 \) és \( u_0 \) azonos paritású. Ennek alapján (2a) átírható az

\[ x_0^2 = \left( \frac{z_0 + u_0}{2} \right)^2 + \left( \frac{z_0 - u_0}{2} \right)^2 \] (3)

alakba. Itt

\[ \left( x_0, \frac{z_0 + u_0}{2}, \frac{z_0 - u_0}{2} \right) = 1, \] (4)

mivel \( z_0 \) relatív prim a másik két szám összegéhez, \( z_0 \)-hoz.

(3) és (4) alapján \( \frac{z_0 + u_0}{2} \), \( \frac{z_0 - u_0}{2} \) és \( z_0 \) primitív pitagorasi számhármast alkot. Az \( T 7.2.1 \) Tétel szerint ekkor léteznek olyan ellentétes paritású és relatív prim \( z_0 > u > 0 \) egészek, amelyekre

\[ \frac{z_0 + u_0}{2} = 2mr \] és \[ \frac{z_0 - u_0}{2} = ml^2 - n^2, \] (5)

vagy fordítva.

A (2b)-vel ekvivalens

---

248
Végül \( m \) és \( n \) relatív prímek és különböző paritásúak, ezért a (6) jobb oldalán szereplő négy pozitív egész páronként relatív prim. Ebből következik, hogy mind a négyen négyzetszámok, azaz

\[
m = x_1^2, \quad n = y_1^2, \quad m + n = z_1^2, \quad \text{és} \quad m - n = z_2^2.
\]  

(7) alapján \( x_1 \cdot y_1 \cdot z_1 \cdot z_2 \) megoldása az (1a)–(1b) egyenlőtrendszernek, továbbá

\[
z_1 \leq z_1^2 - m + n \leq (m + n)(m - n) = \frac{z_0 + w_0}{2} < z_0,
\]
ami ellentmond \( z_0 \) minimalitásának.

Most ráterünk a T 7.7.2 Tétel bizonyítására. Tegyük fel indirekt, hogy az \( a, b, c \) pozitív egészekre teljesül

\[
e^4 - e^4 = b^2.
\]  

Ha \( \langle a, b, c \rangle = \delta \), akkor \( a/d, b/d^2, c/d \) is megoldása az egyenlőtrendszernek, ezért feltehetjük, hogy \( \langle a, b, c \rangle = 1 \). Ebből a már többször látott módon kapjuk, hogy \( a, b \) és \( c \) páronként is relatív prímek.

A (8) bal oldalát szorzattá bontva

\[
(e^2 + a^2)(e^2 - a^2) = b^2
\]  

adódik. Jelöljük \( \delta \) -val a (9) bal oldalán álló két tényező legnagyobb közös osztóját: \( \hat{\delta} = \langle c^2 + a^2, e^2 - a^2 \rangle \). Mivel \( \langle e^2, a^2 \rangle = 1 \), ezért \( \hat{\delta} \) csak 1 vagy 2 lehet. A számmelmélet alapétele szerint a (9) bal oldalán álló tényezők az első esetben külön-külön is négyzetszámok, a második esetben pedig egy-egy négyzetszám két részei.

A \( \hat{\delta} = 1 \) esetben tehát \( e^2 = c^2 + a^2 \) és \( e^2 = e^2 - a^2 \) négyzetszámok, ami a L 7.7.3 Lemma szerint lehetetlen.

Ha \( \hat{\delta} = 2 \), akkor alkalmas \( u > v > 0 \) egészekkel

\[
\langle c^2 + a^2, c^2 - a^2 \rangle = 2v^2
\]  

adódik, és így ismét ellentmondásba kerültünk a L 7.7.3 Lemmával.

A Fermat-sejtés \( k = 3 \) kitevős esetének bizonyításához egy, a Gauss-egészekhez hasonló újabb gyűrűben, az Euler-egészek körében építtünk fel számmelméletet.

7.7.4 Definíció . D 7.7.4

Euler-egészeknek azokat az \( a - b\omega \) komplex számokat nevezzük, ahol \( a, b \) egész számok és
Az $\omega$ és $\omega^2 = -1 - \omega$ komplex számok éppen a primitív harmadik egységgyökök, és ennek megfelelően az

$$x^3 - y^3 = (x - y)(z - y)(z - y\omega)(z - y\omega^2) \quad (11)$$

szorzattá bontás mutatja az $x^3 + y^3 = z^3$ Fermat-egyenlet és az Euler-egészek kapcsolódását. A Fermat-sejtés $k = 3$ esetének igazolásához is lényegében egy (11)-hez hasonló egyenlet vizsgálata vezet majd el, és a bizonyítás során alapvetően támaszkodni fogunk az Euler-egészek származéletrére.

7.7.5 Definíció. D 7.7.5

Az Euler-egész normájának nevezzük és $N(e)$-val jelöljük az $e$ abszolút értékének négyzetét:

$$N(e) = |e|^2 = e\bar{e} = (a + b\omega)(a + b\omega^2) = a^2 - ab + b^2.$$ 

Nyilván $N(e)$ nemnegatív egész szám, és $N(e) = 0 \iff e = 0$. Megjegyezzük még, hogy az $a + b\omega$ Euler-egész normájának $a^2 - ab + b^2$ alakja mindig átírható alkalmas $\epsilon\ , \ \bar{\epsilon}$ egészekkel $\epsilon^2 + 3\bar{\epsilon}^2$ alakba, lásd a 7.7.10a feladatot [257].

Az Euler-egészek egy paralelogrammaráccsot alkotnak a komplex számsíkon: ez egységnyi oldalú rombuszokból áll, amelyek szögei 120 és 60 fokosak.

Az oszthatóság, egység, legnagyobb közös osztó, felbonthatatlan és prím fogalmát pontosan ugyanúgy definíáljuk, mint a Gauss-egészeknél (lásd a D 7.4.4 , D 7.4.6 , D 7.4.9 , D 7.4.10 és D 7.4.11 Definíciókat, a „Gauss-” jelző helyére természetesen mindenhol „Euler-” kerül).

Az Euler-egészek és az Euler-prímek leírásától eltekintve a Gauss-egészeknél szereplő tételek és az azokra adott bizonyítások ugyanúgy érvényesek az Euler-egészekre is:

— a norma tulajdonságai (T 7.4.3, T 7.4.5 Tételek);
— maradékos osztás (T 7.4.8 Tétel, a bizonyítás során rácsnégyszet helyett a megfelelő rácsrombuszt kell tekinteni);
— a prím és felbonthatatlan ekvivalenciája (T 7.4.12 Tétel);
— a szármelmélet alaptétele (T 7.4.13 Tétel);
— az Euler-prímek és a (Z-belí) prímszámok kapcsolata (T 7.4.14 Tétel).

Az egységeket karakterizáló T 7.4.7 Tétel és annak bizonyítása is átvihető az Euler-egészekre, ha az egységeket konkrétan megadó (iv) pontot a következőképpen módosítjuk:

7.7.6 Tétel. T 7.7.6

Az Euler-egészek körében 6 egység van:

$$\pm 1, \quad \pm \omega, \quad \pm \omega^2 = \mp (1 + \omega),$$

ezek éppen a hatodik komplex egységgyökök. ☞

Végül, az Euler-prímeket a következő tétel írja le:

7.7.7 Tétel. T 7.7.7
Az alábbi Euler-egészek adják az összes Euler-prímet (\(c\) tetszőleges egységet jelöl):

(A) \(\bar{c}(i\sqrt{3}) = \bar{c}(1 + 2\omega)\);

(B) \(\bar{c}q\), ahol \(q\) pozitív \(3^k - 1\) alakú prímszám;

(C) \(\pi\), ahol \(N(\pi)\) egy pozitív \(3^k + 1\) alakú prímszám; minden ilyen prímszámhoz egységszerestől eltekintve két Euler-prím tartozik, amelyek egymás konjugáltjai, de nem egymás egységszeresei.

Bizonyítás: A T 7.4.15 Tétel bizonyítását kell értelemszerűen módosítani, ezért csak röviden jelezzük az eltéréseket.

A T 7.4.14 Tétel megfelelője szerint az összes Euler-prímet a pozitív prímszámoknak az Euler-prímek szorzatára történő felbontásaiból kaphatjuk meg. Más és más típusú felbontást kapunk attól függően, hogy ez a pozitív prímszám (A) a 3; (B) \(3^k - 1\) alakú; illetve (C) \(3^k + 1\) alakú.

(A) Mivel \(3 = (-1)(i\sqrt{3})^2\), ezért a 3-nak egységszerestől eltekintve egyetlen Euler-prím osztója az \(i\sqrt{3}\).

(B) A \(3^k - 1\) alakú pozitív prímszámok Euler-prímek is; ehhez azt kell igazolni, hogy egy Euler-egész normája nem lehet \(3^k\) alakú, a gondolatmenet további része ugyanaz, mint a Gauss-egészeknél volt.

(C) Ha \(P\) egy pozitív \(3^k + 1\) alakú prímszám, akkor \(\overline{\left(\frac{-3}{P}\right)} = 1\) (lásd a 4.2.2c feladatot [108]), tehát van olyan \(c\) egész szám, amelyre \(P \mid c^2 + 3\). Az Euler-egészek körében

\[c^2 + 3 = (c + i\sqrt{3})(c - i\sqrt{3}) = (c + 1 + 2\omega)(c - 1 - 2\omega),\]

a gondolatmenet további része megegyezik a Gauss-egészeknél látottal.

A Fermat-sejtés köbszámokra vonatkozó speciális esetének bizonyításánál fontos szerepet játszik az \(i\sqrt{3}\) Euler-prím néhány tulajdonsága. Ezek kényelmes megfogalmazásához előbb az Euler-egészek körében is bevezetjük a kongruencia fogalmát:

7.7.8 Definíció . D 7.7.8

Legyenek \(\alpha\) és \(\beta\) Euler-egészek és \(\mu \not\equiv 0\) Euler-egész. Azt mondjuk, hogy \(\alpha\) kongruens \(\beta\)-val modulo \(\mu\), ha \(\mu \mid \alpha - \beta\).

Most is az \(\alpha \equiv \beta (\text{mod } \mu)\) vagy röviden \(\alpha \equiv \beta (\text{mod } \mu)\) jelölést használjuk. A kongruenciák elemi tulajdonságai az Euler-egészek körében ugyanúgy érvényesek, mint az egész számoknál.

Az alábbi tételben az \(i\sqrt{3}\) Euler-prím néhány fontos tulajdonságát foglaljuk össze:

7.7.9 Tétel . T 7.7.9

Legyen \(\lambda = i\sqrt{3} = 1 + 2\omega\).

(i) A \(\lambda\) összes egységszeresei a következők: \(\pm (1 + 2\omega), \pm (2 + \omega), \pm (1 - \omega)\).

(ii) Bármely Euler-egész a 0 és \(\pm 1\) Euler-egészek közül pontosan az egyikkel kongruens modulo \(\lambda\).

(iii) Bármely \(\alpha\) Euler-egészre \(\alpha^3 \equiv \alpha (\text{mod } \lambda)\).
(iv) $a \equiv \pm 1 \pmod{\lambda} \implies a^5 \equiv \pm 1 \pmod{\lambda^4}$.

Bizonyítás: (i) A T 7.7.6 Tétel alapján a $\lambda$ egységszeresei $\pm \omega$, $\mp \omega \lambda$ és $\pm \omega^2 \lambda$. A szorzásokat elvégezve, valamint az $\omega^2 = -1 - \omega$ és $\omega^5 = 1$ összefüggéseket felhasználva éppen a tételben megadott hat Euler-egész került.

(ii) Az

$$a + b \omega = a + b(1 - \omega) = a - b \omega^2 \lambda$$

azonosságból kerül, hogy

$$a + b \equiv a + b \pmod{\lambda}.$$

Mivel $a + b = 0$, 1 vagy $-1 \pmod{3}$ és $\lambda \mid 3$, ezért

$$a + b = 0, 1 \text{ vagy } -1 \pmod{\lambda}$$

is teljesül. Ezzel belátható, hogy bármely $a + b \omega$ Euler-egész kongruens 0-val, 1-gyel vagy $-1$-gyel modulo $\lambda$.

Azt kell még megmutatni, hogy a $0, 1$ és $-1$ páronként inkongruensek modulo $\lambda$, azaz $\lambda$ nem osztója semelyik két szám különbözőségeinek, $\pm 1$-nek, illetve $\pm 2$-nek. Ha $\lambda \mid \pm 1$, illetve $\lambda \mid \pm 2$ teljesülne, akkor $N(\lambda) \mid 1$, illetve $N(\lambda) \mid 4$ is fennállna, de ez $N(\lambda) = 3$ miatt lehetetlenné.

(iii) Azaz azonosít és következik (ii)-ből és az

$$\alpha^5 - \alpha = \alpha(\alpha - 1)(\alpha + 1)$$

azonosságból.

(iv) Ha $\alpha \equiv 1 \pmod{\lambda}$, akkor $\alpha = 1 + \beta \lambda$ (ahol $\beta$ alkalmas Euler-egész). A köbrel emelést elvégezve

$$\alpha^3 = 1 + 3\beta \lambda + 3\beta^2 \lambda^2 + \beta^3 \lambda^3$$

adódik. Innen a $-\lambda^2$ összefüggés alapján kerül, hogy

$$\alpha^3 = 1 - \beta^5 \lambda + \beta^2 \lambda^4 - \beta^5 \lambda^5 - 1 - \beta^2 \lambda^4 + (\beta^5 - \beta) \lambda^5.$$  \hspace{1cm} (12)

Mivel (iii) szerint $\lambda \mid \beta^5 - \beta$, ezért (12)-ből következik, hogy $\alpha^3 \equiv 1 \pmod{\lambda^4}$.

Az $\alpha \equiv -1 \pmod{\lambda}$ esetben hasonlóan járhatunk el, vagy $-\alpha \equiv 1 \pmod{\lambda}$ alapján visszavezethetjük az előző esetre. ∎

Megjegyzés: A T 7.7.9 Tétel több állítása a $\lambda$ helyett általánosabb modulusokra is érvényes (lásd a 7.7.12 feladatot [257]):

(ii) Bármely $\mu \neq 0$ Euler-egész esetén a „modulo $\mu$ maradékosztályok” száma $N(\mu)$. Ha ráadásul $N(\mu) = \nu = \text{primszám}$, akkor egy Z-beli modulo $\nu$ teljes maradékrendszer elemei egyben teljes maradékrendszer alkotnak az Euler-egészek körében modulo $\mu$. (A T 7.7.9 Tételben a $\mu = \lambda$, $N(\lambda) = \delta$ speciális eset szerepel.)
(iii): Tetszőleges \( \alpha \) Euler-egész és \( \tau \) Euler-prim esetén

\[
\alpha^{N(\tau)} \equiv \alpha \pmod{\tau}. 
\]

(Ez a kis Fermat-tétel megfelelője.)

Az előkészületek után nézzük a Fermat-sejtést a \( k = 3 \) kitevőre:

**7.7.10 Tétel**. \( \Leftrightarrow \) T 7.7.10

Az \( x^5 + y^3 = z^3 \) egyenletnek nincs olyan megoldása, ahol \( x \), \( y \) és \( z \) nullától különböző egész számok. \( \blacklozenge \)

**Bizonyítás:** Azt az általánosabb tételt igazoljuk, hogy a

\[
\zeta^5 + \eta^3 + \zeta^3 = 0
\]

egyenletnek nincs olyan megoldása, ahol \( \zeta \), \( \eta \) és \( \psi \) nullától különböző Euler-egészek.

Indirekt felteszük, hogy mégis létezik ilyen megoldás. A már többször látott módon szoritkozhatunk arra az esetre, amikor \( \zeta \), \( \eta \) és \( \psi \) relatív primek, sőt páronként relatív primek.

Ezután a bizonyítás gondolatmenete a következő. Először megmutatjuk, hogy \( \zeta \), \( \eta \) és \( \psi \) közül pontosan az egyik osztható \( \lambda \) -val, legyen ez mondjuk \( \zeta \). Ekkor \( \zeta \) -ből a maximális \( \lambda \) -hatványt kiemelve és \( \eta \) helyett \( \kappa \) -t irva (13)-at egy

\[
\xi^5 + \eta^3 + \zeta^3 = 0
\]

típusú egyenletre vezethetjük vissza, ahol

\[
\gamma \geq 1, \quad \varepsilon \text{ egység,} \quad \text{tevődhető.} \quad \lambda, \gamma, \kappa \text{ és } \psi \text{ páronként relatív primek.} \]

Itt megmutatjuk, hogy egyrészt \( u \neq 1 \), másrészt pedig ha (14) és (15) teljesül valamely \( n \)-nel, akkor (az \( \varepsilon \), \( \gamma \), \( \kappa \), \( \psi \) változók más értékei mellett) megvalósul \( n \) helyett \( n-1 \)-gyel is. Ez a végleteles leszállás adja az ellentmondást.

A végleteles leszálláshoz a kulcslépés a (14)-nek egy (11) típusú szorzattá bontása, ahol a jobb oldali három tényező közös osztója \( \lambda \), és a \( \lambda \) -val történő leosztás után már három páronként relatív prim szám marad, amelyek a számmelmélet alapétele szerint Euler-egészek köbeinek az egységszeresei.

Nézzük mindezt részletesen.

I. A (13)-ban \( \zeta \), \( \eta \) és \( \psi \) közül a páronként relatív primség miatt legfeljebb egy lehet osztható \( \lambda \) -val.

Ha egyikük sem lenne osztható \( \lambda \) -val, akkor a T 7.7.9 Tétel (iv) állítása szerint

\[
0 = \xi^3 + \eta^5 + \psi^3 \equiv \pm 1 \pm 1 \pm 1 = \pm 1 \text{ vagy } \mp 3 \pmod{\lambda^4}. 
\]

Innen \( \lambda^4 \mid 3 \), azaz \( 9 \mid 3 \) következik, ami lehetetlen.

II. Ezzel beláttuk, hogy \( \zeta \), \( \eta \) és \( \psi \) közül pontosan az egyik osztható \( \lambda \) -val, legyen ez mondjuk \( \zeta \), azaz

\[
\xi = \lambda^{\kappa}\gamma, \quad \text{ahol} \quad \lambda \mid \gamma. 
\]

\[253\]
Írjuk be (16)-ot (13)-ba, és jelöljük \(-\eta \cdot \kappa\)-val, ekkor átrendezés után éppen a (14) egyenletet és a (15) feltételeket kapjuk (speciálisan \(\varepsilon = 1\)).

Így elég azt megmutatni, hogy a (14) egyenlet és a (15) feltételek (semmilyen \(\varepsilon\) egységgel) nem teljesülhetnek.

III. Most azt igazoljuk, hogy (14)-ben \(\eta \neq 1\).

Tekintsük (14)-et modulo \(\lambda^4\), ekkor a T 7.7.9 Tétel (iv) állításából kapjuk, hogy

\[ \varepsilon \lambda^{3n} \gamma^3 = \kappa^4 - \psi^4 \equiv +1 - 1 = 0 \text{ vagy } +2 \quad (\text{n. on} \ \lambda^4). \tag{17} \]

A \(\pm 2\) eset lehetetlen, mert ebből \(\lambda \mid 2\) következne. Ezért (17) jobb oldalán 0 áll, azaz

\[ \lambda^4 \mid \varepsilon \lambda^{3n} \gamma^3, \]

és így \(\langle \lambda, \varepsilon \gamma \rangle = 1\) miatt \(\lambda^4 \mid \lambda^{3n}\), azaz \(n \geq 2\).

IV. Most következik a kulcs lépés, a vég指定 leszállás: ha (14) és (15) teljesül valamely \(\eta\) -nel, akkor (az \(\varepsilon\), \(\gamma\), \(\kappa\), \(\psi\) változók más értékei mellett) megvalósul \(\eta\) helyett \(\eta - 1\)-gyel is.

A (14) jobb oldalát szorzattá bontva

\[ \varepsilon \lambda^{3n} \gamma^3 = (\kappa - \psi)(\kappa - \psi \omega)(\kappa - \psi \omega^2) \tag{18} \]

adódik.

Mivel \(\lambda\) osztója (18) bal oldalának és \(\lambda\) Euler-prím, ezért \(\lambda\) a jobb oldal legalább egyik tényezőjének is osztója. Továbbá az egyes tényezők különbözők rendre \((\omega - 1)\psi\), \((\omega^2 - 1)\psi\), illetve \((\omega^2 - \omega)\psi\), amelyek valamennyien oszthatók \(\omega - 1 = \varepsilon \lambda\)-val. Ebből következik, hogy \(\lambda\) a (18) jobb oldalán szereplő mindhárom tényezőnek osztója.

Most belátjuk, hogy (18) jobb oldalán bármelyik két tényező legnagyobb közös osztója \(\lambda\). Nézzük ezt például az első két tényezőre, a többi hasonlóan megy.

Legyen \(\delta = (\kappa - \psi, \kappa - \psi \omega)\). Ekkor

\[ \delta \mid (\kappa - \psi) - (\kappa - \psi \omega) = \psi(\omega - 1) \]

és

\[ \delta \mid \omega(\kappa - \psi) - (\kappa - \psi \omega) = \kappa(\omega - 1), \]

tehat

\[ \delta \mid (\psi(\omega - 1), \kappa(\omega - 1)) = (\omega - 1)(\kappa, \psi) = \omega - 1 = \varepsilon \lambda. \]

Ezt a már korábban láttott \(\lambda \mid \delta\) oszthatósággal összeveto valóban \(\delta = \lambda\) adódik.

A fentiek alapján

\[ \frac{\kappa - \psi}{\lambda}, \frac{\kappa - \psi \omega}{\lambda}, \frac{\varepsilon \kappa - \psi \omega^2}{\lambda} \]

páronként relatív prímek, ezért a szármelmélet alaptételeből következik, hogy
ahol \( \varepsilon_1, \varepsilon_2, \varepsilon_3 \) egységek és \( \nu_1, \nu_2, \nu_3 \) páronként relatív prim Euler-egészek.

Most a \( \nu_i \)-ket a \( \lambda \)-val való oszthatóság szempontjából vizsgáljuk. Mivel a \( \nu_i \)-k páronként relatív prímek, ezért (mondjuk) \( \nu_2 \) és \( \nu_3 \) nem osztható \( \lambda \)-val. Legyen a \( \nu_1 \) „kanonikus alakjában” a \( \lambda \) kifejezése \( \kappa \), megmutatjuk, hogy \( s = n - 1 \).

Ennek igazolásához hasonlítsuk össze, hogy a (18) egyenlőség két oldala \( \lambda \)-nak pontosan hányadik hatványával osztható. A (18) bal oldalon ez a kitevő \( 3u \). A (18) jobb oldalon a tényezők (19)-beli előállításából azt kapjuk, hogy a \( \lambda \) mindhárom tényezőben előfordul az első hatványon, és emellett még \( \nu_3^3 \)-ben szerepel \( 3s \) kitevővel. Ennek alapján \( 3u = 3 + 3s \), azaz valóban \( s = u - 1 \), tehát

\[
\nu_1 = \lambda^{u-1}\gamma_1, \quad \text{ahol} \quad (\gamma_1, \lambda) = 1. \quad (20)
\]

Itt \( n \geq 2 \) miatt \( u - 1 \geq 1 \).

A következő lépésben megmutatjuk, hogy a (19)-beli egyenletek alakos lineáris kombinációját véve egy olyan (14) típusú egyenlőségekre jutunk, amelyben \( n \) helyett \( n - 1 \) szerepel (és ezzel kész a bizonyítás).

Adjuk össze a (19)-beli első egyenletet, a második egyenlet \( \omega \)-sorozat és a harmadik egyenlet \( \omega^2 \)-sorszámát:

\[
(\kappa - \psi) + \omega(\kappa - \psi_\omega) + \omega^2(\kappa - \psi_\omega^2) = \varepsilon_1\lambda
+ \varepsilon_4\lambda
+ \varepsilon_5\lambda
, \quad (21)
\]

ahol \( \varepsilon_4 = \varepsilon_2\omega \) és \( \varepsilon_5 = \varepsilon_3\omega^2 \) is egységek. A (21) bal oldala

\[
(\kappa - \psi) + \omega(\kappa - \psi_\omega) + \omega^2(\kappa - \psi_\omega^2) = (1 + \omega + \omega^2)(\kappa - \psi) = 0. \quad (22)
\]

Így (20), (21) és (22) alapján azt kapjuk, hogy

\[
0 = \varepsilon_1\lambda^{3(u-1)}\gamma_1^3 + \varepsilon_4\lambda\nu_2^3 + \varepsilon_5\lambda\nu_3^3.
\]

Innen \( \varepsilon_3 \lambda \)-val való osztás és átrendezés után

\[
\varepsilon_6\lambda^{3(u-1)}\gamma_1^3 = \varepsilon_7\nu_2^3 - \nu_3^3 \quad (23)
\]

adódik (ahol \( \varepsilon_6 \) és \( \varepsilon_7 \) egységek).

Belátjuk, hogy \( \varepsilon_7 = \pm 1 \), és így az \( \varepsilon_7\nu_2^3 \) tag helyére \( (\pm \nu_2)^3 \) irható.

Vizsgáljuk a (23) egyenletet modulo \( \lambda^3 \). Mivel \( u - 1 \geq 1 \), továbbá \( \lambda \mid \nu_2 \) és \( \lambda \mid \nu_3 \), ezért a T 7.7.9 Tétel (iv) pontja alapján azt kapjuk, hogy

\[
\varepsilon_7(\pm 1) - (\pm 1) \equiv 0 \pmod{\lambda^3},
\]

azaz \( \lambda^3 \) osztója \( \varepsilon_7 - 1 \)-nek vagy \( \varepsilon_7 + 1 \)-nek. Ekkor

\[
N(\lambda^3) \mid N(\varepsilon_7 + 1), \quad N(\lambda^3) = 27 \quad \text{és} \quad N(\varepsilon_7 + 1) < 27
\]
DIOFANTIKUS EGYENLETEK

miatt \( c_T + 1 = 0 \), vagyis valóban csak \( c_T = \pm 1 \) lehetséges.

Ennek alapján (23) átírható az

\[
\varepsilon \lambda^{3(\nu_1-1)} \gamma T = (\pm \nu_2)^3 - \nu_3^2
\]

alakba. Ez azt jelenti, hogy a (14) egyenlet kielégíthető \( n \) helyett \( n - 1 \) -re is, és a (15) feltételek is teljesülnek (\( \varepsilon, \gamma, \kappa \), illetve \( \psi \) helyére rendre \( \varepsilon n, \gamma T, \pm \nu_2 \), illetve \( \nu_3 \) került).

Feladatok

7.7.1 (a) Mutassuk meg, hogy ha \( \hat{k} \mid m \), és két pozitív \( \hat{k} \)-adik hatvány összege sohasem \( \hat{k} \)-adik hatvány, akkor két pozitív \( \hat{m} \)-edik hatvány összege sem lehet \( \hat{m} \)-edik hatvány.

(b) Indokoljuk meg, miért elég a Fermat-sejtést a \( \hat{k} = 4 \) és \( \hat{k} = \varphi = \text{prim kitevőkre igazolni}.

7.7.2 Hány megoldása van az alábbi egyenleteknek a pozitív egészek körében?

(a) \( x^{20} + y^{24} = z^{28} \);

(b) \( x^5 + y^4 = z^5 \).

7.7.3 Oldjuk meg a \( \hat{k}^2 + \hat{m}^2 = k^2 \) „exponenciális” Fermat-egyenletet (ahol \( \hat{k}, \hat{w}, y, z \) pozitív egészek).

7.7.4 Az alábbiakban megvizsgáljuk a „Fermat-egyenletet” néhány olyan esetben, amikor a kitevő nem pozitív egész. Határozzuk meg az összes \( x, y, z \) pozitív egész megoldást.

(a) \( k = -4 \) : \( \frac{1}{x^2} + \frac{1}{y^2} = \frac{1}{z^2} \).

(b) \( k = -2 \) : \( \frac{1}{x^2} + \frac{1}{y^2} = \frac{1}{z^2} \).

(c) \( k = \sqrt{2} \) : \( \sqrt{x} + \sqrt{y} = \sqrt{z} \).

(d) \( k = \sqrt{3} \) : \( \sqrt[3]{x} + \sqrt[3]{y} = \sqrt[3]{z} \).

7.7.5 Bizonyítsuk be az alábbi állításokat.

(a) Az \( x^4 + y^2 = z^2 \) és \( x^2 + y^2 = z^2 \) egyenleteknek végétlen sok olyan pozitív egész megoldása van, ahol \( \{ x, y, z \} = 1 \).

(b)(M [595]) * Az \( x^4 + y^4 = z^2 \) egyenlet nem oldható meg a pozitív egészek körében.

Megjegyzés: A (b) részből egy újabb bizonyítást nyerünk a Fermat-sejtés \( \hat{k} = 4 \) esetére.

7.7.6 (*) Oldjuk meg az \( x^4 + 2y^2 = -1 \) diofantikus egyenletet.

7.7.7 (M [596]** ) Milyen alapú számrendszerben igaz, hogy az 1111 alakú szám négyzetszám?

7.7.8 Mely Euler-egészek oszthatók a konjugáltjukkal?

7.7.9 Igazoljuk az alábbi azonosságot (\( a, b, c, d \) tetszőleges valós számok):

256
(a) Bizonyítsuk be, hogy az \( x^2 - py + y^2 = n \) diofantikus egyenlet akkor és csak akkor oldható meg, ha megoldható az \( x^2 + 2y^2 = n \) diofantikus egyenlet.

(b) Milyen \( n \)-ekre oldható meg az (a)-beli két diofantikus egyenlet, és mennyi a megoldásszám?

7.7.11 (M [599]*) Oldjuk meg az \( x^2 + 243 = y^3 \) diofantikus egyenletet.

7.7.12 Legyen \( \mu \neq 0 \) Euler-egész. A \( \vartheta_1, \ldots, \vartheta_r \) Euler-egészeket teljes maradékrendszernek nevezzük modulo \( \mu \), ha bármely \( \alpha \) Euler-egészre az \( \alpha \equiv \vartheta_i \pmod{\mu} \) kongruencia pontosan egy \( \vartheta_i \)-re teljesül. Bizonyítsuk be az alábbi állításokat.

(a) Egy modulo \( \mu \) teljes maradékrendszer elemszáma \( N(\mu) \).

(b) Ha \( N(\mu) = p \) prímszám, akkor \( \vartheta_1, \vartheta_2, \ldots, N(\mu) - 1 \) teljes maradékrendszert alkotnak modulo \( \mu \).

(c) Érvényes a kis Fermat-tétel megfelelője: tetszőleges \( \alpha \) Euler-egész és \( \pi \) Euler-prím esetén

\[ \alpha^{N(\pi)} \equiv \alpha \pmod{\pi}. \]

7.7.13 Oldjuk meg az alábbi diofantikus egyenletet:

\[ \frac{x}{y} + \frac{v}{w} - \frac{z}{w}. \]

7.7.14 (a) Mutassuk meg, hogy ha egy derékszögű háromszög oldalai egész számok, akkor a háromszög területe nem lehet négyzeteszám. 

(b) Bizonyítsuk be, hogy ha egy derékszögű háromszög oldalai páronként relatív prim egész számok, akkor a háromszög területe nem lehet köbszám.

(c) Van-e olyan egész oldalú derékszögű háromszög, amelynek a területe köbszám?

(d) Vizsgáljuk meg a probléma általánosítását magasabb hatványokra.

7.8 Pell-egyenlet

Pell-egyenletnek egy

\[ x^2 - ny^2 = 1 \]  \hspace{1cm} (1)

alakú diofantikus egyenletet nevezzünk, ahol az \( n \) (rögzített) pozitív egész és nem négyzetszám. Az (1) egyenlet két triviális megoldása \( x = \pm 1, \ y = 0 \), az ezektől különböző (azaz \( y \neq 0 \) típusú) megoldások a nemtriviális megoldások.

Az (1) bal oldalát szorzattá bontjuk:

\[ (x + y\sqrt{n})(x - y\sqrt{n}) = 1. \]  \hspace{1cm} (2)

Ebből következik, hogy ha \( x, y \) megoldása (1)-nek, akkor az \( a + b\sqrt{n} \) alakú számok körében (ahol \( a \) és \( b \) egészek) az \( \omega + y\sqrt{n} \) és \( \omega - y\sqrt{n} \) számok osztói az 1-nek, és így mindkettő egységek.
Mivel egy egység tetszőleges (egész kitevős) hatványa is egység, ezért ha létezik egy \( \epsilon \neq \pm 1 \) egység, akkor az \( \epsilon \) hatványnak végétében sok egységet adnak. Ez a Pell-egyenletre „visszafogalmazva” azt jelenti, hogy ha (1)-nek létezik nemtriviális megoldása, akkor végétlen sok megoldás van. (Az \( m = 2 \), illetve \( m = 3 \) speciális eset lényegében szerepelt az 1.1.22 feladatban [4], illetve az T 5.2.4 Tétel bizonyítása során.)

Az alábbiakban először megmutatjuk, hogy a Pell-egyenletnek mindig végétlen sok megoldása van (az előbbiek szerint ehhez előég azt bizonyítani, hogy legalább egy nemtriviális megoldás létezik). Ezután megadjuk, hogyan lehet az összes megoldást megkapni.

Megjegyezzük még, hogy az (1) egyenlet az \( m \leq 0 \) és \( m = k^2 \) esetekben alapvetően másképpen viselkedik, lásd a 7.8.1 feladatot [261].

7.8.1 Tétel.  T 7.8.1

Legyen \( m \) olyan pozitív egész, amely nem négyzeteszám. Ekkor az (1) diofantikus egyenletnek végétlen sok megoldása van. ♣

A bizonyítás során fel fogjuk használni a következő fejezetből a T 8.1.1 Tételt.

Bizonyítás: Ha \( \eta \neq 0 \), akkor az (1)-gyel ekvivalens (2) egyenlőség az

\[
\frac{x}{y} - \sqrt{m} = \frac{1}{y(x + y\sqrt{m})}
\]

alakra hozható.

(3)-ból látszik, hogy \( x > 0 \), \( y > 0 \) esetén \( x \), \( y \) csak akkor lehet megoldás, ha \( x/y \) „nagyon közel” van \( \sqrt{m} \)-hez: \( \sqrt{m} > 1 \) miatt (3) fennállása esetén

\[
\left| \sqrt{m} - \frac{x}{y} \right| < \frac{1}{y^2}.
\]

A \( \sqrt{m} \) irracionalitása miatt a T 8.1.1 Tételből következik, hogy (4) valóban végétlen sok \( x \), \( y \) egész számpárra teljesül. Ezt a tényt felhasználva most azt igazoljuk, hogy (2)-nek is végétlen sok megoldása van. (A (4) és (2) feltételek nem ekvivalensek, a (4)-et kielégítő \( x \), \( y \) értékeknek csak egy része teljesíti majd (2)-t is.)

I. Első lépésként megmutatjuk, hogy van olyan \( t \neq 0 \) egész, amelyre az

\[
x^2 - my^2 = t
\]

diofantikus egyenletnek végétlen sok megoldása van.

Legyenek \( c_j \), \( d_j \) (\( j = 1, 2, \ldots \)) olyan pozitív egész számpárok, amelyek eleget tesznek (4)-nek, azaz

\[
\left| \sqrt{m} - \frac{c_j}{d_j} \right| < \frac{1}{d_j^2}, \quad j = 1, 2, \ldots
\]

Ekkor

\[
c_j^2 - md_j^2 = d_j \left( \frac{c_j}{d_j} \sqrt{m} - \sqrt{m} \right) < \frac{1}{d_j^2} + 2\sqrt{m} < 1 + 2\sqrt{m}. \quad (5)
\]
A (6)-ból következik, hogy a \( c_j^2 - \frac{mn}{m_j} \) értékek csak a \((-1 - 2\sqrt{m}, 1 + 2\sqrt{m})\) intervallumba eső véges sok egész szám közül kerülhetnek ki, továbbá \( \sqrt{m} \) irracionálitása miatt a 0 nem jöhet szóba.

A skatulyaelv értelmében ekkor található ebben az intervallumban olyan \( t \neq 0 \) egész szám, hogy
\[
c_j^2 - \frac{mn}{m_j} = t
\]

végten sok \( c_j \), \( d_j \) párra teljesül. Ez azt jelenti, hogy az (5) diofantikus egyenletnek végiglen sok megoldása van.

II. Most megmutatjuk, hogy az (5) egyenlet alkalmazó megoldásainak „hányadosaiból” az (1) egyenlet megoldásaikhoz jutunk.

Legyen \( x = a_1 \), \( y = b_1 \), illetve \( x = a_2 \), \( y = b_2 \) az (5) egyenlet két megoldása, azaz
\[
a_1^2 - nb_1^2 = (a_1 + b_1\sqrt{m})(a_1 - b_1\sqrt{m}) = t, \tag{7a}
\]
\[
a_2^2 - nb_2^2 = (a_2 + b_2\sqrt{m})(a_2 - b_2\sqrt{m}) = t, \tag{7b}
\]

\( t \) és teygük fel, hogy
\[
a_1 = a_2 \pmod{\mid t\mid} \quad \text{és} \quad b_1 = b_2 \pmod{\mid t\mid}. \tag{8}
\]

A (7a), (7b) és (8) feltételek teljesülése esetén az \( a_1 \), \( b_1 \) és \( a_2 \), \( b_2 \) számpárokat az (5) egyenlet modulo \( \mid t\mid \) kongruens megoldásainak fogjuk nevezni.

A (7a) egyenlőséget (7b)-vel elosztva azt kapjuk, hogy
\[
\frac{a_1 + b_1\sqrt{m}}{a_2 + b_2\sqrt{m}} \cdot \frac{a_1 - b_1\sqrt{m}}{a_2 - b_2\sqrt{m}} = 1. \tag{9}
\]

A (9) bal oldalán szereplő első tört
\[
\frac{a_1 + b_1\sqrt{m}}{a_2 + b_2\sqrt{m}} = u + v\sqrt{m}
\]

alakba írható (ahol \( u \) és \( v \) racionális számok), és ekkor a második törtre szükségképpen fennáll
\[
\frac{a_1 - b_1\sqrt{m}}{a_2 - b_2\sqrt{m}} = u - v\sqrt{m}.
\]

Belátjuk, hogy (8) miatt \( u \) és \( v \) egész számok, tehát \( u \) és \( v \) valóban az (1) egyenlet egész megoldását adják.

A nevező szokásos „gyökeltelenítésével” és (7b) felhasználásával kapjuk, hogy
\[
\frac{a_1 + b_1\sqrt{m}}{a_2 + b_2\sqrt{m}} - (a_1 + b_1\sqrt{m})(a_2 - b_2\sqrt{m}) = \frac{(a_1 + b_1\sqrt{m})(a_2 - b_2\sqrt{m})}{l}, \tag{9}
\]

Így azt kell igazolnunk, hogy az
\[
(a_1 + b_1\sqrt{m})(a_2 - b_2\sqrt{m}) = r + s\sqrt{m}
\]

felirásban \( r \) és \( s \) osztható \( t \)-vel. Ez (8)-ból és (7a)-ból következik:
DIOFANTIKUS EGYENLETEK

\( r + \sqrt{m} = (a_1 + b_1 \sqrt{m})(a_2 - b_2 \sqrt{m}) = a_1^2 - b_1^2 m = \ell = 0 \mod |k| \).

(A kongruenciát az \( a + b \sqrt{m} \) számokra a már többször látott „természetes” értelemben használtuk.)

III. Mivel egy \( a \) és \( b \) számparában az \( a \) és \( b \) is \( |k| \)-féle maradékoval hatod modulo \( |k| \), ezért az (5) egyenlet páronként inkongruens megoldásainak a száma legfeljebb \( p^2 \). Ismét a skatulyaelvet alkalmazva ebből következik, hogy az (5) egyenlet végében sok megoldása között kell lennie végtelelen sok olyannak, amelyek közül bármelyik kettő kongruens modulo \( |k| \). Legyenek \( x = f_i \), \( y = g_i \), \( i = 1, 2, \ldots \) ilyen megoldások.

Ekkor a II. rész szerint az \( f_i \), \( g_i \) és \( f_i \), \( g_i \) „hányadosaként” keletkező \( r_i \), \( s_i \) értékek az (1) diofantikus egyenlet végében sok (különböző) megoldását adják.

\[ 7.8.2 \text{ Tétel.} \quad T \, 7.8.2 \]

Legyen \( m \) olyan pozitív egész, amely nem négyzeteszám, és \( x_0 \), \( y_0 \) az (1) diofantikus egyenletnek az (az egyértelműen meghatározott) megoldása, amelyre \( x_0 > 0 \), \( y_0 > 0 \) és \( x_0 + y_0 \sqrt{m} \) minimális. Ekkor az összes megoldást az

\[ x + y \sqrt{m} = \pm (x_0 + y_0 \sqrt{m})^n, \quad n = 0, \pm 1, \pm 2, \ldots \quad (10) \]

képlettel meghatározott \( x \), \( y \) egész számpárok adják. ✤

A (2) egyenlőségből látszik, hogy

\[ (x_0 + y_0 \sqrt{m})^n - (x_0 - y_0 \sqrt{m})^n, \quad (11) \]

ezért (10) az

\[ x + y \sqrt{m} = \pm (x_0 \pm y_0 \sqrt{m})^n, \quad n = 0, 1, 2, \ldots \]

formában is megadható.

Az \( n = 0 \) esetben a két triviális megoldást kapjuk.

\textbf{Bizonyítás:} Többször fel fogjuk használni, hogy két megoldásnak az alábbi értékeken vett szorzata is megoldás.

Tegyük fel, hogy \( x_1 \), \( y_1 \), illetve \( x_2 \), \( y_2 \) egy-egy megoldása (1)-nek, azaz

\[ (x_1 + y_1 \sqrt{r}) (x_1 - y_1 \sqrt{r}) = 1, \quad (12a) \]

\[ (x_2 + y_2 \sqrt{r}) (x_2 - y_2 \sqrt{r}) = 1. \quad (12b) \]

A (12a) és (12b) egyenlőségeket összeszorozva

\[ (x_1 x_2 + y_1 y_2 + x_1 y_2 + y_1 x_2 \sqrt{r}) (x_1 x_2 + y_1 y_2 - x_1 y_2 - y_1 x_2 \sqrt{r}) = 1 \]

adódik, ami azt jelenti, hogy

\[ x_3 = x_1 x_2 + y_1 y_2, \quad y_3 = x_1 y_2 + y_1 x_2 \]

is megoldása (1)-nek. (Minden a bevezetőben jelzett, az egységekre vonatkozó átfogalmazásban annak felel meg, hogy két egység szorzata is egység.)

260
A fentiekből és (11)-ből nyilvánvalóan következik, hogy a (10) képlettel megadott \( x, y \) számpárok kielégítik (1)-et.

Most belátjuk, hogy ez az összes megoldás. Tegyük fel indirekt, hogy létezik egy \( x, y \) megoldás, amely nem ilyen alakú. Ekkor nyilván \( -x, -y \) is megoldás és ez sem szerepel a (10)-beli megoldások között. Ezért feltehető, hogy \( x + y\sqrt{m} > 0 \).

Ekkor létezik olyan \( k \) egész szám, amelyre

\[
(x_0 + y_0\sqrt{m})^k < x + y\sqrt{m} < (x_0 + y_0\sqrt{m})^{k+1}. \tag{13}
\]

A (13)-at \( (x_0 - y_0\sqrt{m})^k \)-nál beszorozva

\[
1 < (x + y\sqrt{m})(x_0 - y_0\sqrt{m})^k < x_0 + y_0\sqrt{m} \tag{14}
\]

adódik. Itt

\[
(x - y\sqrt{m})(x_0 - y_0\sqrt{m})^k = x' + y'\sqrt{m}
\]

megoldások összeszorzásával keletkezett, tehát \( x', y' \) is megoldás, azaz

\[
(x' + y'\sqrt{m})(x' - y'\sqrt{m}) = 1. \tag{15}
\]

A (14)-beli első egyenlőtlenség szerint

\[
x' + y'\sqrt{m} > 1, \tag{15a}
\]

így (15) miatt

\[
0 < y' < y'\sqrt{m} < 1. \tag{16b}
\]

A (16b) miatt nem lehetségesek az \( y' = 0 \), az \( x' < 0 \), \( y' > 0 \) esetek, valamint az \( x' > 0 \), \( y' < 0 \) esetek, a (16a) miatt pedig nem fordulhat elő \( x' < 0 \), \( y' > 0 \). Ezért \( x' > 0 \), \( y' < 0 \), ez azonban (14) szerint ellentmond \( x_0 + y_0\sqrt{m} \) minimalitásának.

Feladatok

7.8.1 Határozzuk meg az \( x^2 - r y^2 = 1 \) diofantikus egyenlet összes megoldását, ha \( m \leq 0 \), illetve ha \( m \) négyzetszám.

7.8.2 Hány olyan négyzetszám van, amely után (tízes számrendszerben) egy 1-est írva ismét négyzetszámot kapunk?

7.8.3 Legyen \( m \) olyan pozitív egész, amely nem négyzetszám, és \( r \) tetszőleges egész szám. Bizonyítsuk be, hogy ha az \( x^2 - r y^2 = 1 \) diofantikus egyenlet megoldható, akkor végig sok megoldása van.

7.8.4 (a) Hány olyan négyzetszám van, amely

(a1) 1-gyel nagyobb; (a2) 1-gyel kisebb

egy négyzetszám kétszeresénél?
(b) Vizsgáljuk meg a kérdést kétszeres helyett háromszorosra is.

7.8.5 Hány olyan \( n \) van, amelyre \( \binom{2}{2} \) négyzetszám?

7.8.6 Hány olyan (páronként nem egybevágó) derékszögű háromszög van, amelynek a befogói szomszédos egész számok és az átfogója is egész szám?

7.8.7 Hány megoldása van az alábbi diofantikus egyenleteknek:

(a) \( x^2 - 3y^2 = 2 \);
(b) \( x^2 - 3y^2 = 7 \);
(c) \( x^2 - 3y^2 = 13 \);
(d) \( x^2 - 3y^2 = 39 \);
(e) \( 2x^2 - 3y^2 = 1 \);
(f) \( 3x^2 - 2y^2 = 1 \).

7.8.8 (*) Mely prímszámok esetén oldható meg az \( x^2 - py^2 = -1 \) diofantikus egyenlet?

7.8.9 Legyenek az \( a \), \( b \), \( c \) nem nulla egészek páronként relatív prímek, és tegyük fel, hogy az \( ax^2 + by^2 + cz^2 = 0 \) diofantikus egyenletnek létezik nemtriviális (vagyis az \( x = y = z = 0 \) -tól különböző) megoldása. Bizonyítsuk be, hogy ekkor \( a \), \( b \) és \( c \) előjele nem lehet azonos, továbbá megoldhatók az

\[
\begin{align*}
\alpha^2 &\equiv -bc \mod |a|, \\
\beta^2 &\equiv -ac \mod |b|, \\
\gamma^2 &\equiv -ab \mod |c|
\end{align*}
\]

kongruenciák.

Megjegyzés: Megmutatható, hogy ezek a feltételek nemcsak szükségesek, hanem elégségesek is ahhoz, hogy az \( ax^2 + by^2 + cz^2 = 0 \) diofantikus egyenletnek létezzék nemtriviális megoldása.

7.8.10 Hány olyan \( k \) egész szám létezik, amelyre \( 2 + 2\sqrt{28k^2 + 1} \) négyzetszám?

7.8.11 (*) Mutassuk meg, hogy az \( x^2 - 2y^2 = 1 \) Pell-egyenlet nemtriviális megoldásaiban sem \( x \), sem \( y \) nem lehet négyzetszám.

7.9 Partíciók

7.9.1 Definíció .  

Az \( n \) pozitív egész \( p \)-réz az \( n \) -nek pozitív egészek összegeként történő lényegesen különböző előállításait értjük (azaz azonosnak tekintjük a csupán az összeadandók sorrendjében eltérő előállításokat). Itt az egytagú összeget is megengedjük.

Az \( n \) partícióinak számát \( p(n) \) -nel jelöljük. ♦

Példa: A 4 összes partíciói

\[
4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1,
\]
Bizonyítás nélkül közöljük a \( p(n) \) függvényre vonatkozó aszimptotikus eredményt: (\( n \to \infty \) esetén)

\[
p(n) \sim \frac{c}{\sqrt{n}}, \quad \text{ahol} \quad c = \frac{1}{4\sqrt{3}}, \quad \text{és} \quad d = \frac{\pi \sqrt{6}}{3}.
\]

Gyakran vizsgálunk olyan partíciós kérdéseket, amikor az \( n \)-et előállító összeadandókra vagy azok számára teszünk bizonyos megkötéseket: például előírhatjuk, hogy csupa páratlan szám vagy csupa különböző szám szerepeljen összeadandóként stb.

A partíciós feladatok kezelésének alapvető eszköze a generátorfüggvény. Ennek illusztrálására tekintsük az ún. pénzkifizetési (vagy pénzváltási) problémát: hányféleképpen lehet \( n \) forintot (például 50 forintosnál kisebb pénzértékkel kifizetni. Ekkor az \( n \) olyan partícióiról van szó, ahol összeadandóként csak az 1, 2, 5, 10 és 20 számokat engedjük meg, jelöljük az ilyen partíciók számát \( f(n) \) -nel.

A feladatot a következő módon érdemes átfogalmazni. Jelölje egy ilyen kifizetésnél a felhasznált 1, 2, 5, 10, illetve 20 forintosok számát rendre \( u_1, \ldots, u_5 \), ekkor \( f(n) \) az

\[
1u_1 + 2u_2 + 5u_3 + 10u_4 + 20u_5 = n
\]
diofantikus egyenlet nemnegatív egész megoldásainak a száma.

Az \( f(n) \) függvény generátorfüggvényén az

\[
P(x) = 1 + \sum_{n=1}^{\infty} f(n)x^n
\]

hatványsort értjük. Először megmutatjuk, hogy ez a sor \(|x| < 1/2\) esetén abszolút konvergens.

Mivel (1)-ben bármely \( i \) -re \( 0 \leq u_i \leq n \), ezért

\[
0 \leq f(n) \leq (n+1)^5.
\]

Könnyen látható, hogy ha \( n \) elég nagy, akkor \((n + 1)^5 \) \( < 2^n\) , így a (2) végahlenes sor \(|x| < 1/2\) esetén majorálható a

\[
\sum_{n=0}^{\infty} (2|x|)^n
\]

konvergens végahlenes mértani sorral. Ezzel beláttuk, hogy \(|x| < 1/2\) esetén \( P(x) \) abszolút konvergens.

(Ez igazolható \(|x| < 1\) -re is.)

Most \( P(x) \)-et előállítjuk konvergens mértani sorok szorzataként (továbbra is feltesszük, hogy \(|x| < 1/2\)).

\[
P(x) = (1 + x + x^2 + \ldots)(1 + x^2 + (x^2)^2 + \ldots)(1 + x^5 + (x^2)^2 + \ldots) \cdot (1 + x^{10} + (x^{10})^2 + \ldots)(1 + x^{20} + (x^{20})^2 + \ldots). \quad (3)
\]

Mivel egy függvény a 0 körül csak egyféléleképpen fejlődhető hatványsorba, így azt kell megmutatnunk, hogy (3) jobb oldalán a véges sok abszolút konvergens sor szorzását elvégezve \( x^n \) együtthatója éppen

\[
= \frac{(n+1)^5}{4\sqrt{3}}.
\]

tehát \( P(4) = 5 \).

DIOFANTIKUS EGYENLETEK

263
DIOFANTIKUS EGYENLETEK

$f(n)$ lesz. Az $n$ minden (1)-beli előállításának feleltessük meg azt a szorzatot, amelyet úgy kapunk, hogy (3) jobb oldaláról rendre a

tagokat szorozzuk össze. Ez a szorzat éppen

$$x^{u_1} (x^2)^{u_2} (x^5)^{u_3} (x^{10})^{u_4} (x^{20})^{u_5} = x^{u_1 + 2u_2 + 5u_3 + 10u_4 + 20u_5} = x^n.$$  

Mivel a szóban forgó előállítások és szorzatok között kölcsönösen egyértelmű megfeleltetés áll fenn, ezért (3) jobb oldalán a szorzást elvégezve $x^n$ együthatója valóban $f(n)$ lesz.

A mértani sorok összegképletét felhasználva (3) átírható az

$$F(x) = \frac{1}{(1-x)(1-x^2)(1-x^5)(1-x^{10})(1-x^{20})} \quad (|x| < 1/2)$$

alakba.

A fentiak teljesen azonos módon kapjuk az alábbi általánosabb eredményt is:

7.9.2 Tétel. T 7.9.2

Legyenek $a_1, a_2, \ldots, a_r$ különböző pozitív egészek, és jelöljük $f(n)$-nel az $n$ pozitív egésznek az $a_1, a_2, \ldots, a_r$ összeadandókból képzett partíciói számát. Ekkor $|x| < 1/2$ esetén az

$$1 + \sum_{n=1}^{\infty} f(n)x^n \quad \text{végében sor abszolút konvergens és}$$

$$1 + \sum_{n=1}^{\infty} f(n)x^n = \prod_{i=1}^{r} \frac{1}{1-x^{a_i}}.$$  

Hasonlóan adódik $\varphi(n)$ generátorfüggvénye is:

7.9.3 Tétel. T 7.9.3

$$F(x) = 1 + \sum_{n=1}^{\infty} \varphi(n)x^n = \prod_{i=3}^{\infty} \frac{1}{1-x^i} \quad (|x| < 1).$$  

A (4) jobb oldalán szereplő végében szorzat (az 5.6.6 [149] és 5.6.7 feladatokban [149] megadott módon) az alábbi határértéket jelenti:

$$\prod_{i=3}^{\infty} \frac{1}{1-x^i} = \lim_{r \to \infty} \prod_{i=1}^{r} \frac{1}{1-x^i}.$$  

A T 7.9.3 Tétel igazolásához a T 7.9.2 Tételt kell az $a_i = i$ esetre alkalmazni, majd az $r \to \infty$ határátmenetet kell képzezi. A bizonyítást nem részletezzük.

A partíciók kezeléséhez a generátorfüggvények mellett kombinátorikus jellegű meggondolások is jól használhatóak. Az $u = a_1 + a_2 + \cdots + a_r$ partíciót, ahol $a_1 \geq a_2 \geq \cdots \geq a_r$ egy olyan pontsémával ábrázolhatjuk, amelynek első sorában $a_1$ , a második sorában $a_2$ stb. pont van. Például a

$$\cdots \cdots \cdots$$

(5)
séma a $12 = 5 + 3 + 3 + 1$ particiónak felel meg. Az értelmezésből nyilvánvaló, hogy egy ilyen séma egyetlen sorban sem lehet több elem, mint a felette levő sorban.

A sémában az egyes sorok felelnek meg a partició tagjainak, azonban néha hasznos a sémát „oszloponként” is leolvasni. Például az (5) sémánál ekkor a $12 = 4 + 3 + 3 + 1 + 1$ particióhoz jutunk. A sémáknak ebből a kétféle leolvasásából kapjuk az alábbi eredményt:

### 7.9.4 Tétel. T 7.9.4

Legyen $g_r(n)$, illetve $h_r(n)$ az $n$ szám olyan particióinak a száma, ahol az összeadandók száma, illetve maximuma $r$. Ekkor $g_r(n) = h_r(n)$. 

#### Bizonyítás

Tekintsük azokat az $n$ pontból álló sémákat, amelyeknek pontosan $r$ sora van. Egy ilyen sémát soronként nézve az $n$ -nek egy $r$ összeadandóból álló particióját kapjuk, oszloponként nézve pedig az $n$ -nek egy olyan particiójához jutunk, amelyben a legnagyobb összeadandó $r$. Az ilyes ilyen sémát összeszámolva így éppen a kívánt $g_r(n) = h_r(n)$ egyenlőség adódik.

A következőkben az $n$ számnak páros sok, illetve páratlan sok különböző összeadandóból álló particiót vizsgáljuk. Az alábbi, Eulertől származó tételből kiderül, hogy a kétféle partíció száma között bármely $n$ esetén legfeljebb 1 az eltéré.

### 7.9.5 Tétel. T 7.9.5

Jelölje $s(n)$, illetve $t(n)$ az $n$ pozitív egész azon particióinak a számát, ahol minden összeadandó különböző, és a tagok száma páros, illetve páratlan. Ekkor

$$s(n) - t(n) = \begin{cases} (-1)^k, & \text{ha } n = \frac{1}{2}(3k^2 \pm k); \\ 0, & \text{egyébként.} \end{cases}$$

#### Példa

Az $n = 7$ páros, illetve páratlan sok különböző összeadandóból történő előállításai

$6 + 1 = 5 + 2 = 4 + 3$, \quad \text{illetve} \quad 7 = 4 + 2 + 1,$

tehát $s(7) = 3$, $t(7) = 2$. Az $s(7) - t(7) = 3 - 1 = (-1)^2$ egyenlőség összhangban van (6)-tal, hiszen $7 = \frac{1}{2}(3 \cdot 2^2 + 2)$.

#### Bizonyítás

„Majdnem” kölcsönösen egyértelmű megfeleltetést fogunk létesíteni az $n$ páros, illetve páratlan sok különböző összeadandóból álló particiói között.

Az $n$ csupa különböző tagból álló particiói olyan sémáknak felelnek meg, amelyekben az egyes sorokban fentről lefelé szigorúan csökkentő számú elem szerepel, például a $23 = \overline{7 + 5 + 3 + 2}$ particiónak a

$$
\begin{array}{cccccc}
\vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
\end{array}
$$

séma felel meg.

Nevezzük egy ilyen séma élének a jobb felső pontból induló, 45 fokos szögben haladó maximális hosszúságú „ÉK-DNy” irányú pontsort. A (7) séma éle 3 pontból áll. (Az elemértéket általában az határozza meg, meddig tart az összeadandók egyesével történő csökkentése, az él elemértéke lehet természetesen 1 is.)
Legyen $A$, az a transzformáció, amely egy séma élét áthelyezi a séma utolsó sora alá (új utolsó sornak), feltéve, hogy így ismét egy csupa különböző összeadandóból álló partició jön létre, azaz egy szigorúan csökkentő elemszáμú sorokból álló sémat kapunk. Hasonlóképpen, legyen $M$, az a transzformáció, amely egy séma utolsó sorát áthelyezi a séma éle mellé (ferdén, új élnek), amennyiben így ismét egy megfelelő séma keletkezik. A (7) séma esetén $M$-et alkalmazvá a

sémához jutunk, ugyanakkor $A$ nem végezhető el.

Megmutatjuk, hogy néhány kivételtől eltekintve bármely séma esetén $A$ és $M$ közül pontosan az egyik hajtható végre.

Legyen a séma utolsó sorának elemszáma $a$, az él elemszáma pedig $m$.

Ha $a \leq m$, akkor $A$ nem hajtható végre, $M$ viszont igen, kivéve, ha $a = m$ és az utolsó sor és az él összeér (ekkor sem $A$, sem $M$ nem végezhető el):

(*)

Ha $a > m$, akkor $M$ nem hajtható végre, $A$ viszont igen, kivéve, ha $a = m + 1$ és az utolsó sor és az él összeér (ekkor sem $M$, sem $A$ nem végezhető el):

(**)

Az $A$, illetve $M$ transzformáció alkalmazása a séma sorainak számát 1-gyel növeli, illetve csökkenti, tehát az eredeti és a transzformáció után keletkező particióban az összeadandók száma ellentétes paritású. Villágos továbbá, hogy $A$ és $M$ egymás inverzei, azaz bármilyen sorrendben történő egymás utáni alkalmazásukkal a kiindulási sémat kapjuk vissza. Ebből következik, hogy az $A$, $M$ transzformációpár a (•) és (**) típusú partióktól eltekintve kölcsönösen egyértelmű megfeleltetést létesít az $n$ páros, illetve páratlan sok különböző összeadandóból álló partióció között.

Ebből következik, hogy $s(n) = t(n)$, kivéve ha $n$ -nek létezik (•) vagy (**) típusú partiója, amikor is $s(n) - t(n)$ aszerint 1, illetve $-1$, hogy a „rossz” partióiban az összeadandók száma páros, illetve páratlan (ehhez azt is igazolni kell még, hogy egy adott $n$-nek nem lehet egynél több rossz partiója).

Ha a (•) partióiban $k$ tag van (azaz a sémában a sorok száma $k$), akkor

$$s_k = (2k - 1) + (2k - 2) + \cdots + k = \frac{(3k - 1)k}{2}. \quad (\hat{8})$$

Ugyanígy adódik, hogy ha a (**) partió $k$ tagból áll, akkor

$$s_k = 2k + (2k - 1) + \cdots + (k + 1) = \frac{(3k + 1)k}{2}. \quad (\hat{9})$$

Adott $n$, re (8), illetve (9) nyilván legfeljebb egy $k$-val teljesülhet, továbbá $n$ nem lehet egyszerre (8) és (9) alakú is, ugyanis
ami pozitív egész $k$ és $j$ esetén nem állhat fenn.

Így a (8) és (9) képlettel meghatároztuk a kivételes $n$ -eket, és beláttuk, hogy minden ilyen $n$ -nek csak egy rossz partíciója van. Ezzel a (6) képletet teljes egészében igazoltuk.

Mint jeleztük, a T 7.9.5 Tételnek fontos következményei vannak a $P(n)$ függvényre nézve is. Legyen $u(n) = s(n) - t(n)$, ekkor a T 7.9.5 Tétel szerint $u(n)$ generátorfüggvénye

$$U(x) = 1 + \sum_{n=1}^{\infty} u(n) x^n = 1 + \sum_{k=1}^{\infty} (-1)^k \left( x^k \left( \frac{\omega_k^2 (3n^2 - k) + \omega_k (k - i) }{2} \right) \right) =$$

$$= 1 - x - x^2 + x^3 + x^7 - x^{15} + \ldots \quad (10)$$

Ez a végtelen sor (például) $|x| < 1/2$ esetén abszolút konvergens.

Ugyanakkor $U(x)$ az alábbi ($|x| < 1/2$ esetén konvergens) végtelen szorzatként is előállítható:

$$U(x) = \prod_{i=1}^{r} (1 - x^{i}) \quad (11)$$

A (11) igazolásához tekintsük a

$$\prod_{i=1}^{r} (1 - x^{i}) \quad (12)$$

szorzatot. A szorzást elvégzve

$$(-x^{i_1})(-x^{i_2}) \ldots (-x^{i_r}) = (-1)^{i_1 + i_2 + \ldots + i_r} \quad (13)$$

típusú tagok keletkeznek, ahol $0 \leq j \leq r \text{ és } i_1, \ldots, i_r \text{ különböző, } r \text{-nél nem nagyobb pozitív egészek. (A } j = 0 \text{ esetben az üres szorzatnak megfelelő 1 értéket kapjuk.)}$

A (12) szorzás elvégzésekor (13) alapján annyiszor keletkezik $x^n$ -es tag + 1 , illetve - 1 együttáthatóval, ahanyféleképpen az $n$ -et elő tudjuk állítani páros, illetve páratlan sok különböző, $r$ -nél nem nagyobb pozitív egész összegeként. Ha $1 \leq n \leq r$ , akkor $u$ bármely partíciójában eleve csak $r$ -nél nem nagyobb tagok szerepelhetnek. Ez azt jelenti, hogy $r \geq n$ esetén (12)-t polinom alakba átírva $x^n$ együttáthatója éppen $s(n) - t(n) = u(n)$ lesz.

Ezután (11)-et az $r \rightarrow \infty$ határátmenettel kaphatjuk meg, ennek bizonyítását nem részletezzük.

A T 7.9.3 Tételből és (11)-ből következik, hogy $P(n)$ és $u(n)$ generátorfüggvényei egymás reciprokai, azaz

$$\left(1 + \sum_{n=1}^{\infty} P(n) x^n \right) \left(1 + \sum_{n=1}^{\infty} u(n) x^n \right) = P(x) U(x) = 1. \quad (14)$$

Így (14) bal oldalán a két hatványsort összeszorzozva minden $n \geq 1$ -re $x^n$ együttáthatója 0 lesz, vagyis

$$P(n) + P(n-1)u(1) + P(n-2)u(2) + \cdots + P(1)u(n-1) + u(n) = 0. \quad (15)$$
Az $u(i,j)$ értékeket a T 7.9.5 Tételből ismerjük, ezeket (15)-be beírva $p(n)$-re az alábbi rekurziót nyerjük:

$$p(n) = p(n - 1) + p(n - 2) - p(n - 5) + p(n - 7) + p(n - 12) + \ldots \quad (16)$$

A (16) rekurzió érdekessége, hogy a jobb oldalon szereplő tagok száma csak körülbelül $2\sqrt[3]{2n^2}$, és így ez az összefüggés (viszonylag) nagy $n$ esetén is alkalmas $p(n)$ tényleges kiszámítására. Például íly módon határozhatjuk meg $p(200)$ értékét is:

$$p(200) = 3672999026388.$$  

**Feladatok**

7.9.1 Mutassuk meg, hogy $p(n + 1) \leq 2p(n)$. Mikor áll egyenlőség?

7.9.2 Számítsuk ki az alábbi határértékeket:

(a) $\lim_{n \to \infty} \left( p(n + 1) - p(n) \right)$;

(b) $\lim_{n \to \infty} \left( p(n + 1) - 2p(n) \right)$.

7.9.3 Melyek azok a számok, amelyek páratlan sokféleképpen állnak elő különböző pozitív egészek összegeként?

7.9.4 Hányféleképpen írható fel egy $n$ szám pozitív egészek összegeként, ha a csak a tagok sorrendjében eltérő előállításokat is külön számoljuk?

7.9.5 Mutassuk meg, hogy az $n$ pontosan $r$-tagú és az $n - r$ legfeljebb $r$-tagú particióinak a száma azonos.

7.9.6 Írjuk fel a T 7.9.4 Tételben szereplő $h_r(n)$ függvény generátorfüggvényét.

7.9.7 (a) Legyen $v_r(n)$ az $n$ szám csupa különböző pozitív egészből történő előállításainak a száma, $w_r(n)$ pedig a csupa páratlan (de nem feltétlenül különböző) pozitív egészből történő előállítások száma. Mutassuk meg, hogy $v_r(n) - w_r(n)$.

(b) (Az (a) rész általánosítása.) Legyen $v_k(n)$ az $n$ azon particióinak a száma, ahol az összeadandók között nem szerepel egyetlen szám sem $k$-szor (vagy többször), $w_k(n)$ pedig azon particiók száma, ahol egyik összeadandó sem osztható $k$-val. Ekkor $v_k(n) = w_k(n)$.

7.9.8 Bizonyítsuk be, hogy $|x| < 1/2$ esetén

$$\sum_{n=1}^{\infty} p(n)x^n = \sum_{r=1}^{\infty} \left( \frac{x}{1-x}\right)^{r} = \frac{x}{(1-x)(1-x^2)\ldots(1-x^r)}.$$  

7.9.9 (**) Bizonyítsuk be, hogy

$$\sigma(n) - \sigma(n - 1) - \sigma(n - 2) + \sigma(n - 5) + \sigma(n - 7) - \cdots = \begin{cases} (-1)^{k+1}n, & \text{ha } n = \frac{1}{2}(3k^2 \pm k); \\ 0, & \text{egyéb esetek.} \end{cases}$$
8. fejezet - DIOFANTIKUS APPROXIMÁCIÓ

Ebben a fejezetben azt vizsgáljuk, mennyire jól közelíthetők az irracionális számok racionálisokkal. Itt az approximáció jóságát a közelítő tört \( s \) nevezőjéhez viszonyítjuk. Kiderül, hogy az irracionális számok „tipikusan” \( 1/s^2 \) nagyságrendben közelíthetők. A probléma kezelésénél a geometriai számmelmélet egyik alaptételeit, a Minkowski-tételt, valamint a lánctörteket is felhasználjuk. Végül bizonyos számsorozatok törtrészeinek elhelyezkedésével foglalkozunk. A diofantikus approximáció már az előző fejezetben tárgyalt Pell-egyenletehez is kapcsolódott (a T 7.8.1 Tétel bizonyításában felhasználtuk a T 8.1.1 Tételt), és további alkalmazásokat tárgyalunk a következő fejezetben.

8.1 Irracionális szám approximációja

A racionális számok a számegyenesen mindenütt sűrűn helyezkednek el, és így bármely irracionális számnak tetszőlegesen kicsi környezetében található végtelen sok racionális szám. Ebben a fejezetben olyan „erősebb” értelemben vett közelítésekkel foglalkozunk, amikor egy adott irracionális szám és a közelítő tört eltérése a tört nevezőjének függvényében is kicsi. Erre vonatkozik az alábbi alapvető eredmény:

8.1.1 Tétel . T 8.1.1

Tetszőleges \( \alpha \) irracionális számhoz végként sok olyan \( r/s \) tört létezik, amelyre

\[
|\alpha - r/s| < 1/s^2 \tag{1}
\]

Megjegyzés: A közelítő \( r/s \) törtről mindig eleve feltesszük, hogy \( s > 0 \). Az is világos, hogy ha egy tört \( (r,s) > 1 \) esetén kielégíti (1)-et, akkor az egyszerűsítés után kapott \( r'/s' \) törtre ez \( (s' < s \text{ miatt}) \) „még inkább” érvényes. Másfelől az is könnyen igazolható (lásd a 8.1.2 feladatot [274]), hogy egy \( r/s \) törtnek csak véges sok bővített alakja elégítheti ki (1)-et.

Mindezek alapján a T 8.1.1 Tétel (és a későbbi hasonló tételek) állításának igazságát nem befolyásolja, akár végként sok különböző \( r/s \) racionális számt, akár végként sok különböző \( r/s \) törtalkot mondunk (ez utóbbi esetben ugyanannak a racionális számnak két vagy több, az (1) feltételt kielégítő \( r/s \) alakú felirását külön számoljuk). Ugyanígy, az az sem jelentene megszorítást, ha az \( r/s \) közelítő törtekre az \( (r,s) = 1 \) feltételt is előírnánk.

A T 8.1.1 Tétel bizonyításához szükségünk lesz az alábbi tételre:

8.1.2 Tétel . T 8.1.2

Ha \( \alpha \) tetszőleges valós szám és \( n \) pozitív egész, akkor létezik (legalább egy) olyan \( r/s \) tört, amelyre

\[
1 < s \leq n \quad \text{és} \quad |\alpha - r/s| < 1/n^2 \tag{2}
\]

A T 8.1.2 Tétel bizonyítása: Egy \( c \) valós szám törtrészén a \( \{c\} = c - [c] \) különbséget értjük. Például \( \{3\} = 0 \), \( \{2,9\} = 0,9 \), \( \{-2,9\} = 0,1 \). Nyilván \( 0 \leq \{c\} < 1 \).

Tekintsük az

\( \{\alpha\}, \{2\alpha\}, \ldots, \{(n+1)\alpha\} \)
törtrészeket. Ezek valamennyien a \([0, 1]\) intervallumba esnek.

Osszuk fel a \([0, 1]\) intervallumot \(n\) darab \(1/n\) hosszú részekből, jobbról nyúlva részintervallumra.

Mivel a \(\{j\alpha\}\) törtrészek száma \(n + 1\), a részintervallumoké pedig \(n\), ezért a skatulyaelv értelmében lesz két olyan törtrész, amelyek ugyanabból a részintervallumba esnek, és így a távolságuk kisebb, mint \(1/n\). Ez azt jelenti, hogy van olyan \(1 \leq i < j \leq n + 1\), amelyre

\[
|\{ja\} - \{i\alpha\}| < \frac{1}{n}.
\]

A (3) átírható

\[
|(ja - \lfloor j\alpha \rfloor) - (i\alpha - \lfloor i\alpha \rfloor)| = |(j - i)\alpha - \lfloor j\alpha \rfloor - \lfloor i\alpha \rfloor| < \frac{1}{n}.
\]

alakba. Legyen

\[s = j - i\]
\[r = \lfloor j\alpha \rfloor - \lfloor i\alpha \rfloor,\]

ekkor (4)-et \(s\)-sel elosztva éppen a lemma állítását kapjuk.

A T 8.1.1 Tétel bizonyítása: Vegyük észre, hogy (2)-ben \(1 \leq s \leq n\) miatt

\[
|\alpha - \frac{r}{s}| < \frac{1}{ns} \leq \frac{1}{s^2}.
\]

Ez azt jelenti, hogy a lemmát \(n\) -ra és egy tetszőleges \(n\) pozitív egészre alkalmazva kapunk egy olyan \(\tau_1/s_1\) törtet, amelyre

\[
|\alpha - \frac{\tau_1}{s_1}| < \frac{1}{s_1^2}.
\]

Most az előző lépést \(\tau_1\) helyett alkalmas \(\tau_2\)-vel megismételjük, elkor egy \(\tau_2/s_2\) közelítő törtet állítunk elő. Azt kell csak biztosítani, hogy \(\tau_2/s_2\) ne lehessen ugyanaz, mint \(\tau_1/s_1\).

Mivel \(\alpha\) irrationális, így \(\alpha - \tau_1/s_1 \neq 0\), tehát \(\tau_2\) megválasztható úgy, hogy

\[
|\alpha - \frac{\tau_2}{s_2}| > \frac{1}{n_2}
\]

teljesüljön. Ekkor a lemma alapján

\[
|\alpha - \frac{\tau_2}{s_2}| < \frac{1}{n_2s_2} < \frac{1}{n_2} < |\alpha - \frac{\tau_1}{s_1}|,
\]

tehát

\[
\frac{\tau_2}{s_2} \neq \frac{\tau_1}{s_1}.
\]

Az eljárást hasonlóan folytatva végig sok (különböző) megfelelő \(\tau_1/s_1\) törtet kapunk.

Megjegyzés: Ha \(\alpha\) racionális, akkor természetesen az \(\alpha\) -t önmaga approximálja a legjobban. Ezzel együtt az approximációs probléma felvétése racionális \(\alpha\) esetén sem teljesen érdektelen.
például elméleti és gyakorlati szempontból egyaránt szükség lehet kis nevezőjű törtekkel történő jó közelítésre. Racionális \( \alpha \) esetén (magát az \( \alpha \) -t nem engedve meg közelítő törtekből) a T 8.1.1 Tételben szereplő \( 1/\sqrt{2} \)-es nagyságrend helyett csak \( c/\sqrt{s} \) érhető el, ahol \( c \) az \( \alpha \) -tól függő konstans (lásd a 8.1.1 feladatot [274]).

Az alábbi tétel több irracionalis szám közös nevezőjű törtekkel történő approximációja vonatkozik:

8.1.3 Tétel. T 8.1.3

Tetszőleges \( \alpha_1, \ldots, \alpha_k \) irracionalis számokhoz végének sok olyan

\[
\frac{x_i}{s_i}, \ldots, \frac{x_i}{s_i}, \quad i = 1, 2, \ldots
\]

közös nevezőjű racionális szám- \( k \) -as létezik, amelyre

\[
\left| \alpha_j - \frac{x_j}{s_j} \right| < \frac{1}{s_j k}, \quad j = 1, 2, \ldots, k, \quad i = 1, 2, \ldots
\]

A T 8.1.3 Tétel a T 8.1.1 Tételhez hasonló módon igazolható, ekkor a T 8.1.2 Tétel \( k \) -dimenziós változatára van szükség:

8.1.4 Tétel. T 8.1.4

Tetszőleges \( \alpha_1, \ldots, \alpha_k \) valós számokhoz és \( n \) pozitív egészhez létezne olyan \( \tau_1, \ldots, \tau_k \) és \( s \) egészek, amelyekre

\[
1 \leq s \leq n^k \quad \text{és} \quad \left| \alpha_j - \frac{x_j}{s} \right| < \frac{1}{n^k}, \quad j = 1, 2, \ldots, k.
\]

A bizonyítások részletes végiggondolását az Olvasóra bízzuk.

A T 8.1.1 Tételnek az alábbi élesítése is érvényes, amelyet bizonyítás nélkül közlünk:

8.1.5 Tétel. T 8.1.5

Tetszőleges \( \alpha \) irracionális számhoz végének sok olyan \( \tau/\sqrt{s} \) tört létezik, amelyre

\[
\left| \alpha - \frac{\tau}{\sqrt{s}} \right| < \frac{1}{\sqrt{s} \cdot \sqrt{2}}.
\]

Ennél valamivel gyengébb állítást, a \( \sqrt{2} \) helyett \( 1/\sqrt{3} \) teljesíti két különböző módon is a 8.2, illetve 8.3 pontban.

A T 8.1.5 Tétel tovább már nem javítható:

8.1.6 Tétel. T 8.1.6

Legyen \( \varepsilon > 0 \) tetszőleges és \( \alpha = (1 + \sqrt{5})/2 \). Ekkor csak véges sok olyan \( \tau/\sqrt{s} \) tört létezik, amelyre

\[
\left| \alpha - \frac{\tau}{\sqrt{s}} \right| < \frac{1}{(\sqrt{5} + \varepsilon) \cdot \sqrt{s}}.
\]

Bizonyítás: Tegyük fel indirekt, hogy (6) végének sok \( \tau/\sqrt{s} \) -sel teljesül. Mivel adott \( s \) -re az \( s \) nevezőjű törtek távolsága (legalább) \( 1/\sqrt{s} \), és \( s \geq 1 \) miatt
ezért bármely $s$-hez legfeljebb egy olyan $r$ található, amelyre (6) fennáll.

Ebből következik, hogy a (6)-ot kielégítő végtelen sok $r/s$ tört nevezői között akármilyen nagy számok is előfordulnak.

Az $\alpha$ gyöké az $x^2 - x - 1 = 0$ egyenletnek, így $\alpha(\alpha - 1) = 1$. Ennek alapján a (6) bal oldalán álló különbséget a következő módon „gyökelteleníthetjük”:

$$\left(\alpha - \frac{r}{s}\right)\left(\alpha - 1\right) = \alpha(\alpha - 1) + \frac{r}{s}\left(\alpha - (\alpha - 1)\right) - \frac{r^2}{s^2} = 1 + \frac{r - r^2}{s^2}. \quad (7)$$

A (7) jobb oldalán egy $s^2$ nevezőjű tört áll, amely $\alpha$ irracionalitása miatt nem nulla, és így abszolút értéke legalább $1/s^2$. Ebből (7) alapján következik, hogy

$$\left|\alpha - \frac{r}{s}\right| \leq \left|\frac{r}{s}\right| < \frac{1}{s^2}. \quad (8)$$

Mivel (6) szerint $r/s$ „közel” van $\alpha$-hoz, ezért a (8) bal oldalán álló második tényező értéke „körülbelül” $2r - 1 = \sqrt{5}$ és ezzel ellentmondásba kerülünk (6)-tal. Ennek precíz kivitelezéséhez induljunk ki az

$$\left|\frac{r}{s}\right| < \sqrt{5} + \frac{1}{\sqrt{5}s^2} \quad (9)$$

felső becslésből. Ha $s$ elég nagy, akkor

$$\frac{1}{\sqrt{5}s^2} < \varepsilon,$$

tehát (9)-ből kapjuk, hogy

$$\left|\alpha - \frac{r}{s}\right| < \sqrt{5} + \varepsilon. \quad (10)$$

A (8) és (10) egyenlőtlenségekből következik, hogy elég nagy $s$-re

$$\left|\alpha - \frac{r}{s}\right| > \frac{1}{(\sqrt{5} + \varepsilon)s^2},$$

ami ellentmond az indirekt feltevésnek. ■

A T 8.1.6 Tétel mutatja, hogy a T 8.1.5 és T 8.1.1 Tételek az irracionalis számok approximálhatóságának a helyes nagyságrendjét jelentik, hiszen van olyan $\alpha$ irracionalis szám, amely egyáltalán nem (illetve csak „alig”) approximálható jobban, mint amit ezek a tételek biztosítanak.

A következőben belátjuk, hogy a T 8.1.5 és T 8.1.1 Tételek más értelemben véve is az irracionalis számok approximálhatóságának a helyes nagyságrendjét adják: olyan irracionalis szám is csak „kevés” van, amelyre „lenyegesen” jobb közelítés érhető el. A „kevés” pontos megfogalmazásához bevezetjük a nullmértékű halmaz fogalmát:

8.1.7 Definíció . D 8.1.7
A valós számok egy $H$ részhalmaza nullmértékű, ha tetszőleges $\varepsilon > 0$-hoz létezik megszámlálható sok olyan intervallum, amelyek együttesen lefedik $H$-t és amelyek összhossza kisebb, mint $\varepsilon$. Könnyen adódik, hogy minden megszámlálható $H$, így speciálisan a racionális számok halmaza is nullmértékű, léteznek azonban kontinuum számosságú nullmértékű halmazok is (lásd a 8.1.9 feladatot [276]).

8.1.8 Tétel. T 8.1.8

Legyen $\kappa > 0$ tetszőleges valós szám és $\overline{H}$ azoknak az $\alpha$ valós számoknak a halmaza, amelyekhez végleten sok olyan $\tau/\varepsilon$ található, hogy

$$\left| \alpha - \frac{\tau}{\varepsilon} \right| < \frac{1}{\varepsilon^{2^s + e}}$$

(11)
teljesül. Ekkor $\overline{H}$ nullmértékű. ❄

Bizonyítás: Legyen

$$H_i = H \cap \left[ i, i+1 \right], \quad i = 0, \pm 1, \pm 2, \ldots$$

A (11) szerinti approximálhatóság csak az $\alpha$ törtrészétől függ, ezért a $H_i$ halmazok közül bármely kettő egybevágó. Így elég belátni, hogy $H_i$ nullmértékű, hiszen

$$H = \bigcup_{i=-\infty}^{\infty} H_i$$

és megszámlálható sok nullmértékű halmaz egyesítése is nullmértékű (lásd a 8.1.10c feladatot [276]).

Adott $s > 1$ pozitív egészhez legyen $A_s$ azoknak a $0 \leq \alpha < 1$ valós számoknak a halmaza, amelyekre (11) teljesül alkalmas $\tau$-rel. Ekkor $A_s$ nyilván a körüli $1/s^{2^s + e}$ sugarú nyílt intervallumokból, illetve ezeknek a $[0,1)$-be eső részeiből tevődik össze, azaz

$$A_s = \left( \bigcup_{r=1}^{s-1} \left( \frac{r}{s} - \frac{1}{s^{2^s + e}}, \frac{r}{s} + \frac{1}{s^{2^s + e}} \right) \right) \bigcup [0, \frac{1}{s^{2^s + e}}) \bigcup \left( 1 - \frac{1}{s^{2^s + e}}, 1 \right).$$

(12)

Az $A_s$-t alkotó intervallumok összhossza

$$(s-1)\frac{2}{s^{2^s + e}} + 2 \frac{1}{s^{2^s + e}} = \frac{2s}{s^{2^s + e}} = \frac{2}{s^{1 + e}}.$$  

(13)

Ha $\alpha \in H_0$, akkor a feltétel szerint végleten sok olyan $s$ van, amelyre $\alpha \in A_s$ . Ebből következik, hogy tetszőleges $n$ esetén

$$H_0 \subseteq \bigcup_{s=1}^{\infty} A_s.$$  

(14)
Ekkor (12), (13) és (14) alapján \( H \) lefedhető megszámlálható sok intervallummal, amelyek összhossza

\[
\sum_{s=\tau}^{\infty} \frac{2}{s^{1+n}}. 
\]

Mivel a

\[
\sum_{s=1}^{\infty} \frac{1}{s^{1+n}}
\]

végtelen sor konvergens, ezért tetszőleges \( \varepsilon > 0 \) -hoz található olyan \( \tau \), amelyre a (15)-beli összeg kisebb, mint \( \varepsilon \). Ezzel beláttuk, hogy \( H_{\tau} \), és így \( H \) is nullmértékű.

A T 8.1.8 Tétel általánosításaként a következő kérdést is megvizsgálhatjuk. Legyen \( f \) a pozitív egészeken értelmezett pozitív értékű függvény, amelyre \( f(s)/s \) monoton nő, és \( H(f) \) azoknak az \( \alpha \) valós számoknak a halmaza, amelyekhez végtesten sok olyan \( \tau/s \) található, hogy

\[
\left| \alpha - \frac{\tau}{s} \right| < \frac{1}{s f(s)}. 
\]

A T 8.1.8 Tétel bizonyításához hasonlóan igazolható, hogy ha

\[
\sum_{s=1}^{\infty} \frac{1}{f(s)} < \infty,
\]

akkor \( H(f) \) nullmértékű.

Ha azonban

\[
\sum_{s=1}^{\infty} \frac{1}{f(s)} = \infty,
\]

akkor teljesen megfordul a helyzet: ekkor nullmértékű halmaztól eltekintve \( H(f) \) minden valós számot tartalmaz. Ez utóbbi eredménynek jóval nehezebb a bizonyítása.

### Feladatok

#### 8.1.1
Legyen \( \alpha \) rögzített racionális szám: \( \alpha = \frac{a}{b} \), ahol \( \langle a, b \rangle = 1 \) és \( b > 0 \).

(a) Bizonyítsuk be, hogy

\[
\frac{\tau}{\bar{a}} \neq \frac{\alpha}{b} \implies \left| \alpha - \frac{\tau}{s} \right| \geq \frac{1}{s b^k}. 
\]

(b) Mutassuk meg, hogy végtelen sok olyan \( \tau/s \) tört létezik, amikor (16) jobb oldalán egyenlőség teljesül.

#### 8.1.2
A T 8.1.1 Tételben az (1) egyenlőtlenséget esetleg egy adott racionális számnak több \( \tau/s \) alakja is kielégítheti. Mutassuk meg, hogy (1) nem teljesülhet ugyanannak a racionális számnak végtelen sok \( \tau/s \) alakjával.
8.1.3 Legyen $\alpha$ irracionális szám, és tekintsünk végtelen sok olyan $r_i/s_i$ törtet, amelyre

$$\left| \alpha - \frac{r_i}{s_i} \right| < \frac{1}{s_i^2}, \quad i = 1, 2, \ldots$$

Bizonyítsuk be, hogy

(a) $\lim_{i \to \infty} s_i = \infty$ ;

(b) $\lim_{i \to \infty} \frac{r_i}{s_i} = \alpha$ .

8.1.4 Bizonyítsuk be az alábbi állításokat:

(a) Minden $\alpha$ valós számhoz végtelen sok olyan $r_i/2^k$ alakú tört létezik, amelyre

$$\left| \alpha - \frac{r_i}{2^k} \right| \leq \frac{1}{3 \cdot 2^k}.$$  

(b) Van olyan $\alpha$ , hogy bármely $r_i/2^k$ alakú tört esetén

$$\left| \alpha - \frac{r_i}{2^k} \right| \geq \frac{1}{3 \cdot 2^k}.$$  

(c) Minden $\alpha$ valós számhoz végtelen sok olyan $r_i/3^k$ alakú tört létezik, amelyre

$$\left| \alpha - \frac{r_i}{3^k} \right| \leq \frac{1}{2 \cdot 3^k}.$$  

(d) Van olyan $\alpha$ , hogy bármely $r_i/3^k$ alakú tört esetén

$$\left| \alpha - \frac{r_i}{3^k} \right| \geq \frac{1}{2 \cdot 3^k}.$$  

(e) Minden $\alpha > 0$ irracionális számhoz végtelen sok $r_i^2/s^2$ alakú tört létezik, amelyre

$$\left| \alpha - \frac{r_i^2}{s^2} \right| < \frac{c(\alpha)}{s^2},$$  

ahol $c(\alpha)$ egy $\alpha$ -től függő konstans.

(f) Van olyan $\alpha > 0$ irracionális szám és $c$ konstans, hogy bármely $r_i^2/s^2$ alakú tört esetén

$$\left| \alpha - \frac{r_i^2}{s^2} \right| > \frac{c}{s^2}.$$  

8.1.5 Bizonyítsuk be, hogy minden $\alpha$ irracionális számhoz végtelen sok olyan különböző számlálójú $r_i/s$ tört létezik, amelyre

$$\left| \alpha - \frac{r}{s} \right| < \frac{c(\alpha)}{r^2},$$  

ahol $c(\alpha)$ az $\alpha$ -től függő konstans.
8.1.6 Bizonyítsuk be, hogy létezik olyan \( c \) konstans, hogy bármely \( \tau / s \) tört esetén

\[
\left| \sqrt{2} - \frac{\tau}{s} \right| > \frac{c}{s^2}
\]

8.1.7 Legyen \( \alpha > 1 \) tetszőleges valós szám. Nevezzünk egy \( \alpha \) valós számot \( t \)-edrendben approximálhatónak, ha végig tetszőleges \( \alpha \) valós számot \( t \)-edrendben approximálható, ha végig tetszőleges \( \alpha \) valós számot approximáló konstans, (Így a T 8.1.1 Tételből következik, hogy minden irracionális szám másodrendben approximálható, a T 8.1.8 Tétel szerint viszont a 2-nél nagyobb rendben approximálható valós számok halmaza nullmértékű.)

Tegyük fel, hogy az \( \alpha \) valós szám 20-adrendben approximálható. Bizonyítsuk be, hogy ekkor

(a) \( a_\alpha + b \) is 20-adrendben approximálható, ha \( a, b \) racionális és \( a \neq 0 \);
(b) \( a_\alpha \) 10-adrendben approximálható.

8.1.8 Határozzuk meg a törtrészekből képzett alábbi kifejezések összes lehetséges értékét, ha \( \alpha \) és \( \beta \) egymástól függetlenül befutják a valós számokat:

(a) \( \{\alpha\} + \{\beta\} - \{\alpha + \beta\} \);
(b) \( \{\alpha\} \{\beta\} - \{\alpha \beta\} \);
(c) \( * (\text{M}[601]) \{\alpha\}^2 - \{\alpha^2\} \).

8.1.9 (a) Mutassuk meg, hogy a valós számok minden megszámlálható részhalmaza nullmértékű.

(b) * Tekintsük azokat a 0 és 1 közé eső valós számokat, amelyek hármas alapú származott kifejezésben „szereplő” tört alakjában nem szerepel 1-es számjegy (ez az ún. Cantor-halmaz). Bizonyítsuk be, hogy ennek a halmaznak kontinuum sok eleme van, ugyanakkor nullmértékű.

8.1.10 Bizonyítsuk be az alábbi állításokat:

(a) Egy nullmértékű halmaz bármely részhalmaza is nullmértékű.
(b) Véges sok nullmértékű halmaz egyesítése is nullmértékű.
(c) Megszámlálható sok nullmértékű halmaz egyesítése is nullmértékű.
(d) Megszámlálhatónál több nullmértékű halmaz egyesítése lehet nullmértékű, de nem feltétlenül az.

8.2 Minkowski-tétel

Ebben a pontban egy fontos geometriai számelméleti tétellel és annak néhány alkalmazásával foglalkozunk.

8.2.1 Tétel (Minkowski-tétel) . T 8.2.1

Legyen \( L \) a síkon egy tetszőleges paralelogrammarács, és \( H \) olyan zárt, konvex, síkbeli halmaz, amely középpontosan szimmetrikus az egyik rácsontra. Tegyük fel, hogy \( H \) területe legalább 4\( \Delta \)
2. Feltehetjük, hogy \( H \) korlátos. Ugyanis megmutatható, hogy ha egy konvex halmaz nem korlátos, akkor a területe csak nulla vagy végtelen lehet, így ez utóbbi esetben a \( H \) -nak egy a középpontja körüli elég nagy sugarú (zárt) köreél való metszete már olyan középpontosan szimmetrikus, korlátos, zárt, konvex halmaz lesz, amelynek a területe legalább \( 4\Delta \).
3. A tétel magasabb dimenziós, illetve nagyobb területű halmazok esetén több rácspontot garantáló általánosításaira vonatkozóan lásd a 8.2.1 [281] és 8.2.2 feladatokat [281].

A Minkowski-tételre két bizonyítást adunk. Jelöljük \( H \) szimmetria-középpontját \( O \) -val, területét pedig \( h \)-val.

Első bizonyítás: Tekintsük először azt az esetet, amikor \( h > 4\Delta \).

Kicsinyítsük le az \( L \) rácst az \( O \) pontból \( 2/k \) arányban, ahol \( k \) (nagy) egész szám, és legyen \( N(k) \) az így kapott \( L_k \) rácscsoportok száma, amelyek benne vannak \( H \) -ban. Az \( L_k \) rácspontos geometriájának a területe \( 4\Delta/k^2 \), ezért \( h \) területe
\[
\hat{h} = \lim_{k \to \infty} \frac{4\Delta}{k^2}.
\]
Mivel \( \hat{h} > 4\Delta \), ezért (1)-ből következik, hogy elég nagy \( k \) esetén \( N(k) > k^2 \).

Vegyük azt a (általában ferdeszögű) koordinátarendszert, amelynek a kezdőpontja \( O \), a tengelyek pedig párhuzamosak az alapparalelogramma oldalainál. Ekkor az \( L \) rácspontjainak a koordinátái \((ia,jb)\), az \( L_k \) rácspontjainak koordinátái pedig
\[
\left( \frac{2i}{k} a, \frac{2j}{k} b \right),
\]
ahol \( a \), illetve \( b \) az \( L \) rácspalapparalelogrammájának megfelelő oldalai, \( i \) és \( j \) pedig tetszőleges egész számok.

Mivel az \((i,j)\) számpárok \( k \)-val való maradékos osztásakor \( k \) -féle „maradékpár” keletkezhet, és \( N(k) > k^2 \), ezért a skatulyaelv szerint létezik az \( L_k \) rácspontjainak két olyan (különböző) rácspontja,
\[
Q_1 = \left( \frac{2i}{k} a, \frac{2j}{k} b \right), \quad Q_2 = \left( \frac{2i}{k} a, \frac{2j}{k} b \right),
\]
amelyekre
\[
k \mid i_1 - i_2 \quad \text{és} \quad k \mid j_1 - j_2. \tag{2}
\]
Ekkor \( H \) középpontos szimmetriája miatt a \( Q_2 \) pontnak az \( O \)-ra vonatkozó tükröklepek
\[
Q_2 = \left( \frac{-2i_2}{k} a, \frac{-2j_2}{k} b \right)
\]
is \( H \)-beli, továbbá a konvexitás miatt a \( Q_1Q_2 \) szakasz felezőpontja
A (2)-beli oszthatóságok miatt $F = (ra, sb)$, ahol $r$ és $s$ egész számok, tehát $F$ az eredeti $L$ rácsnak is ráspontja. Mivel $Q_1 \neq Q_2$, ezért $F \neq O$. Ezzel igazoltuk, hogy $H$ az $O$-n kívül is tartalmaz $L$-beli ráspontot.

Háttravan még annak az esetnek az igazolása, amikor $h = 4\Delta$. Tegyük fel indirekt, hogy $H$ az $O$ középpontján kívül nem tartalmaz $(L$-beli) ráspontot. Legyen a $P \neq O$ ráspontok $H$-tól való távolságának a minimuma $m$. Mivel $H$ zárt, ezért $m > 0$. Ez azt jelenti, hogy $H$-t az $O$-ból ki tudjuk úgy nagyítani, hogy a kinagyított $H'$ sem tartalmaz $O$-tól különböző ráspontot. Ez azonban lehetetlen, hiszen $H'$ területe nagyobb, mint $4\Delta$. ♦

 Második bizonyítás: Először egy lemmát igazolunk, amely azt a „szemléletesen nyilvánvaló” tényt fejezi ki, hogy ha egy korlátos sokbeli halmaznak az összes rácsvektorral eltolt példányai páronként diszjunktak, akkor a halmaz területe nem lehet nagyobb a rács alapparalelogrammájának a területénél.

8.2.2 Lemma. L 8.2.2

Legyen az $L$ paralelogrammáracs alapparalelogrammájának területe $\Delta$, a $K$ korlátos sokbeli halmaz területe pedig $t$. Legyen továbbá $O$ rögzített ráspont, $P$ tetszőleges ráspont, és jelöljük $K_P$-vel a $K$ halmaznak az $OP$ vektorral való eltoltját ($K_O = K$). Végül tegyük fel, hogy a $K_P$ halmazok diszjunktak. Ekkor $t \leq \Delta$. ♦

A L 8.2.2 Lemma bizonyítása: A bizonyítás lényege a következő észrevétel: Az alapparalelogrammát (minden irányban) nagyítsuk ki $s$-szeresére, ahol $s$ egy „nagy” szám, és az így kapott $M$ paralelogrammát helyezzük el úgy, hogy az $O$ pont körülbelül $M$ „közepére” essen. Ekkor a $K$-nak az $M$-beli ráspontok szerinti eltoltjai „nem nagyon lóghatnak ki” $M$-ből, és így ezen eltolt példányok együtt területe, ami (körülbelül) $t^2$, nem lehet „sokkal” nagyobb az $M$ területénél, azaz $r^2\Delta$-nél. Az állítás innen határátmenettel adódik.

Nézzük mindezt pontosan és részletesen. Veggük azt a (T 8.2.1 Tétel első bizonyításában már használt, általában ferdeszögű) koordináta-rendszert, amelynek a kezdőpontja $O$, a tengelyek pedig párhuzamosak az alapparalelogramma oldalaival. Ekkor az $L$ rács ráspontjainak koordinátái $(ai, jbi)$, ahol $a$, illetve $b$ az alapparalelogramma megfelelő oldalai, $i$ és $j$ pedig tetszőleges egész számok.

Legyen $n$ tetszőleges pozitív egész, és tekintsük azt a $(2n + 1)^2$ darab $P_i = (ia_i, jbi)$ ráspontot, amelyre $|i| \leq n$ és $|j| \leq n$. Az ezerhez tartozó $K_P$ halmazok egyesítését jelöljük $U_n$-nel. Ekkor $U_n$ területe $(2n + 1)^2$. A $K$ korlátossága miatt van olyan $c > 0$, hogy $K$ bármely pontjának koordinátái kisebb abszolút értékűek, mint $cn$, illetve $cb$. Ekkor $U_n$ része annak a $G_n$ paralelogrammának, amelynél a négy csúcs koordinátái

$$(\pm a(n + c), \pm b(n + c)),$$

és így $G_n$ területe $(2n + 2c)^2\Delta$. A tartalmazás miatt $U_n$ területe legfeljebb akkora, mint $G_n$ területe, azaz

$$(2n + 1)^2 \leq (2n + 2c)^2\Delta.$$

Ebből kapjuk, hogy

$$P = \left(\frac{2t_1 - 2j_2}{2k}, \frac{2j_1 - 2j_2}{2k}\right)$$
t \leq \left(1 + \frac{2c-1}{2n+1}\right)^2 \Delta.

Innen a kívánt \( t \leq \Delta \) egyenlőtlenség az \( n \to \infty \) határátmenettel következik.

Rátérve a T 8.2.1 Tétel bizonyítására, most is elég a \( \beta > 4 \Delta \) esetet tekintenünk.

Kicsinyítsük le \( \mathcal{H} \)-t az \( \mathcal{O} \) középpontból a felére, az így kapott halmazt jelöljük \( \mathcal{K} \)-val. A feltétel szerint \( \mathcal{K} \) területe \( i = 1/4 > \Delta \), így a L 8.2.2 Lemma alapján létezik olyan \( \mathcal{Q} \) és \( \mathcal{R} \) rácspon, amelyre \( \mathcal{K} \mathcal{Q} \)-nak és \( \mathcal{K} \mathcal{R} \)-nak van közös pontja. A \( \mathcal{Q} \mathcal{O} \) vektorral történő eltolással azt kapjuk, hogy \( \mathcal{K} \mathcal{O} = \mathcal{K} \)-nak és \( \mathcal{K} \mathcal{P} \)-nak is van közös pontja, ahol \( \mathcal{P} \) alkalmas (az \( \mathcal{O} \)-től különböző) rácspon. Azt fogjuk igazolni, hogy a \( \mathcal{P} \) rácspon benne van \( \mathcal{H} \)-ban (és ezzel a tétel állítását beláttuk).

Legyen \( A \) közös pontja \( \mathcal{K} \)-nak és \( \mathcal{K} \mathcal{P} \)-nak, \( B \) az \( A \)-nak a \( \mathcal{P} \mathcal{O} \) vektorral való eltoltja, \( C \) a \( B \) tükörképe \( \mathcal{O} \)-ra, és végül \( D \) az \( \mathcal{A}C \) szakasz felezőpontja.

Mivel \( A \) eleme \( \mathcal{K} \mathcal{P} \)-nak, ezért \( B \) eleme \( \mathcal{K} \)-nak. A \( \mathcal{K} \) középpontos szimmetriája miatt \( C \) is eleme \( \mathcal{K} \)-nak. Végül \( A \) és \( C \) is \( \mathcal{K} \)-beli, tehát a konvexitás miatt a \( D \) felezőpont is \( \mathcal{K} \)-beli.

Ugyanakkor a konstrukció szerint \( \text{Par} \mathcal{O} \mathcal{C} \) paralellogramma, hiszen az \( \mathcal{O} \mathcal{C} \) és \( \mathcal{A} \mathcal{P} \) oldalak párhuzamosak és egyenlők. Ezért \( D \) az \( \mathcal{O} \mathcal{P} \) átlónak is felezőpontja, és így \( D \)-t az \( \mathcal{O} \) középpontú kétszeres nagyítás \( \mathcal{P} \)-be viszi. Mivel ez a nagyítás a \( \mathcal{K} \) halmaz éppen \( \mathcal{H} \)-ba viszi, és a \( D \) pont \( \mathcal{K} \)-ban van, ezért a \( \mathcal{P} \) pont szükségképpen \( \mathcal{H} \)-beli. Ezzel beláttuk, hogy \( \mathcal{H} \) tartalmazza az \( \mathcal{O} \)-től különböző \( \mathcal{P} \) rácsponot is. 

A Minkowski-tételt először a diofantikus approximációnál alkalmazzuk a T 8.1.1 Tétel javítására. 

**8.2.3 Tétel.** T 8.2.3

Tetszőleges \( \alpha \) irrationális számhoz végtele sok olyan \( \frac{x}{\sqrt{s}} \) tört létezik, amelyre

\[
|\alpha - \frac{x}{s}| < \frac{1}{2s^\gamma}.
\]

**Bizonyítás:** Az (3) egyenlőtlenség \( s \neq 0 \) esetén ekvivalens

\[
|s(\alpha x - y)| < \frac{1}{2} y.
\]

teljesülésével. Vezessük be az

\[
x = s\alpha - y, \quad y = s
\]

új változókat. Ha \( x \) és \( y \) egymástól függetlenül végigfut az egész számokon, akkor az \( (x, y) \) pontok egy olyan paralellogrammára csoportozat alkotnak, amelynél az alapparalellogramma csúcsai

\[
(0,0), \quad (-1,0), \quad (\alpha,1), \quad (\alpha-1,1).
\]

Az új változók szerint (4) az \( |\frac{xy}{x+y}| < 1/2 \) feltételt jelenti, azaz azokat az \( (x,y) \) rácsponokat keressük, amelyek az \( \frac{xy}{x+y} = \frac{1}{2} \) és \( \frac{xy}{x+y} = -\frac{1}{2} \) hiperbolák által határolt (az origót is tartalmazó) tartományba esnek. Rácspontra az \( \frac{xy}{x+y} = \pm\frac{1}{2} \) egyenlőség az \( \alpha \) iracionálisitása miatt sohasem teljesülhet, így nem jelent változást, ha (3)-ban, illetve (4)-ben a \( \gamma \) jel helyett \( \leq \) jelet írunk. Ennek alapján az iménti
tartományhoz a határoló hiperbolaágakat is hozzávehetjük, és a továbbiakban az így keletkező zárt \( Z \) halmazt tekintjük.

Az \( \theta \neq 0 \) feltétel azt jelenti, hogy az \( \mathcal{X} \) -tengelyre eső rácsponstokat figyelmen kívül kell hagynunk.

A rács (5) alapparalelogrammájában a „vízszintes” oldal és az ehhez tartozó magasság is egységnyi hosszúságú, tehát az alapparalelogramma területe \( \Delta = 1 \).

A \( Z \) halmaz nem konvex és nem korlátos, ezért Minkowski tétele nem tudjuk közvetlenül magára \( Z \) -re alkalmazni. Ehelyett \( Z \) alakos konvex részhalmazait fogjuk tekinteni: olyan rombuszokat, amelyek csúcsai a hiperbola tengelyein vannak, és érintik a négy hiperbolaágát. Ezek a rombuszok konvex, zárt és az origóra szimmetrikus halmazok.

Megmutatjuk, hogy minden ilyen rombusz területe 4. Ha a rombusz az első siknegyedbeli hiperbolaágot az \( (u,1/(2\omega)) \) pontban érinti, akkor az érintő egyenlete

\[
y - \frac{1}{2\omega} x = -\frac{1}{2\omega^2}(x - u).
\]

Ez az egyenes a koordinátatengelyeket az \( x = 2u \), illetve \( y = \frac{1}{\omega} \) pontokban metszi. Így az origó és ezen két csúcs alkotta derékszögű háromszög területe \( \frac{3}{2}(2\omega)(1/\omega) = 1 \), és a rombusz területe ennek négyszerese, azaz 4.

Mivel a terület \( 4 = 4\Delta \), ezért Minkowski tétele szerint minden ilyen rombusz tartalmaz az origón kívül rácsponstot.

Válasszuk a rombuszokat rendre úgy, hogy az \( \mathcal{Y} \) -tengely irányában egyre „keskenyebebb” legyenek. Ekkor elérhető, hogy minden újabb rombusz az előző rombuszok által tartalmazott nemtriviális rácsponstok egyikét se tartalmazza, továbbá egyáltalán ne tartalmazzon az \( \mathcal{X} \) -tengelyen az origótól különböző rácsponstot. Ily módon végig sok megfelelő rácsponstot kapunk (a középpontos szimmetria miatt a szokásos \( s > 0 \) feltétel is elérhető).

A Minkowski-tétel második alkalmazásaként új bizonyítást adunk a T 7.5.1 Tétel azon részállítására, hogy minden \( 4k + 1 \) alakú \( p \neq 0 \) prímszám előáll két négyzetszám összegeként.

**8.2.4 Tétel.** T 8.2.4

Minden \( 4k + 1 \) alakú \( p > 0 \) prímszám felírható két négyzetszám összegeként.

*Bizonyítás: A T 4.1.4 Tétel alapján létezik olyan \( c \), amelyre \( c^2 \equiv -1 \pmod{p} \).

Tekintsük a síkon az

\[
x = pm + cu, \quad y = u \tag{8}
\]

koordinátajú pontokat, ahol \( u \) és \( v \) egymástól függetlenül befutják az egész számokat. Ezek egy paralelogrammarácsot alkotnak, amelyben az alapparalelogramma területe \( \Delta = p \).

Bármely rácsponst esetén

\[
x^2 + y^2 = (pm + cu)^2 + u^2 = p(pm^2 + 2cu^2 + c^2) + u^2(c^2 + 1) \equiv 0 \pmod{p},
\]

azaz \( p \mid x^2 + y^2 \). Ebből következik, hogy ha egy, az origótól különböző rácspontra \( x^2 + y^2 < 2p \), akkor a kívánt \( x^2 + y^2 = p \) előállítás adódik.
Alkalmazzuk Minkowski tételét az \( x^2 + y^2 \leq \frac{4\rho}{\pi} \) egyenletű, origó körüli \( 4\rho = 4\Lambda \) területű (zárta) körlapra. A tétel szerint ez a kör az origin kívül is tartalmaz legalább egy \( (x, y) \) rácspontot. Így erre a rácspontra teljesül

\[ x^2 + y^2 \leq \frac{4\rho}{\pi} < \frac{4\rho}{\pi} \]

Megjegyezzük, hogy a 3-dimenziós Minkowski-tételnek (lásd a 8.2.1a feladatot [281]) a fentiekhez hasonló elveken alapul, de jóval bonyolultabb alkalmazása a három-négyszögmérték-szám-tétel (T 7.5.2 Tétel) bizonyítás nélkül közölt „nehéz” részének igazolásához is elvezet (közben a számvektor sorozatok primszámaira vonatkozó Dirichlet-tételt is fel kell használni).

A Minkowski-tétel néhány további alkalmazására nézve lásd a 8.2.3 [281]–8.2.5 feladatokat [281].

**Feladatok**

8.2.1 (a) Bizonyítsuk be a térbeli Minkowski-tételt: Legyen \( \bar{L} \) a térben egy tetszőleges paralelepipedonrács, és \( \bar{H} \) olyan zárt, konvex, térbeli halmaz, amely középpontosan szimmetrikus az egyik rácspontra. Tegyük fel, hogy \( \bar{H} \) térfogata legalább \( 8\Delta \), ahol \( \Delta \) a rács alapparalelepipedonjának a térfogata. Ekkor \( \bar{H} \) a középpontján kívül is tartalmaz rácsponcot.

(b) Általánosítsuk a tételt tetszőleges dimenzióra.

8.2.2 Igazoljuk a Minkowski-tétel alábbi általánosítását: Ha \( \bar{L} \) és \( \bar{H} \) eleget tesznek a T 8.2.1 Tétel feltételeinek, és \( \bar{H} \) területe legalább \( 2r \Delta \), ahol \( r > 0 \) egész, akkor \( \bar{H} \) a középpontján kívül legalább \( 2r \) darab rácsponcot tartalmaz.

8.2.3 Bizonyítsuk be, hogy minden \( 3k + 1 \) alakú pozitív prímszám felírható alkalmas \( x \), \( y \) egész számok \( r^2 + 3s^2 \) alakban.

8.2.4 Legyenek \( a_{11}, a_{12}, a_{21}, a_{22} \) olyan egész számok, amelyekre

\[ D = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \neq 0. \]

Bizonyítsuk be, hogy ha a \( b_1, b_2 \) pozitív számokra \( a_1b_2 \geq |D| \), akkor az

\[ |a_{11}x_1 + a_{12}x_2| \leq b_1, \quad |a_{21}x_1 + a_{22}x_2| \leq b_2 \]

eyenlőtlenlenségre látjuk nemtriviális (azaz az \( (x_1, x_2) = (0, 0) \) -tól különböző) egész megoldása.

8.2.5 (*) Bizonyítsuk be, hogy tetszőleges \( \alpha_1 \) és \( \alpha_2 \) irrationális számokhoz végletesen sok olyan közös nevezőjű \( \tau_1/\phi \), \( \tau_2/\phi \) racionális számpár létezik, amelyre

\[ \left| \alpha_j - \frac{\tau_j}{\phi} \right| < \frac{2}{3} \cdot \frac{1}{5^{j/2}}, \quad j = 1, 2. \]

**8.3 Lánctörtek**

Tetszőleges \( \alpha \) valós szám esetén tekintsük a következő algoritmust. Legyen
\[ c_0 = \lfloor \alpha \rfloor \quad \text{és} \quad c_1 = \{ \alpha \}, \quad \text{akkor} \quad \alpha = c_0 + \frac{1}{c_1}. \quad (1) \]

Ha \( \alpha_1 \neq 0 \), akkor legyen
\[ c_1 = \left\lfloor \frac{1}{\alpha_1} \right\rfloor \quad \text{és} \quad \alpha_2 = \left\lfloor \frac{1}{\alpha_1} \right\rfloor, \quad \text{akkor} \quad \alpha = c_0 + \frac{1}{c_1 + \alpha_2}. \]

Ha \( \alpha_2 \neq 0 \), akkor \( 1/\alpha_2 \) egész- és törtrészét képezzük stb. Általában, ha a \( c_0, c_1, \ldots, c_n \) és \( \alpha_1, \ldots, \alpha_{n+1} \) értékeket már meghatároztuk, és \( \alpha_{n+1} \neq 0 \), akkor legyen
\[ c_{n+1} = \left\lfloor \frac{1}{\alpha_{n+1}} \right\rfloor \quad \text{és} \quad \alpha_{n+2} = \left\lfloor \frac{1}{\alpha_{n+1}} \right\rfloor, \quad (2) \]
ekkor
\[ \alpha = c_0 + \frac{1}{c_1 + \frac{1}{c_2 + \frac{1}{c_3 + \frac{1}{\ddots + \frac{1}{c_{n+1} + \frac{1}{\alpha_{n+2}}}}}}}. \quad (3) \]

A (3) jobb oldalán álló sokemeletes törtet (véges) \( \text{lánctörtek} \) nevezzük, és az egyszerűbb írásmód kedvéért bevezetjük rá az \( \lfloor \alpha_0, \alpha_1, \ldots, c_n, c_{n+1} = \alpha_{n+2} \rfloor \) jelölést. (A (3) képlet jobb oldalára ezt a jelölést néha olyan esetben is fogjuk alkalmazni, amikor a \( \ell_i \) értékek nem feltétlenül egész számok.)

Ha \( \alpha_{n+1} = 0 \), akkor az eljárás véget ér.

Az ily módon kapott \( c_0, c_1, \ldots \) egész számokat az \( \alpha \) \( \text{lánctörjegyein} \) nevezzük.

8.3.1 Definíció . D 8.3.1

Egy \( \alpha \) valós szám \( \text{lánctörjegyein} \) az (1) és (2) képletekkel definiált (véges vagy végtelen) \( c_0, c_1, \ldots \) számsorozatot értjük.  ◆

A definíció alapján világos, hogy a \( \text{lánctörjegyek} \) egyértelműen meghatározott egész számok, és \( c_i \geq 0 \), ha \( i \geq 1 \).

Példák:

P1 Legyen \( \alpha = 111/25 \). Ekkor
\[
\begin{align*}
\frac{111}{25} &= 4 + \frac{11}{25}, & c_0 &= 4, \\
\frac{11}{25} &= 2 + \frac{3}{25}, & c_1 &= 2, \\
\frac{3}{25} &= 1 + \frac{3}{25}, & c_2 &= 1, \\
\frac{3}{25} &= 2 + \frac{1}{25}, & c_3 &= 2.
\end{align*}
\]

A \( 111/25 \) \( \text{lánctörjegyei} \) tehát 4, 2, 3, 1, 2. Ez egyúttal azt is jelenti, hogy
\[
\frac{111}{25} = \ell(4, 2, 3, 1, 2) = 4 + \frac{1}{2 + \frac{1}{3 + \frac{1}{2}}}
\]
P2 Legyen $\alpha = \sqrt{2}$. Ekkor

$$\sqrt{2} = 1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \ddots}}}}, \quad c_0 = 1,$$
$$\frac{1}{\sqrt{2} - 1} = 2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \ddots}}}, \quad c_1 = 2,$$
$$\frac{1}{\sqrt{2} - 1} + 1 = 2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \ddots}}}, \quad c_2 = 2,$$
$$\vdots$$

A $\sqrt{2}$ lánctörtjegyei tehát $1, 2, 2, 2, \ldots$ Erre is bevezetjük (egyelőre formálisan) a $\sqrt{2} = L(1, 2, 2, \ldots)$ jelölést és a „végtesen lánctört” elnevezést.

8.3.2 Tétel. T 8.3.2

Az $\alpha$ valós szám lánctörtjegyeinek sorozata akkor és csak akkor véges, ha $\alpha$ racionális.

Bizonyítás: Legyen a lánctörtjegyek sorozata véges, azaz megfelelő $c_i$ egészekkel $\alpha = L(c_0, c_1, \ldots, c_k)$. Ekkor az emeltese törteket lebontva $\alpha$ végül két egész szám hányadosaként írható, tehát racionális.

Megfordítva, legyen $\alpha = a/b$, ahol $b > 0$ és $a$ egész számok. Megmutatjuk, hogy ekkor a lánctörtjegyeket megadó algoritmus lépései tulajdonképpen az $a$ -ra és $b$ -re vonatkozó euklideszi algoritmus lépésein felelnek meg. Ebből következik, hogy a lánctörtjegyeket előállító algoritmus véges sok lépésben befejeződik.

Az euklideszi algoritmus első lépésében az $a$ számot maradékosan elosztjuk $b$-vel:

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b.$$ 

Ez átírható az

$$\frac{a}{b} = q_1 + \frac{r_1}{b} = \left\lfloor \frac{a}{b} \right\rfloor + \left\{ \frac{a}{b} \right\}$$

alakba, tehát (a lánctört-algoritmus jelöléseivel) $c_0 = q_1$ és $c_1 = r_1/b$.

Ha $r_1 \neq 0$, akkor az euklideszi algoritmus következő lépése

$$b = r_1q_2 + r_2, \quad 0 \leq r_2 < r_1,$$

azaz

$$\frac{1}{c_1} = \frac{b}{r_1} = q_2 + \frac{r_2}{r_1} = \left\lfloor \frac{b}{r_1} \right\rfloor + \left\{ \frac{b}{r_1} \right\},$$

tehát $c_1 = q_2$ és $c_2 = r_2/r_1$.

Ugyanígy adódik, hogy a további lánctörtjegyek is rendre az euklideszi algoritmusban szereplő hányadosok lesznak.

A továbbiakban feltesszük, hogy $\alpha$ irracionalis, és megmutatjuk, hogy a lánctört segítségével az $\alpha$-t jól közelítő racionális számokat tudunk előállítani. Ezek az $\alpha$ (végtelei) „lánctörttalajkának” a (véges) „szeletei” lesznak, azaz azok a (véges) lánctörtek, amelyeket tetszőleges $n \geq 0$ egészre az $\alpha$ első $n + 1$ darab lánctörtjegyéből képezünk. Jelöljük ezeket a racionális számokat $L_n(\alpha)$-val, azaz ha $\alpha = L(c_0, c_1, \ldots)$, akkor
8.3.3 Tétel. T 8.3.3

Legyenek az $\alpha$ irrationális szám lánctörtjegyei $q_0, q_1, \ldots$, és

$$L_n(\alpha) = L(q_0, q_1, \ldots, q_n) = \frac{r_n}{s_n}, \quad \text{ahol} \quad (r_n, s_n) = 1, \quad s_n > 0. \quad (5)$$

Ekkor bármely $n$ esetén fennáll

$$|\alpha - \frac{r_n}{s_n}| < \frac{1}{s_n^2}, \quad (6)$$

sőt, ha $n > 0$, akkor az

$$|\alpha - \frac{r_n}{s_n}| < \frac{1}{2s_n^2}, \quad |\alpha - \frac{r_{n+1}}{s_{n+1}}| < \frac{1}{2s_{n+1}^2}. \quad (7)$$

egyenlőtlenségek közül is legalább az egyik teljesül.

Megjegyzések:
1. A T 8.3.3 Tétel egyrészt nyilván magában foglalja a T 8.1.1 és T 8.2.3 Tételek állításait, másrészt nemcsak a jó közelítő törtek létezését biztosítja, hanem egyúttal a gyakorlatban is használható algoritmust ad ezek előállítására.

2. Megmutatható, hogy az „igazán jól közelítő” törtek kivétel nélkül az (5)-ben megadott $r_n/s_n$ törtek közül kerülnek ki: Ha

$$|\alpha - \frac{r_n}{s_n}| < \frac{1}{2s_n^2}$$

(azaz $r_n/s_n$ a T 8.2.3 Tételben előírt mértékben approximálja az $\alpha$-t), akkor $r_n/s_n$ szükségképpen valamelyik $r_{n+1}/s_{n+1}$-nel egyenlő.

3. A lánctörtek a (bizonyítás nélkül közölt) T 8.1.5 Tétel igazolására is alkalmasak: A T 8.3.3 Tétel alábbi bizonyításához hasonló elveket alapján, csak kissé bonyolultabban az is igazolható, hogy három egymást követő indexű $L_n(\alpha)$ tört közül legalább az egyik a T 8.1.5 Tételben előírt közelítést is teljesíti.

4. A T 8.3.3 Tételből a 8.1.3a feladat [275] alapján következik, hogy

$$\lim_{n \to \infty} L_n(\alpha) = \alpha, \quad \text{azaz} \quad \lim_{n \to \infty} L(q_0, \ldots, q_n) = L(q_0, q_1, \ldots).$$

Ennek alapján természetes jelentést nyert az (eddig formális) $\alpha = L(c_0, c_1, \ldots)$ végtelen lánctört.

A T 8.3.3 Tétel bizonyításához szükségünk lesz a következő lemmára:

8.3.4 Lemma. L 8.3.4

Legyenek $c_0, c_1, c_2, \ldots$ tetszőleges valós számok, ahol $c_i > 0$, ha $i > 1$, és képezzük az alábbi rekurstíókat:

$$r_0 = c_0, \quad r_1 = c_1 c_0 + 1, \quad r_n = c_n r_{n-1} + r_{n-2}, \quad (8a)$$

$$s_0 = 1, \quad s_1 = c_1, \quad s_n = c_n s_{n-1} + s_{n-2}. \quad (8b)$$
Ekkor
\[ L(q_1, c_1, \ldots, c_n) = \frac{r_n}{s_n} \]  
és
\[ \frac{r_n}{s_n} - \frac{r_{n-1}}{s_{n-1}} = \frac{(-1)^{n-1}}{s_n - 1 s_{n-1}} \quad (n \geq 1). \]  

Ha a \( c_n \) számok egészek, akkor \( r_n \) és \( s_n \) is egész, \( (r_n, s_n) = 1 \), valamint \( u > 0 \) esetén \( s_{n+1} > s_n \).

Megjegyzés: A L 8.3.4 Lemmából azonnal következik, hogy a T 8.3.3 Tételben az (5) képlettel megadott \( r_n \) és \( s_n \) számsorozatok kielégítik a (8a)–(8b) rekurziót, tehát a L 8.3.4 Lemma és a T 8.3.3 Tétel \( c_u \), \( r_n \) és \( s_n \) jelölései egymással összhangban vannak.

A L 8.3.4 Lemma bizonyítása: I. A (9) egyenlőséget \( u \) szerinti teljes indukcióval igazoljuk.

Az \( u = 0 \), illetve 2 esetekben
\[ L(q_0) = c_0 = \frac{c_0}{1} = \frac{r_0}{s_0}, \]
\[ L(q_0, c_1) = c_0 + c_1 = \frac{c_0 + c_1}{1} = \frac{r_1}{s_1}, \]
\[ L(q_0, c_1, c_2) = c_0 + c_1 + c_2 = \frac{c_0 + c_1 + c_2}{1} = \frac{r_2}{s_2}. \]

tehát (9) valóban teljesül.

Tegyük fel, hogy (9) az \( u = m \geq 2 \) esetben igaz, azaz
\[ L(q_1, q_2, \ldots, c_m) = \frac{r_m}{s_m} = \frac{c_m r_m - 1 + r_{m-2}}{c_m s_m - 1 + s_{m-2}}. \]

ahol \( r_{m-1} \), \( s_{m-1} \), \( r_{m-2} \) és \( s_{m-2} \) csak a \( c_0, \ldots, c_{m-1} \) értékektől függ. Ekkor
\[ L(q_0, \ldots, c_{m-1}, c_m, c_{m+1}) = L(q_0, \ldots, c_{m-1}, c_m + 1, \ldots) = \]
\[ = \frac{(c_m + 1)}{c_{m+1}} \frac{r_{m-1} + r_{m-2}}{s_{m-1} + s_{m-2}} - \frac{c_m + 1}{c_{m+1}} \frac{c_m r_{m-1} + r_{m-2}}{c_m s_{m-1} + s_{m-2}} - \frac{r_m}{s_m + 1} \]
\[ = \frac{r_m}{s_m + 1} + \frac{r_{m-1}}{s_{m-1} + 1} \quad (8.1) \]

tehát (9) az \( u = m + 1 \) esetben is teljesül.

II. Most rá térünk (10) igazolására. A (8a)–(8b) képletek alapján
\[ r_n s_{n-1} - r_{n-1} s_n = (c_n r_n - 1 + r_{n-2})s_{n-1} - r_{n-1}(c_n s_{n-1} + s_{n-2}) = -r_{n-1}(s_n - 2 r_{n-2}). \]

Ugyanezt \( n \) helyett az \( u = 1, 2, \ldots, 2 \) értékekre megismételve kapjuk, hogy
\[ r_n s_{n-1} - r_{n-1} s_n = (-1)^{n-1}(r_1 s_0 - r_0 s_1) = (-1)^u - 1. \]  

Innen (10)-et \( s_n s_{n-1} - 1 \)-gyel való osztással nyerjük.
III. Az egész \( q \)-kre vonatkozó állítások a relatív prímég kivételével a feltételekből nyilvánvalók, 
\( (\tau_n; s_n) = 1 \) pedig (11)-ből következik. 

\[ A T 8.3.3 \] Tétel bizonyítása: Mint már említettük, a L 8.3.4 Lemmából következik, hogy az (5) képlettel megadott \( \tau_n \) és \( s_n \) számok sorozatok kielégítik a (8a)–(8b) rekurziót. 

A továbbiakban fel fogjuk használni, hogy maga az \( \alpha \) is felirható véges láncértékként: (3) alapján bármely \( n \) -re 

\[ \alpha = \theta(\alpha_0, \alpha_1, \ldots, \alpha_n, \alpha_{n+1} + \alpha_{n+2}) \], 

ahol (2) és \( \alpha \) irracionális és \( 0 < \alpha_{n+2} < 1 \). 

Így az \( \alpha - \tau_n/s_n \) különbség becsülésehez a L 8.3.4 Lemmát az \( \alpha, \alpha_1, \ldots, \alpha_n \) és \( \tau_n+s_n \) számkrokra fogjuk alkalmazni és itt megállunk. Ekkor a (8a)–(8b) rekurzióval az 

\[ \tau_0, \tau_1, \ldots, \tau_n, \tau_{n+1} : \quad s_0, s_1, \ldots, s_n, s'_{n+1} \] 

számokhoz jutunk, ahol \( n \geq 1 \)-re 

\[ \begin{align*} 
\tau'_{n+1} &= \tau'_{n} + \tau_n + \tau_{n-1} = (c_{n+1} + \alpha_{n+2})\tau_n + \tau_{n-1}, \\
\tau'_{n+1} &= \tau'_{n+1} + s_n - s_{n-1} = (c_{n+1} + \alpha_{n+2})s_n + s_{n-1}. 
\end{align*} \]

A (12), (9) és (4) képletek szerint 

\[ \alpha - \frac{\tau'_{n+1}}{s'_{n+1}} \quad \text{és} \quad \theta(\alpha) = \frac{\tau_n}{s_n}, \]

amiből (10) felhasználásával azt nyerjük, hogy 

\[ \alpha = \frac{\tau_n}{s_n} = \frac{\tau'_{n+1}}{s'_{n+1}} - \frac{\tau_n}{s_n} = \frac{(-1)^{s_n}}{s_n s'_{n+1}}. \] 

(13) szerint az \( \alpha - \tau_n/s_n \) és \( \alpha - \tau_{n+1}/s_{n+1} \) különbségek ellenkező előjelűek, tehát \( \alpha \) az \( \tau_n/s_n \) és \( \tau_{n+1}/s_{n+1} \) tört közé esik. Ennek megfelelően 

\[ \left| \alpha - \frac{\tau_n}{s_n} \right| \geq \frac{1}{2s_n^2} \quad \text{és} \quad \left| \alpha - \frac{\tau_{n+1}}{s_{n+1}} \right| \geq \frac{1}{2s_{n+1}^2}. \] 

(14) helyett (13) szerint az \( \alpha - \tau_n/s_n \) és \( \alpha - \tau_{n+1}/s_{n+1} \) különbségek elegendő előjelűek, tehát \( \alpha \) az \( \tau_n/s_n \) és \( \tau_{n+1}/s_{n+1} \) tört közé esik. Ennek megfelelően 

\[ \left| \alpha - \frac{\tau_n}{s_n} \right| + \left| \alpha - \frac{\tau_{n+1}}{s_{n+1}} \right| = \left| \frac{\tau_n}{s_n} - \frac{\tau_{n+1}}{s_{n+1}} \right|. \]

(15) szerint az \( \alpha - \tau_n/s_n \) és \( \alpha - \tau_{n+1}/s_{n+1} \) különbségek ellenkező előjelűek, tehát \( \alpha \) az \( \tau_n/s_n \) és \( \tau_{n+1}/s_{n+1} \) tört közé esik. Ennek megfelelően 

\[ \frac{1}{2s_n^2} + \frac{1}{2s_{n+1}^2} \leq \frac{1}{s_n s_{n+1}}, \quad \text{azaz} \quad (s_{n+1} - s_n)^2 \leq 0. \]

adódnak. Mivel \( n > 0 \) -ra \( s_{n-1} > s_n \), ezért (16) nem teljesülhet, vagyis ellentmondásra jutottunk. \( \blacksquare \)
Feladatok

8.3.1 Határozzuk meg az alábbi számok láncértjegyeit:
(a) \( \frac{53}{11} \);
(b) \( \sqrt{3} \);
(c) \( \sqrt{5} \);
(d) \( \frac{1}{2} \).

8.3.2 Melyek azok a számok, amelyeknek a láncértkifejtése
(a) 1, 2, 3, 4;
(b) 1, 2, 1, 2, 1, 2, …?

8.3.3 Bizonyítsuk be, hogy bármely \( \alpha \) irracionalis számhoz végzeten sok olyan \( \tau/\varepsilon \) tört létezik, amelyben \( \varepsilon \) páratlan és
\[
|\alpha - \frac{\tau}{\varepsilon}| < \frac{1}{\varepsilon^2}.
\]

8.3.4 Bizonyítsuk be, hogy bármely \( \alpha \geq 1 \) esetén
\[
|\frac{1}{\sqrt{5}} - \frac{\varphi_{n+1}}{\varphi_n}| < \frac{1}{\varphi_n^2},
\]
ahol \( \varphi_n \) az \( n \)-edik Fibonacci-szám (lásd az 1.2.5 feladatot [7]).

8.3.5 (M [602]) Bizonyítsuk be, hogy a L 8.3.4 Lemma feltételeinek teljesülése esetén bármely \( \alpha \geq 2 \) esetén
\[
\frac{\tau_n}{s_n} - \frac{\tau_{n-2}}{s_{n-2}} = \frac{(-1)^n a_n}{s_{n-2} s_n},
\]

8.3.6 (M [602]*) Tegyük fel, hogy az \( \alpha \) irracionalis szám láncértjegyei periodikus sorozatot alkotnak (azaz létezik olyan \( k \) és \( M \), hogy minden \( n > M \) esetén \( c_n = c_{n-k} \)). Bizonyítsuk be, hogy ekkor van olyan másodfokú, egész együtthatós polinom, amelynek az \( \alpha \) gyöke.

Megjegyzés: A fenti állítás megfordítása is igaz.

8.4 A törtrészek eloszlása

Ebben a pontban valós számsorozatok törtrészeinek az eloszlásával foglalkozunk.

8.4.1 Tétel . T 8.4.1

Tetszőleges irracionalis szám többszöröseinek a törtrészei mindenütt sűrűn helyezkednek el a \([0,1]\) intervallumban.

Ez részletesen kifejtve a következőt jelenti: Legyen \( \alpha \) irracionalis szám és \( \varepsilon \in [0,1] \). Ekkor bármely \( \varepsilon > 0 \)-hoz létezik olyan \( n > 0 \) egész, amelyre \( \left|\{nx\} - \varepsilon\right| < \varepsilon \).
**Bizonyítás:** A T 8.1.1 Tétel alapján végigen sok olyan $\frac{r}{s}$ tört létezik, amelyre

\[
\left| a - \frac{r}{s} \right| < \frac{1}{s^2}, \quad s \alpha a x, \quad \left| b - \frac{r}{s} \right| < \frac{1}{s^2}.
\]

Válasszunk olyan közelítő törtet, amelyben $s > 1/\varepsilon$, ekkor $|s\alpha - r| < \varepsilon$. Jelöljük $|s\alpha - r|$-et $d$-vel (tehát $d < \varepsilon$), és tekintsük az

\[
\left\{ \frac{m}{s} \right\}, \left\{ \frac{2m}{s} \right\}, \ldots, \left\{ \frac{nm}{s} \right\}
\]

törtrészeket, ahol $m = \left\lfloor \frac{1}{d} \right\rfloor$ (nyilván feltetett $\varepsilon < 1$, és így $m \geq 1$).

Vegyük először azt az esetet, amikor $s\alpha - r > 0$. Ekkor bármely $1 \leq i \leq m$-re

\[
0 < i\alpha - i\alpha - r = i(s\alpha - r) = id < 1,
\]

tehát $\left\{ i\alpha \right\} = id$.

Ez azt jelenti, hogy egy olyan törtrész a $s\alpha$-val, amely való mértékben közelítő jelenléte van a $\frac{r}{s}$-re. Az (1) esetben megállapíthatjuk, hogy bármely $1 \leq i \leq m$-re

\[
\left| i\alpha - \frac{r}{s} \right| < \frac{1}{s^2},
\]

és ez az (1)-ben megadott tört részek olyan monoton fogyó sorozatot alkottak, amelyben a szomszédos elemek távolsága $d < \varepsilon$, továbbá az első elemnek a 0-tól, az utolsónak pedig az 1-től való távolsága is kisebb, mint $\varepsilon$. Ebből következik, hogy a sorozat elemei között van olyan, amelynek a $\frac{r}{s}$-től való távolsága kisebb, mint $\varepsilon$.

Az $s\alpha - r < 0$ eset is ugyanig kezelhető: ekkor $1 < i \leq m$-re

\[
\left| \frac{r}{s} - i\alpha \right| = \left| id \right| < 1,
\]

tehát $\left\{ i\alpha \right\} = id$. Ez azt jelenti, hogy a $\frac{r}{s}$-től való távolsága kisebb, mint $\varepsilon$. Ebből következik, hogy csak az $\frac{r}{s}$-től való távolsága kisebb, mint $\varepsilon$.

Most a T 8.4.1 Tételben felvetett probléma többdimenziós változatával foglalkozunk. Tekintsük először a legegyszerűbb esetet: Legyenek $\alpha_1$ és $\alpha_2$ irracionális számok, és vizsgáljuk meg az $P_{a} = \left\{ n\alpha_1, n\alpha_2 \right\}$ pontok elhelyezkedését az egységégyezetben.

A T 8.4.1 Tétel bizonyításához hasonlóan a T 8.1.3 Tételből kapjuk, hogy bármely $\varepsilon > 0$-hoz léteznek olyan $r_1$, $r_2$ és $s > 0$ egész számok, amelyekre

\[
\left| s\alpha - r_1 \right| < \varepsilon, \quad s\alpha - r_1, \quad \left| s\alpha - r_2 \right| < \varepsilon.
\]

Ez azt jelenti, hogy a $P_{a} = \left\{ n\alpha_1, n\alpha_2 \right\}$ pont az egységégyezet valamelyik csúcsának a közelében helyezkedik el. Ebből a T 8.4.1 Tétel bizonyításához hasonlóan az is következik, hogy ezt a csúcsot a $P_{a}$ ponttal összekötő egyenesen egymáshoz közel sorakoznak a $P_{a}, P_{3a}, \ldots$ pontok.

Az azonban nem igaz, hogy a $P_{a}$ pontok bármely $\alpha_1$ és $\alpha_2$ esetén mindenütt sűrűek az egységégyezetben. Legyen például $\alpha_2 = \alpha_1 + 1$. Ekkor nyilván bármely $n$-re

\[
\left\{ n\alpha_1 \right\} = \left\{ n\alpha_2 \right\},
\]

tehát a $P_{a}$ pontok kivétel nélkül az $y = x$ egyenesre esnek.

A mindenütt sűrű elhelyezkedés feltételét a lineáris függetlenség segítségével fogalmazhatjuk meg:

**8.4.2 Tétel.**

Az $\alpha_1, \ldots, \alpha_k$ valós számokra a

\[
P_{a} = \left\{ n\alpha_1, n\alpha_2, \ldots, n\alpha_k \right\}, \quad n = 1, 2, 3, \ldots
\]

pontok akkor és csak akkor helyezkednek el mindenütt sűrűn a $k$-dimenziós egységkockában, ha $1, \alpha_1, \ldots, \alpha_k$ lineárisan függetlenek a racionális test felett.
A tételben megadott lineáris függetlenség azt jelenti, hogy racionális \( c_i \)-kkel \( a_1 + c_1 a_1 + \cdots + c_n a_n = 0 \) csak a triviális \( c_1 = c_2 = \cdots = c_n = 0 \) esetben teljesülhet. Ebből speciálisan az is következik, hogy minden \( \alpha \) szükségképpen irritacionális.

Az illusztrációként vizsgált \( k = 2 \), \( \alpha_2 = \alpha_1 + 1 \) példában láttuk, hogy a \( P_n \) pontok nem lesznek mindenütt sűrűek az egységnégyzetben, és ez összhangban van azzal, hogy \( 1 \cdot 1 + 1 \alpha_1 + (-1) \alpha_2 = 0 \) szerint \( 1, \alpha_1, \alpha_2 \) nem lineárisan függetlenek.

A T 8.4.2 Tételben megadott feltétel elégseggességét nem bizonyítjuk, a szükségesség igazolását a 8.4.3 feladatban [290] tüzött ki.

Visszatérve az egydimenziós esetre, most a mindenütt sűrű elhelyezkedésnél jóval erősebb követelményt támasztó egyenletes eloszlás kérdését vizsgáljuk.

Az egyenletes eloszlás azt jelenti, hogy az \( u_1, u_2, \cdots \) végtelel számsorozat törtrészei a \([0, 1]\) intervallum bármely \( I \) részintervallumában az \( I \) hosszával „arányosan” találhatók: nagy \( n \) esetén az első \( n \) darab \( \{u_i\} \) közül „körülbelül” \( d \) darab esik \( I \)-be, ahol \( d \) az \( I \) hossza. A pontos definíció a következő:

8.4.3 Definíció. D 8.4.3

Az \( u_1, u_2, \cdots \) végtelel valós számsorozat modulo 1 egyenletes eloszlású (vagy röviden egyenletes eloszlású), ha a \([0, 1]\) intervallum bármely \( I \) részintervallumára

\[
\lim_{n \to \infty} \frac{f_n(I)}{n} = d,
\]

ahol \( d \) az \( I \) intervallum hossza és \( f_n(I) \) az \( \{u_1\}, \cdots, \{u_n\} \) törtrészek közül az \( I \)-be esők száma. ♠

A számsorozatok egyenletes eloszlására vonatkozó Weyl alábbi tétel, amelyet bizonyítás nélkül közlünk:

8.4.4 Tétel. T 8.4.4

Az \( u_1, u_2, \cdots \) sorozat akkor és csak akkor egyenletes eloszlású, ha bármely \( \tau n \neq 0 \) egészre

\[
\lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} e^{2\pi i \tau n u_i} = 0. \]

Mind az egyenletes eloszlás fogalma, mind pedig a Weyl-kritérium kiterjesztett több dimenzióra is.

Weyl tételének felhasználásával most azt igazoljuk, hogy egy irracionális szám tőbszörösei egyenletes eloszlású sorozatot alkotnak.

8.4.5 Tétel. T 8.4.5

Ha \( \alpha \) irracionális szám, akkor az \( \alpha, 2\alpha, \cdots, n\alpha, \cdots \) sorozat egyenletes eloszlású. ♠

Bizonyítás: A T 8.4.4 Tétel alapján azt kell megmutatni, hogy bármely \( \tau n \neq 0 \) egészre

\[
\lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} e^{2\pi i \tau n u_i} = 0. \tag{2}
\]

A (2) bal oldalán szereplő összeg egy \( n \) -tagú mértani sorozat, amelynek hányadosa \( e^{2\pi i \tau n u} \neq 1 \), mivel \( \alpha \) irracionális. Ezért
Feladatok

8.4.1 (M [602]) Vizsgáljuk meg, hogy az alábbi számsorozatok törtrészei mindenütt sűrűek-e a \([0, 1]\) intervallumban:

(a) \((1 + \sqrt{2})^n\);
(b) \(\sqrt{n}\);
(c) \(\sqrt{n^2 + 1}\);
(d) \(\sqrt{2n^2 + 1}\);
(e) \(\sin(n\pi/180)\);
(f) \(\sin n\pi\);
(g) \(\log n\).

8.4.2 (*) Mutassuk meg, hogy létezik olyan \(\alpha\) valós szám, amelyre az számsorozat törtrészei mindenütt sűrűk \([0, 1]\)-ben.

8.4.3 (M [603]) Bizonyítsuk be, hogy a T 8.4.2 Tételben megadott lineáris függetlenségi feltétel szükséges ahhoz, hogy a \(P_d\) pontok mindenütt sűrűn helyezkedjenek el a \(k\)-dimenziós egységkockában.

8.4.4 Bizonyítsuk be a következő állításokat.

(a) Ha egy sorozat törtrészei mindenütt sűrűk \([0, 1]\)-ben, akkor a sorozat átindexezhető egyenletes eloszlású sorozattá.
(b) Bármely egyenletes eloszlású sorozat átindexezhető nem egyenletes eloszlású sorozattá.

8.4.5 Melyek igazak az alábbi állítások közül?

(a) Egy egyenletes eloszlású sorozat részsorozata is egyenletes eloszlású.
(b) Egy egyenletes eloszlású sorozat minden eleméhez ugyanazt a valós számot hozzáadva ismét egyenletes eloszlású sorozatot kapunk.
(c) Egy egyenletes eloszlású sorozat minden elemét ugyanazzal a nemnulla valós számmal megszorozva ismét egyenletes eloszlású sorozatot kapunk.
(d) Két egyenletes eloszlású sorozat összege is egyenletes eloszlású.
(e) Két egyenletes eloszlású sorozat szorzata is egyenletes eloszlású.
(f) Egy egyenletes eloszlású sorozat négyzete is egyenletes eloszlású.

(g) Egy egyenletes eloszlású sorozat négyzete sohasem egyenletes eloszlású.

8.4.6 Mutassuk meg, hogy az alábbi számsorozatok nem egyenletes eloszlásúak:

(a) \( \log n \);

(b) \( \sin n \).

8.4.7 Lássuk be, hogy ha a \( \ell \) természetes szám nem \( 10^k \) alakú, akkor van olyan pozitív egész kitevős hatványa, amelynek első öt jegye 54321 (tízes számrendszerben).
9. fejezet - ALGEBRAI ÉS TRANSZCENDENS SZÁMOK

Egy \( \alpha \) komplex számot aszerint nevezünk algebrainak, illetve transcenzensnek, hogy létezik-e vagy sem olyan racionális (illetve egész) együtthatós, nemnulla polinom, amelynek az \( \alpha \) gyöke. Megmutatjuk, hogy a komplex számok „tulnyomó többsége” transcenzens, ugyanakkor egy konkrét számról általában igen nehéz eldönteni, hogy algebrai-e vagy transcenzens. Ezt jól érzékelheti az \( \varepsilon \) transcenzenciáját bemutató bizonyítás és a számos megoldatlan probléma felsorolása.

Az algebrai számok tárgyalását a minimálpolinom és a fokszám tulajdonságaival, valamint az algebrai számoknak a műveletekhez való viszonyával kezdjük. Ezután belátjuk, hogy az algebrai számok rosszul approximálhatók. Ennek alapján egyrészt egyszerűen lehet transcenzens számot konstruálni, másrészt fontos következményként kapjuk, hogy bizonyos típusú diofantikus egyenleteknek csak véges sok megoldása van. A fejezet végén az egész számok általánosításaként definiált algebrai egészekkel foglalkozunk.

Az algebrai számok és algebrai egészek fontos szerepet játszanak a következő két fejezetben is.

### 9.1 Algebrai szám, transcenzens szám

A racionális számokat az összes komplex szám között az tünteti ki, hogy elsőfokú racionális együtthatós polinomok gyökei. Ha itt a fokszámmal vonatkozó korlátozást elejük, akkor az algebrai szám fogalmához jutunk:

#### 9.1.1 Definíció

Egy \( \alpha \) komplex szám algebrai szám (vagy röviden algebrai), ha létezik olyan racionális együtthatós, nemnulla \( f \) polinom, amelyre \( f(\alpha) = 0 \).

Megjegyzések:

1. Az polinomot nyilván ki kell zárni, hiszen ennek a polinomnak minden komplex szám gyöke.
2. Ha \( \alpha \) gyöke egy racionális együtthatós polinomnak, akkor a polinomot a nevezők legkisebb közös többszörösevé beszorozva egy olyan egész együtthatós polinomot kapunk, amelynek az \( \alpha \) továbbra is gyöke. Így ugyanahhoz a fogalomhoz jutunk, ha a D 9.1.1 Definícióban „racionális együtthatós polinom” helyett „egész együtthatós polinom” létezését írjuk elő.
3. Alapvetően megváltozik a helyzet, ha a racionális vagy egész együtthatók helyett például valós vagy komplex együtthatókat írunk elő: minden komplex számhoz található olyan valós együtthatós, nemnulla polinom (és így komplex együtthatós is), amelynek az adott szám gyöke (lásd a 9.1.7 feladatot [295]).
4. Az „algebrai szám” helyett a „racionális test felett algebrai szám” (vagy a „racionális test felett algebrai elem”) kifejezést is szokás mondani, mert a fogalom általánosítása és definiált algebrai test felett más test feletti algebrai elemet is lehet értelmezni (lásd a D 10.1.4 Definíciót).

Példák:

Mint említettük, minden racionális szám egyen algebrai szám is.

Irracionális algebrai szám például a \( \sqrt{2} \) vagy az \( \sqrt[3]{15} \), hiszen gyöke az \( x^2 - 2 \), illetve \( x^3 - 13 \) polinomnak.

Algebrai szám minden komplex egységgyökök is, ezek az \( x^n - 1 \) alakú polinomok gyökei.
A nem algebrai számokat transzcendent számoknak nevezzük:

**9.1.2 Definíció.** D 9.1.2

Egy komplex szám transzcendir szám (vagy röviden transzcendens), ha a nullpolinomon kívül nem gyöké egyetlen racionális együtthatós polinomnak sem. 

**9.1.3 Tétel.** T 9.1.3

Létezik transzcendens szám, sőt „majdnem minden” szám transzcendens: az algebrai számok számossága megszámlálható, míg a transzcendens számok számossága kontinuum.

**Bizonyítás:** Mivel a komplex számok számossága kontinuum, ezért a tétel valamennyi állítása következni fog abból, hogy az algebrai számok számossága megszámlálható, azaz az algebrai számok sorozatba rendezhetők.

Az algebrai számok az egész együtthatós, nemnulla polinomok gyökei, ezért először ezeket a polinomokat fogjuk sorozatba rendezni. Ebből ezután úgy kapjuk meg az algebrai számok egy sorozatba rendezését, hogy rendre vesszük a polinomok összes olyan (komplex) gyökét, amely korábbi polinomok gyökeként még nem lett felsorolva.

Legyen \( f = a_0 + a_1 x + \cdots + a_n x^n \) tetszőleges egész együtthatós polinom, ahol \( a_n \neq 0 \), és definiáljuk \( H(f) \)-et a következőképpen:

\[
H(f) = |a_0| + |a_1| + \cdots + |a_n|.
\]

Például

\[
\begin{align*}
H(f) = 1 & \iff f = \pm 1; \\
H(f) = 2 & \iff f = \pm 2, \pm x; \\
H(f) = 3 & \iff f = \pm 3, \pm x \pm 1, \pm 2x, \pm x^2; \\
H(f) = 4 & \iff f = \pm 4, \pm x \pm 2, \pm 2x \pm 1, \pm 3x, \pm x^2 \pm 1, \pm x^2 \pm x, \pm 2x^2 \pm x, \pm x^3.
\end{align*}
\]

A \( H(f) \) definíciójából világos, hogy bármely \( k \) esetén csak véges sok olyan \( f \) létezik, amelyre \( H(f) = k \). Ezért egy megfelelő felsorolást kapunk, ha vesszük rendre azokat a polinomokat, amelyekre \( H(f) = 1, 2, 3, \ldots \)

Innen a már jelzett módon nyerjük az algebrai számok egy sorozatba rendezését. Ennek első néhány tagja az \( f \)-ek (1)-beli sorrendjét figyelembe véve

\[
0, 1, -1, 2, -2, \frac{1}{2}, -\frac{1}{2}, i, -i, \ldots
\]

(a nemnulla konstans polinomoknak nincs gyöke, a 0 az \( x \)-ből, a \( \pm 1 \) az \( x \pm 1 \)-ből adódik stb., a konstansszorzosok, illetve a korábban már számításbá vett polinomok szorzatai, valamint ilyenek osztói nem adnak újabb gyököket).

A fentiakból világos, hogy elég azokra az \( f \)-ekre szorítkozni, amelyekben \( \gamma > 0 \), \( a_n > 0 \), \( \{a_0, a_1, \ldots, a_n\} = 1 \) és \( f \) irreducibilis a racionális test felett.
Néhány további nevezetes transzcendens szám:

- \( \pi \)
- \( \sin n \pi \), ahol az \( n \) szög (ívmeértékben mérve) egész szám;
- \( \lg n \pi \), ahol \( n \) pozitív egész szám és a 10-nek nem egész kitevőjű hatványa (lásd a 9.3.7 feladatot [302]);
- \( 2^{\sqrt{2}} \) (lásd a T 9.3.5 Tételt);
- \( \zeta(2) = \sum_{k=1}^{\infty} \frac{1}{k^2} \) (lásd a 9.1.3 feladatot [295]).

Általában egy adott számról igen nehéz eldönteni, hogy algebrai-e vagy transzcendens, az imént felsorolt példák bármelyike esetén a transzcendencia bizonyítása meghaladja a könyv kereteit (a hivatkozásként jelzett T 9.3.5 Tétel bizonyítás nélkül szerepel, a másik két hivatkozás pedig erre a tételre, illetve a \( \pi \) transzcendenciájára vezeti vissza a kérdést).

Megoldatlan például, vajon \( e + \pi \) transzcendens-e, illetve egyáltalán irracionalis-e. Ugyancsak megoldatlan, hogy \( \zeta(3) = \sum_{k=1}^{\infty} k^{-3} \) transzcendens-e, ennek a számnak az irracionalitását is csak 1975-ben igazolták. A \( \zeta(5) \) ról az sincs tisztázva, vajon irracionalis-e.

**Feladatok**

9.1.1 Igazoljuk, hogy az alábbi számok algebraiak:

(a) \( \sqrt[3]{7} \);
(b) \( \sqrt{2} + 3 \);
(c) \( \sqrt{2} + \sqrt{3} \);
(d) \( \sqrt{2} + \sqrt[4]{4} \);
(e) \( \sqrt[3]{2} + \sqrt[4]{4} \);
(f) \( \sqrt{2} + \sqrt{3} + \sqrt{5} \).

9.1.2 Bizonyítsuk be, hogy ha \( \alpha \) algebrai szám, akkor

(a) \( - \alpha \);
(b) \( \overline{\alpha} \);
(c) \( \alpha \neq 0 \) esetén \( \frac{1}{\alpha} \); továbbá bármely \( \tau \) racionális, illetve \( k \) pozitív egész szám esetén
(d) \( \tau + \alpha \);
(e) \( \tau \alpha \).
(f) $\sqrt[3]{2}$ is algebraic.

9.1.3 Felhasználva, hogy $\pi$ transzcendens szám, mutassuk meg, hogy $\zeta(2) = \sum_{k=1}^{\infty} k^{-2}$ is transzcendens.

9.1.4 Tegyük fel, hogy $\alpha$ transzcendens és $f \neq 0$ egész együtthatós polinom. Igazoljuk, hogy ekkor $f'(\alpha)$ is transzcendens.

9.1.5 Legyen $g$ komplex együtthatós, nemnulla polinom. Bizonyítsuk be, hogy akkor és csak akkor létezik olyan $h$ egész együtthatós, nemnulla polinom, amelyre $g \mid h$, ha $g$ minden (komplex) gyöke algebrai szám.

9.1.6 Bizonyítsuk be, hogy az $\alpha$ komplex szám akkor és csak akkor algebrai, ha létezik olyan $u$ pozitív egész, amelyre az $1, \alpha, \ldots, \alpha^n$ számok lineárisan összefüggők a racionális test felett.

9.1.7 Bizonyítsuk be, hogy bármely komplex szám gyöke egy alcámas
(a) komplex;
(b) valós
együtthatós polinomnak.

9.2 Minimálpolinom és fokszám

Legyen $\alpha$ algebrai szám. Ekkor nyilván végletes sok olyan racionális együtthatós polinom van, amelynek az $\alpha$ gyöke: ha $f$ egy ilyen polinom, akkor az $f$ bármely (racionális együtthatós) polinomszorosa is megfelel. Így ezek közül a polinomok közül azokat érdemes kitüntetni, amelyeknek a lehető legkisebb a fokszáma:

9.2.1 Definíció. D 9.2.1

Az $\alpha$ algebrai szám minimálpolinomja egy olyan, minimális fokú, racionális együtthatós polinom, amelynek az $\alpha$ gyöke. Az $\alpha$ minimálpolinomját $m_{\alpha}$-val jelöljük.

A minimálpolinom nem teljesen egyértelmű: ha $f$ az $\alpha$ (egyik) minimálpolinomja, akkor nyilván $c f$ is megfelel a feltételeknek, ahol $c \neq 0$ tetszőleges racionális szám. Ettől eltekintve azonban már egyértelmű a minimálpolinom:

9.2.2 Tétel. T 9.2.2

Ha $f$ és $g$ is minimálpolinomja az $\alpha$ algebrai számnak, akkor van olyan $c \neq 0$ racionális szám, amelyre $g = c f$.

Bizonyítás: Legyen

$$f = a_0 + a_1 x + \cdots + a_n x^n; \quad a_n \neq 0,$$
$$g = b_0 + b_1 x + \cdots + b_n x^n; \quad b_n \neq 0.$$

Ekkor $\alpha$ gyöke a $\hat{h} = b_n f - c \alpha g$ polinomnak, amely vagy a nullpolinom, vagy legfeljebb $n - 1$-edfokú. Így a minimálpolinom definíciója miatt csak $\hat{h} = 0$ lehetséges. Innen $g = c f$, ahol $c = b_n / a_n$. □
Az $m_\alpha$ jelölés a továbbiakban is az $\alpha$ akármelyik minimálpolinomját jelentheti, ez a T 9.2.2 Tétel alapján nem okoz majd problémát.

A minimálpolinom legfontosabb tulajdonságait a következő tételben foglaljuk össze.

**9.2.3 Tétel.** T 9.2.3

(i) Legyen $g \in \mathbb{Q}[x]$. Ekkor $g(\alpha) = 0 \iff m_\alpha | g$.

(ii) $m_\alpha$ irreducibilis $\mathbb{Q}$ felett.

(iii) Ha $f$ irreducibilis $\mathbb{Q}$ felett, és $f(\alpha) = 0$, akkor $f$ az $\alpha$ (egyik) minimálpolinomja.

**Bizonyítás:** (i) Először tegyük fel, hogy $m_\alpha | g$, azaz az $\alpha$-val alkalmazott $h \in \mathbb{Q}[x]$ -re $g = h \cdot m_\alpha$. Ekkor

$$g(\alpha) = h(\alpha) \cdot m_\alpha(\alpha) = h(\alpha) \cdot \alpha = 0.$$

Megfordítva, tegyük fel, hogy $g(\alpha) = 0$. Osszuk el a $g$ polinomot maradékosan $m_\alpha$-val:

$$g = m_\alpha h + r, \quad h, r \in \mathbb{Q}[x], \quad \deg r < \deg m_\alpha \quad \text{vagy} \quad r = 0.$$

Ekkor

$$0 = g(\alpha) = m_\alpha h(\alpha) + r(\alpha) = 0 + r(\alpha),$$

azaz $\deg r < \deg m_\alpha$ esetén ellentmond a minimálpolinom definíciójának. Így csak $r = 0$ lehetséges, azaz valóban $m_\alpha | g$.

(ii) Indirekt tegyük fel, hogy $m_\alpha = g h$, ahol $g$ és $h$ az $m_\alpha$-nél alacsonyabb fokú racionális együtthatós polinomok. Ekkor (a komplex számtest nullosztómentessége miatt)

$$0 = m_\alpha(\alpha) = g(\alpha) h(\alpha) \implies g(\alpha) = 0 \quad \text{vagy} \quad h(\alpha) = 0,$$

ami ellentmond a minimálpolinom definíciójának.

(iii) Az (i) állítás szerint $m_\alpha | f$, ezért $f$ irreducibilitása miatt $m_\alpha = c$ vagy $f = c m_\alpha$, ahol $c$ konstans. Az első eset nem lehetséges, így $f$ valóban (az egyik) minimálpolinom.

**9.2.4 Definíció.** D 9.2.4

Az $\alpha$ algebrai szám foka (vagy fokszáma) a minimálpolinomjának a foka: $\deg \alpha = \deg m_\alpha$.

** Példák: **

P1 $A 0$ (egyik) minimálpolinomja $m_0 = x$, az $1 \cdot m_4 = x - 1$, és általában egy $r$ racionális számé $m_r = x - r$. Az is világos, hogy az elsőfokú algebrai számok éppen a racionális számok, 0-adjukú algebrai számok pedig nincs.

P2 Az $i$ minimálpolinomja $x^2 + 1$, és így $\deg i = 2$.

P3 Az $\sqrt{3}$ minimálpolinomja $x^2 - 3$, mivel ez a polinom a Schönemann–Eisenstein-kritérium szerint irreducibilis $\mathbb{Q}$ felett.
P4 Bármely k pozitív egészhez végig sok k-adfokú algebrai szám létezik, hiszen (például ismét a Schönemann–Eisenstein-kritérium alapján) végtelen sok, \( \mathbb{Q} \) felett irreducibilis, k-adfokú polinom van.

P5 Egy \( \vartheta \) primitív \( n \)-edik komplex egységgyök minimálpolinomja \( f_n \), az \( n \)-edik körösztási polinom (mert \( f_n, \vartheta^2 = \mathbb{Q} \) irreducibilis \( \mathbb{Q} \) felett). Ennélfogva \( \deg \vartheta = \deg \vartheta_n = \rho(n) \). (A P2 példa tulajdonképpen ennek a speciális esete volt.)

**Feladatok**

9.2.1 Milyen kapcsolat van a 9.1.2 feladatban \([294]\) szereplő számok foka és \( \alpha \) foka között?

9.2.2 Határozzuk meg az alábbi (algebrai) számok fokát:

(a) \( \sqrt[3]{12} \);

(b) \( \cos 20^\circ \);

(c) \( \sqrt[3]{3} - \sqrt[3]{9} \);

(d) \( \sqrt{7^2 - 4 \sqrt{3}} \);

(e) \( \sqrt[2]{2} + \sqrt{7} \);

(f) \( \sqrt[2]{2} + \sqrt[2]{7} + \sqrt[3]{3} \).

9.2.3 Mutassuk meg, hogy \( \alpha \) akkor és csak akkor másodfokú algebrai szám, ha \( \alpha = r + \sqrt{s} \), ahol \( r \) és \( s \) racionális számok, és \( s \) nem négyzete egy racionális számnak.

9.2.4 Mutassuk meg, hogy az \( n \)-edfokú algebrai számok

(a) \( n \geq 1 \) esetén a valós számegyenesen;

(b) \( n \geq 2 \) esetén a komplex számsíkon mindenütt sűrűn helyezkednek el.

9.2.5 Legyen \( f \) egy \( n \)-edfokú racionális együtthatós polinom (\( n \geq 1 \)), és legyenek a (multiplicitással számolt, komplex) gyökei \( \alpha_1, \ldots, \alpha_n \).

(a) Bizonyítsuk be, hogy \( \sum_{i=1}^{n} \deg \alpha_i \leq n^2 \).

(b) Mikor áll (a)-ban egyenlőség?

(c) Mutassuk meg, hogy ha (a)-ban szigorú egyenlőség érvényes, akkor \( \sum_{i=1}^{n} \deg \alpha_i \leq n^2 - 2^n + 2 \) is teljesül.

9.2.6 Tudjuk, hogy \( \deg \alpha = 6 \) és \( \alpha \) gyöke az

\[
f = x^7 + 8x^5 + 15x^3 + 10x^3 + 35x^2 + 5x - 30
\]

polinomnak. Mi az \( \alpha \) minimálpolinomja?
9.2.7 Tegyük fel, hogy az $\alpha$ és $\beta$ komplex számok gyökei az $f$ racionális együtthatós, nemnulla polinomnak és $\alpha \alpha = \beta \beta$. Bizonyítsuk be, hogy $m_\alpha = m_\beta$.

9.2.8 (M [604]) Tegyük fel, hogy az $f \neq 0$ és $g$ racionális együtthatós polinomokra és az $\alpha$ és $\beta$ komplex számokra $f(\alpha) = g(\alpha) = f(\beta) = g(\beta) = 0$. Bizonyítsuk be, hogy $f$ reducibilis $\mathbb{Q}$ felett.

9.3 Műveletek algebrai számokkal

Ebben a pontban elsősorban az algebrai számok és a négy alapművelet, illetve a hatványozás kapcsolatát tárgyaljuk.

9.3.1 Tétel. T 9.3.1

Az algebrai számok résztestet alkotnak a komplex számtestben, azaz két algebrai szám összege, különbsége, szorzata és (ha a nevező nem nulla, akkor) hányadosa is algebrai.

A tételt a szimmetrikus polinomok segítségével igazoljuk. (Egy másik bizonyítás szerepel majd a 10.2 pontban.)

Egy $R$ gyűrű feletti $k$-változós (vagy $k$-határozatlanú) $\prod(x_1, \ldots, x_k)$ polinomot akkor nevezzük szimmetrikusnak, ha az $x_i$ változók tetszőleges permutációja esetén ugyanazt a polinomot kapjuk. Ilyen polinom például a változók összege, a változók szorzata, vagy általában a (különböző) változókból képzett összes $j$-tényezős szorzatok összege:

$$\sigma_j(x_1, \ldots, x_k) = \sum_{1 \leq i_1 < \cdots < i_j \leq k} x_{i_1} \cdots x_{i_j} = \sum_{i_1 < \cdots < i_j} x_{i_1} x_{i_2} \cdots x_{i_j} + \sum_{i_1 < \cdots < i_j} x_{i_1} x_{i_2} \cdots x_{i_j-1} x_{i_{j+1}} + \cdots + x_{i_1} x_{i_2} \cdots x_{i_{k-j+1}} x_{i_{k-j+2}} \cdots x_{i_{k-1}} x_{i_k},$$

ahol $\sigma_j$ az $x_1, \ldots, x_k$ változók elemi szimmetrikus polinomjainak nevezzük.

A $\sigma_j$-ket az $x_1, \ldots, x_k$ változók elemi szimmetrikus polinomjainak nevezzük.

Mivel szimmetrikus polinomok összege és szorzata is szimmetrikus polinom, így például $\sigma_1 + \sigma_2$, és általában a $\sigma_j$-k tetszőleges ($R$ -beli együtthatókkal képzett) polinomja is (az $x_i$ változók szerint nézve) szimmetrikus polinom.

Az elemi szimmetrikus polinomok jelentőségét elsősorban az adja, hogy az iménti észrevetelnek a megfordítása is igaz: Minden szimmetrikus polinom felírható az elemi szimmetrikus polinomok polinomjáként.

9.3.2 Tétel (A szimmetrikus polinomok alaptétele) . T 9.3.2

Legyen $\prod(x_1, \ldots, x_k)$ egy $R$ gyűrű feletti tetszőleges ($k$-változós) szimmetrikus polinom. Ekkor létezik olyan $\prod$ feletti, $k$-változós $G$ polinom, amelyre

$$\prod(x_1, \ldots, x_k) = G(\sigma_1, \ldots, \sigma_k),$$

ahol $\sigma_j = \sigma_j(x_1, \ldots, x_k)$ az $x_i$ változókból képzett ($1$)-beli elemi szimmetrikus polinomokat jelenti.

Példa: Az $x_i$ változók négyzetösszege a következőképpen állítható elő a $\sigma_j$-kkel:
A szimmetrikus polinomok alaptételének bizonyítása megtalálható bármely bevezető algebratankönyvben.

A tételt kiegészíthetjük azzal a megjegyzéssel, hogy a tételben szereplő \( G \) polinom egyértelmű, és \( G \) együtható polinom együthatóiból csak az összeadás és kivonás segítségével kapjuk.

A tételt elsősorban arra a két esetre fogjuk alkalmazni, amikor \( \mathbb{R} \) a racionális számtest, illetve az egész számok gyűrűje. Ha tehát az \( F \) szimmetrikus polinom együthatói racionális, illetve egész számok, akkor a megfelelő \( G \) polinom is racionális, illetve egész együthatós lesz.

A T 9.3.1 Tétel bizonyítása: A 9.1.2 feladatban [294] láttuk, hogy egy algebrai szám ellentettje és egy nemnulla algebrai szám reciproka is algebrai, így elég azt igazolni, hogy két algebrai szám összege és szorzata is algebrai.

Legyen \( \alpha \) és \( \beta \) algebrai szám, és tegyük fel, hogy \( \alpha \), illetve \( \beta \) gyöke az

\[
f(x) = \prod_{i=1}^{n}(x - \alpha_i), \quad \text{illetve} \quad g(x) = \prod_{i=1}^{n}(x - \beta_i)
\]

racionális együthatós polinomnak (ahol \( \alpha_1 = \alpha \), illetve \( \beta_1 = \beta \)). Ekkor \( \alpha + \beta \) gyöke a

\[
h(x) = \prod_{i=1}^{n} \prod_{j=1}^{n}(x - \alpha_i - \beta_j)
\]

polinomnak. Megmutatjuk, hogy \( h \) racionális együthatós.

Legyen \( h = c_0 + c_1 x + \ldots + c_{nm-1} x^{nm-1} + x^{n+1} \). Írjuk át a \( h \) polinomot

\[
h(x) = \prod_{x=1}^{c_n} g(x - \alpha_i)
\]

alakba. Ebből látszik, hogy az \( \alpha_i \)-k tetszőleges permutációja esetén a \( h \) polinom, és így annak minden \( c_r \) együthatója is változatlan marad. Ez azt jelenti, hogy ha az \( \alpha_1, \ldots, \alpha_m \) számokat változóknak tekintjük, akkor minden \( c_r \) együtható ezeknek az \( \alpha_i \) változóknak szimmetrikus polinomja:

\[
c_r = F_r(\alpha_1, \ldots, \alpha_m), \quad r = 0, 1, \ldots, nm - 1,
\]

ahol \( F_r \) szimmetrikus polinom és \( F_r \) együthatói racionális számok (hiszen ezeket \( g \) együthatóiból kapjuk). A T 9.3.2 Tétel szerint így \( h \) felírható az \( \alpha_i \)-kból képzett \( \sigma_j \) elemi szimmetrikus polinomok polinomjaként, azaz alkalmaz \( G_r \) racionális együthatós polinomra

\[
c_r = F_r(\sigma_1, \ldots, \sigma_m) = G_r(\sigma_1, \ldots, \sigma_m).
\]

Az \( \alpha_i \)-k elemi szimmetrikus polinomjai azonban a gyökök és együthatók közötti összefüggés alapján éppen az \( f \) polinom együthatói, illetve azok ellentettjei, tehát racionális számok, ezért \( c_r = G_r(\sigma_1, \ldots, \sigma_m) \) is racionális szám. Ezzel beláttuk, hogy \( h \) racionális együthatós, tehát \( \alpha + \beta \) algebrai szám.

Hasonlóan igazolható, hogy \( \alpha \beta \) is algebrai szám; ekkor a
polinomot kell tekinteni (ha $\alpha \neq 0$, akkor feltehetjük, hogy egyik $\alpha_i$ sem nulla, az $\alpha = 0$ esetben pedig $\alpha^2 = 0$ nyilvánvalóan algebrai).

A T 9.3.1 Tétel egyik fontos következménye, hogy a komplex számok algebrai, illetve transzcendens voltának eldöntése visszavezethető a valós számok hasonló vizsgálatára:

9.3.3 Tétel . T 9.3.3

Egy komplex szám akkor és csak akkor algebrai, ha a valós része is és a képzetes része is algebrai. ♦

Bizonyítás: Legyen $\alpha = a + bi$ (ahol $a$ és $b$ valós számok).

Először tegyük fel, hogy $a$ és $b$ algebrai. Mivel $i$ is algebrai (gyöke az $x^2 + 1$ polinomnak), és algebrai számok szorzata és összege is algebrai, ezért $\alpha = a + bi$ is algebrai.

Megfordítva, tegyük fel, hogy $a$ algebrai. Ekkor $a$ is algebrai (lásd a 9.1.2b feladatot). Mivel algebrai számok összege, különbsége és hányadosa is algebrai, valamint $\Re$ és $\Im$ algebrai, ezért

$$a = \frac{\alpha + \overline{\alpha}}{2}, \quad b = \frac{\alpha - \overline{\alpha}}{2i}$$

is algebrai. ♦

Most ráterünk a hatványozásra. Mivel a 0-nak csak pozitív (valós) kitevős hatványai vannak értelmezve, és ezek értéke 0, ezért a továbbiakban elég a nemnulla algebrai számok hatványozásával foglalkoznunk.

9.3.4 Tétel . T 9.3.4

Egy algebrai szám tetszőleges racionális kitevőjű hatványa is algebrai. ♦

Bizonyítás: Mivel algebrai számok szorzata és reciprokája, valamint az 1 is algebrai, ezért egy algebrai szám tetszőleges egész kitevőjű hatványa is algebrai. Ennek alapján a törtkitevőre vonatkozó állítás abból következik, hogy egy algebrai számból pozitív egész kitevőjű gyököt vonva ismét algebrai számot kapunk (lásd a 9.1.2f feladatot [294]). ♦

A nem racionális kitevővel kapcsolatban talán a legegyszerűbb kérdés, vajon $2^{\sqrt{2}}$ transzcendens-e, illetve egyáltalán irracionalis-e. Ez a kérdés is szerepelt a híres Hilbert-problémák között, és Hilbert ezt jóval nehezebben tartotta, mint a Fermat-sejtést vagy a Riemann-sejtést. Mindez nem riasztotta el a kutatókat, és 1934-ben Gelfond és Schneider egymástól függetlenül (és eltérő módszerekkel) igazolták a következő általános tételt, amelyet bizonyítás nélkül közlünk:

9.3.5 Tétel (Gelfond–Schneider-tétel) . T 9.3.5

Ha $\alpha$ és $\beta$ algebrai számok, $\alpha \neq 0$ vagy 1, és $\beta$ nem racionális, akkor $\alpha^\beta$ transzcendens. ♦

Ebből könnyen következik például, hogy ha $\pi$ egész szám és nem 10-hatvány, akkor $\ln\pi$ transzcendens (lásd a 9.3.7 feladatot [302]).

A T 9.3.5 Tétel (az általában végtelel sok értékű) komplex kitevőjű hatványokra is vonatkozik. Így például $e^{-\pi}$ mindegyik értéke, köztük $e^\pi$ is transzcendens (vő, azzal a 9.1 pontban említett megoldatlan problémával, hogy $e + \pi$ transzcendens-e, vagy egyáltalán irracionalis-e).
A T 9.3.4 Tételben (illetve a 9.1.2f feladatban [294]) láttuk, hogy az algebrai számok köréből az egész kitevőjű gyökvonás nem vezet ki. Ezt a tényt a következőképpen is megfogalmazhatjuk: Ha \( \alpha \) algebrai szám, akkor az \( \omega^k - \alpha \) algebrai együtthatós polinom gyökei is algebraiak. Ez nemcsak ilyen speciális alakú, hanem tetszőleges algebrai együtthatós polinom esetén is igaz:

9.3.6 Tétel .  T 9.3.6

Ha az \( f \neq 0 \) polinom együtthatói algebrai számok, akkor \( f \) minden (komplex) gyöke algebrai szám.

Bizzonyítás: Ismét a szimmetrikus polinomok alaptételét (T 9.3.2 Tétel) fogjuk felhasználni. (Egy másik bizonyítást adunk majd a 10.2 pontban.)

Legyen \( f = \alpha + \beta x + \cdots + \xi x^n \), ahol \( \alpha, \beta, \cdots, \xi \) algebrai számok, és jelölje rendre \( \alpha_i, \beta_j, \cdots, \xi_k \) az \( \alpha, \beta, \cdots, \xi \) minimálpolinomjának többi gyökét (\( \alpha_1 = \alpha \) stb.). Tekintsük a

\[
 h = \prod_{i,j,\cdots,k} (c_{i1} + \beta_{j1} x + \cdots + \xi_{k1} x^n) 
\]

polinomot. Mivel \( h \) tényezői között szerepel \( f \) is, ezért \( f \) minden gyöke \( h \)-nak is gyöke. Így a tétel állításához elég megmutatni, hogy \( h \) racionális együtthatós.

Legyen \( c_s \)- a \( h \) polinom tetszőleges együtthatója. A T 9.3.1 Tétel bizonyításának gondolatmenetéhez hasonlóan \( c_v \) az \( c_{ij} \)-nek egy \( F_r \) szimmetrikus polinomja, ahol \( F_r \) együtthatói a \( \beta_j, \cdots, \xi_k \) számokból összeadás, kivonás és szorzás segítségével adódnak. A T 9.3.2 Tétel szerint \( F_r \) előáll az \( c_{ij} \)-k elemi szimmetrikus polinomjainak a polinomjaként. Az \( m_r \), polinomra a gyökök és együtthatók közötti összefüggést alkalmazva kapjuk, hogy a szóban forgó elemi szimmetrikus polinomok racionális számok. Ennek alapján \( c_{ij} \)-ból „kiküszöböltük” az \( \alpha_i \)-ket. Ugyanezt a gondolatmenetet a \( \beta_j \)-kre stb. megismételve kapjuk, hogy \( c_r \) racionális szám.

A T 9.3.1 és T 9.3.6 Tételek együttesen azt a tényt fejezik ki, hogy az algebrai számok egy algebraílag zárt testet alkotnak.

Feladatok

9.3.1  (a) Igazoljuk, hogy egy algebrai és egy transzcendens szám összege mindig transzcendens.
(b) Mutassuk meg, hogy két transzcendens szám összege lehet transzcendens, de lehet algebrai is.
(c) Vizsgáljuk meg a hasonló kérdéseket összeg helyett szorzatra is.

9.3.2  Mit állíthatunk \( \alpha \) -ról és \( \beta \) -ról (algebrai, illetve transzcendens szempontból), ha
(a) \( \alpha + \beta \) és \( \alpha - \beta \) algebrai;
(b) \( \alpha + \beta \) algebrai, \( \alpha - \beta \) transzcendens;
(c) \( \alpha + \beta \) és \( \alpha - \beta \) transzcendens;
(d) \( \alpha \beta \) és \( \alpha / \beta \) algebrai;
(e) \( \alpha + \beta \) algebrai, \( \alpha \beta \) transzcendens;
(f) $\alpha + \beta$ transzcendens, $\alpha\beta$ algebrai;

(g) $\alpha + \beta$ és $\alpha\beta$ transzcendens;

(h) $\alpha - \beta$ és $\alpha\beta$ algebrai?

Mennyiben változik a helyzet, ha ($\alpha$ és $\beta$ valós számok, és) az „algebrai”, illetve „transzcendens” szavak helyett „racionális”-t, illetve „irracionális”-t írnunk?

9.3.3 Tegyük fel, hogy $\alpha + \beta$ és $\alpha + \gamma$ algebrai, $\beta + \gamma$ transzcendens. Az alábbi számok mindegyikéről döntsük el, hogy algebrai-e vagy transzcendens:

(a) $\alpha$ ;

(b) $2\alpha + (1 - i)\beta + (1 + i)\gamma$ ;

(c) $3\alpha + (2 - i)\beta + (2 + i)\gamma$ .

9.3.4 Mint jeleztük, megoldatlan probléma, vajon $e + \pi$ , illetve $e - \pi$ transzcendens-e.

(a) Bizonyítsuk be, hogy $e + \pi$ és $e - \pi$ közül legalább az egyik transzcendens.

(b) Igazoljuk, hogy $e + i\pi$ transzcendens.

9.3.5 Az alábbi számok mindegyikéről döntsük el, hogy algebrai-e vagy transzcendens:

(a) $\sin 7\pi$ ;

(b) $i\pi + \pi/i$ ;

(c) $\pi^7 + i\pi^5 + \sqrt{2}\pi$ .

9.3.6 (M [604]) Legyen $\alpha \neq 0$ trigonometrikus alakja $\alpha = r(\cos \varphi + i \sin \varphi)$. Bizonyítsuk be, hogy $\alpha$ akkor és csak akkor algebrai, ha $r$ és $\cos \varphi$ algebrai.

9.3.7 Tegyük fel, hogy az $n$ pozitív egész a 10-nek nem egész kitevőjű hatványa. Bizonyítsuk be, hogy $\log n$ transzcendens.

9.3.8 Legyenek $\alpha$ és $\beta$ komplex számok, és tekintsük a

$$H = (a + \beta, a^2 + \beta^2, \ldots, a^k + \beta^k, \ldots)$$

sorozatot. Mutassuk meg, hogy ha $H$ -nak legalább két eleme algebrai, és ezek közül nem mindkettő 0, akkor $H$ minden eleme algebrai.

9.3.9 Mutassuk meg, hogy bármely $\alpha > 0$ , $\alpha \neq 1$ (valós) algebrai számnak végtelen sok olyan valós transzcendens kitevőjű hatványa van, amely algebrai, és olyan is végtelen sok van, amely transzcendens.

9.4 Algebrai számok approximációja

Ebben a pontban algebrai számok diofantikus approximációját és ennek néhány következményét tárgyaljuk. Mivel egy nem valós komplex szám eleve nem közelíthető jól racionális számokkal, ezért csak valós algebrai számok approximációjával foglalkozunk.
A 8.1.1 feladatban [274] láttuk, hogy a racionális számok „nagyon rosszul” approximálhatók. A T 8.1.6 Tételben, illetve a 8.1.6 feladatban [276] megmutattuk, hogy az irracionalis számok közül az $(1 + \sqrt{5})/2$, illetve a $\sqrt{2}$ szintén „elég rosszul” approximálható. Liouville bebizonyította, hogy az algebrai számok általában is rosszul approximálhatók, a következő értelemben:

9.4.1 Tétel.  T 9.4.1

Legyen $\alpha \geq 2$ és $\alpha$ egy $\mathbb{N}$-edfokú (valós) algebrai szám. Ekkor létezik olyan $c = c(\alpha) > 0$ valós konstans, hogy bármely $r/s$ racionális számra

$$\left| \alpha - \frac{r}{s} \right| > \frac{c(\alpha)}{s^\alpha},$$

(1)

Megjegyzések: 1. A T 9.4.1 Tételt szokás a következő alakban is megfogalmazni: Létezik olyan $c = c(\alpha) > 0$ valós konstans, hogy az

$$\left| \alpha - \frac{r}{s} \right| < \frac{c(\alpha)}{s^\alpha},$$

eyenlőtlenség csak véges sok $r/s$ racionális számra teljesül. Ez tulajdonképpen azt jelenti, hogy (1)-nél véges sok kivételt megengedünk az $r/s$ értékekre. Ez a véges sok kivétel azonban könnyen megszűntethető, ha (1)-ben ettől a véges sok „rossz” $\tau/n$ -től függően alkalmaz kisebb $c$ értéket választunk $c(\alpha)$-nak. Ezzel beláttuk, hogy a tétel kétféle alakja ekvivalens (azaz bármelyik változatból azonnal következik a másik).

2. A T 9.4.1 Tételből az is következik, hogy bármely $k > n$ és $c^k > 0$ valós számokra az

$$\left| \alpha - \frac{r}{s} \right| < \frac{c^k}{s^k},$$

eyenlőtlenség csak véges sok $r/s$ racionális számra teljesülhet, ugyanis ha $s$ (a $k$ -től és $c^k$ -től függően) elég nagy, akkor

$$\frac{c^k}{s^k} < \frac{c^k(\alpha)}{s^k}.$$  

Ezt a tényt a 8.1.7 feladatban [276] bevezetett szóhasználat szerint úgy is megfogalmazhatjuk, hogy egy $n$ -edfokú algebrai szám biztosan nem approximálható $n$ -edrendnél jobban, azaz semmilyen $k > n$: esetén nem approximálható $k$ -edrendben. Ennél sokkal élesebb eredmény is igaz, lád a T 9.4.3 Tételt.

3. A 8.1.1 feladat [274] szerint a T 9.4.1 Tétel $n = 1$ -re is érvényes, ha az $\alpha = r/s$ lehetőséget kizárjuk.

Bizonyítás: Tegyük fel indirekt, hogy bármely $c > 0$ -hoz létezik olyan $r/s$, amelyre

$$\left| \alpha - \frac{r}{s} \right| \leq \frac{c}{s^n},$$

Ez azt jelenti, hogy létezik racionális számoknak olyan $r_i/s_i$ sorozata, hogy $(s_i > 0)$ és

$$\lim_{i \to \infty} s_i^k \left( \alpha - \frac{r_i}{s_i} \right) = 0.$$  

(2)
Ebből azonnal adódik az is, hogy
\[
\lim_{s_i \to \infty} \left( \alpha - \frac{r_i}{s_i} \right) = 0 \quad \text{azaz} \quad \lim_{s_i \to \infty} \frac{r_i}{s_i} = \alpha. \tag{3}
\]

Tekintsük \( \alpha \) minimálpolinomjának egy egész együtthatós alakját, és legyenek \( m_\alpha \) komplex gyökei \( \alpha_1, \alpha_2, \ldots, \alpha_n \). Ekkor
\[
m_\alpha = a_0 + a_1 x + \cdots + a_n x^n = a_n \prod_{j=1}^{n} (x - \alpha_j), \tag{4}
\]
ahol \( a_0, a_1, \ldots, a_n \) egész és \( a_n \neq 0 \). Mivel \( m_\alpha \) irreducibilis \( \mathbb{Q} \) felett, ezért nem lehet többszörös (komplex) gyöke (lásd a 9.4.4 feladatot [308]), vagyis az \( \alpha_j \) számok mind különbözők.

Az \( m_\alpha \)-ba \( \frac{r_i}{s_i} \)-t behelyettesítve (4) alapján azt kapjuk, hogy
\[
a_0 + a_1 \left( \frac{r_1}{s_1} \right) + \cdots + a_n \left( \frac{r_n}{s_n} \right)^n = a_n \prod_{j=2}^{n} \left( \frac{r_j}{s_j} - \alpha_j \right). \tag{5}
\]

Az (5) bal oldalán álló kifejezés egy \( \frac{r_i}{s_i} \) nevezőjű tört, továbbá nem lehet 0, mivel \( m_\alpha \)-nak nincs racionális gyöke. Ezért (5) bal oldalának az abszolút értéke legalább \( \frac{1}{s_i^n} \). Igé (5)-'ot \( s_i^n \)-nel beszorzva azt kapjuk, hogy
\[
1 \leq \left| s_i^n \alpha_{\alpha} \left( \alpha - \frac{r_i}{s_i} \right) \prod_{j=2}^{n} \left( \frac{r_j}{s_j} - \alpha_j \right) \right|. \tag{6}
\]
A (2)-beli, valamint a (3)-ból adódó
\[
\lim_{s_i \to \infty} \prod_{j=2}^{n} \left( \frac{r_j}{s_j} - \alpha_j \right) = \prod_{j=2}^{n} (\alpha - \alpha_j)
\]
határértékek alapján (6) jobb oldala \( i \to \infty \) esetén 0-hoz tart. Ez azonban nyilvánvalóan ellentmond a (6)-beli egyenlőtlenségnek.

A T 9.4.1 Tételre támaszkodva a következőképpen lehet transzcendens számot konstruálni: ha egy \( \alpha \) valós szám „nagyon jól” approximálható, akkor \( \alpha \) szükségképpen transzcendens. Ilyen \( \alpha \) számot egy olyan, racionális számokból képzett vektort sor összegeként kaphatunk, amelynek a részletösszegei rendkívül gyorsan konvergálnak a végtelen sor összegéhez. Az alábbiakban ezt a Liouville-tól származó konstrukciót ismertetjük.

9.4.2 Tétel . T 9.4.2

Az
\[
\alpha = \sum_{k=1}^{\infty} \frac{1}{10^k} = 0.1100100000000000000000000000\ldots \tag{7}
\]
szám transzcendens. (A tizedes törtben a \( k! \) sorszámú tizedesjegyek értéke 1, a többei jegy 0.)

A (7) képlet valóban egy valós számot definiál, ez közvetlenül leolvasható a tizedesértől-alakkal (de azonnal adódik abbl is, hogy a megadott vektort sor konvergens, hiszen majorálható a \( \sum_{k=1}^{\infty} 10^{-k} \) végteleten mértani sorral).
Bizonyítás: Megmutatjuk, hogy a (7) végére sor részletösszegei „nagyon jól” approximálják \( \alpha \)-t.

Írjuk fel az \( n \)-edik részletösszeget \( r_n/s_n \)-alakban, ahol \( (r_n, s_n) = 1 \) és \( s_n > 0 \). Ezt közös nevezőre hozzással kapjuk:

\[
\sum_{k=1}^{m} \frac{1}{10^k} = \frac{10.4 - 1}{10^{m+1}},
\]

tehát \( s_n = 10^{m+1} \). Ekkor

\[
0 < \alpha - \frac{r_n}{s_n} = \sum_{k=n+1}^{\infty} \frac{1}{10^k} < \sum_{j=(m+1)}^{\infty} \frac{1}{10^j} = \frac{10}{9} \cdot \frac{1}{10^{m+1}} = \frac{10}{9s_n-1}.
\]

Ebből következik, hogy

\[
|\alpha - \frac{r_n}{s_n}| < \frac{10}{9s_n+1}.
\]

Tegyük fel indirekt, hogy valamely \( n \)-re \( \alpha \) egy \( n \)-edfokú algebrai szám. Mivel \( \alpha \) nem szakaszos tizedes tört, ezért \( \alpha \) irrationális, azaz \( \alpha > 2 \). Ekkor a T 9.4.1 Tétel szerint van olyan \( c_1(\alpha) > 0 \), hogy bármely \( \varepsilon/\delta \) racionális számra (1)-nek kell teljesülnie. Így speciálisan \( r_n/s_n \)-esetén is

\[
|\alpha - \frac{r_n}{s_n}| > \frac{c_1(\alpha)}{s_n^\varepsilon}.
\]

Ezt (8)-cal összevetve

\[
\frac{c_1(\alpha)}{s_n^\varepsilon} < \frac{10}{9s_n^{-\varepsilon+1}},
\]

azaz

\[
s_n^{\varepsilon-\eta+1} < \frac{10}{9c_1(\alpha)}
\]

adódik, ami elég nagy \( n \)-re ellentmondás.

Mint a T 9.4.1 Tétel utáni 2. megjegyzésben jeleztük, a T 9.4.1 Tétel állítása jelentősen élesíthető. Erre vonatkoznak Thue, illetve Roth alábbi eredményei, amelyeket bizonyítás nélkül közlünk:

9.4.3 Tétel

(i) (Thue tétele.) Legyen \( \alpha \geq 3 \) és \( \alpha \) egy \( n \)-edfokú (valós) algebrai szám. Ekkor bármilyen (nagy) \( c > 0 \) valós konstans esetén az

\[
|\alpha - \frac{r_n}{s_n}| < \frac{c}{s_n^\varepsilon}
\]

eyenlőtlenséget csak véges sok \( r_n/s_n \) racionális szám elégti ki.

(ii) (Roth tétele.) Legyen \( \alpha \) tetszőleges algebrai szám és \( \alpha \) tetszőleges. Ekkor az

\[
|\alpha - \frac{r_n}{s_n}| < \frac{1}{s_n^{\varepsilon+\delta}}
\]

eyenlőtlenséget csak véges sok \( r_n/s_n \) racionális szám elégti ki.

Megjegyzések: 1. Roth tétele nyilván jóval erősebb Thue eredményénél, azonban már Thue tételének is igen fontos következményei vannak a diofantikus egyenletek elméletében (lásd a T 9.4.4 Tételt).
2. Roth tétele szerint a T 8.1.8 Tételben szereplő kivételes $H$ halmaz csupa transzcendens számából áll. Ugyanakkor a T 8.1.8 Tétel azt is mutatja, hogy (az összes algebrai számon kívül) a transzcendens számok „többsége” is „nagyon rosszul” approximálható.

A diofantikus approximáció szoros kapcsolatban áll bizonyos diofantikus egyenletek vizsgálatával. A 7.8 pontban láttuk, hogy ha az $n$ pozitív egész nem négyzetszám, akkor az $x^2 - ny^2 = 1$ Pell-egyenletnek végelen sok megoldása van (T 7.8.1 Tétel); ehhez azt használtuk fel, hogy a $\sqrt{n}$ irracionalis szám másodrendben approximálható. Most az algebrai számok rosszul approximálhatóságára támaszkodva azt fogjuk igazolni, hogy bizonyos magasabb fokú diofantikus egyenleteknek legfeljebb véges sok megoldása lehet.

9.4.4 Tétel. T 9.4.4

Legyen $f = a_0 + a_1 x + \cdots + a_n x^n$ egy $n$-edfokú egészegységes polinom, ahol $a_i \geq 3$ és $f$ reducibilis $\mathbb{Q}$ felett. Ekkor bármely (rögzített) $u$ egész szám esetén a
doitranszcendens számokból áll. Ugyanakkor a T 8.1.8 Tétel azt is mutatja, hogy (az összes algebrai számon kívül) a transzcendens számok „többsége” is „nagyon rosszul” approximálható.

Bizonyítás: Tegyük fel indirekt, hogy a (12) diofantikus egyenletet végelen sok $\left(\xi_i, \eta_i\right)$ egész számpár kielégíti. Mivel egy adott $y_i$-hoz nyilván legfeljebb $u$ darab $z$ tartozhat, ezért

$$\lim_{y_i \to \infty} |y_i| = \infty,$$  \hspace{1cm} (13)

és azt is feltehetjük, hogy az $y_i$ értékek egyike sem 0.

A (12) egyenletbe az $\left(\xi_i, \eta_i\right)$ megoldást behelyettesíte, majd az egyenlőséget $y_i^{\#i}$-nel elosztva azt kapjuk, hogy

$$f \left(\xi_i \eta_i\right) = \frac{b}{y_i^{\#i}}.$$  \hspace{1cm} (14)

A (13) és (14) összefüggésekből az is következik, hogy

$$\lim_{y_i \to \infty} f \left(\xi_i \eta_i\right) = 0.$$  \hspace{1cm} (15)

Legyen $\hat{f}$ gyöktényezős alakja

$$\hat{f} = a_n \prod_{j=1}^{\eta} (x - \alpha_j).$$  \hspace{1cm} (16)

Ekkor az $f \left(\xi_i \eta_i\right)$ helyettesítési értékre

$$f \left(\xi_i \eta_i\right) = a_n \prod_{j=1}^{\eta} \left(\xi_i \eta_i - \alpha_j\right).$$  \hspace{1cm} (17)

adódik. Mivel (15) szerint $i \to \infty$ mellett (17) bal oldala 0-hoz tart, ezért az $i$ indexek alkalmas részsorozatát véve a jobb oldal valamelyik ténylegjéné is 0 a határértéke. Legyen ez mondjuk a jobb oldal első ténylesője, és az egyszerűség kedvéért jelöljük a szóban forgó részsorozatok ugyanúgy, mint az eredeti sorozatot, ekkor tehát

306
Ebből speciálisan az is következik, hogy $\alpha_1$ valós szám.

(18) alapján

\[
\lim_{{n \to \infty}} \frac{y_n}{z_n} = 1,
\]

azaz

\[
\lim_{{n \to \infty}} \frac{z_n}{y_n} = \alpha_1.
\]

Jelöljük a (19)-beli határértéket $d$-vel. Az $f$ irreducibilitása miatt az $\alpha_j$ számok különbözők, tehát $d \neq 0$. Így elég nagy $i$ esetén

\[
\left| a_n \prod_{j=2}^{n} \left( \frac{z_j}{y_j} - \alpha_j \right) \right| \geq \left| \frac{d}{2} \right|.
\]

Végül (14), (17) és (20) alapján kapjuk, hogy minden elég nagy $i$-re

\[
\left| b_i \right| = \left| b_i \right| = \left| a_n \prod_{j=2}^{n} \left( \frac{z_j}{y_j} - \alpha_j \right) \right| =
\]

\[
\left| \alpha_1 - \frac{z_1}{y_1} \right| \cdot \left| a_n \prod_{j=2}^{n} \left( \frac{z_j}{y_j} - \alpha_j \right) \right| > \left| \alpha_1 - \frac{z_1}{y_1} \right| \cdot \left| \frac{d}{2} \right|,
\]

azaz

\[
\left| \alpha_1 - \frac{z_1}{y_1} \right| < \frac{2b_i}{d} \cdot \frac{1}{b_i^2}.
\]

Mivel $\alpha_1$ egy $n$-edfokú algebrai szám, ezért (21) ellentmond a T 9.4.3 Tétel (i) állításának.

Megjegyezzük, hogy hasonló gondolatmenettel még sokkal általánosabb diofantikus egyenletekről lehet kimutatni a megoldásszám végességét, ha a T 9.4.3 Tétel (ii) állítását használjuk fel (lásd a 9.4.3 feladatot [308]).

**Feladatok**

**9.4.1** Liouville-számoknak azokat az $\alpha$ irrationális számokat nevezzük, amelyekhez bármely $n$ esetén található olyan $\frac{i^n}{b}$ tört, hogy

\[
\left| \alpha - \frac{i^n}{b} \right| < \frac{1}{a^n}.
\]

A T 9.4.1 Tétel szerint minden Liouville-szám transzcendens.

(a) (M [604]) Tegyük fel, hogy $\alpha$ Liouville-szám. Mutassuk meg ekkor bármely $i \neq 0$ iracionális szám, illetve $k$ pozitív egész esetén

(a1) $i \alpha + \alpha$;

(a2) $i \alpha k$;

(a3) $\alpha k$;
(a4) \( \frac{1}{\alpha} \)

is Liouville-szám.

(b) Bizonyítsuk be, hogy végteken sok, sőt kontinuum számosságú Liouville-szám létezik.

9.4.2 Igazoljuk, hogy a T 9.4.4 Tétel állítása akkor is érvényben marad, ha az \( f \) egész egyúthatós, legalább harmadfokú polinomról a \( \mathbb{Q} \) feletti irreducibilitás helyett csak az alábbi enyhébb feltételek valamelyikét tesszük fel:

(a) Az \( f \)-nek nincs első- vagy másodfokú osztója a racionális egyúthatós polinomok körében.

(b) Ha \( b = 0 \), akkor \( f \)-nek nincs racionális gyöke, ha pedig \( b \neq 0 \), akkor \( f \)-nek nincs többszörös (komplex) gyöke.

9.4.3 Legyen \( g(y; z) \) a T 9.4.4 Tételben definiált kétváltozós polinom, és \( h(y; z) \) egy tetszőleges egész egyúthatós, legfeljebb \( n - 3 \)-adfokú, kétváltozós polinom. A T 9.4.3 Tétel (ii) állításának felhasználásával bizonyítsuk be, hogy a \( g(y; z) = h(y; z) \) diofantikus egyenletnek csak véges sok megoldása lehet.

9.4.4 (M [606]) Tegyük fel, hogy az \( f \in \mathbb{Q}[x] \) polinom irreducibilis \( \mathbb{Q} \) felett. Bizonyítsuk be, hogy \( f \)-nek nem lehet többszörös (komplex) gyöke.

## 9.5 Az e transzcendens szám

Először megmutatjuk, hogy \( e \) (a természetes logaritmus alapszáma) és \( \pi \) irracionális számok, majd \( e \) transzcendenciáját igazoljuk. Megjegyezzük, hogy a módszer (jelentős) továbbfejlesztésével az is belátható, hogy \( \pi \) transzcendens. Ez utóbbi tény fontos következménye, hogy egy adott körhöz (euklideszi szerkesztéssel) nem szerkeszthető vele azonos területű négyzet.

9.5.1 Tétel . T 9.5.1

Az \( e \) irracionális szám. ♦

**Bizonyítás:** Az \( e \) szám előáll az alábbi végtelen sor összegeként:

\[
e = 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!} + \cdots
\]

(1)

Tegyük fel indirekt, hogy \( e = \frac{a}{b} \), ahol \( a \) és \( b \) pozitív egészek. Ekkor \( b!e \) egész szám, továbbá (1)-et \( b! \)-sal beszorozva kapjuk, hogy

\[
b!e = n_b + \frac{1}{b+1} + \frac{1}{(b+1)(b+2)} + \cdots,
\]

ahol \( n_b \) egy \( b \)-től függő egész szám. Innen a \( b!e - n_b \) egész számra az alábbi becsléseket nyerjük:

\[
0 < b!e - n_b = \frac{1}{b+1} + \frac{1}{(b+1)(b+2)} + \cdots < \frac{1}{b+1} + \frac{1}{(b+1)^2} + \cdots = \frac{1}{b} \cdot \frac{1}{1 - \frac{1}{b+1}} = \frac{1}{b},
\]

Ez azt jelenti, hogy a \( b!e - n_b \) egész szám 0 és \( 1/b \) közé esik, ami nyilvánvaló ellentmondás. ♦
9.5.2 Tétel. \( T 9.5.2 \)

A \( \pi \) irrationális szám. 

Bizonyítás: Tegyük fel indirekt, hogy \( \pi = \frac{a}{b} \), ahol \( a \) és \( b \) pozitív egészek.

Legyen \( n \) (nagy) pozitív egész és \( f \) a következő \( 2n \)-edfokú polinom:

\[
f(x) = \frac{x^n(1-x)^n}{n!}.
\]

Tekintsük az

\[
I = e^{2n+1} \int_0^1 \sin(\pi x) f(x) dx
\]

integrált. Megmutatjuk, hogy egyrészt

(A) \( I \) egész szám,

másrészt

(B) elég nagy \( n \) esetén \( 0 < I < 1 \), ami nyilvánvaló ellentmondás.

(B) igazolásával kezdjük. Mivel \( 0 < x < 1 \) esetén

\[
0 < \sin(\pi x) \leq 1 \quad \text{és} \quad 0 < f(x) < \frac{1}{n!},
\]

ezért

\[
0 < I < \frac{a^{2n+1}}{n!}.
\]

Ha \( n \) elég nagy, akkor \( a^{2n+1}/n! < 1 \), tehát ezzel a (B) állítást beláttuk.

Rátérve (A)-ra, először megmutatjuk, hogy az \( \hat{f} \) függvény és valamennyi (első, második stb.) deriváltja a 0 és az 1 helyen egész értéket vesz fel, azaz

\[
\hat{f}^{(m)}(0) \quad \text{és} \quad \hat{f}^{(m)}(1) \quad \text{egész szám}, \quad m = 0, 1, 2, \ldots \quad (2)
\]

Mivel \( \hat{f}(x) = f(1-x) \), ezért bármely \( x \) -re \( \hat{f}^{(m)}(x) = (-1)^m f^{(m)}(1-x) \), és így speciálisan \( \hat{f}^{(m)}(0) = (-1)^m f^{(m)}(1) \). Ennek alapján elég az \( x = 0 \) helyet vizsgálni.

Az \( \hat{f} \) polinom

\[
f(x) = \frac{1}{n!} (c_n x^n + c_{n+1} x^{n-1} + \cdots + c_{2n} x^{2n})
\]

alakba írható, ahol a \( c_i \) együtthatók egész számok. Innen kapjuk, hogy

\[
f^{(m)}(0) = \begin{cases} 0, & \text{ha } 0 \leq m < n \text{ vagy } m \geq 2n; \\ c_{m+n}! & \text{ha } n \leq m \leq 2n. \end{cases}
\]

Ezzel (2)-t beláttuk.
Az \( I \) integrálról sorozatos parciális integrálással mutatjuk meg, hogy egész szám. Az első parciális integrálásnál, a \( \pi = e^{1/b} \) indirekt feltevést is felhasználva, az adódik, hogy

\[
I = a^{2n+1} \int_0^1 \sin(\pi x) f(x) \, dx = \\
= a^{2n+1} \left[ \frac{-c\cos(\pi x) f(x)}{\pi} \right]_0^1 - \frac{a^{2n+1}}{\pi} \int_0^1 \cos(\pi x) f'(x) \, dx = \\
= -a^{2n} b \left( f(1) \cos \pi - f(0) \cos 0 \right) + I_1,
\]

ahol

\[
I_1 = a^{2n} b \int_0^1 \cos(\pi x) f'(x) \, dx.
\]

Mivel \( a, b, f(1), f(0), \cos \pi \) és \( \cos 0 \) egész számok, ezért (3) alapján \( I \) pontosan akkor egész szám, ha \( I_1 \) is egész szám.

Az \( I_1 \)-et ismét parciálisan integráljuk, és újra felhasználjuk a \( \pi = e^{1/b} \) indirekt feltevést is:

\[
I_1 = a^{2n} b \int_0^1 \cos(\pi x) f'(x) \, dx = \\
= a^{2n} b \left[ \frac{\sin(\pi x) f'(x)}{\pi} \right]_0^1 - \frac{a^{2n} b}{\pi} \int_0^1 \sin(\pi x) f''(x) \, dx = \\
= a^{2n-1} b \left( f'(1) \sin \pi - f'(0) \sin 0 \right) - I_2,
\]

ahol

\[
I_2 = a^{2n-1} b \int_0^1 \sin(\pi x) f''(x) \, dx.
\]

Az előzőkhöz hasonlóan adódik, hogy \( I_1 \) pontosan akkor egész szám, ha \( I_2 \) is az.

Az eljárást ugyanily folytatva eljutunk az

\[
I_{2n+1} = a^{2n+1} \int_0^1 \cos(\pi x) f^{(2n+1)}(x) \, dx
\]

integrálhoz, és azt kell belátni, hogy ez egész szám. Mivel az \( f \) egy \(?n\) -edfokú polinom volt, ezért \( f^{(2n+1)}(x) = 0 \), tehát \( I_{2n+1} = 0 \). Ennél fogva \( I_{2n+1} \), és így \( I \) is valóban egész szám. Ezzel az \( (A) \) állítást is beláttuk.

9.5.3 Tétel. T 9.5.3

Az \( e \) transzcendens szám. ♦

Bizonyítás: Tegyük fel indirekt, hogy \( e \) algebrai, azaz alkalmas \( u \geq 1 \) és \( a_0 \neq 0, a_1, \ldots, a_n \) egész számokra

\[
a_0 + a_1 e + \cdots + a_ne^n = 0.
\]

A \( \pi \) irracionalitásának bizonyításához hasonlóan most is egy integrál segítségével jutunk majd ellentmondásra.
Legyen \( f \) később alkalmasan megválasztandó polinom, \( \deg f = k \), és tetszőleges \( s \geq 0 \) egész számra tekintsük az alábbi integrált:

\[
I(s) = \int_0^k e^{-s} f(x)dx. \tag{5}
\]

Parciális integrálással kapjuk, hogy

\[
I(s) = \left[ -e^{-s} f\left(x\right) \right]_0^k + \int_0^k e^{-s} f'(x)dx = f(0) - f(s)e^{-s} + I_1(s), \tag{6}
\]

ahol

\[
I_1(s) = \int_0^k e^{-s} f'(x)dx.
\]

Hasonló módon, \( I_1(s) \) parciális integrálásával adódik, hogy

\[
I_1(s) = \left[ -e^{-s} f'(x) \right]_0^k + \int_0^k e^{-s} f''(x)dx = f'(0) - f'(s)e^{-s} = I_2(s), \tag{7}
\]

ahol

\[
I_2(s) = \int_0^k e^{-s} f''(x)dx.
\]

Így (6) és (7) alapján

\[
I(s) = \left[ f(0) - f'(0) \right] - \left[ f(s) + f'(s) \right] e^{-s} + I_2(s).
\]

Az eljárást folytatva végül \( f^{(k+1)} = 0 \) miatt \( I_{k+1} = 0 \), és így

\[
I(s) = \int_0^k e^{-s} f(x)dx = \left[ f(0) + f'(0) + \cdots + f^{(k)}(0) \right] - \left[ f(s) + f'(s) + \cdots + f^{(k)}(s) \right] e^{-s} \tag{8}
\]

adódik.

Szorozzuk be (8)-at \( a_s e^s \) -sel, majd adjuk össze az \( s = 0, 1, \ldots, n \) értékekre ily módon kapott egyenlőségeket. Ekkor a

\[
\sum_{s=0}^n a_s e^s I(s) = \sum_{s=0}^n a_s e^s \int_0^k e^{-s} f(x)dx = \sum_{s=0}^n a_s e^s \left[ f(0) + f'(0) + \cdots + f^{(k)}(0) \right] - \sum_{s=0}^n a_s \left[ f(s) + f'(s) + \cdots + f^{(k)}(s) \right] \tag{9}
\]

összefüggéshez jutunk. A (9) középső sorában szereplő összeg értéke a (4)-beli indirekt feltevés miatt 0, ezért (9) átírható a

\[
\sum_{s=0}^n a_s e^s \int_0^k e^{-s} f(x)dx = - \sum_{s=0}^n a_s \left[ f(s) + f'(s) + \cdots + f^{(k)}(s) \right] \tag{10}
\]
ALGEBRAI ÉS
TRANSZCENDENS SZÁMOK

Az ellentmondás abból fog adódni, hogy alkalmas \( f \) -re (10) bal oldala 1-nél kisebb abszolút értékű, jobb oldala pedig egy nullától különböző egész szám.

Legyen \( p > v \lvert v_0 \rvert \) egy (nagy) prímszám és

\[
f(x) = \frac{a^{p-1}(x-1)^p \ldots (x-v)^p}{(p-1)!}.
\]

A T 9.5.2 Tétel bizonyításában szereplő (2) állítás általánosításaként ugyanúgy igazolható az alábbi észrevétel: Ha \( t \geq 0 \) és \( j \) egész számok, \( \hat{h}(x) \) egész együthathos polinom, akkor a

\[
g(x) = \frac{(x-j)^t \hat{h}(x)}{t!}
\]
polinom és valamennyi deriválja a \( j \) helyen egész értéket vesz fel: \( g^{(m)}(j) \) minden \( m \) -re egész szám. Valóban: \( g(x) \) -et

\[
g(x) = \frac{d_t(x-j)^t + d_{t-1}(x-j)^{t-1} + \ldots + d_0(x-j)^0}{t!}
\]
alakba írva azt kapjuk, hogy

\[
g^{(m)}(j) = \begin{cases} 0, & \text{ha } 0 \leq m < t \text{ vagy } m > r; \\ \frac{d_{m-r} - d_r(t+1)}{r} \ldots m, & \text{ha } t \leq m \leq r. \end{cases}
\]

Mivel

\[
f(x) = \frac{(x-1)^p \hat{h}(x)}{p!},
\]

ahol \( \hat{h}(x) \) egész együthathos polinom, ezért (12)-t a \( g(x) = f(x)/p, \ t = p \), \( j = 1 \) és \( \hat{h}(x) = h_1(z) \) szereposztással alakíthatjuk, hogy minden \( m \) -re \( f^{(m)}(1) \) egész szám, sőt osztható \( p \) -vel. Ugyanígy adódik, hogy

\[
p \mid f^{(m)}(j), \quad j = 1, 2, \ldots, n, \quad m = 0, 1, 2, \ldots \quad (13)
\]

Végül, írjuk az \( f(x) \) -et

\[
f(x) = \frac{x^{p-1}h_0(x)}{(p-1)!}
\]
alakba, ahol \( \hat{h}_0(x) \) egész együthathos polinom, és alkalmazzuk (12)-t a \( g(x) = f(x), \ t = p - 1 \), \( j = 0 \) és \( \hat{h}(x) = h_0(x) \) szereposztással. Ekkor azt kapjuk, hogy \( f^{(m)}(0) \) is minden \( m \) -re egész szám, továbbá

\[
p \mid f^{(p-1)}(0) = (-1)^n v_0^n, \quad \text{de} \quad p \mid f^{(m)}(0), \quad \text{ha} \quad m \neq p - 1 \quad (14)
\]

(ez utóbbi onnan adódik, hogy (12) alapján \( m < p - 1 \) esetén \( f^{(m)}(0) = 0 \), \( m \geq p \) esetén pedig az \( f^{(m)}(j) = d_m p \ldots m \) szorzatban szerepel a \( p \) tényező).
Így (13) és (14) alapján azt kapjuk, hogy a (10) jobb oldalán álló (kettős) összeg minden tagja egész szám és az \( a_0 \cdot \frac{e^{-\xi}}{(p - 1)!} \) tag kivételével minden tag osztható \( p \) vel. Ebből következik, hogy (10) jobb oldala egy \( p \) -vel nem osztható egész szám, tehát speciálisan nem lehet nulla.

Most megmutatjuk, hogy élég nagy \( p \) esetén (10) bal oldalának abszolút értéke kisebb, mint 1. Mivel \( 0 < \xi < n \) esetén

\[
|e^{-\xi}| < 1 \quad \text{és} \quad |f(x)| = \frac{|x^{\nu-1}(x-1)^{\nu-2} \ldots (x-n)^{\nu-1}}{(p-1)!} < \frac{e^{(n+1)\nu-1}}{(p-1)!},
\]

ezért

\[
\left| \sum_{s=0}^{n} a_s e^{\xi} \int_0^\infty e^{-x} f(x)\,dx \right| \leq e^{\nu} \left( \sum_{s=0}^{n} |a_s| \right) \left( \frac{\nu^{\nu-1}}{(p-1)!} \right), \tag{15}
\]

A (15) jobb oldala \( A \cdot B^\nu/(p - 1)! \) alakú, ahol \( A \) és \( B \) konstansok. Ez a kifejezés \( p \to \infty \) mellett 0-hoz tart, tehát élég nagy \( p \) -re kisebb lesz, mint 1.

Ezzel befejeztük annak igazolását, hogy a (12) egyenlőség bal oldalának abszolút értéke 1-nél kisebb, a jobb oldal pedig egy nemnulla egész szám. A (6) indirekt feltevés tehát ellentmondásra vezetett, és így az \( e \) nem lehet algebrai szám. ■

Feladatok

9.5.1 Legyen \( a_1 < a_2 < \ldots < a_n < \ldots \) pozitív egészeknek olyan sorozata, ahol minden \( u \) -re \( a_n > 1 \), továbbá bármely \( k \) pozitív egészhez létezik olyan \( n \), amelyre \( k \mid a_n \). Bizonyítsuk be, hogy a \( \sum_{n=1}^{\infty} 1/a_n \) végletes konvergens, és az összege irrationális szám.

9.5.2 Jelöljön \( r \) racionális számot. Igazoljuk, hogy

(a) \( \sin 1 \) és \( \cos 1 \) irrationális;

(b) \( 0 < r \leq \pi \) esetén \( \sin r \) és \( \cos r \) közül legalább az egyik irrationális;

(c) \( 0 < r < \pi/2 \) esetén \( \tan r \) irrationális.

(A szögek ívmértékben vannak megadva. Ne használjuk fel azt a korábban bizonyítás nélkül említett tényt, hogy ha \( n \) egész szám, akkor \( \sin n \) transzcendens. A „fokokban mérve racionális” szögek szögfüggvényeire nézve lásd a 9.6.11 feladatot [316].)

9.5.3 (*) A T 9.5.2 Tétel bizonyításának gondolatmenetét finomítva, mutassuk meg, hogy \( \pi^2 \) irrationális.

9.6 Algebrai egész

Az algebrai egészek olyan speciális algebrai számok, amelyek az egész számok általánosításainak tekintethetők.

A fogalom előkészítéséhez először az egészeknek a racionálisokon belül egy olyan jellemzését adjuk meg, hogy az ebben megfogalmazott tulajdonságot a racionálisok helyett az algebrai számokra is ki lehessen majd terjeszteni.
A racionális számok éppen az elsőfokú algebrai számok, az \( \tau \) racionális szám (egyik) minimálpolinomja \( x - \tau \). Ez a normált (azaz 1 főegyütthatójú) minimálpolinom nyilván pontosan akkor egész együthathós, ha az \( \tau \) egész szám. A racionális számok közül tehát az tünteti ki az egészeket, hogy \( a(z \text{ egyik}) \) minimálpolinomja normált és egész együthathós.

A minimálpolinomra előírt fenti tulajdonságot az algebrai számok körére kiterjesztve kapjuk az algebrai egész fogalmát:

9.6.1 Definíció . D 9.6.1

Egy algebrai számot algebrai egésznek nevezzük, ha \( a(z \text{ egyik}) \) minimálpolinomja normált és egész együthathós. ♦

Az egyszerűbb szóhasználat érdekében ebben a pontban egy algebrai szám minimálpolinomján mindig annak normált alakját fogjuk érteni.

Példák:

P1 Egy \( \tau \) racionális szám akkor és csak akkor algebrai egész, ha \( \tau \) egész szám (az algebrai egész fogalmát éppen ennek szem előtt tartásával definiáltuk).

P2 A \( \sqrt{2} \) és \( \sqrt[3]{\sqrt{3}} \) számok közül az első algebrai egész, de a második nem az, hiszen a minimálpolinomjuk \( x^3 - 2 \), illetve \( x^3 - (1/2) \).

P3 A 7.4 pontban szerepelt Gauss-egészek szintén algebrai egészek. Sőt, az is igaz, hogy ha tekintjük a Gauss-racionálsokat, vagyis az összes olyan \( a + b \) komplex számot, ahol \( a \) és \( b \) racionális, akkor ezenkívül éppen a Gauss-egészek lesznek az algebrai egészek. Hasonló állítás érvényes a 7.7 pontban bevezett Euler-egészekre (és a hozzájuk kapcsolódó Euler-racionálsokra) is. A 10. és 11. fejezetben részletesen foglalkozunk majd hasonló típusú algebrai egészek számlémi fogalmával.

Az alábbi tétel lehetőséget ad arra, hogy egy algebrai számról a minimálpolinomja meghatározása nélkül is igazoljuk, hogy algebrai egész (de a tétel gyakorlatilag nem alkalmas annak bizonyítására, hogy a szám nem algebrai egész):

9.6.2 Tétel . T 9.6.2

Egy \( \alpha \) komplex szám akkor és csak akkor algebrai egész, ha létezik olyan \( f \) normált, egész együthathós polinom, amelyre \( f(\alpha) = 0 \).

Bizonyítás: Ha \( \alpha \) algebrai egész, akkor az \( m_{\alpha} \) (normált) minimálpolinom megfelel \( f \)-nek.

A megfordításban tegyük fel, hogy létezik olyan \( f \) normált, egész együthathós polinom, amelyre \( f(\alpha) = 0 \). Ekkor a T 9.2.3 Tétel szerint \( m_{\alpha} | f \), azaz van olyan \( g \) racionális együthathós polinom, amelyre \( f = q m_{\alpha} \). Ilyen \( f \) és \( m_{\alpha} \) főegyütthatója 1, így \( g \) főegyütthatója is 1. Továbbá \( f \) egész együthathós, ezért a racionális együthathós polinomokra érvényes Gauss-tétel szerint létezik olyan \( c \) racionális szám, amelyre \( c g \) és \( \frac{1}{c} m_{\alpha} \) polinomok mindketten egész együthathósak. Ekkor \( c g \), illetve \( \frac{1}{c} m_{\alpha} \) főegyütthatója \( c \), illetve \( \frac{1}{c} \), amelyek egyszerre csak akkor lehetnek egészek, ha \( c = \pm 1 \). Ez viszont azt jelenti, hogy már maga \( m_{\alpha} \) (és \( g \) is) (normált és) egész együthathós polinom, tehát \( \alpha \) valóban algebrai egész. ♦

Megjegyzések:
1. A T 9.6.2 Tétel segítségével például a komplex egységgyökök körétől a körösszáti polinomokra történő hivatkozás nélkül is megállapíthatjuk, hogy algebrai egészek, hiszen egy \( n \) -edik egységgyűk gyöke az \( x^n - 1 \) normált, egész együthathós polinomnak.

2. Mint említettük, a T 9.6.2 Tétel alapján nem lehet kimutatni, hogy egy adott szám nem algebrai egész. Ugyanis abból, hogy \( \alpha \) gyöke egy (vagy akár végletlen sok) olyan normált, racionális
együttthatós polinomnak, amely nem egész együtthatós, semmilyen következtetést nem tudunk levonni arra vonatkozólag, hogy $\alpha$ algebrai egész-e vagy sem. Például az 1 algebrai egész, ugyanakkor gyöke az $f_n = (x - 1)(x - 1/2)^n$ polinomoknak ($n = 1, 2, \ldots$), és mindegyik $f_n$ normált, racionális együtthatós, de nem egész együtthatós. Azt, hogy egy adott $\alpha$ nem algebrai egész, a minimálpolinomja segítségével igazolhatjuk.

Most az algebrai egészek és a műveletek kapcsolatát vizsgáljuk. A következő tételekben a T 9.3.1, T 9.3.4 és T 9.3.6 Tételek algebrai egészekre vonatkozó megfelelőit foglaljuk össze.

**9.6.3 Tétel.**

(i) Az algebrai egészek részgyűrűt alkotnak a komplex számtestben, azaz algebrai egészek összege, különbsége és szorzata is algebrai egész (a hányadosuk azonban általában nem az).

(ii) Egy algebrai egész tetszőleges pozitív racionális kitevőjű hatványa is algebrai egész.

(iii) Ha az $\tilde{f}$ normált polinom együtthatói algebrai egészek, akkor $\tilde{f}$ minden (komplex) gyöke is algebrai egész.

**Bizonyítás:** Mindhárom állítás ugyanúgy adódik, mint ahogy az algebrai számokra vonatkozó megfelelőket (a T 9.3.1, T 9.3.4, illetve T 9.3.6 Tételben) igazoltuk: a gondolatmenetben az „algebrai szám” kifejezést „algebrai egész”-re, a „racionális szám”-ot „egész szám”-ra, a „racionális együtthatós”-t pedig „normált, egész együtthatós”-ra kell cserélni (és természetesen a reciprokra vonatkozó részeket figyelmen kívül kell hagyni, valamint a T 9.3.6 Tétel bizonyítását nézve most a normáltság miatt $\tilde{c} = 1$, tehát a $\tilde{c}$-ra nincs szükség). A fentiek minden lépésre kiterjedő, részletes ellenőrzését az Olvasóra bízzuk.

**Feladatok**

**9.6.1** Mutassuk meg, hogy ha $\alpha$ algebrai egész, akkor $\overline{\alpha}$, $2\text{Re}(\alpha)$, $2\text{Im}(\alpha)$ és $|\alpha|$ is algebrai egész.

**9.6.2** Az alábbi számok közül melyek algebrai egészek?

(a) $\sqrt[5]{5} - (\sqrt[7]{2}/2)$

(b) $(1 + \sqrt{3})/2$

(c) $(1 + i\sqrt{2})/2$

(d) ccs 1°

**9.6.3** Tekintsük az $\alpha = a + bi$ komplex számot (ahol $a$ és $b$ valós szám). Melyek igazak az alábbi állítások közül?

(a) Ha $\alpha$ és $b$ algebrai egész, akkor $\alpha$ is algebrai egész.

(b) Ha $\alpha$ algebrai egész, akkor $\alpha$ is algebrai egész.

(c) Ha $\alpha$ és $|\alpha|$ algebrai egész, akkor $\alpha$ is algebrai egész.

(d) Ha $\alpha$ algebrai egész, akkor $\alpha$ és $b$ is algebrai egész.

(e) Ha $\alpha$ és $a$ algebrai egész, akkor $b$ is algebrai egész.

(f) Ha $\alpha$ algebrai egész, továbbá $a$ és $b$ racionális, akkor $a$ és $b$ egész szám.
(g) Ha $\alpha + 3\beta$ és $5\alpha + 7\gamma$ algebrai egész, akkor $\alpha$ és $\beta$ is algebrai egész.

(h) Ha $\alpha + \beta$ és $\alpha \beta$ algebrai egész, akkor $\alpha$ és $\beta$ is algebrai egész.

9.6.4 Vizsgálguk meg a Fermat-sejtés algebrai egészekre vonatkozó változatát: Rögzített $n \geq 3$ egész kitevő mellett létezik-e megoldása az $x^n + y^n = z^n$ egyenletnek a nemnulla algebrai egészek körében?

9.6.5 (M [606]) Legyen $f$ olyan normált, racionális együtthatós polinom, amelynek nem minden együtthatója egész szám, és tekintsük $\bar{f}$ (komplex) gyökeit. Melyek igazak az alábbi állítások közül?

(a) Az $\bar{f}$-nek létezik olyan gyöke, amely nem algebrai egész.

(b) Az $\bar{f}$ egyetlen gyöke sem algebrai egész.

(c) Ha $\bar{f}$ irreducibilis $\mathbb{Q}$ felett, akkor $\bar{f}$ egyetlen gyöke sem algebrai egész.

(d) Ha az $\bar{f}$ különböző gyökei között pontosan egy olyan van, amely nem algebrai egész, akkor $\bar{f}$-nek létezik racionális gyöke.

9.6.6 Bizonyítsuk be, hogy minden algebrai szám felirható két algebrai egész hányadosaként, sőt az is elérhető, hogy ezek közül az egyik (akár az osztandó, akár az osztó) egész szám legyen.

9.6.7 Hogyan olvasható le az $\alpha$ algebrai egész minimálpolinomjáról, hogy $1/\alpha$ is algebrai egész?

9.6.8 Bizonyítsuk be az alábbi állításokat.

(a) Bármely $\alpha$ algebrai egészhez végteken sok olyan $\beta$ algebrai egész létezik, amelyre $\alpha / \beta$ is algebrai egész.

(b) Bármely olyan $\alpha \neq 0$ algebrai egészhez, amelynek a reciproka nem algebrai egész, végteken sok olyan $\beta$ algebrai egész létezik, amelynek a reciproka nem algebrai egész, és amelyre $\alpha / \beta$ algebrai egész.

(c) Bármely $\alpha \neq 0$ algebrai egészhez csak véges sok olyan $b$ egész szám létezik, amelyre $\alpha / b$ algebrai egész.

9.6.9 Van-e az egységnyi abszolút értékű komplex számok között az egységgyökökön kívül

(a) * algebrai szám;

(b) * algebrai egész?

9.6.10 (*) (a) Mutassuk meg, hogy ha $\eta \geq 2$, akkor az $\eta$-edfokú algebrai egészek mindenütt sűrűn helyezkednek el a valós számegyenesen.

(b) Mindenütt sűrűk-e a komplex számsíkon az $\eta$-edfokú algebrai egészek, ha (b1) $\eta = 2$; (b2) $\eta = 4$?

9.6.11 (a) Legyen $\tau$ tetszőleges valós szám. Igazoljuk, hogy $\tau$ és $\cos \tau \gamma$ közül legalább az egyik irracionalis, kivéve ha $\tau$ olyan egész szám, amely osztható 60-nal vagy 90-cel.

(b) Fogalmazzuk meg és bizonyítsuk be a szinuszos és tangensre vonatkozó hasonló állítást.
10. fejezet - ALGEBRAI SZÁMTESTEK

Algebrai számtesteknek a racionális test egyszerű algebrai bővítéseit nevezzük. Ebben a fejezetben az ilyen testbővítésekkel és az ezekben található algebrai egységek aritmetikai tulajdonságáival foglalkozunk. Részletesen tárgyaljuk a másodfokú bővítések algebrai egészeit. Ezek speciális eseteként a 7. fejezetben már találkoztunk a Gauss-, illetve Euler-egészekkel, amelyeket sikerrel alkalmaztunk az \( y^2 = -1 \), illetve \( x^2 + y^3 = z^3 \) diofantikus egyenletek megoldásánál. Az algebrai számtestek vizsgálatát az ideálelmélet eszközeinek bevonásával a következő fejezetben is folytatjuk.

Megjegyezzük, hogy a testbővítésekől szóló általános bevezető tetszőleges (kommutatív) test esetén érvényes, bár a továbbiakban ezt mindig csak a komplex test résztestére fogjuk alkalmazni. Előrebszújítjuk még, hogy ebben a fejezetben számos helyen felhasználunk néhány alapvető, elsősorban a vektorterek dimenziójához kapcsolódó lineáris algebrai fogalmat és tételeit.

10.1 Testbővítés

Testen mindig kommutatív testet fogunk érteni.

10.1.1 Definíció .  D 10.1.1

Az \( \bar{M} \) testet az \( L \) test bővítésének nevezzük, ha \( L \) részteste \( M \) -nek, azaz \( L \subseteq \bar{M} \) és az \( L \)-testben a műveletek éppen az \( M \)-beli műveletek megszorításai.

Ennek a kapcsolatnak a szokásos jelölése \( \bar{M}|L \) vagy \( M/L \), de mivel ez könnyen félreérthető, ezért inkább az \( M : L \) jelölést fogjuk alkalmazni.

Ha \( \bar{M} \) bővítése \( L \)-nek, akkor \( \bar{M} \) egyben vektortér is \( L \) felett a „természetesen” adódó műveletekre. Ezek a vektorterműveletek az \( \bar{M} \) test műveleteiből származnak: két \( M \)-beli „vektor” mint az \( M \) két elemét adjuk össze, továbbá egy \( L \)-beli „skalárral” úgy szorzunk meg egy \( M \)-beli „vektort”, hogy az \( M \) testnek ezt a két elemét összeszorozzuk.

Az \( \bar{M} \)-nek mint az \( L \) test feletti vektortérnek a dimenziójára külön elnevezést és jelölést vezetünk be:

10.1.2 Definíció .  D 10.1.2

Ha \( \bar{M} \) bővítése \( L \)-nek, akkor \( \bar{M} \)-nek mint \( L \)-feletti vektortérnek a dimenzióját a testbővítés fokának nevezzük és \( \deg(\bar{M} : L) \)-lel jelöljük. Ha ez a dimenzió véges, akkor véges (vagy véges fokú) bővítésről beszélünk.

Példák: \( \deg(\mathbb{C} : \mathbb{R}) = 2, \deg(\mathbb{R} : \mathbb{Q}) = \infty \).

Alapvetően fontos tétele, hogy az egymás utáni testbővítések esetén a fokszámok összeszorozódnak:

10.1.3 Tétel (Testbővítések fokszámértéke) .  T 10.1.3

Ha az \( L \subseteq M \subseteq N \) bővítésláncban \( \deg(N : M) < \infty \) és \( \deg(M : L) < \infty \), akkor

\[ \deg(N : L) = \deg(N : M) \cdot \deg(M : L). \]  (1)

Megjegyezzük, hogy a tétel végtelen dimenzióra is kiterjeszthető: Ha \( \deg(N : M) \) és \( \deg(M : L) \) közül legalább az egyik végtelen, akkor \( \deg(N : L) \) is végtelen, sőt (1) abban a finomabb értelemben is érvényes marad, ha a fokszámot a Hamel-bázis számosságaként tekintjük. \textit{Bizonyítás:} Jelöljük \( L \) elemeit görög betűkkel, \( M \) elemeit latin kisbetűkkel, \( N \) elemeit pedig latin nagybetűkkel.
Legyen az \( M : L \) vektortér egy bázisa \( b_1, \ldots, b_n \), az \( N : M \) vektortéré pedig \( C_1, \ldots, C_k \). Megmutatjuk, hogy ekkor a
\[
 b_i C_j, \quad i = 1, 2, \ldots, n, \quad j = 1, 2, \ldots, k \tag{2}
\]
elemek bázist alkotnak az \( N : L \) vektortérben, amiből a tétele állítása már következik.

Először azt igazoljuk, hogy a (2)-beli elemek lineárisan függetlenek \( N : L \)-ben. Tegyük fel, hogy a \( \lambda_{ij} \in L \), „skalárokra”
\[
 \sum_{i=1}^{n} \sum_{j=1}^{k} \lambda_{ij} (b_i C_j) = 0. \tag{3}
\]
A (3) bal oldalát a(\(N\)) testbeli azonosságok felhasználásával átalakítva azt kapjuk, hogy
\[
 \sum_{j=1}^{k} \left( \sum_{i=1}^{n} \lambda_{ij} b_i \right) C_j = 0. \tag{4}
\]
Mivel \( C_1, \ldots, C_k \) lineárisan független \( N : M \)-ben, ezért (4)-ből következik, hogy
\[
 \sum_{i=1}^{n} \lambda_{ij} b_i = 0, \quad j = 1, \ldots, k. \tag{5}
\]
Felhasználva, hogy \( b_1, \ldots, b_n \) lineárisan független \( M : L \)-ben, (5) alapján adódik, hogy mindegyik \( \lambda_{ij} = 0 \). Ezzel a \( b_i C_j \) elemek \( N : L \)-beli lineáris függetlenségét beláttuk.

Most megmutatjuk, hogy a \( b_i C_j \) elemek generátorrendszer alkotnak \( N : L \)-ben. Mivel \( C_1, \ldots, C_k \) generátorrendszer \( N : M \)-ben, ezért bármely \( U \in N \) felírható
\[
 U = v_1 C_1 + \cdots + v_k C_k \tag{6}
\]
alakban, ahol \( v_j \in M \). Most felhasználjuk, hogy \( b_1, \ldots, b_n \) generátorrendszer \( M : L \)-ben, és így minden \( v_j \) elôáll a \( b_i \)-k lineáris kombinációjaként:
\[
 v_j = \alpha_{1j} b_1 + \cdots + \alpha_{nj} b_n, \quad \alpha_{ij} \in L, \quad 1 \leq i \leq n, \quad 1 \leq j \leq k. \tag{7}
\]
A (7)-beli elôállításokat (6)-ba beírva kapjuk, hogy
\[
 U = \sum_{i=1}^{n} \sum_{j=1}^{k} \alpha_{ij} b_i C_j.
\]
Ezzel beláttuk, hogy a \( b_i C_j \) elemek generátorrendszt alkotnak \( N : L \)-ben.

Most az algebrai szám fogalmát általánosítjuk:

10.1.4 Definíció . D 10.1.4

Legyen \( T \) részteste \( M \)-nek. A \( \hat{f} \in M \) elem algebrai az \( T \) test felett, ha létezik olyan nemnulla \( f \in L[x] \) polinom, amelynek a \( \hat{f} \) gyöke, azaz \( f(\hat{f}) = 0 \).

\[ \text{Példák:} \]
Az algebrai szám fogalmát az \( L = \mathbb{Q}, M = \mathbb{C} \) speciális esetben kapjuk.

A valós, illetve a komplex test felett minden komplex szám algebrai (lásd a 9.1.7 feladatot [295]).

Az algebrai elem minimálpolinomját és fokát értélemszerűen, a D 9.2.1 és D 9.2.4 Definíciók mintájára definiáljuk:

10.1.5 Definíció . \( D 10.1.5 \)

Legyen \( L \) részteste \( M \)-nek. Az \( L \) felett algebrai \( \alpha \in M \) elem minimálpolinomjának a(z egyik) legalacsonyabb fokú \( L[x] \)-beli polinomot nevezzük, amelynek a \( \alpha \) gyöke. A \( \alpha \) foka (vagy fokszáma) a minimálpolinomjának a foka. ♦

Ne felejtsük el, hogy a \( \alpha \) minimálpolinomja és így a foka is nemcsak magától a \( \alpha \)-tól függ, hanem attól is, hogy melyik \( L \) test felett tekintettük a \( \alpha \)-t: például \( \sqrt{2} \) -nek a \( \mathbb{Q} \) feletti minimálpolinomja \( x^2 - 2 \), az \( \mathbb{R} \) feletti minimálpolinomja viszont \( x - \sqrt{2} \). (Megmutatható, hogy \( M \) változtatása nem befolyásolja \( \alpha \) minimálpolinomját.)

Ennek megfelelően a minimálpolinom és a fokszám \( m_\alpha L \), illetve \( \deg_L \alpha \) jelölésében az \( L \) testet is feltüntetjük (az algebrai számoknak megfelelő \( L = \mathbb{Q} \) esetben továbbra is a sima \( m_\alpha \), illetve \( \deg \alpha \) jelölést használjuk).

Az algebrai elem minimálpolinomjára is érvényesek a T 9.2.2 és T 9.2.3 Tételeknek megfelelő állítások:

10.1.6 Tétel . \( T 10.1.6 \)

Legyen \( L \) részteste \( M \)-nek, és \( \alpha \in M \) algebrai elem \( L \) felett. Ekkor

(i) az \( m_\alpha L \) minimálpolinom egy \( L \) -beli konstans szorzótól eltekintve egyértelmű;

(ii) egy \( f \in L[x] \) polinomra \( f(\alpha) = 0 \iff m_\alpha L \mid f \); 

(iii) egy \( g \in L[x] \) polinom pontosan akkor minimálpolinomja \( \alpha \)-nak, ha \( g(\alpha) = 0 \) és \( g \) irreducibilis \( L \) felett. ♦

A bizonyítás pontosan a T 9.2.2 és T 9.2.3 Tételeknél láttot módon történik.

A bővítések szerkezetére vonatkozóan fontos információt tartalmaz az alábbi egyszerű észrevétel:

10.1.7 Tétel . \( T 10.1.7 \)

Ha \( \deg(M : L) < \infty \), akkor \( M \) minden eleme algebrai \( L \) felett. ♦

Bizonyítás: Legyen \( \deg(M : L) = n \), és jelöljük \( 1 \)-gyel a(z \( L \) és \( M \)) test (közös) egységelemét. Ekkor tetszőleges \( \mu \in M \) esetén az \( 1, \mu, \mu^2, \ldots, \mu^n \) elemek száma nagyobb, mint az \( M : L \) vektortér dimenziója, ezért ezek az elemek lineárisan összefüggők. Ez azt jelenti, hogy léteznek olyan \( \alpha_0, \ldots, \alpha_n \in L \) „skalárok”, amelyek közül nem mindegyik 0, és

\[
\alpha_0 + \alpha_1 \mu + \cdots + \alpha_n \mu^n = 0.
\]

Így \( \mu \) gyöke az \( f = \alpha_0 + \alpha_1 \mu + \cdots + \alpha_n \mu^n \neq 0 \) polinommnak, vagyis \( \mu \) algebrai elem \( L \) felett. ♦

Megjegyzések: 1. A bizonyításból az is leolvasható, hogy \( \deg_L \mu \leq \deg(M : L) \). A T 10.2.5 Tételben a még erősebb \( \deg_L \mu \mid \deg(M : L) \) állítást fogjuk igazolni.
2. A T 10.1.7 Tétel megfordítása nem igaz. Legyen például $L$ a racionális test, $M$ pedig az összes ($Q$ feletti) algebrai számok teste. Ekkor $M$ minden eleme (definíció szerint) algebrai $L$ felett, azonban $\deg(M : L) = \infty$, ugyanis $\deg(M : L) = n < \infty$ esetén az előző megjegyzés szerint minden algebrai szám foka legfeljebb $n$ lehetne, ami ellentmond annak, hogy létezik akármilyen magas fokszámú algebrai szám (9.2 pont, P4 példa).

Feladatok

**10.1.1** Legyen $\deg(M : L)$ prímszám, és tegyük fel, hogy $T$ az $M$-nek olyan részteste, amely tartalmazza $L$-et. Mutassuk meg, hogy $T = M$ vagy $T = L$.

**10.1.2** Legyen $G = \{a + bi \mid a, b \in Q\}$ a Gauss-racionálisok, $A$ pedig az algebrai számok teste. Számítsuk ki az alábbi testbővítések fokát:

(a) $\deg(G : Q)$;

(b) $\deg(C : A)$;

(c) $\deg(A : G)$.

**10.1.3** Legyen $K = \{a + b\sqrt{2} \mid a, b \in Q\}$. Könnyen adódik, hogy $K$ részteste $R$-nek.

(a) Bizonyítsuk be, hogy egy $\alpha$ komplex szám akkor és csak akkor algebrai $Q$ felett, ha algebrai $K$ felett (azaz algebrai szám).

(b) Határozzuk meg az alábbi komplex számoknak a $K$ feletti fokát:

(b1) $3 + 7\sqrt{2}$;

(b2) $\sqrt{2} + i$;

(b3) $\sqrt[3]{2}$;

(b4) $\sqrt[3]{2}$.

**10.1.4** Tekintsük az $L \subset M \subset N$ bővítésláncot, és legyen $\emptyset \subset N$.

(a) Melyek igazak az alábbi állítások közül?

(a1) Ha $\emptyset$ algebrai $L$ felett, akkor $\emptyset$ algebrai $M$ felett.

(a2) Ha $\emptyset$ algebrai $M$ felett, akkor $\emptyset$ algebrai $L$ felett.

(b) Ha $\emptyset$ algebrai $M$ és $L$ felett, akkor milyen kapcsolat van $\emptyset, M$ és $\emptyset, L$, illetve $\deg(M : \emptyset)$ és $\deg(L : \emptyset)$ között?

**10.2 Egyszerű algebrai bővítés**

A testbővítések legegyszerűbb és egyben legfontosabb típusát az egyetlen elem által generált bővítések jelentik. Ezt a fogalmat az egyszerűség kedvéért csak a $Q(\sqrt{d})$ speciális esetre, azaz a racionális testek a $\sqrt{d}$ komplex számmal történő bővítésére tárgyaljuk, azonban az elmondottak ugyanúgy érvényesek
A $\mathbb{Q}$-nak a $\mathbb{Q}$-tól komplex számmal történő egyszerű bővítésénél a $\mathbb{Q}$-ból és a $\mathbb{Q}$-tól komplex testbeli műveletek (és inverzeik) segítségével előálló elemek halmazát fogjuk érteni. Ehhez tekintjük az összes $a_0 + a_1 b + \cdots + a_n b^n$ alakú elemet, ahol $n$ tetszőleges nemnegatív egész és az $a_i$ racionális számok, majd vesszük ilyenek hányadosait. Az $a_0 + a_1 b + \cdots + a_n b^n$ elem nem más, mint a $g = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Q}[x]$ polinomok a $\mathbb{Q}$ helyen vett $g(b) \in \mathbb{C}$ helyettesítési értéke. A szóban forgó hányadosok tehát $g(b)/h(b)$ alakú komplex számok, ahol $g$ és $h$ tetszőleges $\mathbb{Q}[x]$ beli polinomok és természetesen $h(b) \neq 0$. Az ily módon kapott elemek a komplex számtestnek a $\mathbb{Q}$-t és $\mathbb{Q}$-t tartalmazó legsúgulóbb résztestét alkotják. Mindezt pontosan az alábbi definícióban és tételeben fogalmazzuk meg.

10.2.1 Definíció. D 10.2.1

Tetszőleges $\mathbb{Q}$ komplex szám esetén a $\mathbb{Q}$ testnek a $\mathbb{Q}$-val történő egyszerű bővítésének nevezzük és $\mathbb{Q}(\mathbb{Q})$-val jelöljük az alábbi alakú komplex számok halmazát:

$$\frac{g(b)}{h(b)}, \quad \text{ahol} \quad g, h \in \mathbb{Q}[x], \quad h(b) \neq 0,$$  \hspace{1cm} (1)

illetve ugyanezt részletesen kiírva:

$$\frac{\sum_{i=0}^{n} a_i b_i}{\sum_{j=0}^{k} b_j}, \quad \text{ahol} \quad a_i, b_j \in \mathbb{Q}, \quad \sum_{j=0}^{k} b_j \neq 0, \quad n, k = 0, 1, 2, \ldots$$  \hspace{1cm} (2)

Ha $\mathbb{Q}$ algebrai szám, akkor egyszerű algebrai bővítésről beszélünk.

10.2.2 Tétel. T 10.2.2

$\mathbb{Q}(\mathbb{Q})$ a komplex testnek az a legsúgulóbb részteste, amely a $\mathbb{Q}$-t és a racionális testet tartalmazza, azaz

(i) $\mathbb{Q}(\mathbb{Q})$ résztest $\mathbb{C}$-ben;

(ii) $\mathbb{Q}(\mathbb{Q}) \subseteq \mathbb{Q}(\mathbb{Q})$;

(iii) ha $\mathbb{T}$ résztest $\mathbb{C}$-nek és $\mathbb{Q} \subseteq \mathbb{T}$, akkor szükségképpen $\mathbb{Q}(\mathbb{Q}) \subseteq \mathbb{T}$.

Bizonyítás: (i) Azt kell megmutatni, hogy két (1)-beli elem összege, különbsége, szorzata és (ha a nevező nem nulla, akkor) hányadosa is (1)-beli. Nyilván

$$\frac{g_1(b)}{h_1(b)} + \frac{g_2(b)}{h_2(b)} = \frac{g_1(b) h_2(b) + g_2(b) h_1(b)}{h_1(b) h_2(b)},$$

ahol $g = g_1 h_2 + g_2 h_1$ és $h = h_1 h_2$ is racionális együtthatós polinomok, és a komplex test nulllosztómentessége miatt $h(b) = h_1(b) h_2(b) \neq 0$. A különbségre, szorzatra és hányadosra vonatkozó állítás hasonlóan igazolható.

(ii) Ha $g = f$ és $h = 1$, akkor $g(b)/h(b) = g(b)$, tehát $g \in \mathbb{Q}(\mathbb{Q})$.

Ha $\tau$ tetszőleges racionális szám, akkor a $g = \tau$ és $h = 1$ (konstans) polinomokat választva $g(\tau)/h(\tau) = \tau$, tehát $\tau \in \mathbb{Q}(\mathbb{Q})$.  

321
(iii) Ha $q$ a komplex számok olyan részteste, amely tartalmazza $\sqrt{d}$-t és $\mathbb{Q}$-t, akkor a $\sqrt{d}$-ból és racionális számokból képzett tetszőleges sorozatok összege és ilyenek hányadosa is szükségképpen $T$-beli. Ez azt jelenti, hogy minden $(2)$-beli kompleks szám is eleme $T$-nek, tehát valóban $\mathbb{Q}(\sqrt{d}) \subseteq T$.

Megmutatjuk, hogy ha $\sqrt{d}$ algebrai szám, akkor $\mathbb{Q}(\sqrt{d})$ elemei egyszerűbb alakban is felírhatók.

Tekintsük először példaként a racionális testnek a $\sqrt{2}$-vel vett $\mathbb{Q}(\sqrt{2})$ bővítését. Ez nem más, mint az $a_0 + a_1 \sqrt{2}$ alakú számok $T$-halmaza, ahol $a_i \in \mathbb{Q}$, ugyanis $T$ egy olyan test, amely a $\sqrt{2}$-t és a racionális számokat tartalmazza és nyilván a legszűkebb. Ez azt jelenti, hogy a D 10.2.1 Definícióban felírt alakhoz képest nincs szükség osztásra és a $\sqrt{2}$-nek az egynél magasabb kitevőjű hatványaira.

Ha a $\sqrt{2}$ helyett a $\sqrt{5}$-tel történő $\mathbb{Q}(\sqrt{5})$ bővítést tekintjük, akkor itt $\sqrt{5}$ legfeljebb második hatványaira van szükség, mert a harmadik és magasabb hatványok kifejezhetőek ezekkel (és alkalmas racionális számokkal).

Az általános esetben a következő tétel érvényes:

**10.2.3 Tétel.**

Ha $\sqrt{d}$ egy $n$-edfokú algebrai szám, akkor $\mathbb{Q}(\sqrt{d})$ elemei egyértelműen felírhatók

$$a_0 + a_1 \sqrt{d} + \cdots + a_{n-1} \sqrt{d}^{n-1}$$

alakban, ahol az $a_i$-k racionális számok. Más szóval, minden $\alpha \in \mathbb{Q}(\sqrt{d})$ elemhez pontosan egy olyan $f \in \mathbb{Q}[x]$ polinom létezik, amelyre

$$\alpha = f(\sqrt{d}) \quad \text{és} \quad \deg f \leq n-1 \text{ vagy } f = 0.$$

**Bizonyítás:** I. Először megmutatjuk, hogy (1)-ben a nevezőre „nincs szükség”, azaz bármely $\frac{g}{h}, \frac{h}{g} \in \mathbb{Q}[x]$ és $\hat{h}(\sqrt{d}) \neq 0$ esetén $g(\sqrt{d})h(\sqrt{d})$ előáll alkalmazott polinom $t \in \mathbb{Q}[x]$ polinommal $t(\sqrt{d})$ alakban is.

Ennek igazolásához tekintsük az alábbi ekvivalenciákat (ahol közeből a $\hat{h}(\sqrt{d}) \neq 0$ feltételt és a T 9.2.3(i) Tételt is felhasználjuk):

$$g(\sqrt{d})h(\sqrt{d}) = t(\sqrt{d}) \iff g(\sqrt{d}) = \hat{h}(\sqrt{d})t(\sqrt{d}) \iff (g-h\hat{t})(\sqrt{d}) = 0 \iff m_\phi \mid g-h\hat{t} \iff g = \hat{t} + m_\phi s \iff s \in \mathbb{Q}[x].$$

Így azt kell belátni, hogy létezik olyan $t$ és $s$ racionális egyúthathós polinomok, amelyekre

$$g = \hat{t} + m_\phi s. \quad \text{(3)}$$

A (3) egyenlőség „olyan”, mint egy lineáris diofantikus egyenlet, amelyben $t$ és $s$ az ismeretlenek, csak itt egész számok helyett racionális együtthatós polinomok szerepelnek. A lineáris diofantikus egyenletek megoldhatóságának szükséges és elégséges feltételt az T 1.3.6 Tételben tárgyaljuk, és a bizonyításnál csak a maradékos osztásból adódó euklideszi algoritmus egyik következményét használtuk fel. Mivel a maradékos osztás a test feletti polinomok körében is elvégzhető, ezért a „polinomos” diofantikus egyenlet megoldhatóságának is ugyanaz a feltétele. Így a (3) egyenlet megoldhatóságához azt kell igazolni, hogy $\langle \hat{t}, m_\phi \rangle \mid g$.

Az $m_\phi$ polinom irreducibilis $\mathbb{Q}$ felett, ezért $\langle \hat{t}, m_\phi \rangle = 1$ vagy $m_\phi$. Az utóbbi esetből azonban $\hat{t}(\sqrt{d}) = 0$ következne, így csak $\langle \hat{t}, m_\phi \rangle = 1$ lehetséges, tehát valóban $\langle \hat{t}, m_\phi \rangle \mid g$. Ez, mint láttuk, azt jelenti, hogy a (3) egyenlet megoldható, és az így kapott $\hat{t}$ polinomra $t(\sqrt{d}) = g(\sqrt{d})/\hat{t}(\sqrt{d})$.  

322
II. Eddig azt igazoltuk, hogy minden \( \alpha \in \mathbb{Q}(\theta) \) alakú \( i \in \mathbb{Q}[x] \) polinommal \( \alpha = t(\theta) \) alakba írható. Most megmutatjuk, hogy olyan \( f \in \mathbb{Q}[x] \) polinom is létezik, amelyre \( \deg f \leq n-1 \) vagy \( f = 0 \), és \( \alpha = f(\theta) \).

Osszuk el a \( f \) polinomot maradékosan \( m \theta \)-val, ekkor a maradék megfelel \( \bar{f} \)-nek. Valóban, ha

\[ \tau = q m \theta + \bar{f}, \quad \text{ahol} \quad \deg \bar{f} \leq n-1 \quad \text{vagy} \quad \bar{f} = 0, \]

akkor

\[ \alpha = \tau(\theta) = q(\theta)m(\theta) + f(\theta) = f(\theta) - \bar{f}(\theta). \]

III. Hátravan még \( \bar{f} \) egyértelműségének az igazolása. Tegyük fel, hogy az \( \bar{f}_1 \) és \( \bar{f}_2 \) racionális együtthatós polinomokra

\[ \bar{f}_1(\theta) = \bar{f}_2(\theta) \quad \text{és} \quad \deg \bar{f}_i \leq n-1 \quad \text{vagy} \quad \bar{f}_i = 0, \quad i = 1, 2. \]

Ekkor az \( \bar{f}_3 = \bar{f}_1 - \bar{f}_2 \) polinom racionális együtthatós, \( \bar{f}_3(\theta) = 0 \) és \( \deg \bar{f}_3 < n \) vagy \( \bar{f}_3 = 0 \). Mivel \( \deg \bar{f} = n \), ezért csak \( \bar{f}_3 = 0 \) lehetséges. Ez azt jelenti, hogy \( \bar{f}_1 = \bar{f}_2 \), tehát a tételben szereplő \( \bar{f} \) polinom egyértelmű.

A T 10.2.3 Tétel más megfogalmazásában azt jelenti, hogy az \( 1, \theta, \ldots, \theta^{n-1} \) elemek bázist alkotnak \( \mathbb{Q}(\theta) \)-ban mint \( \mathbb{Q} \)-feletti vektortérben. Így ennek a vektortérnek a dimenziója, azaz az \( \mathbb{Q}(\theta) : \mathbb{Q} \) testbővítés foka megegyezik a \( \theta \) algebrai szám fokával. Ezt a fontos tényt külön tételként is kimondjuk:

**10.2.4 Tétel.**

Ha \( \theta \) algebrai szám, akkor \( \deg(\mathbb{Q}(\theta) : \mathbb{Q}) = \deg \theta \).

A T 10.2.3–T 10.2.4 Tételeket kiegészíthetjük azzal, hogy ha \( \theta \) transzcendens szám, akkor \( \mathbb{Q}(\theta) \) elemei nem adhatók meg a D 10.2.1 Definícióban leírt elemek bázisait alkotnak \( \mathbb{Q}(\theta) \)-ban mint \( \mathbb{Q} \)-feletti vektortér.

Megjegyezzük még, hogy ha \( \theta \) algebrai szám, akkor a T 10.2.3 Tétel alapján \( \mathbb{Q}(\theta) \) elemeit az \( m \theta \) polinom szerinti osztási maradékként képzelhetjük el: ilyenkor a \( \mathbb{Q}(\theta) \) test a \( \mathbb{Q}[x]/(m \theta) \) faktorgyűrűvel izomorf (lásd a T 11.1.6 Tételt és a 11.1.9a feladatot [355]). Az egyszerű algebrai bővítéseknek ez a megközelítési módja a \( \mathbb{Q} \)-helyett tetszőleges \( \mathbb{F} \)-testen, és ugyanilyen értelmezésű a \( \mathbb{Q}(\theta) \)-t. A T 11.1.9b feladatot [355].

Végül megemlíthetjük, hogy ha \( \mathbb{Q} \) bármely véges bővítése előáll alakul \( \theta \) algebrai számmal \( \mathbb{Q}(\theta) \) alakban, azaz \( \mathbb{Q} \) véges bővítési megegyeznek az \( \mathbb{Q} \) egyszerű algebrai bővítéseivel. (Ugyanez fennáll \( \mathbb{Q} \)-helyett bármely olyan testen is, amelyben egy \( \alpha + \alpha + \cdots + \alpha \) összeg csak úgy lehet 0, ha \( \alpha = 0 \).)

A T 10.1.7 Tétel élesítéseként most megmutatjuk, hogy egy véges bővités tetszőleges elemének a foka osztója a bővítés fokának. Az állítást most is csak a \( \mathbb{Q} \) bővítéseire fogalmazzuk meg, de ugyanúgy érvényes tetszőleges (kommutatív) testekre is.
10.2.5 Tétel. \( \text{T 10.2.5} \)

Ha \( M \) részteste \( \mathbb{C} \)-nek és \( \deg(M : \mathbb{Q}) = k < \infty \), akkor bármely \( \alpha \in M \) elemre \( \deg\alpha | k \).

Bizonyítás: A \( \mathbb{Q}(\alpha) \) test a \( T 10.2.2 \) Tétel szerint része \( M \)-nek, azaz

\[
\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq M. \tag{4}
\]

A \( \deg(M : \mathbb{Q}) = k < \infty \) feltételből következik, hogy a (4) bővítéslánc mindkét „láncszeme” is véges bővítés, és így alkalmazhatjuk a fokszámtételt (\( T 10.1.3 \) Tétel). Ebből azt kapjuk, hogy \( \deg(\mathbb{Q}(\alpha) : \mathbb{Q}) | k \). A \( T 10.1.7 \) Tétel alapján \( \alpha \) algebrai szám, ezért a \( T 10.2.4 \) Tétel miatt \( \deg(\mathbb{Q}(\alpha) : \mathbb{Q}) = \deg \alpha \). Vagyis valóban \( \deg \alpha | k \).

Most új bizonyítást adjunk a \( T 9.3.1 \) és \( T 9.3.6 \) Tételekre. A könnyebb áttekinthetőség kedvéért ezeket a tételeket (új sorszámmal) újra ki is mondjuk.

10.2.6 Tétel. \( \text{T 10.2.6} \)

Az algebrai számok résztestet alkotnak a komplex számtestben.

Bizonyítás: Legyen \( \alpha \) és \( \beta \) két algebrai szám. Azt kell megmutatni, hogy \( \alpha + \beta \), \( \alpha - \beta \), \( \alpha \beta \) és (ha \( \beta \neq 0 \), akkor) \( \alpha / \beta \) is algebrai.

Bővítsük \( \mathbb{Q} \)-t \( \alpha \)-val, majd az így kapott \( K = \mathbb{Q}(\alpha) \) testet \( \beta \)-val. Az ekkor keletkező \( N = K(\beta) \) test tartalmazza \( \alpha \)-t és \( \beta \)-t is, ezért a két szám összege, különbsége, szorzata és hányadosa is \( N \)-beli.

Tekintsük a \( \mathbb{Q} \subseteq K \subseteq N \) bővítésláncot [ahol \( K = \mathbb{Q}(\alpha) \) és \( N = K(\beta) \)]. Itt

\[
\deg(K : \mathbb{Q}) = \deg \alpha \quad \text{és} \quad \deg(N : K) = \deg \beta,
\]

ezért a fokszámtétel szerint \( \deg(N : K) < \infty \). Ebből a \( T 10.1.7 \) Tétel alapján következik, hogy \( N \) minden eleme, így speciálisan \( \alpha + \beta \), \( \alpha - \beta \), \( \alpha \beta \) és \( \alpha / \beta \) is algebrai szám.

10.2.7 Tétel. \( \text{T 10.2.7} \)

Ha az \( f \neq 0 \) polinom együthatósai algebrai számok, akkor \( f \) minden (komplex) gyöke algebrai szám.

Bizonyítás: Legyen \( f = a_0 + a_1 \gamma + \cdots + a_n \gamma^n \) és \( \gamma \) az \( f \) tetszőleges komplex gyöke.

Definíáljuk a \( K_i \) testeket a következőképpen:

\[
K_0 = \mathbb{Q}(\alpha_0), \quad K_j = K_{j-1}(\alpha_j), \quad j = 1, 2, \ldots, n, \quad K_{n+1} = K_n(\gamma),
\]

és tekintsük a

\[
\mathbb{Q} \subseteq K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq K_{n+1}
\]

bővítésláncot. Itt minden lépésben az adott testet egy felette algebrai elemmel bővítjük, ezért minden „láncszem” véges bővítés. Ekkor a fokszámtétel miatt \( K_{n+1} : \mathbb{Q} \) is véges bővítés, tehát \( K_{n+1} \) minden eleme, köztük \( \gamma \) is algebrai \( \mathbb{Q} \) felett.
Feladatok

10.2.1 Bizonyítsuk be, hogy bármely \( \theta \) komplex és \( \theta \neq 0 \) racionális számra az alábbi bővítések megegyeznek \( \mathbb{Q}(\sqrt{\alpha}) \)-val:

(a) \( \mathbb{Q}(\sqrt{\theta}) \);
(b) \( \mathbb{Q}(\theta) \);
(c) \( \mathbb{Q}(\sqrt{1/\theta}) \) (ha \( \theta \neq 0 \)).

10.2.2 Legyen \( \alpha \in \mathbb{Q}(\sqrt{\theta}) \). Bizonyítsuk be az alábbi állításokat.

(a) \( \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{\theta}) \).
(b) Algebrai \( \sqrt{\theta} \) esetén \( \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{\theta}) \) \( \iff \) \( \deg \alpha = \deg \sqrt{\theta} \).
(c) Transzcendens \( \sqrt{\theta} \) esetén \( \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{\theta}) \) akkor és csak akkor teljesül, ha \( \alpha = \frac{a_0 + a_1 \sqrt{\theta}}{b_0 + b_1 \sqrt{\theta}} \), ahol \( a_0, b_0, a_1, b_1 \in \mathbb{Q} \) és \( \alpha \notin \mathbb{Q} \).

10.2.3 Melyek igazak az alábbi állítások közül?

(a) \( \mathbb{Q}(\sqrt{\theta}) = \mathbb{Q}(\sqrt{\bar{\theta}}) \).
(b) Ha \( |\theta|^2 \) racionális, akkor \( \mathbb{Q}(\sqrt{\theta}) = \mathbb{Q}(\sqrt{\bar{\theta}}) \).
(c) Ha \( \mathbb{Q}(\sqrt{\theta}) = \mathbb{Q}(\sqrt{\bar{\theta}}) \), akkor \( |\theta|^2 \) racionális.
(d) Ha \( \mathbb{Q}(\sqrt{\theta}) \subseteq \mathbb{Q}(\sqrt{\bar{\theta}}) \), akkor \( \mathbb{Q}(\sqrt{\theta}) = \mathbb{Q}(\sqrt{\bar{\theta}}) \).
(e) \( \mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{\theta} + \bar{\theta}^2) \).

10.2.4 írjuk fel az alábbi számokat \( a_0 + a_1 \sqrt{2} + a_2 \sqrt{3} \) alakban, ahol \( a_0, a_1, a_2 \) racionális számok:

(a) \( \sqrt{2} + 3 \sqrt{3} \);
(b) \( \frac{1}{\sqrt{2}} \);
(c) \( 1 - \frac{3\sqrt{2}}{5} \).

10.2.5 Számítsuk ki az alábbi algebrai számok fokát:

(a) \( (\sqrt{7} + 3i) \);
(b) \( \sqrt[3]{5} \);
(c) \( \sqrt[3]{5} + \sqrt[3]{7} \);
(d) \( \sqrt{5} + \sqrt{7} \).
10.2.6 Adjuk meg egyszerűbb alakban az alábbi halmazokat:

(a) \( \mathbb{Q}(\sqrt[5]{4}) \setminus \mathbb{Q}(\sqrt[5]{16}) \); (b) \( \mathbb{Q}(\sqrt[5]{7}) \cap \mathbb{Q}(\sqrt[5]{7}) \); (c) \( \mathbb{Q}(\sqrt[5]{5}) \cap \mathbb{Q}(\sqrt[5]{5}) \).

10.2.7 (M [607]) Adjuk meg \( \mathbb{Q}(\theta) \) valós elemeit, ha \( \theta \) értéke

(a) \( \sqrt[5]{5} \cos 144^\circ + i \sin 144^\circ \); (b) \( i \sqrt[3]{3} \); (c) \( \sqrt[5]{i} \) valamelyik értéke.

10.2.8 (M [609]*) Bizonyítsuk be, hogy ha \( |\theta| = 1 \), akkor \( \mathbb{Q}(\theta) \cap \mathbb{R} = \mathbb{Q}(\Re \theta) \).

10.2.9 Legyen \( \alpha = 1 + 3 \sqrt[5]{25} + 11 \sqrt[12]{125} + 990 \sqrt[625]{625} \). Bizonyítsuk be, hogy létezik olyan f racionális együtthatós polinom, amelyre \( f(\alpha) = \sqrt[5]{5} \).

10.2.10 Legyen a \( \beta \) algebrai szám foka \( k \). Melyek \( \deg (\beta^p) \) lehetséges értékei?

10.2.11 (M [610]*) Határozzuk meg az egységkörön az összes páratlan fokú algebrai számot.

10.2.12 (a) Bizonyítsuk be, hogy ha \( \alpha \) és \( \beta \) algebrai számok, akkor az \( \alpha + \beta \), \( \alpha - \beta \), \( \alpha \beta \) és (\( \beta \neq 0 \) esetén) \( \alpha/\beta \) számok foka kisebb vagy egyenlő, mint (\( \deg (\alpha) \cdot \deg (\beta) \).

(b) Ha az \( f = a_0 + a_1 x + \cdots + a_k x^k \) polinom együtthatói algebrai számok és \( f(\gamma) = 0 \), akkor \( \deg \gamma \leq n \prod_{j=0}^{n} \deg a_j \).

10.2.13 Legyenek \( a_1, a_2, l_1 \neq 0, l_2 \neq 0 \) racionális együtthatós polinomok és \( \theta \) transzcendens szám. Bizonyítsuk be az alábbi állításokat.

(a) \( \frac{a_1(\theta)}{a_2(\theta)} \leftrightarrow g_1 h_2 = g_2 h_1 \).

(b) A \( \mathbb{Q}(\theta) \) test izomorf a \( \mathbb{Q} \) feletti algebrai törtek, azaz a racionális együtthatós polinomok formálisan képzett hányadosainak testével.

10.3 Másodfokú bővítések

Ebben a pontban a \( \mathbb{Q} \)-nak a (komplex számtesten belüli) másodfokú bővítéseit és azok algebrai egészeit vizsgáljuk.

10.3.1 Tétel . \( \mathbf{T} \) 10.3.1

A \( \mathbb{Q} \) összes másodfokú bővítése \( \mathbb{Q}(\sqrt{t}) \) alakú, ahol \( t \) (pozitív vagy negatív) négyzetmentes egész szám és \( t \neq 1 \). Különböző ilyen \( t \) értékekhez különböző bővítések tartoznak. ❖

Megjegyzés: A \( t > 0 \) esetben valós, a \( t < 0 \) esetben pedig képzetes (vagy imaginárius) másodfokú bővítésről beszélünk. A képzetes esetben \( \sqrt{t} \) két (komplex) értéke közül bármelyiket vehetjük, mert ezek egymás ellentettei és \( \sqrt{t} = \sqrt{-t} \) bármely \( \theta \) -ra teljesül; a továbbiakban ilyenkor jelentse \( \sqrt{t} \) mindig a négyzetgyökök felső félsíkbeli értékét: \( \sqrt{t} = \sqrt{\sqrt{t}} \).
Bizonyítás: Legyen $M$ a $\mathbb{C}$ olyan részteste, amelyre $\deg(M : \mathbb{Q}) = 2$. Ekkor nyilván az $M$ tetszőleges $\alpha$ nem racionális elemére $\deg \alpha = 2$ és $M = \mathbb{Q}(\alpha)$. Belátjuk, hogy $\mathbb{Q}(\alpha)$ megadható alkalmas négyzetmentes $t \neq 1$-gyel $\mathbb{Q}(\sqrt{t})$ alakban is.

Ha az $\alpha$ minimálpolinomja $m_\alpha = a_0 + a_1 x + a_2 x^2$, ahol $a_0, a_1, a_2$ egész számok, akkor a másodfokú egyenlet megoldóképletéből kapjuk, hogy $\alpha = \tau_0 + \tau_1 \sqrt{s}$ alakú, ahol $\tau_1 \neq 0$ és $\tau_0$ racionális számok és $s \neq 0$ egész szám. Az $s$ -ből a lehető legnagyobb négyzetszámot kiemelve $s = k^2 t$ adódik, ahol $t$ négyzetmentes és $t \neq 1$. Így $\alpha = \tau_0 + \tau_1 k \sqrt{t}$. Innen a 10.2.1 feladat [325] alapján következik, hogy $M = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{t})$.

Meg kell még mutatnunk, hogy az így kapott $t$ egyértelmű, azaz ha $\mathbb{Q}(\sqrt{t_1}) = \mathbb{Q}(\sqrt{t_2})$, ahol $t_i$ négyzetmentes és $t_i \neq 1$, akkor $t_1 = t_2$.

A feltételekből következik, hogy

$$\sqrt{t_2} \in \mathbb{Q}(\sqrt{t_1}),$$

azaz

$$\sqrt{t_2} = a + b \sqrt{t_1},$$

ahol $a$ és $b$ racionális. Négyzetre emeléssel

$$t_2 = a^2 + 2ab \sqrt{t_1} + b^2 \sqrt{t_1}$$

adódik. Ez $\sqrt{t_1}$ irracionálitása miatt csak úgy lehetséges, ha $a = 0$ vagy $b = 0$. Az első eset azt jelenti, hogy $\sqrt{t_2}$ racionális, ami ellentmondás. A második esetben azt kapjuk, hogy $\sqrt{t_2}/\sqrt{t_1}$ racionális, amiből $t$ négyzetmentessége miatt $t_1 = t_2$ következik.

**Példák:**

**P1** A Gauss-racionálisok a $\mathbb{Q}(i)$ bővítés elemei, ekkor $i = -1$.

**P2** Az Euler-racionálisok a $\mathbb{Q}(\omega)$ bővítés elemei, ahol

$$\omega = \cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3} = -\frac{1 + \sqrt{3}}{2}.$$

Ekkor $i = -3$.

Most megvizsgáljuk, hogyan adhatók meg egy másodfokú bővítés algebrai egészei.

Tekintsük először a Gauss-racionálisokat, tehát azokat az $a + bi$ komplex számokat, ahol $a$ és $b$ racionális. A 9.6 pontban már említettük (P3 példa, 9.6.3 [315]a és 9.6.3f feladat [315]), hogy egy Gauss-racionális pontosan akkor algebrai egész, ha Gauss-egész, azaz ha $a$ és $b$ egész szám.

Nézzük meg, mi a helyzet az Euler-racionálisoknál, azaz az

$$\alpha = c + d \omega = c + d \cdot \frac{-1 + i \sqrt{3}}{2} = \frac{2c - d}{2} + \frac{d}{2} \sqrt{\frac{-3}{2}} = a + b \sqrt{-3} \quad (a, b, c, d \in \mathbb{Q});$$

(1)

alakú számoknál. A 9.6 pont P3 példájában jeleztük, hogy egy Euler-racionális akkor és csak akkor algebrai egész, ha Euler-egész. Ez azt jelenti, hogy az (1)-beli $\alpha$ Euler-racionális pontosan akkor algebrai egész, ha $c$ és $d$ egész szám, azaz ha $a$ és $b$ mindkettő egész számok, vagy pedig mindkettő olyan 2 nevezőjű tört, amelyek számlálójának páratlan szám.
A fentiek mutatják, hogy a $t = -1$, illetve $t = -3$ esetekben kapott eredmény kissé eltérő jellegű. Az általános esetben is kétféle lehetőség adódik, attól függően, hogy a bővítést jellemző $t$ milyen maradéket ad 4-gyel osztva:

10.3.2 Tétel. T 10.3.2

Legyen $t \neq 1$ négyzetmentes szám. Ekkor a $\mathbb{Q}(\sqrt{t})$ bővítés algebrai egészei éppen a $c + d\sqrt{t}$ alakú számok, ahol $c$ és $d$ egész szám és

$$
\sqrt{t} = \begin{cases} 
\sqrt{t}, & \text{ha } t \equiv 1 \pmod{4}; \\
(1 + \sqrt{t})/2, & \text{ha } t \equiv 3 \pmod{4}.
\end{cases}
$$

Más megfogalmazásban ez azt jelenti, hogy $\mathbb{Q}(\sqrt{t})$-ben egy $a + b\sqrt{t}$ ($a, b \in \mathbb{Q}$) elem akkor és csak akkor algebrai egész, ha

(a) $t \not\equiv 1 \pmod{4}$ esetén $a$ és $b$ egész számok;

(b) $t \equiv 1 \pmod{4}$ esetén $a = u/2$, $b = v/2$, ahol $u$ és $v$ azonos paritású egészek.

A tétel kétféle megfogalmazása nyilván ekvivalens.

A Gauss-, illetve Euler-egészekre kapott eredmény ennek a tételnek a $t = -1 \not\equiv 1 \pmod{4}$, illetve $t = -3 \equiv 1 \pmod{4}$ speciális esete.

Bizonyítás: Mivel egy racionális szám akkor és csak akkor algebrai egész, ha egész szám, ezért a tétel állítása a $\mathbb{Q}(\sqrt{t})$ bővítés racionális elemeire azonnal adódik.

A továbbiakban így elég a bővítés nem racionális elemeivel foglalkozni. Tetszőleges ilyen $\alpha \in \mathbb{Q}(\sqrt{t})$ egyértelműen felírható $\alpha = r_0 + r_1 \sqrt{t}$ alakban, ahol $r_1 \neq 0$ és $r_0$ racionális számok. Közös nevezőre hozva kapjuk, hogy

$$
\alpha = \frac{a + b\sqrt{t}}{c}, \quad \text{ahol } a, b, c \text{ egész számok}, \quad (a, b, c) = 1, \, c > 0, \, b \neq 0.
$$

Az

$$
\alpha - \frac{a}{c} = \frac{b\sqrt{t}}{c}
$$

eyenlőséget négyzetre emelve

$$
\alpha^2 - \frac{2a}{c} \alpha + \frac{a^2 - t\beta^2}{c^2} = 0
$$

adódik. Mivel $\deg \alpha = 2$, ezért (3) alapján $\alpha$ minimálpolinomja

$$
\varphi_\alpha = \alpha^2 - \frac{2a}{c} \alpha + \frac{a^2 - t\beta^2}{c^2}.
$$

Így $\alpha$ pontosan akkor algebrai egész, ha a (4)-beli minimálpolinom egész együtthatós, azaz

$$
c \mid 2a \quad \text{és} \quad c^2 \mid a^2 - t\beta^2.
$$
Általánosságban kell belátnunk, hogy (5) pontosan akkor teljesül, ha

\[ t \not\equiv 1 \pmod{4} \quad \text{és} \quad c = 1; \quad (6a) \]

\[ t = 1 \pmod{4} \quad \text{és} \quad c = 2 \pmod{a, b \ \text{páratlan}}, \text{vagy} \quad c = 1. \quad (6b) \]

Először azt igazoljuk, hogy (5)-ből \( c = 1 \) vagy \( c = 2 \) következik. Ha \( c > 2 \), akkor \( c \)-nek létezik \( p > 2 \)-prímosztója vagy \( c \) osztható 4-vel. Mindkét esetben ellentmondásra fogunk jutni.

Ha \( p \) prím és \( p \mid c \), akkor \( p \mid 2a \) miatt \( p \mid a \), továbbá \( p^2 \mid a^2 - tb^2 \). Innen \( p^2 \mid t \). A \( p \mid c \), \( p \mid c \) és \( (a, b, c) = 1 \) feltételek miatt \( <p, b> = 1 \), tehát \( p^2 \mid t \). Ez azonban ellentmond annak, hogy \( t \) négyzetmentes.

Ha \( 4 \mid c \), akkor \( 4 \mid 2c \) miatt \( 2 \mid c \). Ezután az előző gondolatmenenet \( p \) helyett 2-re megismételve, ugyanúgy ellentmondásra jutunk.

Ezzel megmutattuk, hogy (5) csak \( c = 1 \) vagy \( c = 2 \) esetén állhat fenn.

A \( c = 1 \) esetben nyilván (5) bármely \( a, b \) egész szélében teljesül.

Ha \( c = 2 \), akkor \( c \mid 2a \) bármely \( a \) egészre igaz, az (5)-beli másik oszthatóság pedig átírható

\[ a^2 - tb^2 = 0 \pmod{4} \quad (7) \]

alakba.

Az \( (a, b, c) = 1 \) feltétel és \( c = 2 \) miatt \( a \) és \( b \) nem lehet egyszerre páros.

Ha \( b \) páros és \( a \) páratlan, akkor

\[ a^2 - tb^2 \equiv 1 \pmod{4}, \]

ha pedig \( a \) páros és \( b \) páratlan, akkor

\[ a^2 - tb^2 \equiv -1 \not\equiv 0 \pmod{4} \]

(hiszen \( t \) négyzetmentes), így mindkettő ellentmond (7)-nek.

Végül, ha \( a \) és \( b \) is páratlan, akkor

\[ a^2 - tb^2 \equiv 1 - t \pmod{4}, \]

azaz ekkor (7) pontosan \( a \equiv 1 \pmod{4} \) esetben teljesül.

Jelöljük a \( \mathbb{Q}^+ \) bővítés algebrai egészeinek halmazát \( E(\sqrt{t}) \)-vel. A T 10.3.2 Tétel szerint tehát

\[ E(\sqrt{t}) = \{ c + d\sqrt{t} \mid c, d \in \mathbb{Z} \}, \quad \text{ha} \quad t \not\equiv 1 \pmod{4}; \quad (8a) \]

illetve

\[ E(\sqrt{t}) = \{ c + d \frac{1 + \sqrt{t}}{2} \mid c, d \in \mathbb{Z} \}, \quad \text{ha} \quad t = 1 \pmod{4}. \quad (8b) \]

Mivel \( E(\sqrt{t}) \) az algebrai egészek gyűrűjének és a \( \mathbb{Q}^+ \) testnek a metszete, ezért \( E(\sqrt{t}) \) részgyűrű a komplex számtestben. Ez a gyűrű kommutatív, egységelemes és nullosztómentes, továbbá nem
test, hiszen például a racionális számok közül csak az egészeket tartalmazza. Mindezek alapján — a Gauss-egész és Euler-egészek mintájára — érdemes $E(\sqrt{5})$-ben is megvizsgálni néhány alapvető számelméleti kérdést.

Az oszthatóság, egység, legnagyobb közös osztó, felbonthatlan és prim fogalmát $E(\sqrt{5})$-ben pontosan ugyanúgy definiáljuk, mint a Gauss-egészeknél (lásd a D 7.4.4, D 7.4.6, D 7.4.9, D 7.4.10 és D 7.4.11 Definíciókat, a „Gauss-” jelzőt most természetesen elhagyjuk).

A számelméleti vizsgálatoknál $E(\sqrt{5})$-ben is kulcsszerűt játszik a norma fogalma:

10.3.3 Definíció .

Az $\alpha = a + b\sqrt{5} \in E(\sqrt{5})$ elem normája

$$N(\alpha) = a^2 - 5b^2 = (a - b\sqrt{5})(a + b\sqrt{5}).$$

A 10.3.2 Tételből következik, hogy minden $\alpha \in E(\sqrt{5})$ elem normája egész szám.

Az is azonnal adódik, hogy a normára vonatkozó T 7.4.3 és T 7.4.5 Tételek $t < 0$ esetén bármely $E(\sqrt{5})$-ben érvényesek, és a $t > 0$ esetben is csak annyi a változás, hogy $N(\alpha)$ negatív egész is lehet (továbbá ha $t > 0$ és $\alpha$ nem racionális, akkor $N(\alpha)$ nem az $\alpha$ abszolút értékének a négyzetét jelenti).

Az egységekre vonatkozó T 7.4.7, illetve T 7.7.6 Tétel a következőképpen módosul:

10.3.4 Tétel .

(A) Egy $\varepsilon \in E(\sqrt{5})$ elemre az alábbi feltételek ekvivalensek:

(i) $\varepsilon$ egység.

(ii) $\varepsilon \mid 1$.

(iii) $|N(\varepsilon)| = 1$.

(B) Ha $t > 0$, akkor $\mathbb{Z}(\sqrt{5})$-ben végtelen sok egység van.

(C) Ha $l < 0$ és $t \neq -1, -3$, akkor $E(\sqrt{5})$-ben az összes egység a $\pm 1$.

Bizonyítás: (A): (i) $\implies$ (ii): Ha $\varepsilon$ minden $E(\sqrt{5})$-beli elemnek osztója, akkor speciálisan az 1-nek is osztója.

(ii) $\implies$ (i): Ha $\varepsilon \mid 1$, vagyis van olyan $\beta \in E(\sqrt{5})$, amelyre $\varepsilon \beta = 1$, akkor tetszőleges $\alpha \in E(\sqrt{5})$-re $\varepsilon(\beta \alpha) = \alpha$, azaz $\varepsilon \mid \alpha$, tehát $\varepsilon$ egység.

(ii) $\implies$ (iii): Ha $\varepsilon \mid 1$, akkor $N(\varepsilon) \mid N(1) = 1$, tehát $N(\varepsilon) = \pm 1$.

(iii) $\implies$ (ii): Ha $\varepsilon = a + b\sqrt{5}$ és

$$N(\varepsilon) = (a + b\sqrt{5})(a - b\sqrt{5}) = \pm 1,$$

akkor $a - b\sqrt{5} \in E(\sqrt{5})$ miatt $\varepsilon \mid 1$. 
(B) Ha $t > 0$, akkor az $x^2 - ty^2 = 1$ Pell-egyenletnek végétlen sok $x, \ y$ egész megoldása van (T 7.8.1 Tétel), és az ezeknek megfelelő $\alpha = x + y\sqrt{t} \in E(\sqrt{t})$ elemekre $N(\alpha) = 1$, tehát ezek valamennyien egységek.

(C) Ha $t < 0$, $t \not\equiv 1 \pmod{4}$, akkor $E(\sqrt{t})$ elemei $\alpha = a + b\sqrt{t}$ alakúak, ahol $a, \ b$ egész, és így $t \neq -1$ esetén

$$N(\alpha) = a^2 + |b|^2 = 1$$

csak úgy teljesülhet, ha $b = 0$ és $a = \pm 1$, azaz $\alpha = \pm 1$.

A $t < 0$, $t \equiv 1 \pmod{4}$ esetben $\alpha$ még $(u, \sqrt{2}) + (v, \sqrt{2})\sqrt{t}$ alakú is lehet, ahol $u$ és $v$ páratlan egész. Ekkor

$$N(\alpha) = \frac{u^2 + |v|^2}{4} = 1, \quad \text{azaz} \quad u^2 + |v|^2 = 4 \quad (9)$$

fennállását vizsgáljuk. Ha $|t| > 3$ és $u, \ v$ páratlan, akkor

$$u^2 + |v|^2 > 1 + 3 \cdot 1 = 4,$$

tehát (9) nem teljesülhet. ■

Megjegyzések: 1. A T 10.3.4 Tétel (A)/(iii) feltétele számos $t$-re csak a $N(\varepsilon) = 1$ lehetőséget jelenti, mert $N(\varepsilon) = -1$ nem fordulhat elő. Ez a helyzet bármely $t < 0$ esetén, hiszen ekkor nyilván minden elem normája nemnegatív. Azonban ilyen például minden olyan pozitív $t$ is, amelyre $t \equiv 3 \pmod{4}$, hiszen ekkor $E(\sqrt{t})$ tetszőleges $\alpha = a + b\sqrt{t}$ elemére ($a, \ b$ egész, és)

$$N(\alpha) = a^2 - bt^2 = -1 \pmod{4}.$$  

2. A T 10.3.4 Tétel (C) részét kiegészíthetjük azzal, hogy ha $t > 0$ esetben $E(\sqrt{t})$ összes egységeit az $x^2 - ty^2 = \pm 1$ egyenlet egész, illetve ha $t \equiv 1 \pmod{4}$, akkor ezekben kívül az $x^2 - ty^2 = -4$ egyenlet páratlan megoldásaiból adódó $x - y\sqrt{t}$ elemek szolgáltatják. Ezeknek az áttekintése a T 7.8.2 Tétel felhasználásával történhet (lásd a 7.8.3 feladathoz [261] adott útmutatást is).

Most ráterünk a számmelmélet alaptételénak a kérdésére. A tételnek a felbontatóságra vonatkozó állítása bármely $E(\sqrt{t})$-ben igaz; $E(\sqrt{t})$ minden, a 0-tól és egységektől különböző eleme felbontható véges sok $E(\sqrt{t})$-beli felbonthatatlan szorzatára. Ez az állítás a norma abszolút értékét felhasználva, a Gauss-egészeknél a T 7.4.13 Tétel bizonyításában láttott módon igazolható.

Alapvetően más a helyzet viszont a felbontás egyértelműségével kapcsolatban, ez már általában nem teljesül. Az egyértelműség kérdését először néhány konkrét bővítésben vizsgáljuk meg, majd utána ismertetjük az általános esetre vonatkozó eredményeket és megoldatlan problémákat.

10.3.5 Tétel \ T 10.3.5

A számmelmélet alaptétele érvényes $E(\sqrt{5})$-ben, viszont nem érvényes $E(\sqrt{-5})$-ben és $E(\sqrt{10})$-ben.

Bizonyítás: Mint a tétel kimondása előtt jeleztük, a felbonthatóság bármely $E(\sqrt{t})$-ben igaz, így elég az egyértelműséggel foglalkoznunk.
Megmutatjuk, hogy a Gauss-egészekhez és Euler-egészekhez hasonlóan itt is elvégezhető a maradékos osztás. Ebből a már többször látott módon következik a számelmélet alaptételének egyértelműségi része.

A Gauss-egészeknél és az Euler-egészeknél a norma szerint végezzük a maradékos osztást, ami részletesen kifejtve azt jelenti, hogy a norma nemnegatív egész szám, egyedül a nullelem normája 0, és elérhető, hogy a maradék normája kisebb legyen az osztó normájánál. (Ezek a tulajdonságok biztosítják, hogy az euklideszi algoritmus véget ér, az általánosításra vonatkozóan lásd a 11.3 pontot.)

Mivel $E(\sqrt{2})$-ben egy elem normája negatív is lehet, ezért ír a norma helyett a norma abszolut értéke szerint elvégezhető a maradékos osztás.

Nyilvánvaló, hogy $E(\sqrt{2})$-ben a norma abszolut értéke nemnegatív egész szám és egyedül a nullelem normájának abszolut értéke 0.

Azt kell tehát beláttnunk, hogy $E(\sqrt{2})$ tetszőleges $\alpha$ és $\beta \neq 0$ elemeihez léteznek olyan $\gamma$ és $\vartheta$ elemei, melyekre

$$\alpha = \beta \gamma + \vartheta \quad \text{és} \quad |N(\vartheta)| < |N(\xi)|,$$  \hspace{1cm} (10)

A norma fogalmát $Q(\sqrt{2})$ elemeire is kiterjeszthetjük: $a, b \in Q$ esetén legyen

$$N(a + b\sqrt{2}) = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2.$$

Azonnal adódik, hogy bármely $\xi, \psi \in Q(\sqrt{2})$ esetén $N(\xi)N(\psi) = N(\xi\psi)$.

Ennek megfelelően, a (10)-beli egyenlőséget $\beta$-val elosztva az alábbi, (10)-zel ekvivalens feltételt kapjuk:

$$\frac{\alpha}{\beta} = \gamma + \frac{\vartheta}{\beta} \quad \text{és} \quad \left| N\left(\frac{\vartheta}{\beta}\right) \right| < 1.$$  \hspace{1cm} (11)

A (11) feltételt a következőképpen is megfogalmazhatjuk: $\alpha/\beta$-hoz keresünk olyan $\gamma \in E(\sqrt{2})$ elemet, amelyre

$$\left| N\left(\frac{\alpha}{\beta} - \gamma\right) \right| < 1.$$  \hspace{1cm} (12)

Legyen $\alpha/\beta = a + u\sqrt{5}$, ahol $a, u \in Q$. Válasszuk $\gamma$-nak azt a $a + d\sqrt{5} \in E(\sqrt{5})$ számot, ahol $c$, illetve $d$ az $a$-hoz, illetve $\vartheta$-hez legközelebbi (egyik) egész szám. Ekkor

$$N\left(\frac{\alpha}{\beta} - \gamma\right) = (a + c)^2 - 2(u + d)^2,$$

és $0 \leq |u - c| \leq 1/2$, $0 \leq |v - d| \leq 1/2$ miatt

$$\frac{1}{2} \leq (a + c)^2 - 2(u + d)^2 \leq \frac{1}{4},$$

technik (12) valóban teljesül.

$E(\sqrt{-5})$ : Megmutatjuk, hogy (például) a 6 két lényegesen különböző módon bontható $E(\sqrt{-5})$-beli felbonthatatlannak szorzatúára:
\[ 6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}). \]

Ehhez azt kell beláttnunk, hogy a 2, 3, \(1 + \sqrt{-5}\) és \(1 - \sqrt{-5}\) felbonthatatlannak \(E(\sqrt{-5})\)-ben, továbbá (például) a 3 nem egység, mint a \(\pm 1\).

Az állítás második része nyilvánvaló, hiszen \(E(\sqrt{-5})\)-ben a T 10.3.4 Tétel (C) része szerint nincs más egység, mint a \(\pm 1\).

A felbontatatlanságot a 2-re igazoljuk, a másik három szám esetén ugyanúgy kell eljárni.

Tegyük fel indirekt, hogy \(2 = \alpha \beta\), ahol \(\alpha\), \(\beta\) egyike sem egység \(E(\sqrt{-5})\)-ben. Ekkor \(4 = N(2) = N(\alpha)N(\beta)\), továbbá \(N(\alpha) \neq 1\), \(N(\beta) \neq 1\), és így (mivel \(E(\sqrt{-5})\)-ben a norma nemnegatív) csak \(N(\alpha) = N(\beta) = 2\) lehetséges.

Legyen \(\alpha = a + b\sqrt{-5}\), itt \(a, b\) egész, \(\text{mivel} -5 \not\equiv 1 \pmod{4}\). Ekkor \(N(\alpha) = a^2 + 5b^2 = 2\) nyilván nem állhat fenn. Az ellentmondás igazolja, hogy a 2 valóban felbontatlan \(E(\sqrt{-5})\)-ben.

\(E(\sqrt{10})\): Ekkor (például) a \(-9\)-nek létezik két lényegesen különböző felbontása felbontatlanok szorzatára:

\[ (-9) = 3(-3) = (1 + \sqrt{10})(1 - \sqrt{10}). \tag{13} \]

A (13)-beli felbontásokban \(\pm 3\) nem egység, \(\pm 1 \pm \sqrt{10}\) -nek, mert

\[ \frac{1 \pm \sqrt{10}}{\pm 3} = \pm \frac{1}{3} \pm \frac{1}{3} \sqrt{10} \not\in E(\sqrt{10}). \]

Azt kell még igazolni, hogy a (13)-ban szereplő tényezők valóban felbontatlanok. Ha \(\pm 3\) vagy \(1 \pm \sqrt{10}\) nem lenne felbontatlan, akkor az \(E(\sqrt{-5})\)-nél látott gondolatmenet szerint kapnánk, hogy léteznie olyan \(\alpha = a + b\sqrt{10}\), \(a, b\) egész, amelyre \(N(\alpha) = a^2 - 10b^2 = \pm 3\). Ez azonban lehetetlen, mert \(a^2 \not\equiv \pm 3 \pmod{5}\). \(\square\)

A számelmélet alaptételének kérdése az általános másodfokú bővítések esetén igen nehéz, és jelentős részben ma is megoldatlan probléma.

Kezdjük a valós bővítésekkel:

V1 Megoldatlan, hogy végteken sok olyan \(t > 0\) létezik-e, amelyre \(F(\sqrt{t})\)-ben érvényes az alaptétel.

V2 Meghatározták az összes olyan \(t > 0\) értékét, amikor \(F(\sqrt{t})\)-ben a norma abszolút értéke szerint elvégezhető a maradékos osztás (lásd az alábbi T 10.3.6 Tétel (iii) részét). Ezekre a \(t\) -kre tehát \(E(\sqrt{t})\)-ben biztosan érvényes a számelmélet alaptétele. Léteznek azonban további olyan pozitív \(t\) -k is, amikor igaz az alaptétel, ilyen például a \(t = 14, 22, 23\) vagy 31.

A képzetes bővítésekre 1968 óta ismert a teljes válasz:

K1 Pontosan kilenc olyan \(t < 0\) létezik, amelyre \(E(\sqrt{t})\)-ben érvényes az alaptétel, ezek felsorolását lásd a T 10.3.6 Tétel (i) részében. (Ezek közé tartoznak a korábban már tárgyalt Gauss-, illetve Euler-egészek is.)
A K1, K2 és V2 pontokban jelzett eredményeket (bizonyítás nélkül) az alábbi tételben foglaljuk össze:

10.3.6 Tétel. \( T 10.3.6 \)

(i) A \( t < 0 \) esetben \( E(\sqrt{t}) \)-ben akkor és csak akkor igaz a számmintegél alaptétele, ha

\[
\begin{align*}
t &= -1, -2, -3, -7, -11, -19, -43, -67, -163.
\end{align*}
\]

(ii) Az (i)-ben felsorolt kilenc \( t \)-érték közül pontosan az első öt olyan, amikor \( E(\sqrt{t}) \)-ben a norma szerint elvégezhető a maradékos osztás.

(iii) A \( t > 0 \) esetben \( E(\sqrt{t}) \)-ben akkor és csak akkor végezhető el a norma abszolút értéke szerint a maradékos osztás, ha

\[
\begin{align*}
t &= 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 23, 33, 37, 41, 57, 73.
\end{align*}
\]

A T 10.3.6 Tétel (ii) állításának a bizonyítását a 10.3.4 feladatban [338] tűztük ki.

Végül két tételt tárgyalunk az \( E(\sqrt{t}) \)-beli felbonthatatlanokról, illetve primekről. Az első tétel tetszőleges \( E(\sqrt{t}) \)-re vonatkozik, függetlenül attól, hogy érvényes-e a szármintegél alaptétele vagy sem. Ennek megfelelően itt élesen meg kell különböztetnünk a prim és a felbonthatatlan fogalmát, hiszen ezek nem ekvivalensek. A második tétel olyan másodfokú bővítésekre vonatkozik, ahol igaz a szármintegél alaptétele, így itt a prim és a felbonthatatlan fogalma egybeesik.

10.3.7 Tétel. \( T 10.3.7 \)

Legyen \( \mathcal{P} \) prímszám és \( \langle p, t \rangle = 1 \). Ekkor \( E(\sqrt{t}) \)-ben \( \mathcal{P} \) akkor és csak akkor prim, ha \( \langle \mathcal{P}, t \rangle = -1 \).

Bizonyítás: Először azt igazoljuk, hogy ha \( \langle \mathcal{P}, t \rangle = -1 \), akkor \( \mathcal{P} \) prim \( E(\sqrt{t}) \)-ben.

Tegyük fel, hogy \( \mathcal{P} \mid \alpha \beta \), és mutassuk meg, hogy \( \mathcal{P} \mid \alpha \) és \( \mathcal{P} \mid \beta \) közül legalább az egyik teljesül.

A \( \mathcal{P} \mid \alpha \beta \) oszthatóságból kapjuk, hogy

\[
\mathcal{P}^2 = N(\mathcal{P}) | N(\alpha)N(\beta).
\]

Mivel \( \mathcal{P} \) prímszám \( (\mathbb{Z}, \cdot) \)-ben, ezért \( \mathcal{P} \) a \( N(\alpha)N(\beta) \) szorzat valamelyik ténylegőjét is osztja, monduk \( \mathcal{P} \mid N(\alpha) \). Megmutatjuk, hogy \( \langle \mathcal{P}, t \rangle = -1 \) miatt ebből \( \mathcal{P} \mid \alpha \) is következik.

Legyen \( \alpha = a + b\sqrt{t} \). Vizsgáljuk először a \( t \not\equiv 1 \pmod{4} \) esetet, ekkor \( a \) és \( b \) egész számok. Így a \( \mathcal{P} \mid N(\alpha) = \alpha^2 - t\beta^2 \) feltétel átírható az

\[
\alpha^2 = t\beta^2 \pmod{\mathcal{P}} \quad (14)
\]

alakba. Ha \( \langle a, \mathcal{P} \rangle = \langle b, \mathcal{P} \rangle = 1 \), akkor (14)-ből

\[
\alpha^2 \equiv \beta^2 \pmod{\mathcal{P}}
\]
következik, ami ellentmond a \( \left( \frac{t}{p} \right) = -1 \) feltételnek. Ha \( a \) és \( b \) közül pontosan az egyik osztható \( P \)-vel, akkor (14) egyik oldala osztható \( P \)-vel, a másik viszont nem, ami szintén lehetetlen. Így (14) csak úgy teljesülhet, ha \( a \equiv b \equiv 0 \left( \text{mod} \ p \right) \). Ekkor \( p \mid a \pm b\sqrt{i} \) is igaz, tehát valóban \( p \mid \alpha \).

A \( i = 1 \left( \text{mod} \ 4 \right) \) esetben azt a lehetőséget is figyelembe kell venni, amikor \( a = u/2, b = v/2 \), ahol \( u, v \) páratlan. Ekkor (14) helyett az \( u^2 \equiv v^2 \left( \text{mod} \ p \right) \) kongruencia fentiekhez hasonló vizsgálata igazolja \( p \mid \alpha \) teljesülését.

A megfordításhoz indirekt tegyük fel, hogy \( \left( \frac{\alpha}{p} \right) = 1 \). Ekkor létezik olyan \( e \) egész szám, amelyre \( e^2 \equiv t \left( \text{mod} \ p \right) \). Így

\[
p \mid e^2 - t = (e + \sqrt{i})(e - \sqrt{i}), \quad \text{de} \quad p \nmid e \pm \sqrt{i}.
\]

Ez ellentmond annak, hogy \( P \) prim \( E(\sqrt{i}) \)-ben.

A következő tétel a Gauss- és Euler-egészekre bizonyított T 7.4.12, T 7.4.14, T 7.4.15, illetve T 7.7.7 Tételek általánosítása arra az esetre, amikor \( E(\sqrt{i}) \)-ben érvényes a számelmélet alaptétele:

10.3.8 Tétel

Tegyük fel, hogy \( E(\sqrt{i}) \)-ben igaz a számelmélet alaptétele. Ekkor:

(i) \( E(\sqrt{i}) \) egy eleme akkor és csak akkor felbonthatatlan, ha prim. (Ennek alapján a továbbiakban a felbonthatatlan helyett is a prim szót fogjuk használni.)

(ii) Minden \( \pi \) primhez pontosan egy olyan \( P \) pozitív primcsúz létezik, amelyre \( \pi \mid P \).

(iii) Minden \( P \) pozitív primcsúz vagy maga is prim \( E(\sqrt{i}) \)-ben, vagy pedig pontosan két primnek a szorzata, amelyek normája \( \pm P \), és amelyek egymás „konjugáltjai” a következő értelenben (vó. a D 10.4.1 Definícióval): legyen \( \pi_1 = a + b\sqrt{i} \), ekkor \( \pi_2 = \pm(a - b\sqrt{i}) \).

(iv) Ha \( P > 2 \) primcsúz, \( \left( \frac{\pi}{P} \right) = 1 \) és \( \left( \frac{t}{P} \right) = -1 \), akkor \( P \) prim \( E(\sqrt{i}) \)-ben.

(v) Ha \( P > 2 \) primcsúz, \( \left( \frac{\pi}{P} \right) = 1 \) és \( \left( \frac{t}{P} \right) = 1 \), akkor \( P \) két \( E(\sqrt{i}) \)-beli prim szorzata, amelyek nem egymás egységsgékre.

(vi) Páratlan \( t \) esetén a 2 a következőképpen viselkedik:

(a) ha \( t \equiv 3 \left( \text{mod} \ 4 \right) \), akkor a 2 két olyan prim szorzata, amelyek egymás egységsgérek (azaz a 2 egy prim négyzetének az egységsgerezse);

(b) ha \( t = 1 \left( \text{mod} \ 8 \right) \), akkor a 2 két olyan prim szorzata, amelyek nem egymás egységsgerei;

(c) ha \( t \equiv 5 \left( \text{mod} \ 8 \right) \), akkor a 2 prim.

(vii) Ha a \( P \) primcsúz osztója \( t \)-nek, akkor \( P \) két olyan prim szorzata, amelyek egymás egységsgerei (azaz \( P \) egy prim négyzetének az egységsgerezse).
(viii) A (iv)–(vii) pontokban felsorolt primerek egységszeresei adják az összes prímet \( E(\sqrt{p}) \)-ben.

Bizonyítás: (i) Egy prim mindig szükségképpen felbonthatatlan is, lásd az T 1.4.3 Tétel bizonyítását. Az, hogy minden felbonthatatlan egyben prím is, a számelmélet alaptételeiből következik, lásd az 1.5.8 feladatot [21] (vagy a T 11.3.1 Tételt).

(ii) és (iii) pontosan úgy bizonyítható, mint a T 7.4.14 Tétel.

(iv) következik a T 10.3.7 Tételből.

Az (v)–(vii) állításokkal kapcsolatban először csak azt igazoljuk, hogy a \( P \), illetve a 2 prim-e \( E(\sqrt{p}) \)-ben vagy sem.

(v)-nél ez a T 10.3.7 Tételből következik.

(vi) Ha \( t \equiv 3 \pmod{4} \), akkor
\[
2 \mid t^2 - t = (t - \sqrt{t})(t - \sqrt{t}), \quad \text{de} \quad \text{2} \not\mid \sqrt{t},
\]
tehát a \( 2 \) nem prim.

Ha \( \bar{t} \equiv 1 \pmod{8} \), akkor
\[
2 \mid \frac{1 - \sqrt{t}}{4} = \frac{1 + \sqrt{t}}{2} \cdot \frac{1 - \sqrt{t}}{2}, \quad \text{de} \quad \text{2} \mid \frac{1 + \sqrt{t}}{2},
\]
tehát a \( 2 \) nem prim.

Végül, ha \( \bar{t} \equiv 5 \pmod{8} \) és a 2 nem lenne prim, akkor lenne a 2-nek olyan
\[
a = \frac{u + \sqrt{t}}{2}, \quad \text{azaz} \quad u^2 - t\bar{u}^2 = 28.
\]
Azonban \( u^2 - t\bar{u}^2 \) nem lehet \( 18\bar{k} + 8 \) alakú, ami ellentmondás.

(vii) Mivel
\[
\sqrt{t} \equiv \sqrt{2}, \quad \text{de} \quad \sqrt{2} \not\equiv \sqrt{2}.
\]
(ez \( p = 2 \) esetén is igaz), ezért \( p \) nem lehet prim.

Az (v), (vi)/a, (vi)/b és (vii) esetekben az előzőkből következik, hogy a \( P \), illetve a 2 nem prim. Ekkor (iii) alapján a \( P \), illetve a 2 felírható két prim, \( \pi_1 \) és \( \pi_2 \) szorzataként, ahol
\[
\pi_1 = a + b\sqrt{t}, \quad \text{és} \quad \pi_2 = \pm(a - b\sqrt{t}).
\]
Itt a \( \hat{a} \not\equiv 1 \pmod{4} \) esetben \( a \) és \( b \) egész, a \( \hat{a} \equiv 1 \pmod{4} \) esetben pedig \( u = u/2, b = v/2 \), ahol \( u \) és \( v \) azonos paritású egészek.

Mivel \( |N(\pi_1)| = |N(\pi_2)| = p \) (illetve 2), ezért \( |N(\pi_1/\pi_2)| = 1 \). Így \( \pi_1 \) és \( \pi_2 \) pontosan akkor egységszerese egymásnak, ha
ALGEBRÁI SZÁMTESTEK

\[
\pi_1 = \frac{a + b\sqrt{t}}{\pm(a - b\sqrt{t})} = \frac{a^2 - t b^2}{p} + \frac{2ab}{p} \sqrt{t} \subset E(\sqrt{t}). \tag{15}
\]

(v)-nél (15) nem teljesül, ugyanis \( |N(\pi_1)| = p \) miatt \( 2ab/p \) nem lehet egész szám vagy egy 2 nevezőjű tört.

(vi) a esetén (15)-ben \( p = 2 \), továbbá \( t \equiv 3 \pmod{4} \) miatt \( a \) és \( b \) egészek, valamint \( a^2 - t b^2 = \pm 2 \) alapján \( a \) és \( b \) páratlan. Ezért

\[
\frac{a^2 + t b^2}{2} \equiv 2ab \equiv ab \mod{2}
\]

is egész, tehát \( \pi_1 \) és \( \pi_2 \) egymás egységszeresei.

(vi)/b esetén (15)-ben \( p = 2 \), továbbá

\[
a^2 - t b^2 = -2 \quad \text{és} \quad t = 1 \pmod{4}
\]

miatt \( a \) és \( b \) nem lehet egész. Ezért \( a = u/2 \) és \( b = v/2 \), ahol \( u \), \( v \) páratlan. Ekkor (15)-ben \( 2ab/2 = uv/4 \) nem egész és nem kettő nevezőjű tört, tehát (15) nem teljesül. Így \( \pi_1 \) és \( \pi_2 \) nem egymás egységszeresei.

(vii)-nél vizsgáljuk először azt az esetet, amikor \( a \) és \( b \) egészek. Ekkor

\[
a^2 - t b^2 = \pm p \quad \text{és} \quad p \mid t
\]

miatt \( p \mid a \), és így (15)-ben

\[
\frac{a^2 + t b^2}{p} \equiv 2ab \equiv ab \mod{p}
\]

is egész, tehát \( \pi_1 \) és \( \pi_2 \) egymás egységszeresei.

Hasonlóan kezelhető az az eset is, amikor \( t \equiv 1 \pmod{4} \) és \( a = u/2 \), \( b = v/2 \), ahol \( u \), \( v \) páratlan.

Végül, (viii) azonnal következik (ii)-ből és (iv)-(vii)-ből. ■

Feladatok

10.3.1 (a) Bizonyítsuk be, hogy \( E(\sqrt{3}) \)-ban érvényes a számelmélet alaptétele.

(b) Hogyan fér össze a számelmélet alaptétele az alábbi egyenlőségekkel:

(b1) \( 7 + 3\sqrt{3} = (1 + \sqrt{3})(1 + 2\sqrt{3}) = (-4 + 3\sqrt{3})(5 + 3\sqrt{3}) \);

(b2) \( 19 + 5\sqrt{3} = (5 - \sqrt{3})(5 + 2\sqrt{3}) = (-4 - 3\sqrt{3})(11 + 7\sqrt{3}) \).

(c) Határozzuk meg \( E(\sqrt{3}) \)-ban az összes prímet.

(d) * Milyen \( n \) pozitív egészre oldható meg az \( x^2 - 3y^2 = n \) diofantikus egyenlet, és megoldhatóság esetén mennyi a megoldásszám? 

337
10.3.2 (a) Bizonyítsuk be, hogy \( E(\sqrt{-2}) \)-ben érvényes a számelmélet alaptétele.
(b) Határozzuk meg \( E(\sqrt{-2}) \)-ben az összes prímet.
(c) Oldjuk meg az \( x^2 + 2 = y^4 \) diofantikus egyenletet.

10.3.3 Mutassuk meg, hogy az alábbi \( \ell \) értékekre \( E(\sqrt{\ell}) \)-ben nem igaz a számelmélet alaptétele:
(a) 15;
(b) 26;
(c) \(-6\);
(d) \(-10\).

10.3.4 (*) Izgoljuk a T 10.3.6 Tétel (ii) állítását: Egy képzetes \( E(\sqrt{i}) \) -ben a norma szerint akkor és csak akkor végezheto el a maradékos osztás, ha \( i = -1, -2, -3, -7 \) vagy \(-11\).

10.3.5 (M [611]*) Bizonyítsuk be, hogy ha \( \ell \) (négyzetmentes) negatív összetett szám, akkor \( E(\sqrt{\ell}) \)-ben nem érvényes a számelmélet alaptétele.

10.3.6 (M [611]*) Legyen \( \ell \) egész szám és \( f = x^2 + x + \ell \). Bizonyítsuk be, hogy ha \( E(\sqrt{-4\ell + 1}) \)-ben igaz a számelmélet alaptétele, akkor az \( f(0), f(1), \ldots, f(k - 2) \) számok mindegyike primszám.

Megjegyzés: Megmutatható, hogy az állítást megfordítása is igaz. Így a T 10.3.6(i) Tétel szerint a feladatban szereplő tulajdonság csak a \( k - 2, 3, 5, 11, 17 \) és 41 esetben teljesül. Ha \( k = 41 \), akkor azt az 5.1 pontban már említett tényt kapjuk, hogy \( n^2 + n + 41 \) minden \( 0 \leq n \leq 39 \) esetén primszám. Az előzőek alapján ilyen típusú primszámsorozat \( k > 41 \) esetén nem létezik.

10.3.7 Mutassuk meg, hogy ha egy \( \alpha \in E(\sqrt{i}) \) elemre \( |N(\alpha)| \) primszám, akkor \( \alpha \)
(a) felbonthatatlan;
(b) \( \neq \) prim
\( E(\sqrt{i}) \)-ben (függetlenül attól, hogy \( E(\sqrt{i}) \)-ben igaz-e a számelmélet alaptétele vagy sem).

10.3.8 Bizonyítsuk be, hogy ha \( \alpha, \beta \in E(\sqrt{i}) \) és \( \alpha^2 | \beta^2 \), akkor \( \alpha | \beta \) is teljesül (függetlenül attól, hogy \( E(\sqrt{i}) \)-ben igaz-e a számelmélet alaptétele vagy sem).

10.3.9 Ebben a feladatban megvizsgáljuk, mely \( P > 0 \) primszámok lesznek felbonthatatlannak, illetve primek \( E(\sqrt{-5}) \)-ben.
(a) Az 5 nem felbonthatatlann (és így nem is prim).
(b) A 2 felbonthatlan, de nem prim.
(c) Ha \( P \equiv 11, 13, 17 \) vagy 19 (mod 20), akkor \( P \) prim (és így felbonthatatlann is).

338
(d) Ha \( p = 3 \) vagy 7 (mod 20), akkor \( P \) felbonthatatlan, de nem prím.

(e) \( (M[612]) \) Ha \( p = 1 \) vagy 9 (mod 20), akkor \( P \) nem felbonthatatlan (és így nem is prím).

### 10.4 Norma

Ebben a pontban tetszőleges \( \mathbb{Q}(\theta) \) bővítés elemeire kiterjesztjük a norma fogalmát, ahol \( \theta \) algebrai szám. Ehhez szükségünk lesz egy algebrai szám \( \mathbb{Q} \) feletti konjugáltjainak és az adott bővítésre vonatkozó relatív konjugáltjainak a fogalmára.

#### 10.4.1 Definíció . \( \text{D 10.4.1} \)

Egy \( \alpha \) algebrai szám minimálpolinomjának (komplex) gyökeit az \( \alpha \mathbb{Q} \) feletti konjugáltjainak nevezzük.

Mivel \( m_{\alpha} \) irreducibilis \( \mathbb{Q} \) felett, és egy irreducibilis polinomnak nem lehet többszörös (komplex) gyöke (lásd a 9.4.4 feladatot [308]), ezért egy \( n \)-edfokú algebrai szám \( \mathbb{Q} \) darab (különböző) \( \mathbb{Q} \) feletti konjugáltja van, amelyek közül az egyik maga az adott szám.

Az \( \alpha \mathbb{Q} \) feletti konjugáltjai között szerepel az \( \alpha \) komplex konjugáltja, \( \overline{\alpha} \) is, hiszen \( \alpha \)-nak és \( \overline{\alpha} \)-nak ugyanaz a minimálpolinomja.

A továbbiakban általában a \( \mathbb{Q} \) feletti konjugált helyett röviden csak a konjugált szót fogjuk használni (viszont a komplex konjugáltnál mindig kitesszük majd a komplex jelzőt).

**Példák:**

P1 Egy racionális számnak egyetlen konjugáltja van, önmaga.

P2 Legyen \( \alpha = a + bi \) egy nem valós Gauss-racionális, azaz \( a, b \in \mathbb{Q} \), \( b \neq 0 \). Ekkor \( \alpha \) egyik konjugáltja önmaga, a másik pedig az \( \overline{\alpha} = a - bi \) komplex konjugált. Hasonló a helyzet a nem valós Euler-racionálisok esetén is.

P3 Legyen \( \alpha = a + b\sqrt{2} \) a \( \mathbb{Q}(\sqrt{2}) \) bővítés egy nem racionális eleme, azaz \( a, b \in \mathbb{Q} \), \( b \neq 0 \). Ekkor \( \alpha \)-nak egyik konjugáltja önmaga, a másik pedig \( a - b\sqrt{2} \).

P4 Az \( \alpha = \sqrt{2} \) konjugáltjai a \( \theta \) alakú számok, ahol \( \theta \) tetszőleges ötödik komplex egységgyök.

#### 10.4.2 Definíció \( \text{D 10.4.2} \)

Legyenek a \( \mathbb{Q}[\theta] \)-edfokú algebrai szám konjugáltjai

\[
\tilde{\theta}_1, \tilde{\theta}_2, \ldots, \tilde{\theta}_{(n)},
\]

és \( \alpha \in \mathbb{Q}(\theta) \). Tekintsük (a T 10.2.3 Tétel alapján) azt az (egyértelműen meghatározott) \( f \in \mathbb{Q}[x] \) polinomot, amelyre

\[
\alpha = f(\tilde{\theta}_1) = \ldots = f(\tilde{\theta}_{(n)}), \quad \deg f 
\leq n - 1 \text{ vagy } f = 0.
\]

Ekkor az

\[
f(\tilde{\theta}_j), \quad j = 1, 2, \ldots, n,
\]

számokat az \( \alpha \)-nak a \( \mathbb{Q}(\theta) \)-ra vonatkozó relatív konjugáltjainak nevezzük.
Az \( f(\vartheta_j) \) relatív konjungált tehát a \( Q(\vartheta_j) \) bővítés egy eleme. Ez a \( Q(\vartheta_j) \) bővítés többnyire nem esik egybe \( Q(\vartheta) \)-val, és így általában az \( \alpha \) relatív konjungáltjai nem lesznek elemei \( Q(\vartheta) \)-nak.

A D 10.4.2 Definícióban az \( f(\vartheta_j) \) relatív konjungáltak az \( \alpha \) -n kívül látszólag nemcsak a \( Q(\vartheta) \) bővítésteól, hanem annak konkrét megadási módjától, azaz a \( \vartheta \) választásától is függnek. A T 10.4.3 Tételből azonban azonnal következik majd, hogy valójában nem ez a helyzet: ha \( Q(\vartheta) = Q(\vartheta') \), akkor az \( \alpha \) -nak a \( \vartheta \), illetve a \( \vartheta' \) segítségével képzett relatív konjungáltjai ugyanazok lesznek.

Példák:

P5 Egy \( r \) racionális számnak bármely \( Q(\vartheta) \) bővítés esetén az összes relatív konjungálta önmaga. Ugyanis az \( f(\vartheta) = r \), \( \deg f < \deg \vartheta \) vagy \( f = 0 \) feltételt kielégítő polinom az \( f - r \) konstans polinom, így bármely \( j \)-re is \( f(\vartheta_j) = r \).

P6 Legyen \( \vartheta = i \), akkor \( \vartheta \) konjungáltai \( \vartheta(1) = i \) és \( \vartheta(2) = -i \). A \( Q(i) \) bővítés egy \( \alpha = a + bi \) \( (a, b \in Q) \) elemének a relatív konjungáltjai ezért

\[
a + bi = \alpha \quad \text{és} \quad a + b(-i) = a - bi = \alpha.
\]

Ez azt jelenti, hogy ha \( \alpha \) nem racionális szám, akkor a relatív konjungáltjai ugyanazok, mint a \( Q \) feletti konjungáltjai. Hasonló a helyzet a \( Q(\sqrt{3}) \), a \( Q(\sqrt{2}) \) és általában a másodfokú bővítések esetén.

P7 Legyen \( \vartheta = \sqrt{3} \), ekkor \( \vartheta \) konjungáltai \( \pm \vartheta \) és \( \pm i\vartheta \). Az \( \alpha = \sqrt{3} \in Q(\vartheta) \) elemet a T 10.2.3 Tétel szerint előállító polinom az \( f = 2 \), ugyanis \( \sqrt{3} = (\vartheta^2) \). Ennek megfelelően a \( \sqrt{3} \) relatív konjungáltjai a

\[
(\pm \vartheta)^2 = \sqrt{3} \quad \text{és} \quad (\pm i\vartheta)^2 = -\sqrt{3}.
\]

Ez a négy szám éppen a \( \sqrt{3} \)-nak a \( Q \) feletti két konjungáltja kétszeres multiplicitással.

A példák alapján nem meglepő, hogy egy \( \alpha \in Q(\vartheta) \) elem relatív konjungáltjai ugyanazok, mint az \( \alpha \)-nak a \( Q \) feletti konjungáltjai, megfelelő multiplicitással számolva:

10.4.3 Tétel. T 10.4.3

Legyen \( \alpha \) az \( n \)-edfokú \( Q(\vartheta) \) bővítés egy \( k \)-edfokú eleme. Ekkor az \( \alpha \)-nak a \( Q(\vartheta) \)-ra vonatkozó relatív konjungáltjait úgy kapjuk meg, hogy az \( \alpha \)-nak mindegyik \( Q \) feletti konjungáltját \( n/k \)-szor vesszük.

A tételből következik, hogy a relatív konjungáltakat nem befolyásolja, ha \( Q(\vartheta) \)-ban \( \vartheta \) helyett egy másik generátorelemet választunk, tehát a relatív konjungáltak valóban csak \( \alpha \)-tól és magától a bővítéstől függenek.

A T 10.4.3 Tételből egyúttal új bizonyítást nyertünk arra, hogy \( \deg \alpha \) osztója a \( Q(\vartheta) \) bővítés fokának (vő, a T 10.2.5 Tétellel).

Bizonyítás: Legyen \( \vartheta \), illetve \( \alpha \) minimálpolinomja

\[
\gamma_{\vartheta, \alpha} = \prod_{j=1}^{n}(x - \vartheta_j), \quad n_{\alpha, \vartheta} = \prod_{j=1}^{k}(x - \alpha_{(j)}), \quad n_{\alpha} = \prod_{k=1}^{\lambda}(x - \alpha_k),
\]

340
I. Először azt igazoljuk, hogy az \( \alpha \) mindegyik \( f(\beta(j)) \) relatív konjugáltja megegyezik az \( \alpha \) -nak a \( \mathbb{Q} \) feletti valamelyik \( \alpha_\ast \) konjugáltjával (a multiplicitást egyelőre nem vizsgáljuk).

Tekintsük a \( g(x) = m_\alpha(f(x)) \) polinomot. Nyilván \( g \in \mathbb{Q}[x] \), továbbá

\[
g(\beta) = m_\alpha(f'(\beta)) = m_\alpha(\alpha) = 0.
\]

Ebből következik, hogy \( \forall \beta \in \mathbb{Q} \), és így minden \( f \) -re

\[
0 = g(\beta(j)) = m_\alpha(f(\beta(j)));
\]

Ez azt jelenti, hogy \( f(\beta(j)) \) gyöke \( m_\alpha \) -nak, vagyis \( f(\beta(j)) \) valóban valamelyik \( \alpha_\ast \) -s elmenő.

II. Azt kell még megmutatnunk, hogy mindegyik \( \alpha_\ast \) ugyanannyiszor szerepel az \( f(\beta(j)) \) számok között ( \( j = 1, 2, \ldots, n \) ). E célből tekintsük a

\[
h = \prod_{j=1}^{n}(x - f(\beta(j))
\]

polinomot. A szimmetrikus polinomok alaptételének (9.3.2 Tétel) felhasználásával a T 9.3.1 és T 9.3.6 Tételek bizonyításához hasonló módon kapjuk, hogy \( h \) racionális együthattos: A \( h \) minden \( c_\nu \) egyúthatatja a \( \beta(j) \) -nnek szimmetrikus polinomja, így \( c_\nu \) felirható a \( \beta(j) \) -k \( \sigma_j \) elemi szimmetrikus polinomjainak racionális együthattos polinomjaként. A \( \sigma_j \) -k a gyökök és egyúthatatok közötti összefüggés alapján éppen \( m_\theta \) együthattató, illetve azok ellentettjei, tehát racionális számok, és így \( c_\nu \) is racionális.

Bontsuk fel a \( h \) polinomot a \( \mathbb{Q} \) felett irreducibilis polinomok szorzatára. Mivel a \( h \) gyökei, azaz az \( f(\beta(j)) \) számok valamennyien gyökei az \( m_\alpha \) irreducibilis polinomnak, ezért a \( h \) felbontásában csak \( m_\alpha \) szerepelhet. Figyelembe véve azt is, hogy \( h \) és \( m_\alpha \) is normált, ez azt jelenti, hogy \( h \) az \( m_\alpha \) -nak hatványa: \( h = m_\alpha^t \). A fokszámok összehasonlításából kapjuk, hogy \( t = \frac{n}{k} \), és így az \( f(\beta(j)) \) -k között az \( m_\alpha \) mindegyik \( \alpha_\ast \) gyöke valóban \( \frac{n}{k} \) -szor fordul elő. □

Most már minden készen áll a norma általános definíciójához:

10.4.4 Definíció . D 10.4.4

Egy \( \alpha \in \mathbb{Q}(\theta) \) elem normáján a relatív konjugáltjainak a szorzatát értjük: ha a \( \nu \) konjugáltjai \( \dot{\theta}(1), \dot{\theta}(2), \ldots, \dot{\theta}(\alpha) \) és \( \alpha = f(\theta) \), akkor

\[
N(\alpha) = \prod_{j=1}^{\alpha} f(\theta(j)). \quad \star
\]

Világos, hogy a másodfokú bővítéseknel a D 10.3.3 Definícióban szereplő normafogalom a D 10.4.4 Definíció speciális esete.

A norma legfontosabb tulajdonságait a következő tételben foglaljuk össze:

10.4.5 Tétel . T 10.4.5

(i) Legyen \( \alpha \in \mathbb{Q}(\theta) \), \( \deg \theta = \nu \) és \( \deg \alpha = \frac{k}{\nu} \). Ekkor
\[ N(\alpha) = \left( \prod_{k=1}^{\infty} a_k \right)^{\frac{1}{n_k}} = (-1)^{a_0} \alpha_0^{n/n_k}, \]

ahol \( a_{(1)} = a_{(2)} = \ldots = a_{(k)} \) az \( \alpha \)-nak a \( \mathbb{Q} \) feletti konjugáltjai, és \( a_0 \) az \( \alpha \) normált minimálpolinomjának a konstans tagja.

(ii) \( \alpha, \beta \in \mathbb{Q}(\theta) \Rightarrow N(\alpha\beta) = N(\alpha)N(\beta) \).

(iii) Ha \( \alpha \) algebrai egész, akkor \( N(\alpha) \) egész szám.

**Bizonyítás:** Az (i) állításban szereplő első egyenlőség azonnal következik a T 10.4.3 Tételből, a második egyenlőség pedig az \( m_\theta \) polinom gyűkei és együtthatói közötti összefüggésből. A \( N(\alpha) \) -nak ebből az (i)-beli alakjából rögtön kapjuk a (iii) állítást is.

(ii) igazolásához legyen
\[ \alpha = f_1(\theta^*), \quad \beta = f_2(\theta) \quad \text{és} \quad \alpha \beta = f_3(\theta^*). \]

Ekkor \( \theta \) gyöke a \( h = f_3 - f_1 f_2 \in \mathbb{Q}[x] \) polinomnak, tehát \( m_\theta \mid h \). Ebből következik, hogy \( m_\theta \) többi gyöke, azaz a \( \theta \) minidegyik \( \theta^* \) konjugálta is gyöke \( h \)-nak, azaz
\[ \theta = \theta(h_{(1)}) = f_1(\theta^*) - f_1(\theta h_{(j)}) f_2(\theta h_{(j)}), \quad j = 1, 2, \ldots, n. \]

Az így adódó \( f_3(\theta h_{(j)}) = f_1(\theta^*) f_2(\theta h_{(j)}) \) egyenlőségeket összeszorozva kapjuk, hogy
\[ N(\alpha\beta) = \prod_{j=1}^{n} f_3(\theta h_{(j)}) = \left( \prod_{j=1}^{n} f_1(\theta h_{(j)}) \right) \left( \prod_{j=1}^{n} f_2(\theta h_{(j)}) \right) = N(\alpha)N(\beta). \]

**Feladatok**

10.4.1 Adjuk meg az alábbi algebrai számok \( \mathbb{Q} \) feletti konjugáltjait:

(a) \( \sqrt{2} + \sqrt{3} \);

(b) \( \sqrt{2}(1 + i) \);

(c) \( \cos 30^\circ \);

(d) \( \cos 1^\circ + \sin 1^\circ \).

10.4.2 Jelölje \( \sqrt[3]{(1)} = (1, (2), \ldots, (k)) \) a \( \theta \) algebrai szám \( \mathbb{Q} \) feletti konjugáltjait. Igazoljuk az alábbi állításokat.

(a) Ha \( \deg \theta = 2 \), akkor \( \mathbb{Q}(\theta(1)) = \mathbb{Q}(\theta(2)) \).

(b) Ha \( \theta \) nem valós és \( \deg \theta \) páratlan, akkor van olyan \( j \) és \( k \), amelyre \( \mathbb{Q}(\theta(h_{(j)})) \neq \mathbb{Q}(\theta(h_{(k)})) \).

(c) Ha \( \theta \) nem valós és \( \deg \theta = 3 \), akkor bármely \( j \neq k \) esetén \( \mathbb{Q}(\theta(h_{(j)})) \cap \mathbb{Q}(\theta(h_{(k)})) = \mathbb{Q} \).

10.4.3 Adjuk meg \( \mathbb{Q}(\sqrt[3]{2}) \) alábbi elemeinek relatív konjugáltjait és normáját:
(a) $1 + \frac{\sqrt{2}}{2}$;
(b) $1 + \sqrt{2}$;
(c) $1 + \sqrt{2} + \sqrt{3}$.

10.4.4 Bizonyítsuk be, hogy $\mathbb{Q}(\sqrt{d})$ összes algebrai egészeinek $E(\sqrt{d})$ gyűrűjében egy $\varepsilon$ elem akkor és csak akkor egység, ha $N(\varepsilon) = \pm 1$.

Megjegyzés: Ha $\mathbb{Q}(\sqrt{d})$ nem képzetes másodfokú bővítés és $\mathbb{Q}(\sqrt{d}) \neq \mathbb{Q}$, akkor $E(\sqrt{d})$-ban az egységek száma mindig végtelen.

10.4.5 Igazoljuk az alábbi állításokat.
(a) Létezik olyan Gauss-racionális, amely nem Gauss-egész, de a normája egész szám.
(b) Bármely $\mathbb{Q}(\sqrt{d})$ másodfokú bővítésben van olyan $\alpha$ elem, amely nem algebrai egész, de $N(\alpha)$ egész szám.

10.5 Egész bázis

Ebben a pontban $\sqrt{d}$ végig egy tetszőleges $n$-edfokú algebrai számot jelöl.

A T 10.2.3 Tételből tudjuk, hogy minden $\alpha \in \mathbb{Q}(\sqrt{d})$ elem egyértelműen felírható

$$\alpha = a_0 + a_1 \sqrt{d} + \cdots + a_{n-1} \sqrt{d}^{n-1}, \quad a_j \in \mathbb{Q}, \quad j = 0, 1, \ldots, n-1 \quad (1)$$

alakban, azaz az $1, \sqrt{d}, \ldots, \sqrt{d}^{n-1}$ elemek bázis alkotnak $\mathbb{Q}(\sqrt{d})$-ban mint $\mathbb{Q}$ feletti vektortérben.

Az (1) előállításból általában nem olvasható le, hogy $\alpha$ algebrai egész-e vagy sem. A T 10.3.1 és T 10.3.2 Tételben azonban láttuk, hogy másodfokú bővítések esetén létezik olyan $\omega_1, \omega_2$ bázis, amely erre is alkalmas: Minden másodfokú bővítés előáll $\mathbb{Q}(\sqrt{5})$ alakban, ahol $t$ négyzetmentes egész szám és $t \neq 1$, továbbá, ha

$$\omega_1 = 1 \quad \text{és} \quad \omega_2 = \begin{cases} \sqrt{t}, & \text{ha } t \neq 1 \pmod{4}; \\ \left(1 + \sqrt{t}\right)/2, & \text{ha } t = 1 \pmod{4}, \end{cases}$$

akkor a $\mathbb{Q}(\sqrt{5})$ minden $\alpha$ eleme egyértelműen felírható

$$\alpha = r_1 \omega_1 + r_2 \omega_2, \quad r_1, r_2 \in \mathbb{Q}$$

alakban, és $\alpha$ akkor és csak akkor algebrai egész, ha $r_1$ és $r_2$ egész számok.

Tetszőleges $\mathbb{Q}(\sqrt{d})$ bővítésben egy ilyen tulajdonságú bázist egész bázisnak nevezünk:

10.5.1 Definíció . \quad D 10.5.1

Egy $\mathbb{Q}(\sqrt{d})$ bővítés $\omega_1, \ldots, \omega_n$ elemeit a $\mathbb{Q}(\sqrt{d})$ egész bázisának nevezzük, ha minden $\alpha \in \mathbb{Q}(\sqrt{d})$ egyértelműen felírható

$$\alpha = r_1 \omega_1 + r_2 \omega_2 + \cdots + r_n \omega_n, \quad r_j \in \mathbb{Q}, \quad j = 1, 2, \ldots, n \quad (2)$$
alakban, és \( \alpha \) akkor és csak akkor algebrai egész, ha mindegyik \( T_j \) egész szám.

Célunk annak igazolása, hogy minden \( \mathbb{Q}(\vartheta) \) bővítésben létezik egész bázis.

Legyen \( \vartheta \) tetszőleges \( n \)-edfokú algebrai szám, és tekintsük a \( \mathbb{Q}(\vartheta) \) bővítést. A világosabb megkülönböztetés érdekében a \( \mathbb{Q}(\vartheta) \)-nak mint \( \mathbb{Q} \) feletti vektortérnek a bázisait \( v \)-bázisoknak, ezek közül az egész bázisokat pedig \( e \)-bázisoknak fogjuk nevezni.

Először vizsgáljuk meg, hogyan dönthető el \( \mathbb{Q}(\vartheta) \) adott \( v \) eleméről, hogy \( v \)-bázis alaknak-e. Legyen \( \alpha_1, \ldots, \alpha_n \in \mathbb{Q}(\vartheta) \),

\[
a_i = f_i(\vartheta), \quad \text{ahol} \quad f_i \in \mathbb{Q}[x], \quad d_{i-1} f_i \leq n-1 \quad \text{vagy} \quad f_i = 0, \quad i = 1, \ldots, n, \quad (3a)
\]

azaz

\[
\alpha_k = a_{0k} + a_{1k} \vartheta + \cdots + a_{n-1, k} \vartheta^{n-1}, \quad a_{ki} \in \mathbb{Q}, \quad 0 \leq k \leq n-1, \quad 1 \leq i \leq n. \quad (3b)
\]

Tekintsük a \( \mathbb{Q}(\vartheta) \) vektortérnek azt az \( \mathcal{A} \) lineáris transzformációját, amely az \( 1, \vartheta, \ldots, \vartheta^{n-1} \) v-bázis elemeinek rendre megfelelteti az \( \alpha_1, \ldots, \alpha_n \) „vektorokat”. Ekkor az \( \mathcal{A} \) transzformációnak az \( 1, \vartheta, \ldots, \vartheta^{n-1} \) v-bázisban felírt mátrixa

\[
\mathcal{A} = \begin{pmatrix}
\alpha_{01} & \alpha_{02} & \cdots & \alpha_{0n} \\
\alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\
\vdots & \vdots & \ddots & \vdots \\
\alpha_{n-1,1} & \alpha_{n-1,2} & \cdots & \alpha_{n-1,n}
\end{pmatrix}, \quad (4)
\]

ahol az \( \alpha_{ki} \) elemek a (3b)-ben szereplő racionális számok.

Az \( \mathcal{A} \) transzformáció és az \( \mathcal{A} \) mátrix segítségével könnyen meghatározhatjuk, mikor alkotnak az \( \alpha_1, \ldots, \alpha_n \) vektorek \( v \)-bázist: akkor és csak akkor, ha \( \mathcal{A} \) invertálható, azaz \( \det \mathcal{A} \neq 0 \).

Vegyük észre, hogy az \( \mathcal{A} \) mátrix segítségével az \( \alpha_1, \ldots, \alpha_n \) számokat a következőképpen is megkaphatjuk:

\[
\begin{pmatrix}
\alpha_1 \\
\alpha_2 \\
\vdots \\
\alpha_n
\end{pmatrix} = \mathcal{A}^T \begin{pmatrix}
1 \\
\vartheta \\
\vdots \\
\vartheta^{n-1}
\end{pmatrix}, \quad (3c)
\]

ahol \( \mathcal{A}^T \) az \( \mathcal{A} \) mátrix transzponáltját jelöli.

Az \( e \)-bázis létezésének igazolásához az \( \mathcal{A} \) mátrix helyett egy vele szoros kapcsolatban álló mátrix determinánsának a négyzetét, az ún. diszkrimináns fogjuk felhasználni.

Legyen \( V \) a \( \vartheta \) \( \mathbb{Q} \) feletti konjugáltjai által generált Vandermonde-mátrixa:

\[
V = V(\vartheta(1), \vartheta(2), \ldots, \vartheta(n)) = \begin{pmatrix}
1 & 1 & 1 & \cdots & 1 \\
\vartheta(1) & \vartheta(2) & \vartheta(3) & \cdots & \vartheta(n) \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\vartheta^{n-1}(1) & \vartheta^{n-1}(2) & \vartheta^{n-1}(3) & \cdots & \vartheta^{n-1}(n)
\end{pmatrix}, \quad (5)
\]

és
\[ \hat{A} = A^T V. \] (6)

Ekkor az \( \hat{A} \) mátrix \( i \)-edik sorának \( j \)-edik eleme az \( A \) \( i \)-edik és a \( Vj \)-edik oszlopának a skaláris szorzata, azaz

\[ a_{ij} + a_{i1} \vartheta_{j1} + \cdots + a_{i(n-1)} \vartheta_{j(n-1)}^{-1}. \] (7)

Vegyük észre, hogy a (7)-beli összeg (3a)–(3b) alapján éppen az \( \alpha_i \) szám \( j \)-edik relatív konjugáltja, \( f_i(\vartheta_j) \).

Az \( \alpha_1, \ldots, \alpha_n \) számok \( \Delta(\alpha_1, \ldots, \alpha_n) \) diszkriminánsán az \( \hat{A} \) mátrix determinánsának a négyzetét értjük:

10.5.2 Definíció . D 10.5.2

Tekintsük a \( \mathbb{Q}(\sqrt[d]{d}) \) bővítést, ahol \( d = \alpha \), és jelölje a \( \sqrt[d]{d} \) konjugáltjait \( \vartheta_{(1)}, \vartheta_{(2)}, \ldots, \vartheta_{(n)} \).

Az \( \alpha_1, \ldots, \alpha_n \in \mathbb{Q}(\sqrt[d]{d}) \) számok \( \Delta(\alpha_1, \ldots, \alpha_n) \) diszkriminánsa az \( \hat{A} \) mátrix determinánsának a négyzete, azaz a (3a)–(6) jelöléseket és (7)-et is figyelembe véve

\[ \Delta(\alpha_1, \ldots, \alpha_n) = \det(A^T V)^2 = \begin{vmatrix} f_1(\vartheta_{(1)}) & f_2(\vartheta_{(2)}) & \cdots & f_n(\vartheta_{(n)}) \\ f_1(\vartheta_{(1)}) & f_2(\vartheta_{(2)}) & \cdots & f_n(\vartheta_{(n)}) \\ \cdots & \cdots & \cdots & \cdots \\ f_1(\vartheta_{(1)}) & f_2(\vartheta_{(2)}) & \cdots & f_n(\vartheta_{(n)}) \end{vmatrix}. \]

A diszkrimináns legfontosabb tulajdonságait az alábbi tételben foglaljuk össze:

10.5.3 Tétel . T 10.5.3

(i) A \( \Delta(\alpha_1, \ldots, \alpha_n) \) diszkrimináns racionális szám, és ha az \( \alpha_i \)-k algebrai egészek, akkor egész szám.

(ii) \( \alpha_1, \ldots, \alpha_n \) akkor és csak akkor v-bázis, ha \( \Delta(\alpha_1, \ldots, \alpha_n) \neq 0 \).

(iii) Ha \( C \) egy \( n \times n \)-es racionális elemű mátrix és

\[ \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix} = C \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}, \]

akkor

\[ \Delta(\beta_1, \ldots, \beta_n) = \det C^2 \Delta(\alpha_1, \ldots, \alpha_n). \]

Bizonyítás: (i) A diszkrimináns a \( \vartheta_{(i)} \)-knek szimmetrikus polinomja: két \( \vartheta_{(i)} \) cseréje a determinánsbán két oszlop cseréjét jelenti, a determináns tehát ekkor előjelet vált, és így a négyzete nem változik. Ebből a már többször (a T 9.3.1, a T 9.3.6 vagy a T 10.4.3 Tétel bizonyításában) láttott módon következik, hogy a diszkrimináns racionális szám.

Ha mindegyik \( \alpha_i \) algebrai egész, akkor a konjugáltjaiak, és így a relatív konjugáltjaiak is algebrai egészek. A diszkriminánszt ezekből az összeadás, kivonás és szorzás segítségével kapjuk, és mivel az algebrai egészek gyűrűt alkotnak, ezért a diszkrimináns is algebrai egész. A diszkrimináns ekkor tehát olyan racionális szám, amely algebrai egész, és így szükségképpen egész szám.
(ii) A determinánsok szorzástétele szerint

\[ \Delta(\alpha_1, \ldots, \alpha_n) = (\det A)^2 (\det V)^2. \]

Mivel a \( V \) Vandermonde-mátrix generátoreleme között nincs két azonos, ezért \( \det V \neq 0 \). Így

\[ \Delta(\alpha_1, \ldots, \alpha_n) \neq 0 \iff \det A \neq 0. \]

Azt pedig már igazoltuk, hogy \( \alpha_1, \ldots, \alpha_n \) akkor és csak akkor v-bázis, ha \( \det A \neq 0 \).

(iii) A (3c) összefüggés alapján

\[
\begin{pmatrix}
\alpha_1 \\
\alpha_2 \\
\vdots \\
\alpha_n
\end{pmatrix} = A^T \begin{pmatrix}
1 \\
\phi \\
\vdots \\
\phi^{n-1}
\end{pmatrix} \quad \text{és} \quad \begin{pmatrix}
\beta_1 \\
\beta_2 \\
\vdots \\
\beta_n
\end{pmatrix} = B^T \begin{pmatrix}
1 \\
\phi \\
\vdots \\
\phi^{n-1}
\end{pmatrix}.
\]

Így

\[
\begin{pmatrix}
\beta_1 \\
\beta_2 \\
\vdots \\
\beta_n
\end{pmatrix} = C \begin{pmatrix}
\alpha_1 \\
\alpha_2 \\
\vdots \\
\alpha_n
\end{pmatrix} = C A^T \begin{pmatrix}
1 \\
\phi \\
\vdots \\
\phi^{n-1}
\end{pmatrix},
\]

vagyis (a \( \beta_i \)-khez tartozó \( B \) mátrix egyértelműsége miatt) \( B^T = C A^T \). Ebből következik, hogy

\[
\Delta(\beta_1, \ldots, \beta_n) = (\det(B^T V))^2 = (\det(C A^T V))^2 = (\det C)^2 (\det(A^T V))^2 = (\det C)^2 \Delta(\alpha_1, \ldots, \alpha_n).
\]

Most már rátérhetünk az e-bázis létezésének a bizonyítására.

**10.5.4 Tétel**

Tetszőleges \( \phi \) algebrai szám esetén \( \mathbb{Q}(\phi) \)-ban létezik egész bázis.

**Bizonyítás:** Először megállapítsuk az e-bázisok néhány olyan tulajdonságát, amelyek majd támpontot nyújtanak ahhoz, hogy a v-bázisok közül ki tudjunk választani e-bázist.

Ha \( \omega_1, \ldots, \omega_n \) e-bázis, akkor mindegyik \( \omega_i \) algebrai egész kell hogy legyen, ugyanis az

\[ \omega_i = 0 \cdot \omega_1 + \cdots + 1 \cdot \omega_i + \cdots + 0 \cdot \omega_n \]

előállításban minden együttható egész szám.

Ha \( \omega_1, \ldots, \omega_n \) e-bázis és \( \beta_1, \ldots, \beta_n \) olyan v-bázis, amelynek az elemei algebrai egészek, akkor mindegyik \( \beta_i \) az \( \omega_j \) bázisvektorok egész együtthatós lineáris kombinációja, azaz létezik olyan \( C \) egész elemű, invertálható mátrix, amelyre

\[
\begin{pmatrix}
\beta_1 \\
\beta_2 \\
\vdots \\
\beta_n
\end{pmatrix} = C \begin{pmatrix}
\omega_1 \\
\omega_2 \\
\vdots \\
\omega_n
\end{pmatrix}.
\]

Ekkor a **T 10.5.3/(iii)** Tételből következik, hogy
Mivel \( d \neq 0 \) nullától különböző egész szám, ezért \( |(\alpha \cdot C)|^2 \geq 1 \), és így

\[ |\Delta(\beta_1, \ldots, \beta_n)| \geq |\Delta(\omega_1, \ldots, \omega_n)|. \]

Ez azt jelenti, hogy egy \( e \)-bázis diszkriminánsának abszolút értéke kisebb vagy egyenlő, mint egy algebrai egészekből álló tetszőleges \( v \)-bázis diszkriminánsának az abszolút értéke.

Ennek megfelelően \( e \)-bázis csak egy olyan \( v \)-bázis lehet, amelynek az elemei algebrai egészek, és a diszkriminánsának abszolút értéke az ilyen típusú \( v \)-bázisok közül a legkisebb.

Igazolni fogjuk, hogy ilyen tulajdonságú \( v \)-bázis létezik, és az valóban egyben \( e \)-bázis is.

Először megmutatjuk, hogy létezik olyan \( v \)-bázis, amelynek az elemei algebrai egészek. Legyen \( \gamma_1, \ldots, \gamma_n \) tetszőleges \( v \)-bázis. A 9.6.6 feladat [316] szerint mindegyik \( \gamma_i \) felírható \( \gamma_i = \alpha_i / c_i \) alakban, ahol \( \alpha_i \) algebrai egész és \( c_i \neq 0 \) egész szám. Ekkor nyilván \( \alpha_1, \ldots, \alpha_n \) is \( v \)-bázis.

Tekintsük az összes olyan \( v \)-bázist, amelynek az elemei algebrai egészek. Minden ilyen \( v \)-bázis diszkriminánsa a T 10.5.3/(i)–(ii) Tétel szerint 0-tól különböző egész szám. Vegyünk ezek közül egy olyan \( \omega_1, \ldots, \omega_n \) \( v \)-bázist, amelyre a diszkrimináns abszolút értéke a legkisebb. Belátjuk, hogy \( \omega_1, \ldots, \omega_n \) egyben \( e \)-bázis is.

Ehhez azt kell igazolni, hogy egy \( \alpha \in \mathbb{Q}(\sqrt{d}) \) elem akkor és csak akkor algebrai egész, ha a (2) szerinti

\[ \alpha = r_1 \omega_1 + r_2 \omega_2 + \cdots + r_n \omega_n, \quad r_j \in \mathbb{Q}, \quad j = 1, 2, \ldots, n \]

előállításban mindegyik \( r_j \) egész szám.

Mivel az \( \omega_i \)-k algebrai egészek, ezért ha \( r_1, \ldots, r_n \) egész számok, akkor \( \alpha = \sum_{j=1}^n r_j \omega_j \) is algebrai egész, hiszen az algebrai egészek gyűrűt alkotnak.

Megfordítva, legyen \( \alpha \in \mathbb{Q}(\sqrt{d}) \) tetszőleges algebrai egész. Tegyünk fel indirekt, hogy a (2) szerinti

\[ \alpha = r_1 \omega_1 + r_2 \omega_2 + \cdots + r_n \omega_n \]

előállításban van olyan \( r_i \), például \( r_1 \), amely nem egész szám. Legyen

\[ \beta_1 = \alpha - (r_1 \omega_1 = \{r_1\} \omega_1 + r_2 \omega_2 + \cdots + r_n \omega_n) \quad \text{és} \quad \beta_j = \omega_j, \quad 2 \leq j \leq n. \]

Ez azt jelenti, hogy \( \beta_1, \ldots, \beta_n \) algebrai egészek, és

\[
\begin{pmatrix}
\beta_1 \\
\beta_2 \\
\vdots \\
\beta_n
\end{pmatrix} = C
\begin{pmatrix}
\omega_1 \\
\omega_2 \\
\vdots \\
\omega_n
\end{pmatrix},
\]

ahol

\[
C = \begin{pmatrix}
\{r_1\} & r_2 & r_3 & \cdots & r_n \\
0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 1 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & 1
\end{pmatrix}.
\]
A T 10.5.3/(iii) Tétel alapján
\[ \Delta(\beta_1, \ldots, \beta_n) = \Delta(\omega_1, \ldots, \omega_n)(\det C)^2 = \Delta(\omega_1, \ldots, \omega_n) \{\gamma_1\}^2, \]
e és így \(0 < \{\gamma_1\} < 1\) miatt
\[ 0 < |\Delta(\beta_1, \ldots, \beta_n)| < |\Delta(\omega_1, \ldots, \omega_n)|, \]
ami ellentmond \(|\Lambda(\omega_1, \ldots, \omega_n)|\) minimalitásának. 

Megjegyzések:
1. A fenti bizonyításból kiderült, hogy \(\mathbb{Q}(d)\) -ban bármely két egész bázis diszkriminánsának az abszolút értéke megegyezik. Ennél több is igaz: maguk a diszkriminánsok is egyenlők, lásd a 10.5.2b feladatot [348]. Ezt a közös értéket a \(\mathbb{Q}(d)\) bővítés diszkriminánsának nevezzük.
2. A T 10.5.4 Tételre adott bizonyításunk csak egzisztenciabizonyítás, egész bázis konkrét előállítására nem alkalmas.
3. A másodfokú bővítésekben a T 10.3.2 Tétel alapján kaphatunk egész bázist, magasabb fokú bővítések esetén azonban lényegesen nehezebb egész bázist konstruálni. Megmutatható például, hogy ha \(\sqrt[p]{d}\)-edik primitív egységgyök, ahol \(p > 2\) primszám, akkor \(1, \sqrt[3]{d}, \ldots, \sqrt[p-2]{d}\) egész bázist alkotnak \(\mathbb{Q}(\sqrt[p]{d})\) -ban.

Feladatok

10.5.1 Számítsuk ki a \(\mathbb{Q}(d)\) bővítésben a \(\Lambda(1, \sqrt[p]{d}, \ldots, \sqrt[p-1]{d})\) diszkriminánsát a következő \(d\) számok esetén:
(a) \(d\) ;
(b) \(e^{\cos(2\pi/3)} + i\sin(2\pi/3)\) ;
(c) \(\sqrt{2}\) ;
(d) \(\sqrt[3]{2}\).

10.5.2 Tekintsünk egy rögzített \(\mathbb{Q}(d)\) bővítést, ahol \(\deg d = \nu\). Bizonyítsuk be az alábbi állításokat.
(a) Ha \(\omega_1, \ldots, \omega_n\) egész bázis és \(\beta_1, \ldots, \beta_n \in \mathbb{Q}(d)\) tetszőleges algebrai egészek, akkor \(\Delta(\omega_1, \ldots, \omega_n) \mid \Delta(\beta_1, \ldots, \beta_n)\).
(b) Bármely két egész bázis diszkriminánsa megegyezik.

10.5.3 Mennyi egy egész bázis diszkriminánsa az egyes másodfokú bővítésekben?

10.5.4 Legyen \(\deg d = \nu\) és \(\alpha_1, \ldots, \alpha_n\) olyan algebrai egészek \(\mathbb{Q}(d)\) -ban, amelyekre \(\Delta(\alpha_1, \ldots, \alpha_n)\) négyzetmentes szám. Bizonyítsuk be, hogy \(\alpha_1, \ldots, \alpha_n\) egész bázis \(\mathbb{Q}(d)\) -ban.

10.5.5 (a) Mi a szükséges és elégséges feltétele annak, hogy \(\mathbb{Q}(i)\) -ben az \(a + bi\) és \(c + di\) Gauss-racionálisok egész bázist alkossanak?
(b) Vizsgáljuk meg a hasonló kérdést az Euler-racionálisok körében is.
10.5.6 (M [613]) Mely másodfokú bővítésekben létezik olyan $\omega_1, \omega_2$ egész bázis, ahol $\omega_2$ az $\omega_1$ $\mathbb{Q}$ feletti konjugáltja?

10.5.7 Legyen $\deg \vartheta = n$, és tegyük fel, hogy az $m_\vartheta$ minimálpolinomnak csak valós gyökei vannak. Lássuk be, hogy ekkor $\mathbb{Q}(\vartheta)$ bármely $\beta_1, \ldots, \beta_n$ elemére $\Delta(\beta_1, \ldots, \beta_n) \geq 0$.

10.5.8 (a) Mutassuk példát arra, hogy a $\Delta(\alpha_1, \ldots, \alpha_n)$ diszkrimináns akkor is lehet nullától különböző egész szám, ha az $\alpha_i$-k között van olyan, amely nem algebrai egész.

(b) Bizonyítsuk be, hogy ha $\mathbb{Q}(\vartheta) \neq \mathbb{Q}$, akkor létezik $\mathbb{Q}(\vartheta)$-ban olyan $\vartheta$-bázis, amelynek egyik eleme sem algebrai egész, de a diszkriminánsa egész szám.
11. fejezet - IDEÁLOK

Az ideálok központi szerepet játszanak a gyűrük vizsgálatánál, ebből mi most csak a számelméleti vonatkozásokkal foglalkozunk. Szükséges és elégséges feltételt adunk arra, hogy egy gyűrűben érvényes legyen a számelmélet alaptétele, majd megmutatjuk, hogy főideálgyűrűben és euklideszi gyűrűben mindig igaz az alaptétel. Ezután az ideálok körében építünk ki százmelméletet, és belátjuk, hogy egy algebrai számtest algebrai egészinek ideáljaira már mindig érvényes az egyértelmű prímfaktorizáció. Ennek alkalmazásaként egy konkrét példán keresztül illusztráljuk, hogy ideálok segítségével olyan diofantikus egyenleteket is kezelni tudunk, ahol a megfelelő bővítés algebrai egészéire nem igaz a számelmélet alaptétele.

11.1 Ideál

Az „ideális számokat” Kummer a Fermat-sejtés hatékonyabb kezeléséhez vezette be a 19. század közepén, erről részletesebben is szó lesz majd a 11.2 pontban. Az „ideális számok”-ból kifejlődött ideálfogalom később a számelméleti vonatkozásoktól függetlenül is a gyűrűelméleti vizsgálatok alapvető eszközévé vált.

11.1.1 Definíció . D 11.1.1

Egy \( \mathcal{R} \) gyűrűben egy nemüres részhalmazt az ideállakjának nevezünk, ha

(A) \( \mathcal{I} \) zárt az \( \mathcal{R} \)-beli összeadásra és ellentettképzésre, azaz

\[
i, j \in \mathcal{I} \implies i + j \in \mathcal{I}, -i \in \mathcal{I};
\]

(B) bármely \( \mathcal{I} \)-beli elem egy tetszőleges \( \mathcal{R} \)-beli elemmel akármelyik oldalról megszorozva ismét \( \mathcal{I} \)-beli elem kapunk, azaz

\[
i \in \mathcal{I}, r \in \mathcal{R} \implies ri \in \mathcal{I}, ir \in \mathcal{I}.
\]

Az ideál fogalma könnyen láthatóan ekvivalens azzal, hogy \( \mathcal{I} \) olyan részgyűrű, ahol egy \( \mathcal{I} \)-beli és egy \( \mathcal{I} \)-n kívüli elem szorzata is \( \mathcal{I} \)-beli.

Példák ideáira:

P1 Az egész számok gyűrűjében (rögzített \( \mathbb{N} \) mellett) az \( \mathbb{N} \)-mel osztható számok.

P2 A racionális együtthatós polinomok gyűrűjében azok a polinomok, amelyeknek egy adott \( \alpha \) komplex szám gyöke.

P3 Az egész együtthatós polinomok gyűrűjében azok a polinomok, amelyeknek a konstans tagja páros szám.

P4 Bármely gyűrűben ideál maga a gyűrű és a csak a nullából álló részhalmaz, ezeket triviális ideáloknek nevezzük. Testben csak a két triviális ideál létezik (lásd a 11.1.3 feladatot [354]).

Mivel az ideálok számelméleti vonatkozásait vizsgáljuk, ezért a továbbiakban az egész fejezetben eleve csak kommutatív, egységelemes, nullaozomentes gyűrűkére szorítkozunk. A gyűrűt (általában továbbra is) \( \mathcal{R} \) -rel jelöljük, és mivel általában a komplex test részgyűrűiről, illetve polinomgyűrűkről lesz szó, ezért az egységelemet 1-gyel fogjuk jelölni.

Az ideálok legegyszerűbb és egyben legfontosabb típusát az egyetlen elem által generált ideálok, más néven főideálok jelentik.
11.1.2 Definíció. D 11.1.2

Legyen \( a \) az \( R \) (kommutatív, egységelemes, nullosztómentes) gyűrű tetszőleges eleme. Ekkor az \( \{ra : r \in R\} \) halmazt az \( a \) által generált főideálynak nevezzük és \( (a) \)-val jelöljük.

Az \( a \) által generált \( (a) \) főideál tehát az \( a \) elem (\( R \)-beli elemekkel képzett) többszöröseiből áll.

A definícióban szereplő „\( a \) által generált” és „ideál” szóhasználat jogosságát az alábbi tétel mutatja:

11.1.3 Tétel. T 11.1.3

Az \( (a) \) főideál az \( a \) elemet tartalmazó legszűkebb ideál, azaz

(i) \( (a) \) ideál \( R \)-ben;

(ii) \( a \in (a) \);  

(iii) ha \( I \) ideál \( R \)-ben és \( a \in I \), akkor \( (a) \subseteq I \).

Bizonyítás: (i) Belátjuk, hogy az \( \{ra : r \in R\} \) nemüres halmaz eleget tesz a D 11.1.1 Definíciónak (a jelölések egyértelműsége érdekében a képletekben szögletes zárójelet használunk közönséges zárójel céljaira, és a kerek zárójelet fenntartjuk az ideál jelölésére):  

\[
r_1a + r_2a = [r_1 + r_2]a; \quad -r_1a = [-r_1]a; \quad \text{és} \quad r_1[a]r_2 = r_1[r_2]a = [r_2r_1]a.
\]

(ii) \( a = 1a \in \{ra : r \in R\} \).

(iii) Ha az \( I \) ideál tartalmazza \( a \)-t, akkor a D 11.1.1 Definíció (B) követelménye szerint minden \( r \in R \)-re \( ra \) -t is tartalmazna kell, azaz valóban \( (a) \subseteq I \).

Az \( R \) gyűrű kommutativitását, illetve az egységelem létezését (i), illetve (ii) igazolásánál használtuk fel (a nullosztómentességre nem volt szükség a bizonyításhoz).

Példák:

A (P4 példában szereplő) két triviális ideál főideál; ezeket az egységelem, illetve a nullelem generálja: \( R = \{1\} \), illetve \( \{0\} = \{0\} \).

Főideál P1 és P2 is: az \( m \)-mel osztható számok \( \mathbb{Z} \)-ben az \( (m) \) főideált, az \( f(\alpha) = 0 \) tulajdonságú polinomok pedig \( \mathbb{Q}[x] \)-ben transzcendens \( \alpha \) esetén a \( \{0\} \), algebrai \( \alpha \) esetén az \( (m_\alpha) \) főideált alkotják (ahol \( m_\alpha \) az \( \alpha \) minimálpolinomja).

A P3 példa viszont nem főideál. Jelöljük \( \overline{I} \)-vel azoknak az egész együtthatós polinomoknak a halmazát, amelyek konstans tagja páros, és tegyük fel indirekt, hogy alkalmaz \( \overline{f} - \text{re} \overline{I} = \{ \overline{f} \} \). Ekkor az \( \overline{I} \) minden eleme, így speciálisan a \( 2 \) is, többszöröse, azaz egész együtthatós polinomszoros \( \overline{f} \)-nek. Ebből következik, hogy csak \( \overline{f} = \pm 1, \pm 2 \) lehetséges. Azonban \( \{ \pm 1\} \) az összes egész együtthatós polinomot tartalmazza, \( \{ \pm 2\} \) pedig azokból a polinomokból áll, amelyek minden együtthatója páros, és így ezek a főideálok nem egyenlők \( \overline{I} \)-vel. Ezzel ellentmondásra jutottunk, tehát \( \overline{I} \) valóban nem főideál.

A főideál általánosításaként most bevezetjük a végesen generált ideál fogalmát:

11.1.4 Definíció. D 11.1.4
Legyenek \( a_1, \ldots, a_k \) az \( R \) (kommutatív, egységelemes, nullosztómentes) gyűrű tetszőleges elemei. Ekkor a \( \{ \sum_{j=1}^k r_j a_j | r_j \in R \} \) halmazt az \( a_1, \ldots, a_k \) által generált ideálának nevezzük és \( \langle a_1, \ldots, a_k \rangle \)-val jelöljük.

Egy \( I \) ideál végesen generált, ha léteznek olyan \( a_1, \ldots, a_k \) elemei, amelyekre \( I = \langle a_1, \ldots, a_k \rangle \).

A T 11.1.3 Tétel megfelelője a végesen generált ideálokra is igaz:

11.1.5 Tétel. \( T \) 11.1.5

Az \( \langle a_1, \ldots, a_k \rangle \)-ideál az \( e_j \) elemeket tartalmazó legszűkebb ideál, azaz

(i) \( \langle a_1, \ldots, a_k \rangle \)-ideál \( R \)-ben;

(ii) \( a_j \in \langle a_1, \ldots, a_k \rangle \), \( j = 1, 2, \ldots, k \);

(iii) ha \( I \) ideál \( R \)-ben és \( a_j \in I \), \( j = 1, 2, \ldots, k \), akkor \( \langle a_1, \ldots, a_k \rangle \subseteq I \).

A T 11.1.5 Tétel bizonyítása a T 11.1.3 Tételhez hasonlóan történik, ennek végiggondolását az Olvasóra bízzuk.

Példák:

Nyilván minden föideál végesen (egyetlen elem által) generált ideál.

A P3 példa \( I \) ideálja is végesen generált: \( I = \langle 2, x \rangle \).

Az összes algebrai egész \( E \) gyűrűjében

\[
K = \{ \xi \sqrt{2} \mid \xi \in E, k = 2, 3, 4, \ldots \}
\]

ideál, de nem generálható véges sok elemmel (lásd a 11.1.4 feladatot [354]).

Ha \( \mathfrak{d} \) algebrai szám, akkor \( E(\mathfrak{d}) \) minden ideálja végesen generált (lásd a 11.1.10 feladatot [355]).

A D 11.1.1 Definíció utáni P1 példában láttuk, hogy az egész számok \( \mathbb{Z} \) gyűrűjében az \( \mathfrak{m} \)-mel osztható számok egy \( I \) ideál által alkotnak. Az \( I \) segítségével az \( a \) egész számot tartalmazó (azaz az \( a \) által „reprezentált”) modulo \( m \) maradékosztályt

\[
a + I = \{ \xi + \mathfrak{m} \xi \in I \}
\]

alakban is megadhatjuk. A maradékosztályok összeadását és szorzását a reprezentánsok segítségével értelmeztük, ami az (1) szerinti felirásban a következőket jelenti:

\[
[a + I] + [b + I] = [a + b] + I \quad \text{és} \quad [a + I][b + I] = ab + I.
\]

Be kellett látni, hogy (2) az osztályokra valóban műveleteket definiál, azaz az eredményül kapott osztály egyértelmű, nem független attól, hogy az egyes osztályokból melyik reprezentánsokat választottuk. Ha végiglemezzük ennek a bizonyítását, akkor kiderül, hogy a szóban forgó egyértelműséget éppen \( I \) ideál volt biztosítja. Mindezek alapján a következő általánosítást kapjuk:

11.1.6 Tétel. \( T \) 11.1.6
Legyen $I$ ideál az $\mathbb{Z}/m\mathbb{Z}$ maradékosztálygyűrűben. Ekkor az $I$ szerinti (1) maradékosztályok az $\mathbb{Z}/m\mathbb{Z}$ gyűrű diszjunkt részhalmazai, melyek egyesítése $\mathbb{Z}/m\mathbb{Z}$, és ezek a (2)-ben definiált összeadásra és szorzásra nézve gyűrűt alkotnak. Ezt a gyűrűt az $\mathbb{Z}/I$ -nak az $I$ szerinti maradékosztálygyűrűjének vagy faktorgyűrűjének nevezzük és $\mathbb{Z}/I$ -vel jelöljük.

Ennek megfelelően a modulo $m$ maradékosztályok gyűrűjé éppen az egész számoknak az $(\mathbb{Z}/m\mathbb{Z})$ föideál szerinti faktorgyűrűje, azaz $\mathbb{Z}/(m)$.

A T 11.1.6 Tétel bizonyítását nem részletezzük. Mint jeleztük, az $I$ ideál-tulajdonságaival igazolható az $\mathbb{Z}/I$ -beli műveletek egyértelműsége (valamint az, hogy az (1) osztályok lefedik $\mathbb{Z}/I$ -et, és két ilyen osztály vagy diszjunkt, vagy pedig egybeesik). Az $\mathbb{Z}/I$ -re vonatkozó gyűrűazonosságok az $\mathbb{Z}/I$ megfelelő azonosságából következnek, az $\mathbb{Z}/I$ nulleleme a 0 + $I$ maradékosztály, azaz maga az $I$ ideál, az $a + I$ maradékosztály ellentétje pedig a $[-a] + I$ maradékosztály.

Példa: Tekintsük a racionális együthathós polinomok gyűrűjének az $(\mathbb{Q}[x]/(x^2 - 2))$ föideál szerinti faktorgyűrűjét, azaz a $\mathbb{Q}[x]/(x^2 - 2)$ maradékosztálygyűrűt.

Hasonló megondolásokat alkalmazhatunk, mint az egész számoknál képzett modulo $m$ maradékosztályok, azaz a $\mathbb{Z}/(m)$ faktorgyűrű konstrukciójánál. Most azok a polinomok kerülnek az $(x^2 - 2)$ föideál szerinti maradékosztályba, amelyek ugyanazt a maradéket adják $x^2 - 2$-vel osztva. Ily módon minden maradékosztály egyértelműen jellemezhető egy „maradékkal”, azaz egy legfeljebb elsőfokú $a + bx$ (racionális együthathós) polinommal (idesorolva a 0 polinomot is, amely magát az ideállal reprezentálja).

A maradékosztálygyűrűben tulajdonképpen ezekkel a maradékokkal számolunk, azaz pl. két maradékosztály szorzásakor ezeket a maradékoat összeszorozzuk és vesszük a szorzatnak az $x^2 - 2$-vel való oszta mi maradékot. Ily módon minden polinom $a + bx + cx^2$ jellemezhető egy egy benne megőrizett „ideál”-mal (azaz egy $(a + bx + cx^2)$ maradékosztály).

Ennek megfelelően az összeadást az

$$[a + bx] + [c + dx] = [a + d + c] + [b + e],$$

a szorzást pedig az

$$[a + bx][c + dx] = ac + ad + bc + bd + bx^2 =$$

$$= ac + ad + bd + bc + bx^2 = [ac + bd + bc] + [ad + bd + bx^2],$$

szabály szerint kell végezni, azaz pontosan ugyanúgy, ahogy $\mathbb{Q}(\sqrt{2})$-ben (képzeljünk az „$x$” betű helyére mindenhol „$\sqrt{2}$”-t).

Ez azt jelenti, hogy a $\mathbb{Q}[x]/(x^2 - 2)$ maradékosztálygyűrű izomorf (azaz szó szerinti fordításban „azonos alakú”) a $\mathbb{Q}(\sqrt{2})$ testtel.

A fentiekhez hasonlóan általában is igaz, hogy tetszőleges algebrai $\mathfrak{p}$ esetén $\mathbb{Q}(\mathfrak{p})$ jellemzően maradékosztálygyűrüként: a $\mathbb{Q}(\mathfrak{p})$ test izomorf a $\mathbb{Q}[x]/(\mathfrak{p}x)$ faktorgyűrűvel, lást a 11.1.9 feladatot [355].

Feladatok

11.1.1 Legyen $G$ a Gauss-egészek gyűrűje, és tekintsük $G$ -ben az alábbi tulajdonságú $\alpha = a + bi$ Gauss-egészekből álló részhalmazokat:
IDEÁLOK

(a) $a$ és $b$ páros;
(b) $a \equiv b \pmod{2}$;
(c) $a = b \pmod{3}$;
(d) $2 \mid N(\alpha)$;
(e) $5 \mid N(\alpha)$;
(f) $7 \mid N(\alpha)$.


11.1.2 Tekintsük $\mathbb{Z}[x]$-ben az alábbi tulajdonságú $f$ polinomokból álló részhalmazokat:
(a) $f(1/2) = 0$;
(b) $f(\sqrt{2}) = f(\sqrt{3}) = 0$;
(c) $f(\sqrt{2}) = f(\sqrt{3})$
(d) $f(3)$ páros szám;
(e) $f$ főegyütthatója páros szám vagy $f = 0$.

A megadott halmazok közül melyek alkotnak ideált $\mathbb{Z}[x]$-ben, és ezek (legkevesebb) hány elemmel generálhatók?

11.1.3 Mutassuk meg, hogy egy legalább kételemű, kommutatív, egységelemes, nullosztómentes gyűrű pontosan akkor test, ha csak triviális ideáljai vannak.

11.1.4 Legyen $E$ az összes algebrai egész gyűrűje, és

$$K = \{\xi \sqrt{2} \mid \xi \in E, k = 2, 3, 4, \ldots \}.$$ 

Bizonyítsuk be, hogy $K$ ideál $E$-ben, de nem generálható véges sok elemmel.

11.1.5 Legyenek $\alpha_1, \ldots, \alpha_k$ és $\xi$ az $R$ kommutatív, egységelemes, nullosztómentes gyűrű tetszőleges elemei. Bizonyítsuk be, hogy

$$\langle \alpha_1, \alpha_2, \ldots, \alpha_k \rangle = \langle \alpha_1 - \xi \alpha_2, \alpha_2, \ldots, \alpha_k \rangle.$$ 

11.1.6 Legyen $G$ a Gauss-egészek gyűrűje.

(a) Hány elemük az alábbi főideálok szerinti faktorgegyűrűk, és közülük melyek alkotnak testet:

a1: $(2)$;
a2: $(3)$;
a3: $(2 + i)$?

(b) * Vizsgáljuk meg általánosan is a fenti kérdéseket a $G$ tetszőleges eleme által generált főideálról.
11.1.7 Tekintsük az $E(\sqrt{-5})$ gyűrút.

(a) Mutassuk meg, hogy $E(\sqrt{-5})$-ben $\langle 2, 1 + \sqrt{-5} \rangle$ nem főideál.

(b) Hány eleműek az alábbi ideálok szerinti faktorgyűrűk, és közülük melyek alkotnak testet:

b1: $\langle 2, 1 + \sqrt{-5} \rangle$

b2: $\langle 1 + \sqrt{-5} \rangle$

b3: $\langle 11 \rangle$

11.1.8 (M 614]) (a) Az alábbi faktorgyűrűk közül melyek alkotnak testet:

a1: $\mathbb{R}[x]/(x^2 - 2)$

a2: $\mathbb{R}[x]/(x^2 + 1)$

a3: $\mathbb{C}[x]/(x^2 + 1)$

(b) Legyen $T$ tetszőleges kommutatív test és $f \in T[x]$. Mi a szükséges és elégséges feltétele annak, hogy a $T[x]/(f)$ faktorgyűrű test legyen?

(c) Igazoljuk, hogy a $\mathbb{Z}[x]/(2, x^2 + x + 1)$ faktorgyűrű test.

11.1.9 (*) (a) Legyen $\vartheta$ algebrai szám. Igazoljuk, hogy a $\mathbb{Q}(\vartheta)$ test a $\mathbb{Q}[x]/(\text{min}_\vartheta)$ faktorgyűrűvel izomorf.

(b) Legyen $L$ tetszőleges (kommutatív) test és $f$ egy irreducibilis polinom $L$ felett. Konstruáljunk egy olyan $\overline{M}$ testet, amely rendelkezik az alábbi tulajdonságokkal:

(i) $\overline{M}$ -nek van az $I$ -el izomorf $\overline{I}$ részteste;

(ii) ha $f' \in L[x]$ az a polinom, amelynek az együtthatóit az $f$ együtthatóiból az $L \rightarrow \overline{L}$ izomorfizmus szerint kapjuk, akkor $f'$-nak van egy $\vartheta \in \overline{M}$ gyöke;

(iii) $\overline{M} = \overline{I}(\vartheta)$.

Megjegyzés: Ennek a konstrukciónak az alapján akkor is tudjuk az $L$ -et egy irreducibilis polinom — még nem is létező(!) — gyökével bővíteni, ha nincse eleve adva egy, az $L$ -et tartalmazó test.

11.1.10 (*) (a) Legyen $\vartheta$ algebrai szám és $I \neq \emptyset$ tetszőleges ideál $E(\vartheta)$-ban. Bizonyítsuk be, hogy az $E(\vartheta)/I$ faktorgyűrűnek véges sok eleme van.

(b) Igazoljuk, hogy $E(\vartheta)$ ideáljainak szigorúan növő

$$A_1 \subset A_2 \subset \ldots \subset A_j \subset \ldots$$
lánca nem lehet végtelelen.

(c) Mutassuk meg, hogy $E(\vartheta)$ minden ideálja végesen generált.
Megjegyzés: A T 11.5.9 Tételben bebizonyítjuk, hogy $E(a)$ minden ideálja már két elemmel is generálható.

11.2 Elemi szármelméleti kapcsolatok

Ebben a pontban az ideáloknak az oszthatósággal, az egységekkel és a legnagyobb közös osztóval való kapcsolatát tárgyaljuk.

Az oszthatóság és az egység fogalma bármely $R$ (kommutatív, egységelemes, nullosztómentes) gyűrűben a szokásos módon (az D 1.1.1 és D 1.1.2 Definíciók mintájára) értelmezhető, és általában is érvényesek az egészeknél megszokott (az T 1.1.4 és T 1.1.5 Tételnek megfelelő) elemi tulajdonságok.

Először azt mutatjuk meg, hogy az oszthatóság, illetve az egységek szerepe egyszerűen jellemezhető a főideálok segítségével.

11.2.1 Tétel.  T 11.2.1

Tetszőleges $\bar{R}$ (kommutatív, egységelemes, nullosztómentes) gyűrűben

(i) $a \mid b \leftrightarrow b \in (a) \leftrightarrow (b) \subseteq (a)$;

(ii) az $a$ akkor és csak akkor egységszerese $b$-nek, ha $(a) = (b)$. ◆

Bizonyítás: (i) A három (i)-beli feltétel a főideál definícióját felhasználva a következőképpen fogalmazható át:

$a$ osztója $b$-nek;

$b$ szerepel az $a$ többszörösei között;

a $b$ többszörösei mind megtalálhatók az $a$ többszörösei között,

így a három feltétel ekvivalenciája nyilvánvaló.

(ii) Az (i) rész alapján $(a) = (b)$ azt jelenti, hogy $a \mid b$ és $b \mid a$, ami teljesül, ami azzal ekvivalens, hogy az $a$ a $b$-nek egységszerese (lásd az T 1.1.5/(iii) Tételt). ●

Most rátérünk az ideáloknak és a legnagyobb közös osztó kapcsolatára.

A legnagyobb közös osztó (az D 1.3.2, illetve D 7.4.9 Definíciók mintájára) olyan közös osztót jelent, amely minden közös osztónak többszöröse.

Az egészek, Gauss-egészek vagy Euler-egészek gyűrűjében bármely két elemnek létezik legnagyobb közös osztója, ezt a maradékos osztások véges sorozatából álló euklideszi algoritmus biztosítja.

Egy gyűrűben akkor is létezhet bármely két elemnek legnagyobb közös osztója, ha a gyűrűben nem végezhető el a maradékos osztás, ilyen például az egész együtthatós polinomok gyűrűje (ennek részletesebb elemzésére később visszatérünk).

Vannak azonban olyan gyűrűk is, ahol nincs bármely két elemnek legnagyobb közös osztója, ilyen például az $E(\sqrt{-5})$ gyűrű, ahol a $2 + 2\sqrt{-5}$ és $6$ elemeknek nem létezik legnagyobb közös osztója (lásd a 11.2.4 feladatot [359]).

Végül bármely $\bar{R}$ gyűrűben igaz, hogy ha valamely két elemnek létezik legnagyobb közös osztója, akkor ez egységszerestől eltekintve egyértelmű; ez a legnagyobb közös osztó definíciójából azonnal következik.
Két elem legnagyobb közös osztója a két elem által generált ideállal áll szoros kapcsolatban. A jelölések hasonlósága miatt ebben a fejezetben a és b legnagyobb közös osztóját mindig \( \text{lko}(a, b) \) -vel jelöljük, \( (a, b) \) pedig az a és b elemek által generált ideált jelenti.

Nézzük először az egész számok gyűrűjét. Itt például a \((6, 15)\) ideál a \(6u + 15v\) alakú számok halmaza, ahol u és v tetszőleges egész számok. A lineáris diofantikus egyenletek megoldhatóságáról szóló T 1.3.6 Tétel alapján tudjuk, hogy ez a halmaz megegyezik \( \text{lko}(6, 15) = 3 \) többszöröseinek a halmazával, azaz a \((3)\) főideállal. Az egészek körében ugyanígy általában is igaz, hogy ha \( d = \text{lko}(a, b) \), akkor \( (a, b) = (d) \). Tetszőleges gyűrűben ennél kicsit bonyolultabb a helyzet:

11.2.2 Tétel . \( T 11.2.2 \)

Legyen \( R \) tetszőleges (kommutatív, egységelemes, nullosztómentes) gyűrű. 

(i) Ha \( (a, b) = (d) \), akkor \( d = \text{lko}(a, b) \).

(ii) A \( d = \text{lko}(a, b) \) feltételből \( (a, b) \subseteq (d) \) következik, azonban általában \( (a, b) \neq (d) \).

(iii) \( (a, b) = (d) \) akkor és csak akkor teljesül, ha \( d = \text{lko}(a, b) \) és alakmas \( u, v \in R \) elemekre \( d = au + bv \).

Bizonyítás: (i) Az \( (a, b) = (d) \) feltétel alapján \( a \in (a, b) = (d) \), tehát \( d \mid a \), és ugyanígy \( d \mid b \), azaz \( d \) közös osztója \( a \)-nak és \( b \)-nek.

Legyen \( c \) tetszőleges közös osztó, azaz \( c \mid a \) és \( c \mid b \). Ekkor a T 11.2.1 Tétel szerint \( a \in (c) \) és \( b \in (c) \). Mivel \( (a, b) \) az \( a \) és \( b \) elemet tartalmazó legszűkebb ideál, ezért innen \( (d) = (a, b) \subseteq (c) \), azaz (ismét a T 11.2.1 Tételt használva) \( c \mid d \) következik.

(ii) Ha \( d = \text{lko}(a, b) \), akkor \( d \mid a \) és \( d \mid b \). Ez azt jelenti, hogy \( a \) és \( b \) eleme a \( (d) \) ideálának, és így \( (d) \) tartalmazza az \( a \)-t és \( b \)-t tartalmazó legszűkebb ideált, azaz valóban \( (a, b) \subseteq (d) \).

A következő példa mutatja, hogy egyenlőség nem mindig teljesül: az egész együttáthatós polinomok körében a \( 2 \) és \( x \) polinomok legnagyobb közös osztója 1, ugyanakkor \( (2, x) \neq (1) \) (az előző pontban belátunk, hogy \( (2, x) \) nem is főideál).

A 11.2.4c feladatban [359] egy más jellegű olyan példa szerepel, amikor nem teljesül egyenlőség.

(iii) Ha \( (a, b) = (d) \), akkor \( d = \text{lko}(a, b) \) fennállását már (i)-ben igazoltuk, továbbá ekkor \( d \in (a, b) \), azaz \( d \) definíció szerint felírható alkalmas \( R \)-beli elemekek \( d = au + bv \) alakban.

A megfordításhoz induljunk ki abból, hogy \( d = \text{lko}(a, b) \) és \( d = au + bv \). Az első feltételből (ii) alapján kapjuk, hogy \( (a, b) \subseteq (d) \), a második szerint pedig \( d \in (a, b) \), és így \( (d) \subseteq (a, b) \), azaz valóban \( (a, b) = (d) \).\( \Box \)

Megjegyzés: Számos gyűrű esetén a T 11.2.2 Tétel a

\[ d = \text{lko}(a, b) \iff (a, b) = (d) \]

ekvivalenciára egyszerűsödik. Ilyen tulajdonságú például az egész számok gyűrűje, amint azt a tétel kimondása előtt vázoltuk. Hasonló megjegyzésből adódik, hogy (1) minden olyan gyűrűben érvényes, ahol elvégezhető a maradékos osztás.
Mint már jeleztük, az ideálfogalom először a Fermat-sejtéssel kapcsolatban jelent meg Kummer vizsgálataiban. Ennek megértéséhez tekintsük az

\[ x^p + y^p = z^p \]  

(2)

Fermat-egyenletet, ahol \( p > 2 \) prím szám. Az

\[ x^p + y^p = \prod_{j=0}^{p-1} (x + y \zeta^j), \quad \zeta = \exp\left(\frac{2\pi i}{p}\right) = \cos\left(\frac{2\pi}{p}\right) + i\sin\left(\frac{2\pi}{p}\right) \]  

(3)

ez szorzatát bontás alapján a (2) egyenlet szorzat kapcsolatban áll az \( E(\zeta) \) gyűrű számelméletével.

A (2) és (3) összekapcsolásából adódó

\[ \prod_{j=0}^{p-1} (x + y \zeta^j) = z^p \]  

egyenlet bal oldalán álló szorzat \( p \)-edik hatvány. Azt gondolhatnánk, hogy itt is segítene az a korábban többször sikerrel alkalmazott taktika, hogy megpróbáljuk kimutatni, hogy minden tényező külön-külön is \( p \)-edik hatvány \( E(\zeta) \)-ban, majd belátjuk, hogy az így kapott \( p \) darab \( x + y \zeta^j = \zeta^j \) típusú egyenlet (nemtriviális \( x, y, z \) megoldást feltételezve) együttesen ellentmondásra vezet.

Az egész számok körében tudjuk, hogy ha egy szorzat tényezői páronként relatív prímek és a szorzat \( p \)-edik hatvány, akkor a tényezők külön-külön is \( p \)-edik hatványok egységváltozói. Ugyanez igaz a Gauss-egészek vagy az Euler-egészek körében is, és általában minden olyan gyűrűben, ahol érvényes a számelmélet alaptétele. Az alaptétel hiánya esetén az \( E(\sqrt{-5}) \)-ban \( 3^2 = (2 + \sqrt{-5})(2 - \sqrt{-5}) \), itt a jobb oldal tényezői relatív primékek, azonban nem négyzetszámok egységváltozói (hiszen felbonthatatlan).

Az időben a német Kummer is hasonló utat járta be, ő azonban látta, hogy szükség lenne az alaptételre \( E(\zeta) \)-ban, és azt is iszrevette, hogy ez nem mindig teljesül. Azt is látta, hogy ha bármely két elemnek létezik legnagyobb közös osztója, akkor ebből az alaptétel könnyen levezethető. Ezért azokban az \( E(\zeta) \) gyűrűkben, ahol nem volt érvényes az alaptétel, ott \( E(\zeta) \)-hoz hozzávetett „ideális számokat”: ezek voltak hivatva azon elemek legnagyobb közös osztóját „pótolni”, amelyeknek nem létezett \( E(\zeta) \)-ban legnagyobb közös osztójuk. Kummer azt remélte, hogy az így kibővített halmazban már bármely két elemnek lesz legnagyobb közös osztója, és az alaptétel is teljesül.
Az ideális számok konstrukciójához Kummer a legnagyobb közös osztó alábbi tulajdonságából indult ki. Az egész számok körében tudjuk, hogy ha \( \text{lukk} \{a, b\} = d \), akkor \( d \) többszörösei éppen az \( ax + bv \) alakú számok, és mint jeleztük, ugyanez a helyzet minden \( E(\vartheta) \)-ban is. Ennek alapján rögzített \( \alpha \) és \( \beta \) esetén Kummer az

\[
\{\alpha \xi + \beta \psi \mid \xi, \psi \in E(\vartheta)\}
\]

számhalmazt tekintette az \( \alpha \)-höz és \( \beta \)-höz tartozó ideális számnak; ez mai terminológiával éppen az \( \alpha \) és \( \beta \) által generált \( \langle \alpha, \beta \rangle \) ideál. Ha \( \alpha \)-nak és \( \beta \)-nak létezik \( \delta \) legnagyobb közös osztója, akkor ez a számhalmaz megegyezik a \( \delta \) többszöröseiével, így „azonosítható” \( \delta \)-val. Ha viszont nem létezik \( \text{lukk} \{a, \beta\} \), akkor ezzel az ideális számmal „pótoljuk” a legnagyobb közös osztó hiányát. Ezután Kummer az ideális számok (azaz az ideálok) körében épített ki megfelelő számelméletet (ezzel a 11.4 pontban foglalkozunk), és így jelentős előrehaladást tudott elérni a Fermat-sejtéssel kapcsolatban.

Feladatok

11.2.1 Mutassuk meg, hogy az egész számok gyűrűjében az alábbi részhalmazok főideált alkotnak, és adjuk meg ezek egy-egy generátorelemét:

(a) \( \langle 3 \rangle, \langle 50 \rangle, \langle 75 \rangle \);

(b) \( \langle 20 \rangle \cap \langle 30 \rangle \).

11.2.2 Tekintsük a Gauss-egészek \( \mathbb{G} \) gyűrűjét.

(a) Egy adott nemnulla főideál hányféleképpen generálható egy elemmel?

(b) Hány olyan főideál van, amelynek eleme \( 22 + 6\iota \)?

11.2.3 Legyen \( \mathbb{R} \) tetszőleges kommutatív, egységelemes, nullosztómentes gyűrű, és \( a, b \in \mathbb{R} \).

Mutassuk meg, hogy

\[
a + b \in \langle a \rangle \cap \langle b \rangle \iff \langle a \rangle = \langle b \rangle.
\]

11.2.4 Tekintsük az \( E(\sqrt{-5}) \) gyűrűt.

(a) Bizonyítsuk be, hogy a \( 2 + 2\sqrt{-5} \) és \( 6 \) elemeknek nem létezik legnagyobb közös osztója.

(b) Adjuk meg az összes olyan főideált, amely tartalmazza a \( \langle 2 + 2\sqrt{-5}, 6 \rangle \) ideált.

(c) Mutassunk példát olyan \( \alpha \), \( \beta \) elemre, amelyeknek létezik \( \delta \) legnagyobb közös osztójuk, de \( \langle \alpha, \beta \rangle \neq \langle \delta \rangle \).

11.3 Alaptétes gyűrű, főideálgyűrű, euklideszi gyűrű

Ebben a pontban a számmelélet alapítelének a kérdésével foglalkozunk.

A felbontatlan (más néven irreducibilis) elem, illetve a prim fogalmát tetszőleges \( \mathbb{R} \) (kommutatív, egységelemes, nullosztómentes) gyűrűben ugyanúgy értelmezzük, mint a korábban vizsgált konkrét
gyűrűk esetén (lásd az egész számoknál az D 1.4.1, illetve D 1.4.2, vagy a Gauss-egészeknél a D 7.4.10, illetve D 7.4.11 Definíciókat).

Az, hogy \( R \) -ben érvényes a szármelmélet alaptétele (más néven az egyértelmű primfaktorizáció), a szokásos módon azt jelenti, hogy \( R \) -ben a 0-n és az egységeken kívül minden elem felírható véges sok felbonthatatlan szorzatként, és ez az előállítás a tényezők sorrendjétől és egységjegyeketől eltérhet. Az egyértelmű (lásd például az T 1.5.1 Tétel megfogalmazását).

Mint a könyv különböző fejezetekben számos alkalmalmal rámutattunk, a számelméleti vizsgálataknak (az alkalmazások szempontjából is) az egyik kulcskérdése, hogy egy adott gyűrűben érvényes-e a szármelmélet alaptétele. A \( \mathbb{Z} \) -beli alaptételre az egész számok szármelméletének szinte minden fejezete támaszkodik. Az \( x^2 + y^2 = n \), illetve \( x^3 + y^3 = z^3 \) diofantikus egyenletek vizsgálatánál azt használtuk fel, hogy a Gauss-, illetve Euler-egészeknél érvényes az alaptétel. A 11.2 pontban jeleztük, hogy a Fermat-sejtés bizonyítása lényegesen könnyebben megtörtént, ha bizonyos algebrai számtestek algebrai egészre igaz lenne az alaptétel. A racionális együttható polinomok szármelméletének az alaptételéhez kapcsolódó egyes vonatkozásai fontos szerepet játszottak az algebrai számok vizsgálatánál.

Az alábbiakban először szükséges és elégséges feltételt adunk arra, hogy egy gyűrűben érvényes legyen az alaptétel (T 11.3.1 Tétel). Ezután meghatároztuk, hogy a maradékos osztás elvégezhetetlenségéből mindig következik az alaptétel. Ennek igazolása kissé eltér az egész számoknál, Gauss-egészeknél stb. látott úttól: belátjuk, hogy a maradékos osztás elvégezhetetlensége esetén a gyűrű minden ideálja főideál (T 11.3.5 Tétel), valamint bebizonyítjuk, hogy az ilyen tulajdonságú gyűrűkben mindig igaz az alaptétel (11.3.3 Tétel).

A bizonyítások során számos olyan rész lesz, amely szó szerint megegyezik az egész számoknál látott gondolatmenettel, így ezekre csak utalni fogunk, és nem ismételjük meg őket.

Mielőtt rátérnénk a jelzett általános tételekre, a felbonthatatlan és a prim kapcsolatáról ejtünk még néhány szót. A szármelmélet alaptételének megfogalmazásában a két fogalom közül csak a „felbonthatatlan” szerepel, a „prim”-re nincs szükség. Az alaptétel érvényessége azonban szoros összefüggésben áll a prim és a felbonthatatlan közötti viszonyon.

Minden \( R \) (kommutatív, egészelejes, nullosztómentes) gyűrűben teljesül, hogy egy prim szükségképpen felbonthatatlan, ez az T 1.4.3 Tétel bizonyításának első részében láttott módon igazolható. Az állítás megfordítása nem minden gyűrűben igaz, például \( \mathbb{E}(\sqrt{-5}) \) -ben, ahol nem érvényes a szármelmélet alaptétele, a 2 felbonthatatlan, de nem prim. Láttuk ugyanakkor, hogy az egészek, Gauss-egészek, Euler-egészek gyűrűjében minden felbonthatatlan egyben prim is, és ez volt a döntő lépés a szármelmélet alaptétele egyértelműségi részének a bizonyításához. Az alábbi tételekből kiderül, hogy az alaptétel fellépésének az általános esetben is az egyik lényeges feltétele éppen az, hogy minden felbonthatatlan egyben prim is legyen.

11.3.1 Tétel. T 11.3.1

Egy \( R \) (kommutatív, egészelejes, nullosztómentes) gyűrűben akkor és csak akkor érvényes a szármelmélet alaptétele, ha

(i) föideáloknak szigorúan növő

\[ \langle a_1 \rangle \subset \langle a_2 \rangle \subset \cdots \subset \langle a_i \rangle \subset \cdots \]

lánc nem lehet végzetlen, és

(ii) minden felbonthatatlan elem prim.

Bizonyítás: Először az (i) és (ii) feltételek elégségességét igazoljuk.

Az egyértelműség (ii)-ből pontosan ugyanúgy következik, mint az T 1.5.1 Tételnél az egyértelműségre adott első bizonyításban.

360
A felbonthatósághoz (i)-et használjuk fel. Legyen \( a \) az \( \mathbb{Z} \) -nek tetszőleges, a 0-tól és az egységektől különböző eleme. Első lépésként azt mutatjuk meg, hogy \( a \) -nak létezik felbonthatatlan osztója.

Ha \( a \) felbonhatatlan, akkor készen vagyunk. Ha nem, akkor \( a = a_1 b_1 \), ahol \( a_1 \) és \( b_1 \) egyike sem egység. Ekkor a T 11.2.1 Tétel szerint \( \langle a \rangle \subset \langle a_1 \rangle \), és ítt szigorú tartalmazás áll fenn, hiszen \( b_1 \) nem egység.

Ha \( a_1 \) felbonhatatlan, akkor \( a_1 \) az \( a \) -nak egy felbonhatatlan osztója. Ha \( a_1 \) nem felbonhatatlan, akkor \( a_1 = a_2 b_2 \), ahol \( a_2 \) és \( b_2 \) egyike sem egység. Ekkor \( \langle a_1 \rangle \subset \langle a_2 \rangle \) (szigorú tartalmazással).

Megmutatjuk, hogy a gondolatmenetet hasonlóan folytatva, valamelyik \( a \) már szükségszükségesen felbonhatatlan. Ha ugyanis ez nem teljesülne, akkor

\[
\langle a \rangle \subset \langle a_1 \rangle \subset \cdots \subset \langle a_j \rangle \subset \ldots
\]

főideálokak egy végig, szigorúan növő lánccal jelentené, ami ellentmond (i)-nek. Ezzel igazoltuk, hogy \( a \) -nak létezik felbonhatatlan osztója.

Most belátjuk, hogy \( a \) előáll felbonhatatlanok szorzataként. Ha \( a \) felbonhatatlan, akkor készen vagyunk. Egyébként az előzőek szerint \( a = p_1 \langle a \rangle \), ahol \( p_1 \) felbonhatatlan és \( \langle a \rangle \) nem egység. Mivel \( p_1 \) sem egység, ezért \( \langle a \rangle \subset \langle a_1 \rangle \) (szigorú tartalmazással).

Az eljárást folytatva előbb-utóbb valamelyik \( c_i \) szükségszükségesen egység, ugyanis különből az

\[
\langle a \rangle \subset \langle c_1 \rangle \subset \cdots \subset \langle c_j \rangle \subset \ldots
\]

végig, szigorúan növő főideállánc ellentmondana az (i) feltételnek. Ez azt jelenti, hogy az \( a \) -t felbonhatatlanok szorzataként.

Rátérve a szükségsességre, tegyük fel, hogy \( R \) -ben igaz az alaptétel. Ekkor (ii) pontosan ugyanúgy bizonyítható, mint az 1.5.8 feladat [21] megoldásában.

Végül (i) igazoláshoz tegyük fel indirekt, hogy létezik egy

\[
\langle a_1 \rangle \subset \langle a_2 \rangle \subset \cdots \subset \langle a_j \rangle \subset \ldots
\]

végig, szigorúan növő főideállánc. Itt \( a_0 \neq \emptyset \), és \( a_0, a_1, \ldots \) az \( a \) -nek végig sok olyan osztója, amelyek közül semmilyen kettő sem egységszerezse egymásnak. Ez azonban lehetetlen, mert ha \( a_2 = p_1 \cdots p_k \), ahol a \( p_i \) -k felbonhatatlanok, akkor az alaptétel miatt \( a_2 \) minden osztója (vagy egység, vagy pedig) néhány \( p_i \) szorzatának az egységszerese (illetve ha \( a_2 \) egység, akkor minden osztója is egység).

Megjegyzés: A korábbiakban több olyan példa is szerepelt, ahol a szármelélet alaptételeinek az egyértelműségi része nem teljesült (lásd a T 10.3.5 és T 10.3.6 Tételt, valamint a 11.2 pontban a Fermat-sejtéshez kapcsolódó részt). Könnyű azonban olyan gyűrűre is példát mutatni, ahol a felbonhatatlansággal van baj: az összes algebrai egész \( \mathbb{Z} \) gyűrűjében egyáltalán nem léteznek felbonhatatlanok (lásd a 11.3.1 feladatot [364]), és így a 0-tól és egységektől különböző elemek egyáltalán nem bonthatók fel felbonhatatlanok szorzatára.

Most megmutatjuk, hogy ha \( R \) -ben minden ideál főideál, akkor \( R \) -ben érvényes a szármelélet alaptétele.
11.3.2 Definíció .  D 11.3.2

Egy $R$ (kommutatív, egységelemes, nullosztómentes) gyűrű főideálgyűrű, ha minden ideálja főideál.

11.3.3 Tétel .  T 11.3.3

Főideálgyűrűben érvényes a számfelmélet alaptétele. ♦

Bizonyítás: Megmutatjuk, hogy főideálgyűrűben teljesül a T 11.3.1 Tétel (i) és (ii) feltétele.

(i) Tegyük fel indirekt, hogy létezik egy végtelen, szigorúan növő főideállánc. Egyszerű számolással adódik, hogy $A = \bigcup_{j=1}^{\infty} \langle a_j \rangle$ is ideál (lásd a 11.3.4 feladatot [365]). Mivel $R$ főideálgyűrű, ezért $A$ is főideál, $A = \langle b \rangle$. Ekkor

$$b \in A = \bigcup_{j=1}^{\infty} \langle a_j \rangle$$

miatt van olyan $k$, amelyre $b \in \langle a_k \rangle$, azaz $\langle b \rangle \subseteq \langle a_k \rangle$. Igy

$$A = \langle b \rangle \subseteq \langle a_k \rangle \subseteq \langle a_k+1 \rangle \subseteq \bigcup_{j=1}^{\infty} \langle a_j \rangle = A,$$

ami ellentmondás.

(ii) Először azt igazoljuk, hogy bármely $a$ és $b$ elemek létezik legnagyobb közös osztója. Mivel az $\langle a, b \rangle$ ideál is főideál, azaz $\langle a, b \rangle = \langle d \rangle$, így a T 11.2.2 Tételből következik, hogy $d = \text{lcm} \{a, b\}$.

A legnagyobb közös osztó létezéséből már következik (ii): lásd az T 1.3.4 Tételre az 1.3.11 feladat [14] megoldásában adott bizonyítást, az T 1.3.9 Tétel bizonyítását és végül az T 1.4.3 Tétel bizonyításának II. részét. ♦

Megjegyzések:

1. Létezik olyan gyűrű, amely nem főideálgyűrű, és mégis érvényes benne a számfelmélet alaptétele, a legegyszerűbb ilyen példa $\mathbb{Z}[x]$. A 11.1 pontban láttuk, hogy $\mathbb{Z}[x]$ -ben a $\langle 2, x \rangle$ nem főideál, ugyanakkor $\mathbb{Z}[x]$ -ben igaz az alaptétel (ez visszavezethető a $\mathbb{Z}$-beli és a $\mathbb{Q}$-beli alaptétellel, ugyanis a racionális együtthatós polinomokra vonatkozó Gauss-lemmából következik, hogy egy $\bar{f}$ polinom akkor és csak akkor irreducibilis $\mathbb{Z}$ felett, ha $\bar{f}$ vagy egy olyan konstans, amely primiszám, vagy pedig az $\bar{f}$ együtthatói relatív primek és $\bar{f}$ irreducibilis $\mathbb{Q}$ felett).

2. Az algebrai számtestekben az alaptételes gyűrűk és a főideálgyűrűk egybeesnek: egy algebrai számtestben az algebrai egészek $E(a)$ gyűrűje akkor és csak akkor főideálgyűrű, ha érvényes a számfelmélet alaptétele (lásd a 11.3.9b feladatot [365]).

Végül rátérek a maradékos osztás általános megfogalmazására, és annak igazolására, hogy ha $R$ -ben elvégezhető a maradékos osztás, akkor $R$ főideálgyűrű, tehát (a T 11.3.3 Tétel alapján) $R$-ben érvényes a számfelmélet alaptétele.

11.3.4 Definíció .  D 11.3.4
Egy $R$ (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi gyűrű, ha minden $c \in R$ elemehez hozzá tudunk rendelni egy $f(c)$ nemnegatív egész számot úgy, hogy $f(c) = 0 \iff c = 0$ , továbbá minden $a, b \in R$, $b \neq 0$ esetén létezik olyan $q, r \in R$, hogy

$$a = bq + r \quad \text{és} \quad f(r) < f(b). \tag{1}$$

**Megjegyzések:**
1. Az euklideszi gyűrű definícióját sokában abban a formában is megadni, hogy $R$-ben csak a 0-tól különböző elemekhez rendelünk hozzá egy $f(c)$ nemnegatív egész számot, és ekkor (1)-ben $f(r) < f(b)$ mellett az $r = 0$ lehetőséget is megengedjük. Ez nyilván ekvivalens a D 11.3.4 Definícióval.

2. A D 11.3.4 Definícióban nem szükséges kikötni, hogy az $R$ egységelemes legyen: a maradékos osztás elvégezhetőségéből következik, hogy a gyűrűnek létezik egységeleme (lásd a 11.3.6 feladatot [365]).

3. Az alábbiakban felsorolunk néhány olyan korábban már vizsgált gyűrűt, amelyekben elvégezhető a maradékos osztás. Ezeknél a megfelelő $f$ függvény általában további hasznos tulajdonságokkal is rendelkezett, például $f(ab) = f(a)f(b)$ vagy legalábbis $f(a) \leq f(ab)$ teljesült. Ilyen tulajdonságokat azonban az euklideszi gyűrű definíciójában nem kell kikötni.

**Példák:**

P1 Az egész számoknál az $f(c) = |c|$ választás megfelel, azaz $|r| < |b|$ elérhető. Megjegyezzük, hogy ebben az esetben a hányados és a maradék általában nem egyértelmű, például $a = 33$ és $b = 5$ esetén

$$33 = 6 \cdot 5 + 3 = 7 \cdot 5 + (-2).$$

Az T 1.2.1, illetve T 1.2.1A Tételekben azért szerepeltetettük az $|r| < |b|$ -nél szigorúbb $0 \leq r < |b|$ , illetve $-|b|/2 < r \leq |b|/2$ előírást, hogy a hányados és a maradék egyértelmű legyen. Az egyértelműségnek azonban az alaptétel bizonyítása szempontjából nincs jelentősége.

P2 A Gauss- vagy Euler-egészeknél megfelel $f(c) = N(c)$ . (A T 7.4.8 Tétel bizonyítása során láttuk, hogy a hányados és a maradék általában nem egyértelmű.)

P3 $E(\sqrt{2})$-ben megfelel $f(c) = |N(c)|$ .

P4 Test feletti polinomgyűrűben a fokszám szerint elvégezhető a maradékos osztás. Ahhoz, hogy formailag pontosan eleget tegyünk a D 11.3.4 Definíciónak, legyen $f(0) = 0$ és $f(c) = 1 - \deg c$ , ha $c \neq 0$ .

P5 A véges tizedes törtek is euklideszi gyűrűt alkotnak, lásd az 1.5.5c feladatot [21].

11.3.5 Tétel .

Ha $R$ euklideszi gyűrű, akkor $\bar{R}$ főideálgyűrű.

**Bizonyítás:** Azt kell igazolni, hogy az $\bar{R}$ tetszőleges $I$ ideálja főideál.

Ha $I$ csak a 0-ból áll, akkor $I = \{0\}$ . Egyébként tekintsük $I$ -ben a 0-tól különböző $c$ elemekhez rendelt $f(c)$ értékeket. Mivel ezek pozitív egész számok, így van közöttük legkisebb, legyen ez $f(b)$ (itt a $b(\neq 0)$ elem nem egyértelmű). Megmutatjuk, hogy $I = (b)$ .
Mivel \( b \in I \) , ezért \( \langle b \rangle \subseteq I \). Megfordítva, legyen \( a \) az \( I \) ideál tetszőleges eleme. Azt kell megmutatnunk, hogy \( a \in \langle b \rangle \) , vagyis \( b \mid a \).

Osszuk el \( a \) -t maradékosan \( b \) -vel: létezik olyan \( q, r \in R \) , amelyre (1) teljesül. Mivel \( a, b \in I \) és \( I \) ideál, ezért \( r = a - bq \in I \). Továbbá \( f(b) \) minimalis változ és \( f(r) < f(b) \), így csak \( r = 0 \) lehetséges, azaz valóban \( b \mid a \).

**Megjegyzés:** A T 11.3.5 Tétel megfordítása nem igaz, léteznek olyan föideálgyüűrűk, amelyek nem euklideszi gyűrűk: az algebrai számtestek algebrai egészeiből álló gyűrűk közül bizonyítottan ilyenek az

\[
E(\sqrt{-19}), \quad E(\sqrt{-43}), \quad E(\sqrt{-67}) \quad \text{és} \quad E(\sqrt{-163}) \quad (2)
\]

(lásd a 11.3.10 feladatot [366]).

Általában igen nehéz annak az eldöntése, hogy egy \( R \) gyűrű euklideszi-e vagy sem. Természetesen, ha találunk egy megfelelő \( f \)-et, akkor \( R \) euklideszi gyűrű, ha pedig \( R \)-ben nem érvényes a számlamellet alaptétele vagy \( R \) nem föideálgyüűrű, akkor a T 11.3.3 és T 11.3.5 Tételekből következik, hogy \( R \) nem lehet euklideszi gyűrű sem. Nemigen van támponk azonban, ha egy föideálgyüűrűről akarjuk kimutatni, hogy nem euklideszi. Ekkor ugyanis nemcsak azt kell igazolni, hogy egy adott, esetleg „természetes módon” szóba jövő \( f \) függvény nem teljesíti a D 11.3.4 Definícióban előírt kikötéseket, hanem ezt minden lehetséges \( f \)-re be kell látni.

Vizsgáljuk meg mindezt kicsit behatolban az algebrai számtestek egészeiből álló gyűrűk esetén. A T 11.3.3 Tétel utáni 2. megjegyzésben jeleztük, hogy ha \( E(\vartheta) \)-ban érvényes a számlamellet alaptétele, akkor \( E(\vartheta) \) föideálgyüűrű (lásd a 11.3.9b feladatot [365]). Ami a maradékos osztást illeti, az eddigi konkrét esetekben (Gauss-egészek, Euler-egészek, \( E(\sqrt{2}) \) stb.) ezt a norma abszolút értéke szerint próbáltuk elvégezni. Voltak olyan alaptételes \( E(\vartheta) \) gyűrűk is, amikor ez nem sikerült (lásd a T 10.3.6 Tételt). Ilenkor azonban még mindig nyitva áll annak a lehetősége, hogy valamilyen más \( f \) függvény szerint mégis van maradékos osztás. Ezzel kapcsolatos jelenlegi ismereteink a következő paradox helyzet jellemzi:

(A) ilyen, nem a \( |N(\vartheta)| \) szerinti maradékos osztásnak a létezését egyelőre egyetlen esetben sem sikerült kimutatni;

ugyanakkor

(B) bizonyos mély sejtések azt valószínűsíteni, hogy a másodfokú képzetes számtestektől eltekintve, minden alaptételes \( E(\vartheta) \) euklideszi gyűrű, azaz létezik egy alkalmas \( f \) függvény, amely kielégíti a D 11.3.4 Definíciót (akkor is, amikor \( |N(\vartheta)| \) nem felel meg erre a célra).

A kivételként említett másodfokú képzetes számtestekre megmutatható, hogy ha \( E(\vartheta) \) euklideszi, akkor \( |N(\vartheta)| \) szerint is elvégezhető a maradékos osztás (lásd a 11.3.10 feladatot [366]). Így a T 10.3.6 Tételből következik, hogy a (2)-ben felsorolt négy példa föideálgyüűrű, de nem euklideszi gyűrű.

**Feladatok**

11.3.1 Legyen \( E \) az összes algebrai egész gyűrűje.

(a) Jellemezzük az \( E \) -beli egységeket a minimálpolinomjuk segítségével.
(b) Mutassuk meg, hogy $E$-ben nem léteznek felbonthatlanok, és így nem igaz a szármelmélet alaptétele.

11.3.2 Szármelméleti kérdéseket egy $T$ (kommutatív) testben is vizsgálhatunk (csak ennek nincs sok értelme, amint ez az alábbiakból is kiderül).

(a) Milyen $a, b \in T$ esetén teljesül $a \mid b$?

(b) Mik lesznek $T$-ben az egységek, a felbonthatlanok, illetve a prímek?

(c) Mutassuk meg, hogy $T$-ben érvényes a szármelmélet alaptétele, ráadásul $T$ föideálgyüű, sőt euklideszi gyűűrű.

11.3.3 Legyen $W$ a racionális számoknak a páratlan nevezőjű törtekből álló részhalmaza.

(a) Bizonyítsuk be, hogy $W$-ben egységszerestől eltekintve egyetlen felbonthatatlan elem létezik.

(b) Hol bukik meg $W$-ben az a gondolatmenet, amellyel az egész számok körében végtelen sok prímzám létezését igazoltuk (lásd az T 5.1.1 Tételt).

(c) Mutassuk meg, hogy $W$ euklideszi gyűűrű.

(d) Határozzuk meg $W$ összes ideálját.

11.3.4 Legyenek $I_1 \subseteq I_2 \subseteq \cdots$ tetszőleges ideálok egy $R$ gyűűrűben. Mutassuk meg, hogy ekkor $\bigcup_{n=1}^{\infty} I_n$ is ideál $R$-ben.

11.3.5 (M [616]) Legyen $\overline{R}$ kommutatív, egységegellemes, nullosztómentes gyűűrű. Bizonyítsuk be, hogy az $\overline{R}[x]$ polinomgyűűrű akkor és csak akkor föideálgyüűrű, ha $R$ test.

11.3.6 Mutassuk meg, hogy az euklideszi gyűűrű $D$ 11.3.4 Definíciójában nem szükséges kikötni, hogy $R$ egységegellemes, ez a többi feltételből következik.

11.3.7 Legyen $R$ euklideszi gyűűrű, $f$ egy olyan függvény, amely teljesíti a D 11.3.4 Definíció előírásait és $k$ az $f$ függvény legkisebb pozitív értéke. Melyek igazak az alábbi állítások közül?

(a) Ha $f(c) = k$, akkor $c$ egység.

(b) Ha $c$ egység, akkor $f(c) = k$.

11.3.8 Mutassuk meg, hogy az egész számok körében (nemcsak az abszolút érték, hanem) az alábbi $f$ függvény szerint is elvégezhető a maradékos osztás:

$$f(c) = \begin{cases} 
1 + \log_2 |c|, & \text{ha } c \neq 0; \\
0, & \text{ha } c = 0.
\end{cases}$$

azaz

$$f(0) = 0, \quad f(\pm 1) = 1, \quad f(\pm 2) = f(\pm 3) = 2, \quad f(\pm 4) = f(\pm 5) = f(\pm 6) = f(\pm 7) = 3, \quad \ldots$$

11.3.9 (a)(M [617]) Tegyük fel, hogy az $\overline{R}$ (kommutatív, egységegellemes, nullosztómentes) gyűűrűben érvényes a szármelmélet alaptétele, továbbá minden $\overline{I} \neq 0$ ideábra az $\overline{R}/\overline{I}$ faktorgyüűrűnek véges sok eleme van. Bizonyítsuk be, hogy $\overline{R}$ föideálgyüűrű.
(b) Bizonyítsuk be, hogy ha \( \mathcal{O} \) algebrai és \( \mathbb{E}(\vartheta) \)-ban érvényes a szármelélet alaptétele, akkor \( \mathbb{E}(\vartheta) \) főideálgyűrű.

11.3.10 (M [617]*) Legyen \( t \) negatív négyzetmentes egész szám. Bizonyítsuk be, hogy a \( \mathbb{Q}(\sqrt{\xi}) \) másodfokú képzetes bővítés algebrai egészei akkor és csak akkor alkotnak euklideszi gyűrűt, ha \( t = -1, \ -2, \ -3, \ -7 \) vagy \(-11\).

11.4 Ideálok oszthatósága

Ebben a pontban egy \( R \) (kommutatív, egységelemes, nullosztómentes) gyűrű ideáljai között értelmezünk szorzást, majd ennek segítségével oszthatóságot, ezután pedig áttekintjük az ideálokra ebből adódó szármeléleti fogalmak (legnagyobb közös osztó, felbonthatatlan ideál, primideál) jelentését és fontosabb tulajdonságait.

Mivel az ideálok közötti szármelélet kiépítésével a fő célunk az \( \mathbb{E}(\vartheta) \) gyűrűk további vizsgálata, ezért a fogalmak bevezetése során olyan megszorító feltételekkel is fogunk élni, amelyek \( \mathbb{E}(\vartheta) \) ideáljaira teljesülnek, azonban nem minden \( R \) -ben igazak.

11.4.1 Definíció .

Legyen \( A \) és \( B \) az \( R \) (kommutatív, egységelemes, nullosztómentes) gyűrű két tetszőleges ideálja. Ekkor \( A \) és \( B \) szorzatát a következőképpen értelmezzük:

\[
AB = \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \in A, b_i \in B, i = 1, \ldots, n \right\}
\]

(1)

A két ideál szorzata tehát az \( A \) -beli és \( B \) -beli elemek szorzataiból képzett összes lehetséges (akárhány tagú) összegek halmaza.

Az ideálok szorzásának néhány fontos tulajdonságát az alábbi tételben foglaljuk össze.

11.4.2 Tétel .

(i) Az \( A \) és \( B \) ideálok \( AB \) szorzata a legszükebb ideál, amely az összes \( \alpha \beta \) alakú elemet tartalmazza, ahol \( \alpha \in A \) és \( \beta \in B \).

(ii) Végesen generált ideálok szorzata is végesen generált.

(iii) Főideálok szorzata főideál.

(iv) \( AB \subseteq A \cap B \).

(v) Az \( R \) gyűrű ideáljainak szorzása kommutatív és asszociatív művelet, egységelem az \( \{1\} = R \) triviális ideál:

\[
AB = B \cdot A,
\]

\[
(AB)C = A(BC),
\]

\[
(1)A = A(1) = A.
\]

(2)

Inverze csak az egységelemnek létezik, továbbá

\[
AB = \{0\} \iff A = \{0\} \ \text{va} \ B = \{0\}.
\]

Bizonyítás: (i) A következőket kell igazolni:

(a) \( A B \) ideál;
(b) $a \in A, b \in B \implies ab \in AB$ ;

(c) ha egy $I$ ideál tartalmazza az összes $ab$ alakú elemet, ahol $a \in A$ , $b \in B$ , akkor $AB \subseteq I$ .

(a) Megmutatjuk, hogy $AB$ eleget tesz a D 11.1.1 Definíció előírásainak. Két $\sum_{i=1}^{n} \omega_i b_i$ alakú elem összege nyilván ismét ilyen alakú. Egy ilyen elem ellentettje, illetve egy $r \in R$ elemmel való szorzata átírható a

$$\sum_{i=1}^{n} \omega_i b_i = \sum_{i=1}^{n} (-\omega_i) b_i,$$

illetve

$$r \sum_{i=1}^{n} \omega_i b_i = \sum_{i=1}^{n} (r \omega_i) b_i$$

alakba, és $A$ ideáltulajdonsága miatt $-\omega_i$ , illetve $r\omega_i \in A$ .

(b) Az (1) képletben $n = 1$ esetén éppen az $ab$ alakú elemeket kapjuk.

(c) Ha egy $I$ ideál tartalmazza az $\omega_i \hat{b}$ elemeket, akkor az ideáltulajdonság miatt ezek összegét, azaz minden $\sum_{i=1}^{n} \omega_i \hat{b}_i$ alakú elemet is tartalmaznia kell, tehát valóban $AB \subseteq I$ .

(ii) Megmutatjuk, hogy ha

$$A = (\alpha_1, \ldots, \alpha_k) \quad \text{és} \quad B = (\beta_1, \ldots, \beta_m),$$

akkor

$$AB = (\tilde{\alpha}_1 \beta_1, \alpha_1 \beta_2, \ldots, \alpha_1 \beta_j, \ldots, \alpha_k \beta_m),$$

vagyis az $A$ és $B$ generátorelemeinek szorzatai az $AB$ ideál (egyik lehetséges) generátorrendszerét alkotják.

Az $\alpha_i \beta_j$ elemek definíció szerint elemei $AB$ -nek, így az általuk generált ideál része $AB$ -nek.

A fordított irányú tartalmazáshoz (i) alapján elég azt belátni, hogy minden $ab$ alakú elem, ahol $a \in A$ , $b \in B$ , benne van az $\alpha_i \beta_j$ -k által generált ideálban, vagyis $ab$ felírható az $\alpha_i \beta_j$ elemek $R$ -beli együtthatós kombinációjaként. Ez valóban teljesül, ugyanis (alkalmas $\tau_i$ , $\alpha_j \in R$ elemekkel)

$$ab = \left( \sum_{i=1}^{k} \tau_i \omega_i \right) \left( \sum_{j=1}^{m} \beta_j \alpha_j \right) = \sum_{i=1}^{k} \sum_{j=1}^{m} \omega_i \tau_j \alpha_j \beta_j.$$

(iii) A (ii)-re adott bizonyításból a $k = m = 1$ speciális esetben kapjuk, hogy $\langle \alpha \rangle \langle \beta \rangle = \langle \alpha \beta \rangle$ .

(iv) Az $A$ ideáltulajdonsága miatt bármely $a_i \in A$ és $b_i \in B$ esetén $a_i b_i \subseteq A$ , és így $\sum_{i=1}^{n} \omega_i b_i \subseteq A$ , tehát $AB \subseteq A$ . Ugyanígy kapjuk, hogy $AB \subseteq B$ .

(v) A (2)-ben felsorolt azonosságok azonál következnek az ideálok szorzásának definíciójából (és az $R$ gyűrű tulajdonságaitól).

Az $R = (1)$ egységelem inverze önmaga. Megfordítva, ha az $I$ ideálnak létezik inverze, azaz alkalmas $J$ ideálra $JI = R$ , akkor (iv) alapján $R \subseteq I$ , tehát $I = R$ .

Ha $A = \langle 0 \rangle$ vagy $R = \langle 0 \rangle$ , akkor az $AB$ definíciójában szereplő összes összeg 0, tehát $AB = \langle 0 \rangle$ . Ha viszont $A$ -nak, illetve $B$ -nek létezik egy $a \neq 0$ , illetve $b \neq 0$ eleme, akkor $R$ nullosztómentessége miatt $ab \neq 0$ és $a b \in AB$ , tehát $AB \neq \langle 0 \rangle$ .

∎
IDEÁLOK

Megjegyzések: 1. Az \( A \) és \( B \) ideál elemeiből képzett \( ab \) szorzatok általában nem alkotnak ideált (lásd a 11.4.1a feladatot [371]), ezért kellett \( AB \) definíciójában az ilyen szorzatokból képzett összegeket venni.

2. Az ideálok között (egyelőre) csak szorzást értelmeztünk. Az összeadás is definiálható, ezzel kapcsolatban lásd a T 11.4.5 Tétel utáni 4. megjegyzést. Előrebecsájtuk azonban, hogy ez az összeadás nem rendelkezik a szokásos „jó” tulajdonságokkal (csak a nullelemnek lesz ellentettje), és így az \( \mathbb{R} \) ideáljai az ideálok összeadására és szorzására nézve nem alkotnak gyűrűt.

Példák:

P1 Legyen \( R = \mathbb{Z}[x]\), és \( A \), illetve \( B \) álljon azokból a polinomokból, amelyek konstans tagja páros, illetve osztható 3-mal. Ekkor \( AB \) azoknak a polinomoknak a halmaza, amelyek konstans tagja osztható 6-tal:

\[
AB = (2, x)(3, x) = (6, 2x, 3x, x^2) = (6, 2x, 3x - 2x, x^2) = (6, 2x, x, x^2) = (6, x).
\]

P2 Legyen \( R = E(\sqrt{-5}) \), \( A = (3, 1 + \sqrt{-5}) \) és \( B = (3, 1 - \sqrt{-5}) \). Ekkor \( AB \) a \( (3) \) főideál:

\[
AB = (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}) = (3, 3 + 3\sqrt{-5}, 3 - 3\sqrt{-5}, 6) =
\]

\[
= (3 - 6, 3 - 3\sqrt{-5}, 3 - 3\sqrt{-5}, 6) = (3).
\]

Az ideálok szorzása lehetővé teszi, hogy az \( \mathbb{R} \) gyűrű ideáljai között oszthatóságot értelmezzünk:

11.4.3 Definíció . D 11.4.3

A \( B \) ideál osztója az \( A \) ideálnak, ha létezik olyan \( C \) ideál, amellyel \( BC = A \). Ezt a szokásos módon \( B \mid A \) jelöli. ✿

Megjegyzések: 1. Könnyen adódik, hogy főideálok oszthatósága ekvivalens a generátorelemek (\( \mathbb{R} \)-beli) oszthatóságával:

\[
\{\beta\} \mid \{\alpha\} \iff \beta \mid \alpha.
\]

Sőt, ha \( \beta \neq 0 \) és \( \{\alpha\} = \{\beta\}C \), akkor \( C \) is szükségképpen főideál, \( C = \{\gamma\} \), ahol \( \gamma \) úgy is választható, hogy \( \alpha = \beta \gamma \) teljesüljön (lásd a 11.4.3 feladatot [371]). Ez azt jelenti, hogy az ideálok oszthatósága az \( \mathbb{R} \)-beli oszthatóság általánosításának is tekinthető.

2. Az oszthatóság néhány elemi tulajdonságát a 11.4.2 feladatban [371] tárgyaljuk. Ezek közül külön is kiemeljük, hogy

\[
B \mid A \implies A \subseteq B.
\]

Az előző megjegyzés és a T 11.2.1 Tétel alapján főideálokra (3) megfordítása is érvényes, tetszőleges ideálokra azonban (3) megfordítása általában nem igaz, lásd a 11.4.6 feladatot [372].

A továbbiakban csak olyan \( \mathbb{R} \) gyűrükkel foglalkozunk, amelyekben az ideálok szorzásánál érvényes az egyszerűsítési szabály:

\[
AB = AC, A \neq \{0\} \implies B = C,
\]

valamint igaz (3) megfordítása is:

\[
B \mid A \iff A \subseteq B.
\]
A 11.5 pontban megmutatjuk, hogy a fő vizsgálati irányunkat képező $E(d)$ típusú gyűrük eleget tesznek a (4) és (5) követelmények.

Most két ideál legnagyobb közös osztóját definiáljuk, ez a szokásos módon olyan közös osztót jelent, amely minden közös osztónak többszöröse:

### 11.4.4 Definíció . D 11.4.4

Az $A$ és $B$ ideálak legnagyobb közös osztója a $D$ ideál, ha

1. $D | A$, $D | B$; és
2. ha egy $C$ ideálar $C | A$, $C | B$ teljesül, akkor $C | D$. ♠

### 11.4.5 Tétel . T 11.4.5

Bármely $A$ és $B$ ideálaknak létezik és egyértelmű a $D$ legnagyobb közös osztója, és

$$D = \{a-b \mid a \in A, b \in B\}. \quad (6)$$

**Bizonyítás:** A legnagyobb közös osztó definícióját (5) alapján a tartalmazás segítségével is megfogalmazhatjuk: a legnagyobb közös osztó a legszűkebb olyan ideál, amely $A$-t és $B$-t is tartalmazza. Könnyen adódik (lásd a 11.4.4a feladatot [371]), hogy a (6) képletben szereplő $D$ az egyetlen olyan ideál, amely rendelkezik ezzel a tulajdonsággal. ■

**Megjegyzés:**
1. A bizonyításban megfogalmazott tulajdonsága alapján $D$-t tekinthetjük az $A$ és $B$ ideálak által generált ideáknak. Ennek megfelelően a $D = (A, B)$ jelölés összhangban van mind a legnagyobb közös osztóra, mind pedig a generált ideálról alkalmazott szokásos jelölésmóddal.
2. Ha $A$ és $B$ főideál, $A = (\alpha)$, $B = (\beta)$, akkor a (6) képlet szerint a legnagyobb közös osztók $D = \{r \alpha + s \beta \mid r, s \in R\}$, ami éppen az $(\alpha, \beta)$ ideál. Ez ismét rámutat arra, hogy a két elem által generált ideál a legnagyobb közös osztó fogalom általánosításának tekinthető.
3. Ha $A$ és $B$ végesen generált ideál,

$$A = (\alpha_1, \ldots, \alpha_k) \quad \& \quad B = (\beta_1, \ldots, \beta_n),$$

akkor a (6) képlet szerint a legnagyobb közös osztók

$$D = (\alpha_1, \alpha_2, \ldots, \alpha_k, \beta_1, \beta_2, \ldots, \beta_n),$$

vagyis az $A$ és $B$ generátorelemei együttesen a $D$ ideál (egyik lehetséges) generátorrendszeréi alkotják.

4. A (6) képlet alapján $D$ az $A$ és $B$ ideálak összegeként is felfogható. Még egyszer hangsúlyozzuk, hogy az $\mathcal{R}$ ideáljai erre az összeadásra és a D 11.4.1 Definícióban értelmezett szorzásra nem alkothatók gyűrűt (lásd a 11.4.4b feladatot [371]).

Most ráterünk a felbontatlat ideál és a prímideál fogalmára, ezek tulajdonságairól és kapcsolatára.

Mindkét értelmezés a korábbi felbontatlatil, illetve prim fogalomnak megfelelően történik. Mivel egyedül az (1) = $\mathcal{R}$ ideálról igaz, hogy minden ideálnak osztója (lásd a 11.4.2e feladatot [371]), ezért $\mathcal{R}$ ideáljai körében az (1) az egyetlen egység.

### 11.4.6 Definíció . D 11.4.6
Az  $R$ gyűrű egy nemtriviális (azaz $(0)$-től és $(1)$-től különböző) $F$ ideálja felbonthatlan ideál, ha csak úgy bontható fel két ideál szorzatára, hogy valamelyik tényező $(1)$, azaz

$$F = AB \Rightarrow A = (1) \text{ vagy } B = (1).$$  \hspace{1cm} (7)

A $(4)$ és $(5)$ tulajdonság alapján azonnal adódik, hogy egy $F$ nemtriviális ideál felbonthatatlansága az alábbi két feltétel bármelyikével is ekvivalens (itt $A$ tetszőleges ideálét jelöl): $F$-nek csak triviális osztói léteznek, azaz

$$A \mid F \Rightarrow A = (1) \text{ vagy } A = F,$$  \hspace{1cm} (8)

illetve nem létezik az $F$-et valódi módon tartalmazó nemtriviális ideál, azaz

$$F \subseteq A \subseteq R \Rightarrow A = R \text{ vagy } A = F.$$  \hspace{1cm} (9)

A $(9)$ tulajdonsággal rendelkező ideálokat maximális ideáloknak szokás nevezni (olyan gyűrű esetén is, amikor az $(5)$ feltétel nem teljesül).

11.4.7 Definíció . \hspace{1cm} D 11.4.7

Az $R$ gyűrű egy $P$ nemtriviális ideálja prímideál, ha csak úgy lehet osztója két ideál szorzatának, ha legalább az egyik tényezőnek osztója, azaz

$$P \mid AB \Rightarrow P \mid A \text{ vagy } P \mid B. \hspace{1cm} (10)$$

A prímideál definícióját is átfogalmazhatjuk tartalmazásra $(5)$ alapján: a $(0)$-tól és $(1)$-től különböző $P$ ideál akkor és csak akkor prímideál, ha

$$AB \subseteq P \Rightarrow A \subseteq P \text{ vagy } B \subseteq P.$$  \hspace{1cm} (11)

További ekvivalens megfogalmazást jelent az

$$ab \in P \Rightarrow a \in P \text{ vagy } b \in P.$$  \hspace{1cm} (12)

feltétel. A $(11)$ és $(12)$ tulajdonságok ekvivalenciája akkor is igaz, ha $R$ -ben nem teljesül $(5)$ (lásd a 11.4.7 feladatot [372]), és ebben az esetben ezek valamelyikével szokás a primideált értelmezni.

A $(4)$ és $(5)$ feltételek fennállása esetén a primideálokat megegyeznek a felbonthatatlannak ideálokkal:

11.4.8 Tétel . \hspace{1cm} T 11.4.8

Egy $P$ ideál akkor és csak akkor prímideál, ha felbonthatatlan ideál. 🤩

Bizonyítás: Az T 1.4.3 Tétel bizonyításának a gondolatmenetét követjük. Nyilván feltehetjük, hogy $P$ nemtriviális ideál.

Először tegyük fel, hogy $P$ prímideál, és lássuk be, hogy felbonthatatlan ideál is. Induljunk ki egy $P = AB$ szorzat-előállításból; azt kell igazolnunk, hogy $A = (1)$ vagy $B = (1)$.

Mivel $P = AB$, ezért $P \mid AB$ is igaz. Mivel $P$ prímideál, ezért ebből $P \mid A$ vagy $P \mid B$ következik.

Ha $P \mid A$, akkor alkalmas $C$-vel $A = PC = ABC$. Ezt a nyilvánvaló $A = A(1)$ egyenlőséggel összehasonlítva kapjuk, hogy $ABC = A(1)$, ahonnan az $A \neq 0$ ideálall történő egyszerűsítés után $BC = (1)$ adódik. Ebből következik, hogy $B = (1)$ és $C = (1)$.
IDEÁLOK

A $P \mid B$ esetben ugyanígy nyerjük, hogy $A = \{1\}$.

Most tegyük fel, hogy $P$ felbonthatatlan ideál, és lassuk be, hogy prim- ideál is. Induljunk ki egy $P \mid AB$ oszthatóságból; azt kell igazolnunk, hogy $P \mid A$ és $P \mid B$ közül legalább az egyik teljesül.

Ha $P \mid A$, akkor készen vagyunk. Ha $P \nmid A$, akkor $P$ felbonthatatlansága miatt $(P, A) = (1)$.

Mivel $P \mid PB$ és $P \mid AB$, ezért $P \mid (PB, AB)$. A 11.4.4c feladat [371] felhasználásával kapjuk, hogy

$$(PB, AB) = (P, A)B = (1)B = B, \quad \text{és így} \quad P \nmid B.$$ 

Feladatok

Valamennyi feladatban $A$, $B$, illetve $C$ egy $R$ egységelemes, kommutatív, nullosztómentes gyűrű ideáljaik jelölő. A legnagyobb közös osztóval, felbonthatatlan ideálokkal és primideálokkal kapcsolatos feladatoknál — ha mást nem mondunk — eleve feltesszük, hogy $P$-ben érvényes a (4) és (5) tulajdonság is, azaz az ideálokról vonatkozó egyszerűsítési szabály, valamint az oszthatóság és a („fordított irányú”) tartalmazás ekvivalenciája (mint jeleztük, ezek az $E(\delta)$ gyűrükben teljesülnek).

11.4.1 Legyen $H$ az $A$ és $B$ ideálok elemeiből képzett $ab$ szorzatok halmaza: $H = \{ab \mid a \in A, b \in B\}$.

(a) Mutassunk példát arra, hogy $H$ nem feltétlenül ideál.

(b) Bizonyítsuk be, hogy ha $A$ és $B$ közül legalább az egyik főideál, akkor $H$ ideál (és így $H = AB$).

11.4.2 Igazoljuk az ideálok oszthatóságának alábbi elemi tulajdonságait:

(a) Minden $A$ -ra $A \mid A$.

(b) $C \mid B, B \mid A \Longrightarrow C \mid A$.

(c) $B \mid A \Longrightarrow A \subseteq B$.

(d) $A \mid B, B \mid A \Longrightarrow A = B$.

(e) Minden $A$ -ra $B \mid A \iff B = \{1\}$.

11.4.3 Igazoljuk a főideálok oszthatóságára vonatkozó alábbi állításokat:

(a) $(\beta) \mid (\alpha) \iff \beta \mid \alpha$.

(b) Ha $\beta \neq 0$ és $(\alpha) = (\beta)C$, akkor $C$ is szükségképpen főideál, $C = (\gamma)$, ahol $\gamma$ úgy is választható, hogy $\alpha = \beta \gamma$ teljesüljön.

11.4.4 Legyen $D = \{a + b \mid a \in A, b \in B\}$.

(a) Bizonyítsuk be, hogy $D$ a legszűkebb olyan ideál, amely $A$ -t és $B$ -t is tartalmazza.

(b) A $D$ ideált az $A$ és $B$ ideálok összegének tekintve, mutassuk meg, hogy az ideálok összefoglalása kommutatív és asszociatív, nullelem a $(0)$, de ellentétben csak a nullelemek létezik.
IDEÁLOK

Megjegyzés: Az (a) rész alapján \( D \) felfogható az \( A \) és \( B \) által generált ideálnak, és így a tartalmazás és az oszthatóság kapcsolata szerint \( D \) az \( A \) és \( B \) legnagyobb közös osztója (lásd a T 11.4.5 Tételt). Ebben a két szerepkörben \( D \) -re az \( \langle A, B \rangle \) jelölést használjuk. A (b) rész szempontjából a \( D = A + B \) jelölés alkalmazása célszerű.

(c) Igazoljuk az \( A(B, C) = (AB, AC) \) (vagy a másik jelölésmód szerint az \( A(B + C) = AB + AC \) ) disztributivitásai azonosságot.

11.4.5 Defináljuk ideálokra a legkisebb közös többszörös fogalmát, és igazoljuk, hogy a (4) és (5) tulajdonságok fennállása esetén bármely \( A \) és \( B \) ideálaknál egyértelműen létezik az \( M \) legkisebb közös többszöröse, éspedig \( M = A \cap B \).

11.4.6 Mutassunk példát olyan \( A \) és \( B \) ideáira, ahol \( A \subseteq B \), de \( B \nsubseteq A \).

11.4.7 Mutassuk meg, hogy a D 11.4.7 Definíció után szereplő, a primideálokra vonatkozó (11) és (12) tulajdonságok bármely \( R \) (kommutatív, egységelemes, nullosztómentes) gyűrűben ekvivalensek (akkor is, ha \( R \) -ben nem érvényes a (4) és/vagy (5) feltétel).

11.4.8 Tekintsük az \( F(\sqrt{-5}) \) gyűrút.

(a)(M [618]) Határozzuk meg az alábbi ideálok összes osztóját:

\[ a_1: \langle 2, 1 + \sqrt{-5} \rangle ; \]
\[ a_2: \langle 2 \rangle ; \]
\[ a_3: \langle 1 + \sqrt{-5} \rangle . \]

(b) Számítsuk ki az alábbi ideálok legnagyobb közös osztóját:

\[ b_1: \langle 2 \rangle \text{ és } \langle 1 + \sqrt{-5} \rangle ; \]
\[ b_2: \langle 2, 1 + \sqrt{-5} \rangle \text{ és } \langle 3, 1 - \sqrt{-5} \rangle . \]

(c) Döntsük el, hogy az alábbi ideálok közül melyek lesznek felbonthatatlan ideálok:

\[ c_1: \langle 2, 1 + \sqrt{-5} \rangle ; \]
\[ c_2: \langle 2 \rangle ; \]
\[ c_3: \langle 11 \rangle . \]

11.4.9 (M [621]) Melyek igazak az alábbi állítások közül?

(a) Ha \( \alpha \) felbontatlan elem \( R \) -ben, akkor \( \langle \alpha \rangle \) felbontatlan ideál.

(b) Ha \( \langle \alpha \rangle \) felbontatlan ideál, akkor \( \alpha \) felbontatlan elem \( R \) -ben.

(c) Ha \( \alpha \) prímelem \( R \) -ben, akkor \( \langle \alpha \rangle \) primideál.

(d) Ha \( \langle \alpha \rangle \) primideál, akkor \( \alpha \) prímelem \( R \) -ben.

11.4.10 (a) Mutassunk példát arra, hogy \( \mathbb{Z}[x] \) ideáljai között nem érvényes a (4) egyszerűsítési szabály: \( AB = AC \), \( A \neq (0) \neq B - C \).
(b) Bizonyítsuk be, hogy nemnulla föideállal bármely \( R \) (kommutatív, egységelemes, nullosztómentes) gyűrű esetén lehet egyszerűsíteni: Ha \( A = \langle a \rangle \neq \langle 0 \rangle \), akkor \( AB = AC \Rightarrow B = C \).

11.4.11 Tekintsük a nemnegatív racionális kitevőjű, valós együtthatós „polinomok” \( R \) gyűrűjét (ilyen „polinom” például \( 3 + 7x^{4/7} + 11x^{5/9} \)).

(a) Mutassuk meg, hogy \( \tilde{R} \) -ben azok az elemek, amelyekben nem szerepel \( x^n \) tag (azaz a konstans tagjuk 0), egy \( I \) ideált alkotnak.

(b) Bizonyítsuk be, hogy \( I \) csak a következőképpen bontható fel két ideál szorzatára: \( I = (1)I = I(1) = I \cdot I \).

Megjegyzés: A fenti \( I \) ideál eleget tesz a felbonthatatlannak ideáloknak látott (8) és (9) kikötéseken, ezzel együtt az \( I = I \cdot I \) „nemtriviális” felbontással is rendelkezik (ebből is következik, hogy \( \tilde{R} \) -ben nem érvényes a (4) egyszerűsítési szabály). Ilyen és hasonló „furcsaságok” miatt a felbonthatatlanságot (és egyéb számelméleti tartalmú fogalmakat) általában csak olyan gyűrűk ideáljaira szokták vizsgálni, amelyekben érvényes a (4) és (5) tulajdonság.

11.4.12 Legyen \( R \) tetszőleges (kommutatív, egységelemes, nullosztómentes) gyűrű (de a (4) és (5) feltételek érvényességét ebben a feladatban nem követeljük meg). A nemtriviális ideálok körében értelmezzük a maximális ideállal, illetve a prímideál fogalmát a (9), illetve a (12) tulajdonságokkal, kvázi-felbonthatatlan ideálnak pedig egy olyan (nemtriviális) ideált nevezzünk, amely csak úgy bontható két ideál szorzatára, hogy valamelyik tényező önmaga (vö. az előző feladattal).

(a) Bizonyítsuk be, hogy minden prímideál egyben kvázi-felbonthatatlan ideál is.

(b) Mutassunk példát olyan kvázi-felbonthatatlan ideára, amely nem prímideál.

(c) Bizonyítsuk be, hogy minden maximális ideál egyben prímideál (és így kvázi-felbonthatatlan ideál is).

(d) Mutassunk példát olyan prímideára, amely nem maximális ideál.

(e) Bizonyítsuk be, hogy \( I \) akkor és csak akkor maximális ideál, ha az \( \tilde{R}/I \) faktorigyűrű test, illetve \( I \) akkor és csak akkor prímideál, ha \( \tilde{R}/I \) nullosztómentes.

Megjegyzés: A kvázi-felbonthatatlan ideál fogalmát csak a feladat kedvéért vezettük be, viszont a maximális ideálok és a prímideálak az ebben a feladatban adott értelmezés szerinti fogalma tetszőleges gyűrűben fontos szerepet játszik (jelentőségüket a feladat (e) részéből is érzékelhetjük).

11.5 Dedekind-gyűrű

Ebben a pontban \( \mathfrak{d} \) végig algebrai számot jelöl.

Megmutatjuk, hogy \( E(\mathfrak{d}) \) ideáljaira teljesül „a számelmélet alaptétele”, azaz bármely, a \( (0) \)-től és (1)-től különböző ideál prímideálok szorzatára bontható, és ez a felbontás a tényezők sorrendjétől eltérhető egysérelméltő. Az ilyen tulajdonságú gyűrűket Dedekind-gyűrűknek nevezzük.

Először lépésként egy algebrai egész együthatós polinomok szorzatára vonatkozó, önmagában is érdekes eredményt igazolunk (T 11.5.1 Tétel), amely a racionális együthatós polinomokra vonatkozó Gauss-lemma általánosításának is tekinthető (lásd a 11.5.9 feladatot [383]). Ennek felhasználásával bebizonyítjuk, hogy \( E(\mathfrak{d}) \) bármely \( A \neq (0) \) ideáljához található olyan \( B \neq (0) \) ideál, amelyre \( AB \) föideál (T 11.5.5 Tétel). Ebből egyszerűen következik majd az ideálokra vonatkozó egyszerűsítési
szabály (T 11.5.6 Tétel), valamint az ideálok oszthatóságának és a ("fordított irányú") tartalmazásnak az ekvivalenciája (T 11.5.7 Tétel); ezeket a tulajdonságokat kötöttük ki az előző pontban az ideálokkal kapcsolatos általánosabb számelméleti fogalmak vizsgálatánál. Ezután bebizonyítjuk az ideálok egyértelmű primfaktorizációját (T 11.5.8 Tétel). Végül érdekeségként megmutatjuk, hogy \( F(\overline{a}) \) bármely ideálja generálható legfeljebb két elemmel (T 11.5.9 Tétel).

11.5.1 Tétel.

Legyen az

\[
f(x) = a_0 + a_1 x + \cdots + a_m x^m \quad \text{és} \quad g(x) = b_0 + b_1 x + \cdots + b_n x^n
\]

algebrai egész együtthatós polinomok szorzata

\[
f(x)g(x) = \gamma_0 + \gamma_1 x + \cdots + \gamma_{m+n} x^{m+n}.
\]

Tegyük fel, hogy egy \( \delta \) algebrai egészre

\[
\delta \mid \gamma_k, \quad k = 0, 1, \ldots, m + n.
\]

Ekkor

\[
\delta \mid a_i b_j, \quad i = 0, 1, \ldots, m, \quad j = 0, 1, \ldots, n.
\]

Bizonyítás: A bizonyításhoz szükségünk lesz három, egymásra épülő segédtételre.

11.5.2 Lemma.

Egy algebrai egész együtthatós polinom főegyütthatójának és a polinom tetszőleges gyökének szorzata algebrai egész szám.

A L 11.5.2 Lemma bizonyítása: Legyen

\[
l(x) = \lambda_0 + \lambda_1 x + \cdots + \lambda_r x^r = \lambda_r \prod_{i=1}^{r} (x - \xi_i),
\]

és belátjuk, hogy például \( \lambda_r \xi_i \) algebrai egész. A

\[
0 = f(\xi_i) = \lambda_0 + \lambda_1 \xi_i + \cdots + \lambda_r \xi_i^r
\]

eyenlőséget \( \lambda_r^{-1} \)-nel megszorozva kapjuk, hogy

\[
0 = \lambda_0 \lambda_r^{-1} + \lambda_1 \lambda_r^{-2}(\lambda_1 \xi_i) + \cdots + \lambda_{r-1}(\lambda_r \xi_i)^{r-1} + (\lambda_r \xi_i)^r.
\]

Ez azt jelenti, hogy \( \lambda_r \xi_i \) gyöké a

\[
\lambda_0 \lambda_r^{-1} + \lambda_1 \lambda_r^{-2}z + \cdots + \lambda_{r-1} z^{r-1} + z^r
\]

normált, algebrai egész együtthatós polinomnak, és így a T 9.6.3/(iii) Tétel szerint \( \lambda_r \xi_i \) algebrai egész.

11.5.3 Lemma.

Egy algebrai egész együtthatós polinomot bármely gyöktényezőjével leosztva ismét algebrai egész együtthatós polinomot kapunk.
A 11.5.3 Lemma bizonyítása: Legyen \( h \) a (2)-ben megadott polinom, és megmutatjuk, hogy a polinom együtthatói algebrai egészek.

A bizonyítást a \( h \) fokszáma, azaz \( r \) szerinti teljes indukcióval végezzük.

Az állítás \( r = 1 \) esetén igaz: ekkor \( \hat{h}_1(x) \) a \( \lambda_1 \) konstans polinom.

Tegyük fel, hogy az állítás minden legfeljebb \( r - 1 \)-edfokú polinomra igaz. Tekintsük az polinomon. Nyilván \( s(x) \) legfeljebb \( r - 1 \)-edfokú, továbbá \( s(\xi_1) = 0 \), és végül a L 11.5.2 Lemma alapján \( \lambda_1 \xi_1 \) algebrai egész, tehát \( \hat{a}(x) \) algebrai egész együtthatós.

Az indukciós feltétel szerint így az polinom is algebrai egész együtthatós. Mivel \( \lambda_1 \) algebrai egész, ebből következik, hogy \( \hat{h}_1(x) \) együtthatói is algebrai egészek. \( \blacksquare \)

11.5.4 Lemma . L 11.5.4

Egy algebrai egész együtthatós polinom főegyütthatójának és a polinom tetszőleges számú gyökének szorzata algebrai egész szám. \( \blacksquare \)

A 11.5.4 Lemma bizonyítása: Legyen \( h \) a (2)-ben megadott polinom, és megmutatjuk, hogy (például) \( \lambda_1 \xi_1 \ldots \xi_k \) algebrai egész.

Osszuk le \( \hat{h}(x) \)-et a „kimaradó” (azaz a \( k \)-nál nagyobb indexű) gyöktényezőkkel, ekkor a polinomhoz jutunk, amely a L 11.5.3 Lemma (többszörö alkalmazása) alapján algebrai egész együtthatós. Így a \( l(x) \) polinom konstans tagja, azaz

\[ (-1)^k \lambda_1 \xi_1 \ldots \xi_k \]

is algebrai egész. \( \blacksquare \)

Most ráterünk a T 11.5.1 Tétel bizonyítására.

Legyenek az \( f \), illetve \( g \) polinom győkei \( \xi_1, \ldots, \xi_m \), illetve \( \gamma_1, \ldots, \gamma_n \). Ekkor

\[ f(x)g(z) = \sum_{k=0}^{m+n} c_k x^k \prod_{i=1}^{m}(x - \xi_i) \prod_{j=1}^{n}(x - \gamma_j). \quad (3) \]

A (3) egyenlőséget (a T 11.5.1 Tétel állításában szereplő) \( \delta \)-val elosztva kapjuk, hogy...
Az (1) feltétel miatt a (4) bal oldalán álló polinom algebrai egész együththatós. Így a L 11.5.4 Lemma szerint tetszőleges

\[ \sum_{k=0}^{n} \frac{\beta_k}{\delta} x^k = \frac{\alpha \beta_0}{\delta} \prod_{i=1}^{m}(x - \xi_i) \prod_{j=1}^{n}(x - \eta_j). \]  

(4)

Az (1) feltétel miatt a (4) bal oldalán álló polinom algebrai egész együththatós. Így a L 11.5.4 Lemma szerint tetszőleges

\[ \frac{\alpha_0 \beta_0}{\delta} \xi_1 \cdots \xi_m \eta_1 \cdots \eta_n. \]  

(5)

szorzat algebrai egész.

Az \( \mathcal{J} \) polinom tetszőleges \( \alpha \) együththatója a gyöktényezős előállítás alapján úgy keletkezik, hogy bizonyos \( \pm \alpha_0, \xi_1, \ldots, \xi_m \) típusú tagokat összegezünk, és hasonló a helyzet \( \mathcal{G} \)-nél is. Így minden \( \alpha \beta_j \) előáll

\[ \alpha \beta_j = \left( \sum \pm \alpha_0 \xi_1 \cdots \xi_m \right) \left( \sum \pm \beta_0 \eta_1 \cdots \eta_n \right) \]

alakban, azaz

\[ \frac{\alpha \beta_j}{\delta} = \frac{\alpha_0 \beta_0}{\delta} \left( \sum \pm \xi_1 \cdots \xi_m \right) \left( \sum \pm \eta_1 \cdots \eta_n \right). \]  

(5)

A (6) jobb oldala (5) típusú algebrai egészek előjeles összege, tehát algebrai egész. Ezzel beláttuk, hogy a bal oldalon álló \( \alpha \beta_j / \delta \) is algebrai egész. □

Az alábbi, Kroneckertől származó tétel kulcsszerepet játszik ideáljainak vizsgálatánál: a tétel alapján az ideálokkal kapcsolatos számos kérdésre (legalábbis részben) a jóval áttekinthetőbb szerkezetű főideálok segítségével adhatunk választ.

11.5.5 Tétel. T 11.5.5

\( \mathcal{E}(\mathfrak{q}) \) bármely \( \mathcal{A} \neq \{0\} \) ideáljához található olyan \( \mathcal{B} \neq \{0\} \) ideál, amelyre \( \mathcal{AB} \) főideál.

Megjegyzés: A bizonyításból kiderül, hogy olyan \( \mathcal{B} \neq \{0\} \) is választható, amelyre \( \mathcal{AB} = \langle c \rangle \), ahol \( c \) egész szám. Ez a „többlet” azonban a tétel állításából is könnyen levezethető (lásd a 11.5.1 és 11.5.2 feladatot).

Bizonyítás: A 11.1.10c feladat [355] szerint az \( \mathcal{A} \) ideál végesen generált:

\[ \mathcal{A} = \langle \alpha_0, \alpha_1, \ldots, \alpha_k \rangle. \]

Legyenek \( \eta_{(1)}, \eta_{(2)}, \ldots, \eta_{(n)} \) a \( \mathfrak{q} \) \( \mathbb{Q} \)-feletti konjugáltjai (azaz a minimálpolinomjának a gyökei), és jelölje \( f(\eta_{(j)}) \) az \( \alpha \) generátorelem \( j \) -edik relatív konjugaáltját (lásd a 10.4 pontot); speciálisan \( f(\eta_{(1)}) = \alpha \).

Tekintsük az

\[ F_j(x) = f(\eta_{(j)}) + f(\eta_{(j)})x + \cdots + f(\eta_{(j)})x^n, \quad j = 1, 2, \ldots, n \]

polinomokat. (Az \( F_j(x) \) polinomban \( x^j \) együththatója tehát az \( \alpha_j \) generátorelem \( j \) -edik relatív konjugaáltja.) Speciálisan

\[ F_1(x) = \alpha_0 + \alpha_1x + \cdots + \alpha_kx^k. \]
Legyen $G(x) = \prod_{j=1}^t F_j(x)$. A $G(x)$, és így minden együtthatója is szimmetrikus polinomja a $\vartheta_i$ változóknak. Ezért a szimmetrikus polinomok alaptételét és $\vartheta$ minimálpolinomjára a gyökök és együtthatók közötti összefüggéseket felhasználva (a már többször láttott módon) nyerjük, hogy $G(x)$ racionális együtthatós.

Mivel $G(x)$ együtthatóit az $\alpha_i$ algebrai egészekből és szintén algebrai egész relatív konjugáltaikból összeadás és szorzás segítségével kapjuk, ezért $G(x)$ együtthatói algebrai egészek. Az előzőkkel együtt ez azt jelenti, hogy $G(x)$ egész együtthatós,

$$G(x) = a_0 + a_1 x + \cdots + a_{kn} x^{kn}, \quad a_s \in \mathbb{Z}, \quad s = 0, 1, \ldots, kn.$$  

Legyen

$$H(x) = \frac{G(x)}{F_1(x)} = \prod_{j=2}^t F_j(x).$$

Mivel minden $F_j(x)$ algebrai egész együtthatós, ezért $H(x)$ együtthatói is algebrai egészek. Továbbá $G(x)$ és $F_1(x)$ együtthatói $\mathbb{Q}(\vartheta)$-beliek, és a (maradékos) osztási eljárás nem vezet ki az együtthatókat tartalmazó testből, így $H(x)$ együtthatói $\mathbb{Q}(\vartheta)$-beliek. A két megállapítás alapján $H(x)$ együtthatói  $\mathbb{E}(\vartheta)$-ből valók,

$$H(x) = \beta_0 + \beta_1 x + \cdots + \beta_{kn-\vartheta} x^{kn-\vartheta}.$$  

Megmutatjuk, hogy a

$$B = (\beta_0, \beta_1, \ldots, \beta_{kn-\vartheta}) \quad \text{és} \quad c = \operatorname{lko}(a_0, a_1, \ldots, a_{kn})$$

választással $AB = (c)$.

Mivel $c$ a $G \neq 0$ polinom együtthatóinak legnagyobb közös osztója, ezért $c \neq 0$ (és így nyilván $B \neq (0)$).

Először az $AB \subseteq (c)$ tartalmazást igazoljuk. A $c$ definíciója szerint $c$ osztója a $G(x) = F_1(x)H(x)$ polinom minden $\alpha_i$ együtthatójának. Ezért a T 11.5.1 Tétel szerint $c$ mindegyik $\alpha_i\beta_j$ szorzatnak osztója, azaz $\alpha_i\beta_j \mid (c)$. Ebből azonban következik, hogy $AB \subseteq (c)$.

A másik irányú, $(c) \subseteq AB$ tartalmazás igazolásához vegyük észre, hogy a $G(x) = F_1(x)H(x)$, azaz

$$a_0 + a_1 x + \cdots + a_{kn} x^{kn} = (a_0 + a_1 x + \cdots + a_{kn} x^{kn})(\beta_0 + \beta_1 x + \cdots + \beta_{kn-\vartheta} x^{kn-\vartheta})$$

egyenlőség alapján

$$a_s = \sum_{i+j=s} \alpha_i \beta_j \in AB, \quad s = 0, 1, \ldots, kn.$$  

Az egész számok körében a legnagyobb közös osztóra vonatkozó T 1.3.5 Tétel szerint $c$ felírható alkalmas $\mu_s$ egészekkel
IDEÁLOK

\[ c = \sum_{s=0}^{k_n} c_s x_s \]

alakban, ezért

\[ c \in (a_0, a_1, \ldots, a_k) \subseteq A \mathcal{B}, \quad \text{tehát} \quad (c) \subseteq A \mathcal{B}. \]

A kölcsönös tartalmazással beláttuk, hogy valóban \( A \mathcal{B} = (\theta) \).

**11.5.6 Tétel.** \( T \ 11.5.6 \)

\( E(\theta) \) ideáljaira érvényes az egyszerűsítési szabály:

\[ A \mathcal{B} = A \mathcal{C}, A \neq (0) \quad \Rightarrow \quad B = C. \]

**Bizonyítás:** A T 11.5.5 Tétel szerint az \( A \neq (0) \) ideálhoz létezik olyan \( D \neq (0) \) ideál, amelyre \( A \mathcal{D} \) föideál, azaz \( (0, \psi) \in \mathcal{E}(\theta) \)-val \( A \mathcal{D} = (\psi) \) (sőt, \( \psi \) egész számnak is választható).

Az \( A \mathcal{B} = A \mathcal{C} \) egyenlőséget \( D \)-vel megszorozva \( (\psi) \mathcal{B} = (\psi) \mathcal{C} \) adódik. Innen a 11.4.10b feladat [372] alapján következik, hogy \( B = C \).

**11.5.7 Tétel.** \( T \ 11.5.7 \)

\( E(\theta) \) ideáljaira

\[ E(\theta) \mid A \iff A \subseteq D . \]

**Bizonyítás:** A 11.4.2c feladatban [371] láttuk, hogy az \( \Rightarrow \) irány tetszőleges (kommutatív, egységelemes, nullosztómentes) gyűrűben érvényes.

A megfordításhez tegyük fel, hogy \( A \subseteq B \). Nyilván elég a \( B \neq (0) \) esetre szorítkozni. A T 11.5.5 Tétel alapján ekkor létezik olyan \( D \neq (0) \) ideál, amelyre \( B \mathcal{D} = (\psi) \) föideál. Ekkor \( A \mathcal{D} \subseteq B \mathcal{D} = (\psi) \).

Az \( E(\theta) \) gyűrű minden ideálja, így \( A \mathcal{D} \) is végesen generált. Az \( A \mathcal{D} \subseteq (\psi) \) feltétel miatt minden generátorelem osztható \( \psi \)-vel:

\[ A \mathcal{D} = (\gamma_1 \psi, \ldots, \gamma_n \psi) = (\psi)(\gamma_1, \ldots, \gamma_n). \]

Az \( (\gamma_1, \ldots, \gamma_n) \) ideált \( K \)-val jelölve, így

\[ A \mathcal{D} = (\psi)K = B \mathcal{D}K \]

adódik, ahonnan a \( D \neq (0) \) ideálhely megfelelő egyszerűsítve kapjuk, hogy

\[ A = B \mathcal{K}, \quad \text{azaz} \quad B \mid K. \]

A T 11.5.6, illetve T 11.5.7 Tétel szerint \( E(\theta) \) ideáljaira érvényes az egyszerűsítési szabály, illetve az oszthatóság ekvivalens a (fordított irányú) tartalmazással. Ennek megfelelően \( E(\theta) \) ideáljaira érvényesek a 11.4 pontban az ehhez a két tulajdonsághoz kötött eredmények. Ezek közül kijelünk a fellbonthatatlannak ideál és a prímideál ekvivalenciát (T 11.4.8 Tétel). Ez a tény fontos szerepet játszik a következő tételek bizonyításában is: megmutatjuk, hogy \( E(\theta) \) ideáljaira érvényes a szármásmélet alapítétele.

**11.5.8 Tétel.** \( T \ 11.5.8 \)
$E(\emptyset)$ bármely, a $\emptyset$-tól és az $\mathfrak{1}$-től különböző ideálja felbontható véges sok felbonhatatlan ideál szorzatára, és ez a felbontás a tényezők sorrendjétől eltekintve egyértelmű.

Bizonyítás: A bizonyítás szorosan követi a T 11.3.1 Tétel elégségességi részénél látott gondolatmenetet.

Felbonthatóság. Legyen $\mathfrak{a}$ tetszőleges nemtriviális ideál. Első lépésként azt mutatjuk meg, hogy $\mathfrak{A}$-nak létezik olyan osztója, amely felbonthatatlan ideál.

Ha maga az $\mathfrak{A}$ felbonthatatlan ideál, akkor készen vagyunk.

Ha $\mathfrak{A}$ nem felbonthatatlan, akkor $\mathfrak{A} = \mathfrak{A}_1 \mathfrak{B}_1$, ahol $\mathfrak{A}_1 \neq \mathfrak{1}, \mathfrak{B}_1 \neq \mathfrak{1}$. Ekkor $\mathfrak{A} \subset \mathfrak{A}_1$, és itt szigorú tartalmazás áll fenn, hiszen $\mathfrak{A} = \mathfrak{A}_1$ esetén az $\mathfrak{A} (1) = \mathfrak{A} = \mathfrak{A}_1$ egyenlőségből az egyszerűsítési szabály miatt $(1) = \mathfrak{B}_1$ következne.

Ha $\mathfrak{A}_1$ felbonthatatlan, akkor $\mathfrak{A}_1$ az $\mathfrak{A}$-nak egy felbonthatatlan osztója. Egyébként $\mathfrak{A}_1 = \mathfrak{A}_2 \mathfrak{B}_2$, ahol $\mathfrak{A}_2 \neq \mathfrak{1}, \mathfrak{B}_2 \neq \mathfrak{1}$. Ekkor $\mathfrak{A}_1 \subset \mathfrak{A}_2$ (szigorú tartalmazással).

A gondolatmenetet hasonlóan folytatva valamelyik $\mathfrak{A}_i$ már szükségképpen felbonthatatlan ideál, ugyanis ellenkező esetben az

$$\mathfrak{A} \subset \mathfrak{A}_1 \subset \mathfrak{A}_2 \subset \cdots \subset \mathfrak{A}_j \subset \cdots$$

szigorúan növő végleten ideálláncot kapnánk, ami ellentmond a 11.1.10b feladat [355] állításának.

Most belátjuk, hogy $\mathfrak{A}$ előáll felbonthatatlan ideálok szorzataként. Ha $\mathfrak{A}$ felbonthatatlan, akkor készen vagyunk. Egyébként az előzőek szerint $\mathfrak{A} = \mathfrak{A}_1 \mathfrak{C}_1$, ahol $\mathfrak{A}_1$ felbonthatatlan ideál és $\mathfrak{C}_1 \neq (1)$. Mivel $\mathfrak{A}_1 \neq (1)$, ezért $\mathfrak{A} \subset \mathfrak{C}_1$ (szigorú tartalmazással).

Ha $\mathfrak{C}_1$ felbonthatatlan, akkor az $\mathfrak{A} = \mathfrak{A}_1 \mathfrak{C}_1$ felírásban mindkét tényező felbonthatatlan, tehát készen vagyunk. Egyébként $\mathfrak{C}_1 = \mathfrak{A}_2 \mathfrak{B}_2$, ahol $\mathfrak{B}_2 \neq (1)$. Mivel $\mathfrak{A}_1 \subset \mathfrak{A}_2$ (szigorú tartalmazással).

Az eljárást folytatva előbb-utóbb valamelyik $\mathfrak{C}_i = (1)$, ugyanis különben az

$$\mathfrak{A} \subset \mathfrak{C}_1 \subset \cdots \subset \mathfrak{C}_j \subset \cdots$$

végleten, szigorúan növő ideállánc ellentmondana a 11.1.10b feladat állításának. Ez azt jelenti, hogy $\mathfrak{A}$-et előállítottuk felbonthatatlan ideálok szorzataként.

Egyértelműség: Tegyük fel indirekt, hogy valamely $\mathfrak{A}$-nak létezik (legalább) két lényegesen különböző felbontása felbonthatatlan ideálak szorzataként:

$$\mathfrak{A} = \mathfrak{P}_1 \mathfrak{P}_2 \cdots \mathfrak{P}_r = \mathfrak{Q}_1 \mathfrak{Q}_2 \cdots \mathfrak{Q}_s, \quad (7)$$

Ha itt valamelyik $\mathfrak{P}_i$ megegyezik valamelyik $\mathfrak{Q}_i$-vel, akkor az egyszerűsítési szabály miatt ezzel a közös tényezővel egyszerűsíthetünk. Így feltehetjük, hogy a (7)-beli előállításban $\mathfrak{P}_i \neq \mathfrak{Q}_j$.

(7)-ből kapjuk, hogy $\mathfrak{P}_1 | \mathfrak{Q}_1 \mathfrak{Q}_2 \cdots \mathfrak{Q}_s$. Mivel $\mathfrak{P}_1$ felbonthatatlan ideál, így a T 11.4.8 Tétel alapján primideális, ezért $\mathfrak{P}_1$ szükségképpen osztója legalább az egyik $\mathfrak{Q}_j$ tényezőnek.

Azonban ha $\mathfrak{P}_1 | \mathfrak{Q}_j$, akkor $\mathfrak{Q}_j$ felbonthatatlansága miatt $\mathfrak{P}_1 \neq (1)$ vagy $\mathfrak{P}_1 = \mathfrak{Q}_j$, és mindkettő lehetetlen.∎
IDEÁLOK

PÉLDA: Bontsuk fel \( E(\sqrt{-5}) \)-ben a (6) főideált felbonthatatlan ideálok szorzatára.

Korábban láttuk, hogy \( E(\sqrt{-5}) \)-ben a 6 két lényegesen különböző módon is előáll felbonthatatlan elemek szorzataként:

\[
6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).
\]

Ennek megfelelően a (6) főideál is kétféleképpen bomlik főideálok szorzatára:

\[
(6) = (2)(3) = (1 + \sqrt{-5})(1 - \sqrt{-5}).
\]

Itt mindegyik tényező tovább bontható két felbonthatatlan ideál szorzatára:

\[
(2) = (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5}) = (2, 1 + \sqrt{-5})^2;
\]

\[
(3) = (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5});
\]

\[
(1 + \sqrt{-5}) = (2, 1 + \sqrt{-5})(3, 1 + \sqrt{-5}) ;
\]

\[
(1 - \sqrt{-5}) = (2, 1 - \sqrt{-5})(3, 1 - \sqrt{-5}).
\]

Így a (6) főideál a következőképpen áll elő felbonthatatlan ideálok szorzataként:

\[
(6) = (2, 1 + \sqrt{-5})^2(3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}).
\]

Vegyük észre, hogy a fellépő felbonthatatlan ideálok tulajdonképpen a 6 elemnek a felbonthatatlan tényezőkre való kétféle felbontásából származnak: például a \( (3, 1 + \sqrt{-5}) \) ideál úgy is elfoghatjuk mint a bal oldali 3 és a jobb oldali \( 1 + \sqrt{-5} \) tényezőben „ideális számként megbújó közös osztót”, és tulajdonképpen az ilyen „rejtett tényezők” segítségével finomítottuk a fenti két különböző felbontást a (6) főideálakn egy közös felbontásává.

A továbbiakban a felbonthatatlan ideál és a primideál ekvivalenciája alapján mindkét fogalomra a primideál elnevezést fogjuk használni.

A T 11.5.8 Tétel alapján bevezethetjük az ideálok kanonikus alakját: Ha \( A \neq \{0\} \) és \( A \neq \{1\} \), akkor

\[
A = P_1^{a_1} \ldots P_r^{a_r} = \prod_{i=1}^{r} P_i^{a_i},
\]

ahol \( P_1, \ldots, P_r \) különböző primideálok és \( a_1, \ldots, a_r \) pozitív egészek.

Az ideálok legnagyobb közös osztójának (lásd a D 11.4.4 Definíciót és a T 11.4.5 Tételt), illetve legkisebb közös többszörösségnél (lásd a f11.4.5 feladatot [372]) kanonikus alakjára is az egész számoknál megszokott képlet érvényes: az ideálokban szereplő mindegyik primideált az előforduló minimális, illetve maximális hatványon kell venni, és értélemszerűen \( P^0 = \{1\} \). A bizonyítás is ugyanúgy történik, mint az egész számoknál.

Végül a T 11.5.5 és T 11.5.8 Tételek alkalmazásaként bebizonyítjuk, hogy \( E(d) \) minden ideálja „majdnem főideál”:

11.5.9 TÉTEL

\( E(d) \) minden ideálja generálható legfeljebb két elemmel. 

Bizonyítás: Nyilván feltehetjük, hogy \( A \neq \{0\} \) és \( A \neq \{1\} \).
IDEÁLOK

A T 11.5.5 Tétel szerint létezik olyan $B \neq (0)$ ideál, amelyre $AB = (\gamma)$. Olyan $(\gamma)$ főideált keresünk, amelynek az $AB = (\gamma)$ ideállal vett legnagyobb közös osztója $A$, ekkor ugyanis a T 11.4.5 Tétel (illetve az azt követő 2. megjegyzés) alapján

$$A = (\psi, \gamma).$$

Legyen $P_1, \ldots, P_r$ az összes olyan primideál, amely $A$ és $B$ közül legalább az egyiket osztja, és legyen az $A$ kanonikus alakja

$$A = P_1^{\alpha_1} \cdots P_r^{\alpha_r} = \prod_{i=1}^r P_i^{\alpha_i},$$

ahol az előbbieknek megfelelően előfordulhat $\alpha_i = 0$, azaz $P_i^0 = (1)$ is, ha $P_i$ csak a $B$-nek osztója.

Tekintsük a következő ideálokat:

$$C = \prod_{i=1}^r P_i^{1+\alpha_i}, \quad \text{és} \quad C_j = P_j^{\alpha_j} \prod_{i \neq j} P_i^{1+\alpha_i}, \quad j = 1, 2, \ldots, r.$$

Ekkor

$$C_j \mid C_i,$$

ahol az előbbieknek megfelelően előfordulhat $\alpha_j = 0$, azaz $P_j^0 = (1)$ is, ha $P_j$ csak a $B$-nek osztója.

Válasszuk olyan $\gamma_1, \ldots, \gamma_r$ elemeket, amelyekre

$$\gamma_j \in C_j, \quad \text{de} \quad \gamma_j \notin C_i, \quad j = 1, 2, \ldots, r.$$

Megmutatjuk, hogy

$$\gamma_i \in P_i^{1+\alpha_i}, \quad \text{ha} \quad j \neq i,$$

$$\gamma_i \in P_i^{\alpha_i}, \quad \text{és} \quad \gamma_i \notin P_j^{1+\alpha_i}.$$

Ha $j \neq i$, akkor $P_i^{1+\alpha_i} \mid C_j$ miatt $C_j \subseteq P_i^{1+\alpha_i}$, és így $\gamma_j \in C_j$ alapján $\gamma_j \in P_i^{1+\alpha_i}$, amivel (9a)-t beláttuk. Hasonlóan igazolható (9b) is.

A (9c) képletet indirekt bizonyítjuk. Ha $\gamma_i \in P_i^{1+\alpha_i}$, akkor ezt (9a)-val összevetve az adódik, hogy

$$\gamma_i \in \prod_{i=1}^r P_i^{1+\alpha_i}.$$

A 11.4.5 feladat [372] szerint ideálok metszete éppen a legkisebb közös többszörössük, azaz

$$\bigcap_{i=1}^r P_i^{1+\alpha_i} = \text{lkt}(P_1^{1+\alpha_1}, \ldots, P_r^{1+\alpha_r}) = \prod_{i=1}^r P_i^{1+\alpha_i} = C.$$

A (10) és (11) összefüggések ből kapjuk, hogy $\gamma_i \in C$, ami ellentmond a $\gamma_i$ választásának.

Megmutatjuk, hogy a

$$\gamma = \gamma_1 + \cdots + \gamma_r.$$
elem esetén az $\mathbf{A}B$ és $(\gamma)$ ideálak legnagyobb közös osztója $A$, és így (8) valóban teljesül.

Azt kell igazolni, hogy $\mathbf{A}B$ és $(\gamma)$ legnagyobb közös osztójának a kanonikus alakjában

(i) a $P_i$-en kívül más prímideál nem fordulhat elő, és

(ii) a $P_i$ kiveője éppen $\alpha_i$ ($i = 1, 2, \ldots, r$).

Az (i) feltétel teljesül, hiszen $\mathbf{A}B$ kanonikus alakjában csak a $P_i$ prímideálak szerepelnek.

Mivel $\mathbf{A} \mid \mathbf{B}$, ezért $\mathbf{A}B$ kanonikus alakjában a $P_i$ kiveője legalább $\alpha_i$. Ennek alapján (ii)-höz elég azt belátni, hogy $(\gamma)$ kanonikus alakjában a $P_i$ kiveője pontosan $\alpha_i$, azaz

(iii) $P_i^{\alpha_i} \mid (\gamma)$, de

(iv) $P_i^{1+\alpha_i} \not\mid (\gamma)$.

(iii): A (9a) és (9b) feltétel szerint

$$\gamma_{\ell} \in P_i^{\alpha_i}, \quad \ell = 1, 2, \ldots, r,$$

azaz a $\gamma$-t előállító összeg minden tagja eleme $P_i^{\alpha_i}$-nek. Mivel $P_i^{\alpha_i}$ ideál, ezért $\gamma \in P_i^{\alpha_i}$ is teljesül, és így

$$(\gamma) = \sum \alpha_i \quad \text{azaz} \quad P_i^{\alpha_i} \mid (\gamma).$$

(iv): A (9a) és (9c) feltétel szerint

$$\gamma_j \in P_i^{1+\alpha_i}, \quad \text{ha} \quad j \neq i, \quad \text{de} \quad \gamma \notin P_i^{1+\alpha_i},$$

azaz a $\gamma$-t előállító összeg tagjai pontosan egy tag kivételével elemei $P_i^{1+\alpha_i}$-nek. Mivel $P_i^{1+\alpha_i}$ ideál, ezért $\gamma \notin P_i^{1+\alpha_i}$, és így

$$(\gamma) \subset P_i^{1+\alpha_i}, \quad \text{azaz} \quad P_i^{1+\alpha_i} \mid (\gamma).$$

Feladatok

Valamennyi feladat $E(\mathfrak{d})$ ideáljaira vonatkozik.

11.5.1 Bizonyítsuk be, hogy egy $\alpha \in E(\mathfrak{d})$ elemhez és egy $\mathfrak{A}$ ideálhoz akkor és csak akkor létezik olyan $\mathfrak{B}$ ideál, amelyre $\mathfrak{A} \mathfrak{B} = (\mathfrak{d})$, ha $\alpha \in A$.

11.5.2 (a) Mutassuk meg, hogy bármely $\alpha \in E(\mathfrak{d})$ esetén $\alpha \mid N(\alpha)$.

(b) Bizonyítsuk be, hogy $E(\mathfrak{d})$-ban bármely $\mathfrak{A} \neq (0)$ ideál végletlen sok egész számot tartalmaz, amelyek egy (fő)ideált alkotnak $\mathbb{Z}$-ben.

11.5.3 Igazoljuk, hogy bármely $\mathfrak{A} \neq (0)$ ideálának csak véges sok osztója van.

11.5.4 Tekintsük egy adott $E(\mathfrak{d})$ prímideáljait.
IDEÁLOK

(a) Bizonyítsuk be, hogy minden primideál pontosan egy pozitív prímszámot tartalmaz.
(b) Mutassuk meg, hogy a primideálak száma végtelen.
(c) Lehet-e egy prímszám két különböző primideálaknak is eleme?
(d) Lehet-e egy prímszám végtelen sok különböző primideálaknak is eleme?

11.5.5 Bizonyítsuk be, hogy $\mathcal{E}(\sqrt{-5})$-ban bármely két ideál szorzata megegyezik az összegük és a metszetük szorzatával.

11.5.6 Mutassuk meg, hogy bármely $\alpha, \beta \in \mathcal{E}(\sqrt{-5})$ esetén $\alpha\beta \in (\alpha^2, \beta^2)$.

11.5.7 Tekintsük az $\mathcal{E}(\sqrt{-5})$ gyűrűt.
(a) Bontsuk fel a (21) főideál prímidéálak sorzatára.
(b) Melyek azok a $p > 0$ prímszámok, amelyek esetén $(p^4, 1 + \sqrt{-5})$ primideál?
(c)(M [621]) * Melyek azok a $p > 0$ prímszámok, amelyekre alkalmas $\alpha$ egész számmal $(p^4, p + \sqrt{-5})$ primideál?

11.5.8 Bizonyítsuk be, hogy $\mathcal{E}(\sqrt{-5})$ elemeire akkor és csak akkor érvényes a szármelémet alaptétele, ha minden primideál főideál.

11.5.9 (M [623]) Egy egész együttlatható, nemkonstans polinomot primitívnek nevezünk, ha az együttlatható relatív primek. Vezessük le a T 11.5.1 Tételből az alábbi két állítást:
(a) (A Gauss-lemma első alakja.) Két primitív polinom szorzata is primitív.
(b) (A Gauss-lemma második alakja.) Ha egy $H$ egész együttlatható polinom felírható az $F$ és $G$ racionális együttlatható polinomok sorzataként, $H = FG$, akkor $H$ előáll $H = F_1G_1$ alakban is, ahol $F_1$ és $G_1$ olyan egész együttlatható polinomok, amelyek az $F$-nek, illetve a $G$-nek (racionális) konstansszorosai.

Megjegyzés: Az (a) és (b) állítás könnyen levezethető egymásból, ezért szokás mindkettőt Gauss-lemmának nevezni. Az irodalom egy részben azaz az (a) állítást illetik ezzel az elnevezéssel.

11.6 Osztályszám

Ebben a pontban is feltesszük, hogy $\mathcal{O}$ algebrai szám, és $\mathcal{E}(\sqrt{-5})$ nemnulla ideáljai között egy ekvivalenciarelaciót vezetünk be. Az így keletkező ekvivalenciaosztályok száma fontos szerepet játszik $\mathcal{E}(\sqrt{-5})$ szármeléleti vizsgálatánál. Befejezésül, az ideálforkor tanultak alkalmazásaként megmutatjuk, hogy az $x^2 + 17 = y^3$ diofantikus egyenletnek nincs megoldása.

11.6.1 Definíció. D 11.6.1

Az $A \neq (0)$ és $B \neq (0)$ ideálok ekvivalentek, ha léteznek olyan $(\alpha) \neq (0)$ és $(\beta) \neq (0)$ főideálok, amelyekre

$$(\alpha)A = (\beta)B.$$ Jelölés: $A \sim B$.
IDEÁLOK

A továbbiakban mindig eleve feltesszük, hogy a szereplő ideálok egyike sem nulla (beléértve a főideálokat is).

Az ekvivalencia néhány egyszerű, de fontos tulajdonságát az alábbi tételben foglaljuk össze.

11.6.2 Tétel. T 11.6.2

(i) A D 11.6.1 Definícióban definiált $\sim$ valóban ekvivalentreláció, azaz reflexív, szimmetrikus és tranzitív.

(ii) $A \sim B$, $C \sim D \implies AC \sim BD$.

(iii) $A \sim B \iff AC \sim BC$.

(iv) $A \sim \{1\} \iff A$ főideál.

Bizonyítás: (i) Mivel $\{1\}A = A$, ezért $A \sim A$. A szimmetria nyilvánvaló a definícióból. Végül, ha $A \sim B$ és $B \sim C$, azaz alkalmas nemnulla főideálokkal

$$(a)A = (\beta)B \quad \text{és} \quad (\gamma)B = (\delta)C,$$

akkor

$$(a\gamma)A = (\beta\gamma)B = (\delta)C.$$

(ii) Ha $A \sim B$ és $C \sim D$, azaz alkalmas nemnulla főideálokkal

$$(a)A = (\beta)B \quad \text{és} \quad (a)C = (\xi)D,$$

akkor

$$(a\xi)AC = (\beta\xi)BD.$$

(iii) Mivel $C \neq \{0\}$, ezért $(a)A = (\beta)B \iff (a)AC = (\beta)BC$.

(iv) Ha $A = \{1\}$, akkor $(1)A = (1)(\xi) = (\xi)(1)$ miatt $A \sim \{1\}$. Megfordítva, ha $A \sim \{1\}$, azaz $A(\alpha) = (1)(\beta) = (\beta)$, akkor a 11.4.3b feladat [371] szerint $A$ főideál.

A $\sim$ ekvivalenciareláció alapján $E(\varphi)$ nemnulla ideáljai diszjunkt osztályokba sorolhatók. Bizonyítás nélkül közöljük az alábbi alapvető tételt:

11.6.3 Tétel. T 11.6.3

$E(\varphi)$ ideálosztályainak a száma véges.

Az $E(\varphi)$ ideálosztályainak a számát $h(\varphi)$-val jelöljük.

Az alábbi táblázatban néhány negatív $t$-hez tartozó $E(\sqrt{t})$ esetén megadjuk az osztályszámot:

<table>
<thead>
<tr>
<th>$t$</th>
<th>$-1$</th>
<th>$-3$</th>
<th>$-5$</th>
<th>$-17$</th>
<th>$-31$</th>
<th>$-35$</th>
<th>$-71$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$h(\sqrt{t})$</td>
<td>$1$</td>
<td>$1$</td>
<td>$2$</td>
<td>$4$</td>
<td>$3$</td>
<td>$2$</td>
<td>$10$</td>
</tr>
</tbody>
</table>

Können adódik, hogy $E(\varphi)$ elemeire akkor és csak akkor érvényes a számelmélet alaptele, ha $h(\varphi) = 1$ (lásd a 11.6.2 feladatot [387]).
Most megmutatjuk, hogy tetszőleges $E(d)$-ban egy (nemnulla) ideál $\hat{h}_s(d)$-adik hatványa mindig föideál:

11.6.4 Tétel. T 11.6.4

Legyen $E(d)$ ideálosztályainak száma $\hat{h}_s(d)$ és $A \neq \{0\}$ tetszőleges ideál. Ekkor $A^h(d)$ föideál. ♦

Bizonyítás: Az Euler–Fermat-tétel (T 2.4.1 Tétel) bizonyításánál látott gondolatmenetet követjük. Legyen $\hat{h}(d) = h$ és

$$A_1, A_2, \ldots, A_h$$

a különböző ideálosztályok egy-egy reprezentánsa.

Megmutatjuk, hogy ekkor

$$AA_1, AA_2, \ldots, AA_h$$

is mind különböző ideálosztályokba esnek. Ha ugyanis $AA_i \sim AA_j$, azaz alkalmas $\langle d \rangle \neq \{0\}$ és $\langle \tau \rangle \neq \{0\}$ föideálokkal

$$(\hat{h})AA_i = (\tau)AA_j,$$

akkor az $A \neq \{0\}$ ideállal történő egyszerűsítés után $A_i \sim A_j$, azaz (a feltétel miatt) $i = j$ adódik.

Mindezek alapján a (2)-ben felsorolt ideálok rendre ekvivalensek valamilyen sorrendben az (1)-beli ideálokkal. Ez azt jelenti, hogy minden $1 \leq i \leq h$-hoz létezik egy és csak egy olyan $1 \leq j \leq h$, amelyre $AA_i \sim AA_j$. Jelöljük ezt az $A_j \mathbin{\mathbin{\sim}} B_i$-vel:

$$AA_1 \sim B_1,$$

$$AA_2 \sim B_2,$$

$$\vdots$$

$$AA_h \sim B_h.$$  

Itt a $B_1, \ldots, B_h$ ideálok az $A_1, A_2, \ldots, A_h$ ideálok egy permutációját alkotják.

A (3)-beli ekvivalenciákat összeszorozva, a T 11.6.3/(ii) Tétel alapján azt kapjuk, hogy

$$A^hA_1A_2\ldots A_h \sim B_1B_2\ldots B_h = A_1A_2\ldots A_h.$$  

Használjuk fel most a T 11.6.3 Tétel (iii) és (iv) állítását: (iii) szerint a (4) ekvivalenciát az összes $A_i \neq \{0\}$ ideállal egyszerűsíthetjük, és az így keletkező $A^h \sim \{1\}$ ekvivalenciából (iv) szerint következik, hogy $A^h$ föideál. ♦

A fejezetet annak illusztrálásával zárjuk, hogy az ideálok segítségével gyakran olyan diofantikus egyenleteket is kezelni tudunk, ahol a megfelelő bővítés algebrai egészeire nem érvényes a számmelmélet alaptétele.

11.6.5 Tétel. T 11.6.5

Az $x^2 + 17 = y^4$ diofantikus egyenletnek nincs megoldása. ♦

Bizonyítás: Hasonló alakú diofantikus egyenletek már korábban is szerepeltek: ilyen volt az $x^2 + 4 = y^3$ (7.5.10 feladat [241]), illetve az $x^2 + 243 = y^5$ (7.7.11 feladat [257]). Ezeknél a bal
oldalt a Gauss-, illetve Euler-egészek körében szorzattá bontottuk, majd a számelmélet alaptételének felhasználásával kimutattuk, hogy mindkét tényező egy köbszám egységszerese, végül ennek alapján meghatároztuk a megoldásokat.

A mostani egyenlet esetén azt a nehézséget kell áthidalni, hogy az
\[ x + \sqrt{-1} \left( x - \sqrt{-17} \right) = y^3 \]  
(5)
szorzattából után nem járhatunk el a korábbi példák mintájára, mert \( E(\sqrt{-1}) \)-ben nem érvényes a számelmélet alaptétele. Ezért az elemekre vonatkozó (5) egyenletről át kell térni a megfelelő főideálok közötti egyenletre:
\[ (x + \sqrt{-17})(x - \sqrt{-17}) = (y)^3. \]  
(6)

Megmutatjuk, hogy az \((x + \sqrt{-17})\) és \((x - \sqrt{-17})\) ideálok relatív primek. Tegyük fel indirekt, hogy van egy \( P \) prímidéál közös osztójuk. Ekkor \( P \) osztja \((y)^3\)-nak is, és mivel \( P \) primideál, ezért \((y)\)-nak is. Az oszthatóságoknak megfelelő tartalmazások alapján
\[ x + \sqrt{-17} \in P, \quad x - \sqrt{-17} \in P \quad \text{és} \quad y \in P. \]

Ekkor
\[ \sqrt{-17} \left[ \left( x - \sqrt{-17} \right) - \left( x + \sqrt{-17} \right) \right] = 2 \cdot 17 = 34 \in P \]
is igaz.

Megmutatjuk, hogy \( y \) és 34 relatív primek (az egész számok körében).

Ha \( 17 \mid y \), akkor az eredeti egyenletből kapjuk, hogy \( x \) is osztható 17-tel, ekkor azonban a 17-nek \( x^2 + 17 \) pontosan az első, \( y^3 \) viszont legalább a harmadik hatványával osztható, ami lehetetlen.

Ha \( 2 \mid y \), akkor \( x \) páratlan, és az egyenlet bal oldala 2, a jobb oldala viszont 0 maradékot ad 8-cal osztva, ami szintén lehetetlen.

Ezzel beláttuk, hogy \( y \) és 34 relatív primek. Ekkor alkalmas \( u \) és \( v \) egész számokra \( 1 = yu + 34v \).

Mivel \( 34 \) és \( y \) is eleme \( P \)-nek, ezért az 1 is eleme \( P \)-nek, azaz \( P = \langle 1 \rangle \), ami ellentmond annak, hogy \( P \) prímidéál.

Így a (6) egyenlőség bal oldalán szereplő két (fő)ideál valóban relatív prim. Az ideálokra vonatkozó egyértelmű prímfaktorizációból (T 11.5.8 Tétel) következik, hogy mindkét ideál egy alkalmas ideál köbe, azaz (például)
\[ (x + \sqrt{-17}) = A^3. \]  
(7)
Mivel \( E(\sqrt{-17}) \)-ben az ideálitoszályok száma \( \text{í} \langle \sqrt{-17} \rangle = 4 \), ezért a T 11.6.4 Tétel szerint \( A^4 \) főideál, \( A^4 = \langle \gamma \rangle \). Így (7)-et \( A \)-val beszorozva
\[ A(x + \sqrt{-17}) = \langle \gamma \rangle, \]
adódik, amiből a 11.4.3b feladat [371] alapján kapjuk, hogy \( A \) főideál, azaz \( A = \langle \alpha \rangle \). Ekkor (7) átírható az
\[ (x + \sqrt{-17}) = \langle \alpha^3 \rangle, \quad \text{ezért} \quad x + \sqrt{-17} = \varepsilon \alpha^3 \]  
(8)
alakba, ahol \( \varepsilon \) egység \( E(\sqrt{-17}) \)-ben. Az \( E(\sqrt{-17}) \) egységei csak a \( \pm 1 \), és ezek maguk is köbszámok, továbbá \( -17 = -1 \) (mod 4) miatt \( E(\sqrt{-17}) \) elemei \( a + b \sqrt{-17} \) alakúak, ahol \( a \) és \( b \) egész számok. Ezért (8) tovább ekvivalens azzal, hogy

\[
x + \sqrt{-17} = \beta^3 = |c + a \sqrt{-17}|^3.
\]

A köbre emelést elvégezve és a képzetes részeket összehasonlítva

\[
1 = 3a^2b - 17b^3 = b(3a^2 - 17b^2)
\]

adódik. Innen \( b = \pm 1 \), azonban \( a \)-ra nem kapunk egész értéket, tehát az \( x^2 + 17 = y^3 \) diofantikus egyenletnek nincs megoldása.

### Feladatok

11.6.1 Igazoljuk, hogy \( E(\sqrt{-6}) \)-ban a \( (2, \sqrt{-6}) \) és \( (3, \sqrt{-6}) \) ideálok ekvivalensek.

11.6.2 Bizonyítsuk be, hogy \( E(\mathfrak{a}) \) elemeire akkor és csak akkor érvényes a számelmélet alaptétele, ha \( \mathfrak{a}(\mathfrak{a}) = 1 \).

11.6.3 (M [624]) Tegyük fel, hogy a \( k > 0 \) egész és \( \mathfrak{a} = \mathfrak{a}(\mathfrak{a}) \) relatív prímek. Bizonyítsuk be az alábbi állításokat:

(a) \( \mathfrak{A}^k \sim \mathfrak{B}^k \Rightarrow \mathfrak{A} \sim \mathfrak{B} \).

(b) Ha \( \mathfrak{A}^k \) főideál, akkor \( \mathfrak{A} \) is főideál.

11.6.4 Oldjuk meg az alábbi diofantikus egyenleteket:

(a) \( x^2 + 5 = y^3 \);

(b) \( 17x^2 + 1 = y^3 \);

(c) \( x^2 + 71 = y^3 \);

(d)(M [625]) \( x^2 + 35 = y^3 \).
12. fejezet - KOMBINATORIKUS SZÁMELMÉLET

A számelmélet és a kombinatorika határterülete viszonylag rövid múltra tekinthet vissza (legalábbis más számelméleti ágak „életkorához” képest), hiszen „klasszikus” eredményei (Schur és Van der Waerden tételei) is száz évnél fiatalabbak. Ez a terület tematikájában és módszereiben is rendkívül sokszínű: szerteágazó kérdéseinek vizsgálata során szellemes elemi megmondalások mellett gyakran az analízis, az algebra és a valószínűségszámítás kifinomult eszközeit kell felhasználni. Jelenleg is rendkívül dinamikus fejlődésének egyik fő mozgatórugója Erdős Pál munkássága volt, így az ebben a fejezetben tárgyalt problémák szinte mindegyike kapcsolódik az ő nevéhez.

12.1 Csupa különböző összeg

1993-ban az Eötvös Loránd Tudományegyetem felkérte frissen avatott díszdoktorát, a 80 éves Erdős Pált, hogy „A matematika aktuális problémái” címmel tartson az Eötvös-napon előadást. A zsúfolásig megtelt Gólyavárban elhangzott előadás elejének (hangfelvétel alapján történő) felidézésével Erdős lebilincselő egyéniségéről is képet kaphatunk.

„Jól hallanak, ugye? Hátul is? Ha nem hallanak, tessék tiltakozni. Nahát, az előadás címe egy kicsit szemtelen, de ezt nem én fogalmaztam így; nem lehet azt mondani, hogy ezek, amiről beszélni fogok, lennének a matematika aktuális problémái. Az utolsó ilyen előadást Hilbert tartotta 1900-ban, a párizsi matematikai kongresszuson, és nem is teljesen biztos, hogy most volna egy földi halandó, aki tudna egy ilyen előadást tartani. De az biztos, hogy évekig kellene rá készülni, és egy matematikai kongresszuson kellene megtartani. Én erre nem vállalkozom, talán már a magas korom miatt sem, de egy csomó dologról nem is tudok semmit, például algebrai topológiához, algebrai geometriához, logikához kevésbé értek. Így az előadás címe inkább „Kedvenc problémáim”, és mint hogy a hallgatóság egy része nem matematikus itten, elemi geometriáról és elemi számelméletről fogok beszélni.

Hát kezdjük először az elemi számelméleettel. Most mondok két problémát. Az elsőt 1931-ben vetett fel, olyan régen, hogy nem is vagyok biztos benne, hogy ez Krisztus előtt volt vagy Krisztus után. Egyszerű viccém különben, hogy két és fél milliárd éve vagyok. Így az az a bizonyíték, hogy amikor kicsi voltam, a Föld kora kétmilliárd év volt, és most közmert, hogy 4,6 milliárd év. Nyilván a különbség az én korom, és egyszer Los Angelesben tartottam egy előadást, amelynek ez volt a címe: „Az első kétmilliárd évem a matematikában”, és a diákok készítettek egy ábrát, amelyre felrajzoltak egy diagramot: „a Föld születése, Erdős születése, a dinoszauruszok születése”, és volt egy kép, amelyen egy dinoszaurusz hátnál ülök.

De hagyjuk most a viccet, a probléma így hangzik, különben 500 dollárt adok a bizonyításáért vagy cáfolásáért, azt hiszem, talán még csak van, hopp, kaphatok egy kis kétét, mert a [mikrofon]dróttal be vagyok fogva egy kicsit, köszönöm szépen, nahát a következő a probléma:

Legyen egész számoknak egy sorozata megadva: $a_1 < a_2 < \cdots < a_k \leq n$, és tegyük fel, hogy az összes

$$\sum_{j=1}^{k} \varepsilon_j a_j, \quad \varepsilon_j = 0 \text{ vagy } 1,$$

alakú részösszegek mind különbözők. Ilyen számok például a kettő hatványai: 1, 2, 4, 8, 16, ..., mert minden csecsemő tudja, hogy minden szám egyértelműen írható fel kettő hatványainak összegeként. Na most az 500 dolláros probléma az, hogy mennyi $m \leq n$, azaz maximálisan hány számot lehet $n$-ig megadni, hogy ezek az összegek mind különbözők legyenek.”
A kettőhatványok esetén (\(2^0 = 1\) -et is beleértve) \(k = 1 + \left\lfloor \log_2 n \right\rfloor\), és elsős szerint az azt gondolhatnánk, hogy így kapjuk a maximumot. Ez azonban nem így van: Conway és Guy \(n = 2^{2^k}\)-re talált ennél egyetlen elemmel sűrűbb sorozatot is, amelyre tehát \(k = 2 + \left\lfloor \log_2 n \right\rfloor\). Ebből következik, hogy minden \(n \geq 2^{2^k}\)-re is létezik ilyen sorozat, lásd a 12.1.12 feladatot [396]. Nem ismeretes, hogy ez tovább javítható-e.

Másfelől Erdős megmutatta, hogy \(\log_2 n\)-nél „sokkal” több elem már biztosan nem adható meg.

**12.1.1 Tétel.** T 12.1.1

Tegyük fel, hogy az \(1 \leq a_1 < a_2 < \cdots < a_k \leq n\) egész számok közül akárhány (különbözők az) összege mind különböző értéket ad. Ekkor

\[
k \leq \log_2 n + \log_2 \log_2 n + 1,
\]

sőt (\(n > 8\)-ra)

\[
k \leq \log_2 n + \frac{\log_2 \log_2 n}{2} + 2.
\]

Az élesebb (2) eredmény Erdős és Leo Moser közös munkája, ennél jobb felső becsülés ma sem ismeretes (eltekintve attól, hogy a képlet végén szereplő \(2\) helyére kicsit kisebb konstans írható, lásd a 12.1.13 feladatot [396]).

A fentiek alapján az Erdős által keresett maximum az alábbi határok közé esik:

\[
\left\lfloor \log_2 n \right\rfloor + 2 \leq \max k \leq \log_2 n + \frac{\log_2 \log_2 n}{2} + 2.
\]

Erdős az 500 dollárt annak tiszteletéért ajánlotta fel, vajon a \(\max k = \log_2 n\) eltérés \(n\) növekedésével korlátozatos marad-e. Ez a probléma tehát ma is megoldatlan.

**Bizonyítás:** Az \(a_i\) számokból \(\sum_k\) darab \(\sum_j\) összeg képezhető (az \(\sum_j\) -k között szerepel a 0 mint „üres” összeg és \(Z = \sum_{k=1}^{k} a_i\) is). Mindegyik \(\sum_j\) a \([0, nk-1]\) intervallumba esik (ha \(k > 1\)). Mivel a feltétel szerint mindegyik \(\sum_j\) különböző, ezért a darabszámuk legfeljebb annyi lehet, ahány egész szám a fenti intervallumban található, azaz

\[
2^k \leq nk.
\]

Innen logaritmálással kapjuk, hogy

\[
k \leq \log_2 n + \log_2 k.
\]

Most (5) jobb oldalán a második tagot fogjuk \(\log_2 n\) függvényében felülről becsülni. Mivel nyilván \(k \leq n\), ezért \(\log_2 k \leq \log_2 n\), tehát (5)-ből következik

\[
k \leq 2 \log_2 n.
\]

Ezt logaritmálva nyerjük, hogy

\[
\log_2 k \leq 1 + \log_2 \log_2 n,
\]
amit (5)-be beírva éppen a kívánt (1) becslés adódik.

Az élesebb eredmény igazolásához azt fogjuk felhasználni, hogy az $a_j$ -k nem egyenletesen helyezkednek el a $[0, n^k - 1]$ intervallumban, hanem a „zömmük az átlag közelében csoportosul.” Ezt az elemi valószínűségszámítás segítségével fogjuk pontosítani (bár minden elmondható és bizonyítható lenne anélkül is, a lényeget azonban éppen a valószínűségi szemlélet mutatja majd).

Tekintsük azt az $\eta$ valószínűségi változót, amely a $2^k$ darab $a_j$ mindegyikét $2^{-k}$ valószínűséggel veszi fel. A várható értéket $E$ -vel, a szórást $D$ -vel, a valószínűséget pedig $P$ -vel jelölve, a

$$P\left(\eta - E(\eta) > cD(\eta)\right) < e^{-c^2}$$

Csebisev-egyenlőtlenség ekkor azt fejezi ki, hogy az $a_j$ értékeknek csak kevesebb, mint $e^{-c^2}$-szereke esik az $\eta$ középpontú $2cD(\eta)$ hosszúságú intervallumon kívülre, vagyis legalább $1 - e^{-c^2}$-szeresük az adott intervallumban helyezkedik el. Ezután (alkalmaz $c$ -vel) erre az intervallumra és a biztosan itt levő $a_j$ értékek számára fogjuk megismételni az (1) igazolásánál látott gondolatmenet.

Nézzük a részleteket. A várható érték $E(\eta) = Z/2$, ugyanis az $a_j$ -k összepárosíthatók úgy, hogy az egy párban levő $a_j$-k összege $Z$ legyen. A szórás kiszámításához vezessük be a $\xi_i$, $i = 1, 2, \ldots, k$ valószínűségi változókat: $\xi_i$ az $a_i$, illetve 0 értéket 1/2–1/2 valószínűséggel veszi fel. Ennek a $\xi_i$ változók függetlenek és összegük éppen $\eta$, tehát a szórásnégyzetre

$$D^2(\eta) = \sum_{i=1}^{k} D^2(\xi_i) = \frac{1}{4} \sum_{i=1}^{k} a_i^2 < \frac{k n^2}{4}$$

adódik.

Alkalmazzuk most a (8) Csebisev-egyenlőtlenséget az $E(\eta) = Z/2$, $\xi_i D(\eta) < n\sqrt{k}/2$ értékekre és $c = 2$ -re. Ekkor azt kapjuk, hogy a $2^k$ darab (csupa különböző) $a_j$ legalább háromnegyed része a $Z/2$ középpontú $2n\sqrt{k}$ hosszúságú intervallumba esik. Ezért szükségképpen

$$\frac{3 \cdot 2^k}{4} < 2n\sqrt{k}, \quad \text{azaz} \quad 2^k < \frac{8n\sqrt{k}}{3}$$

(lehát a (4)-beli hasonló becsléshez képest lényegében a jobb oldal változott $k$ helyett $\sqrt{k}$ -ra).

A (9) egyenlőtlenséget logaritmicálva

$$k < \log_2 n + \frac{\log_2 k}{2} + \log_2 \left(\frac{8}{3}\right)$$

adódik. (10)-ből ($\eta > 8$ -ra) nyilvánvalóan következik (6), és így (7) is, amit (10)-be beírva kapjuk a kívánt (2) becslést.

A csupa különböző összegeket szolgáltató pozitív egész számhalmazokhoz még egy érdekes Erdős-probléma kapcsolódik:

**12.1.2 Tétel.** T 12.1.2

Ha az $a_1 < a_2 < \cdots < a_k$ pozitív egész számok közül akárhány (különbözőnek az) összege mind különböző értéket ad, akkor
A kétökhatványok példája mutatja, hogy (11)-ben a 2 helyére kisebb érték már nem írható (ha értékét nem korlátozzuk). Rögzített $k$ esetén a legnagyobb reciprokösszeget éppen az első $k$ kettőhatvány (azaz $1, 2, 4, \ldots, 2^{k-1}$) esetén kapjuk, ez a második és a harmadik bizonyításból is leolvasható majd. Ha végében számhalmozokat is megengedünk, akkor a tételek olyan formában igaz, hogy a reciprokösszeg kisebb vagy egyenlő, mint 2, és az egyenlőség csak az összes kettőhatvány esetén teljesül. Ez az eredmény az alábbi bizonyítások bármelyikének értelemszerű módosításával igazolható.

A T 12.1.2 Tétel állítása Erdős egy sejtése volt, és először Ryavec igazolta egy nagyon szellemes trükkkorozzalt (lásd az első bizonyitást). Ez a bizonyítás azonban egyrészt jelentősén támaszkodik az analízisre, másrészt egyáltalán nem könnyű beeleáíni, mitől „működik”. Sok évvel később született két újabb bizonyítás, amelyek csak középiskolai ismereteket használnak és (egymástól is különböző) gondolatmenetetük nagyon természetes (lásd a második és harmadik bizonyítást, ezek Bruentől és Borweintől, illetve Frenkel Pétertől származnak; a harmadik bizonyítást Frenkel Péter középiskolás korában találta). Ez is jól mutatja, hogy a kombinatorikus számelméletben időnként teljesen elemi módon is lehet új eredményeket elérni.

A bizonyítások közül tehát az első a legnehezebb, de a történeti szempontok mellett talán azért is érdemes végigrágnunk magukat rajta, hogy utána még inkább élvezhessük a második és harmadik bizonyítás természetes szépségét és egyszerűségét.

**Első bizonyítás:** Tekintsük az

$$\left(1 + x^{a_1}\right)\left(1 + x^{a_2}\right) \cdots \left(1 + x^{a_k}\right)$$  \hspace{1cm} (12)

szorzatot. A szorzást elvégezve olyan $x^n$ kitevőjű tagokat kapunk, ahol $m$ előáll valahány különböző $a_i$ összegeként (az $1 = x^0$ az üres összegnek fele meg). A feltétel szerint csupa különböző $x^{a_i}$ tag adódik, tehát a (12) szorzat $0 < x < 1$ esetén kisebb, mint az

$$1 + x + x^2 + \cdots + x^n + \cdots = \frac{1}{1-x}$$

végében mértani sor összege, azaz

$$\left(1 + x^{a_1}\right)\left(1 + x^{a_2}\right) \cdots \left(1 + x^{a_k}\right) < \frac{1}{1-x}, \quad \text{ha} \quad 0 < x < 1. \quad (13)$$

Most jön a „trükk”: vegyük mindkét oldal (természetes alapú) logaritmusát, osszunk $x$-szel, majd integráljunk 0-tól 1-ig:

$$\sum_{i=1}^{k} \int_{0}^{1} \log(1 + x^{a_i}) \, \frac{dx}{x} < \int_{0}^{1} \frac{\log(1-x)}{x} \, dx. \quad (14)$$

A bal oldali integráloknál helyettesítést alkalmazmunk:

$$x^{a_i} = y, \quad \text{ekkor} \quad \frac{dy}{dx} = a_i x^{a_i-1} \, dx, \quad \text{és ezzel} \quad dx = \frac{dy}{a_i x^{a_i-1}},$$

és így

$$\int_{0}^{1} \frac{\log(1 + x^{a_i})}{x} \, dx = \int_{0}^{1} \frac{\log(1 + y)}{y} \, \frac{dy}{a_i x^{a_i-1}} \, \frac{dy}{a_i x^{a_i-1}} \frac{dy}{\frac{dy}{a_i x^{a_i-1}}} = \frac{1}{a_i} \int_{0}^{1} \frac{\log(1 + y)}{y} \, dy. \quad (15)$$
(15) alapján (14) átírható a következő alakba:

\[
\left(\sum_{i=1}^{k} \frac{1}{a_i} \right) \int_0^1 \frac{\log(1+y)}{y} \, dy < - \int_0^1 \frac{\log(1-x)}{x} \, dx. \tag{16}
\]

A (16)-ban szereplő integrálokat az integrandusok hatványsorba fejtésével és (a jelen feltételek mellett megengedett) tagonkénti integrálással határozzuk meg:

\[\frac{-\log(1-x)}{x} \]

ahol

\[1 - \frac{x}{2} + \frac{x^2}{3} - \frac{x^3}{4} + \cdots + \frac{x^{j-1}}{j} + \cdots,\]

tehát

\[- \int_0^1 \frac{\log(1-x)}{x} \, dx = \left[ x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots + \frac{x^j}{j} + \cdots \right]_0^1 = \sum_{j=1}^{\infty} \frac{1}{j^2} = \frac{\pi^2}{6}. \tag{17}\]

Hasonló módon nyerjük, hogy

\[
\int_0^1 \frac{\log(1-y)}{y} \, dy = \left[ y - \frac{y^2}{2} + \frac{y^3}{3} - \cdots + (-1)^{j-1} \frac{y^j}{j} + \cdots \right]_0^1 = \sum_{j=1}^{\infty} (-1)^{j-1} \frac{1}{j} = \sum_{j=1}^{\infty} \frac{1}{j} \sum_{s=1}^{\infty} \frac{1}{s} = \left(1 - \frac{1}{2} \right) \sum_{j=1}^{\infty} \frac{1}{j^2} = \frac{\pi^2}{12}. \tag{18}\]

(18)-at és (17)-et (16)-ba beírva kapjuk, hogy

\[
\left(\sum_{i=1}^{k} \frac{1}{a_i} \right) \frac{\pi^2}{12} < \frac{\pi^2}{6}, \quad \text{azaz} \quad \sum_{i=1}^{k} \frac{1}{a_i} < 2. \tag{19}\]

** Második bizonyítás:** A feltétel szerint bármely \(1 \leq i \leq k\) esetén az \(a_1, a_2, \ldots, a_k\) számokból képezett \(2^i - 1\) darab nemüres összeg csupa különböző pozitív egész ad, ezért a legnagyobb ilyen összeg értéke legalább \(2^i - 1\), azaz

\[
a_1 + a_2 + \cdots + a_i \geq 2^i - 1, \quad i = 1, 2, \ldots, k. \tag{20}\]

Bevezetve a

\[b_i = 2^i - 1, \quad i = 1, 2, \ldots, k\]

jelölést, (20) átírható az

\[
a_1 + a_2 + \cdots + a_i \geq b_1 + b_2 + \cdots + b_i, \quad i = 1, 2, \ldots, k \tag{21}\]

alakba. A tétel igazolásához elég belátnunk, hogy ekkor

\[
\frac{1}{a_1} + \cdots + \frac{1}{a_k} \leq \frac{1}{b_1} + \cdots + \frac{1}{b_k}. \tag{22}\]

hiszen (21) jobb oldala

\[1 + \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^k-1} = 2 - \frac{1}{2^k-1} < 2.\]
Azt (a tétel állításánál erősebb eredményt) is be fogjuk bizonyítani, hogy (21)-ben csak az $a_i = b_i$, $i = 1, 2, \ldots, k$ esetben áll egyenlőség, tehát a maximális reciprokösszeget akkor kapjuk, amikor $a_i = 2^{i-1}$.

Megmutatjuk, hogy (20)-ból mindig következik (21), ha

$$0 < a_1 < a_2 < \cdots < a_k, \quad 0 < b_1 < b_2 < \cdots < b_k$$

(22)
tetszőleges valós számok.

(21)-et, illetve (20)-at átrendezve, az

$$\frac{1}{b_1} - \frac{1}{a_1} + \frac{1}{b_2} - \frac{1}{a_2} + \cdots + \frac{1}{b_k} - \frac{1}{a_k} \geq 0$$

egyenlőtlenséget kell igazolnunk, feltéve hogy (22) teljesül és

$$\epsilon_i = a_1 - b_1 - a_2 - b_2 - \cdots - a_i - b_i \geq 0, \quad i = 1, 2, \ldots, k.$$  

(20a)

(2a) bal oldalát a következőképpen alakíthatjuk át (a második és harmadik lépésben az ún. Abel-féle átrendezést alkalmazzuk):

$$\frac{1}{b_i} - \frac{1}{a_i} + \frac{1}{b_2} - \frac{1}{a_2} + \cdots + \frac{1}{b_k} - \frac{1}{a_k} = \frac{a_1 - b_1}{a_1 b_1} + \frac{a_2 - b_2}{a_2 b_2} + \cdots + \frac{a_k - b_k}{a_k b_k}$$

$$= \epsilon_1 + \epsilon_2 + \epsilon_3 + \cdots + \epsilon_{k-1} + \epsilon_k \left( \frac{1}{b_1} - \frac{1}{a_1 b_1} \right) + \epsilon_k \frac{b_k}{a_k b_k}.$$

(23)

A (23) képlet végén kapott előállításban (20a) és (22) alapján a $\epsilon_i \geq 0$ számok pozitív számokkal vannak szorozva, és így az összeg is nemnegatív, amint állítottuk.

A bizonyításból az is kiderült, hogy (21)-ben akkor és csak akkor áll egyenlőség, ha minden $\epsilon_i = 0$, ami (20a) alapján azzal ekvivalens, hogy minden $z$-re $a_i = b_i$. Ebből következik, hogy a csupa különböző összeg probléma esetén a maximális reciprokösszeget akkor kapjuk, amikor $a_i = 2^{i-1}$, amint jeleztük.

**Harmadik bizonyítás:** Csak a második bizonyítás elején látott (19) összefüggést fogjuk felhasználni, és megmutatjuk, hogy ha az $a_1 < a_2 < \cdots < a_k$ pozitív egészre ez teljesül, akkor a reciprokösszeg kisebb, mint 2.

Ha (19)-ben minden $z$-re egyenlőség érvényes, akkor $a_i = 2^{i-1}$ és a reciprokösszeg $2 - 1/2^{k-1} < 2$.

Ha (19)-ben nem minden $z$-re áll egyenlőség, akkor egy vagy két alkalmaz $a_j$ megváltoztatásával növelni fogjuk a reciprokösszeget, miközben (19) továbbra is érvényben marad. Az eljárásból világos lesz, hogy véges sok ilyen lépésben eljutunk ahhoz az állapothoz, amikor (19)-ben végig egyenlőség van. Ezzel (az a tétel állításánál élessebb eredményt) igazoltuk, hogy a reciprokösszeg az $a_i = 2^{i-1}$ esetben a legnagyobb.

Legyen $\tau$ a legkisebb olyan szám, amelyre (19)-ben nem áll egyenlőség ($\tau = 1$ is lehet), azaz

$$a_1 + a_2 + \cdots + a_\tau = 2^\tau - 1, \quad i = 1, 2, \ldots, \tau - 1, \quad \epsilon_\tau > 2^\tau - 1.$$

(24)
Két esetet különböztetünk meg: (A) Egyetlen \( \hat{r} > \tau \)-re sem áll (19)-ben egyenlőség; (B) Van olyan \( \hat{r} > \tau \), melyre (19)-ben egyenlőség teljesül.

(A) Legyen \( a'_1 = a_1 - 1 \), a többi \( a_i \) pedig maradjon változatlan. Ezzel a reciprokösszeg nyilván növekedett (hiszen \( 1/a'_1 > 1/a_1 \)), de (19) továbbra is érvényben maradt, hiszen bármely \( \hat{r} > \tau \)-re (19) bal oldala pontosan 1-gyel csökkent, tehát az egyenlőtlenség továbbra is fennáll, legfeljebb \( \geq \) helyett \( > \) formában.

Meg kell még mutatni, hogy az új számaink is szigorúan növekedő pozitív sorozatot alkotnak. Ha \( r = 1 \), akkor (24)-ből kapjuk, hogy \( a_1 > 1 \), tehát \( a'_1 > 0 \). Ha \( \tau > 1 \), akkor azt kell belátni, hogy \( a'_r = a_r - 1 > a_{r-1} \), azaz \( a_r \geq a_{r-1} + 2 \). Ismét (24) alapján

\[
a_r = (a_1 + \cdots + a_r) - (a_1 + \cdots + a_{r-1}) \geq 2^r - (2^{r-1} - 1) = 2^r - 2^{r-1} + 1 = a_r - 1 = 2.
\]

(B) Legyen \( s \) a legkisebb olyan \( r \)-nél nagyobb szám, amelyre (19)-ben ismét egyenlőség teljesül (\( s = r + 1 \) is lehet), azaz

\[
\begin{align*}
2^r - 1 & \geq \hat{r} = r + 1, \quad s - 1, \quad \text{és} \quad (2^s - 1) = 2^s - 1.
\end{align*}
\]

Legyen \( a'_1 = a_1 - 1 \), \( a'_s = a_s + 1 \), a többi \( a_i \) pedig maradjon változatlan. Ekkor (19) továbbra is érvényben maradt, hiszen ha \( r \leq \hat{r} \leq s - 1 \), akkor (19) bal oldala pontosan 1-gyel csökkent, tehát az egyenlőtlenség továbbra is fennáll (legfeljebb \( \geq \) helyett \( \geq \) formában), az \( \hat{r} \geq s \) (valamint az \( \hat{r} < r \) esetben pedig (19) bal oldala változatlan maradt.

A reciprokösszeg növekedéséhez azt kell megmutatni, hogy

\[
\frac{1}{a_r} + \frac{1}{a_s} < \frac{1}{a'_r} + \frac{1}{a'_s},
\]

azaz

\[
\frac{a_r + a_s}{a_r a_s} < \frac{(a_r - 1) + (a_s + 1)}{(a' = 1) + (a'_s + 1)}.
\]

A számlálók egyenlősége miatt ez ekvivalens a nevezők közötti fordított irányú egyenlőtlenséggel (mindenhol pozitív számok szerepelnek), amit tovább alakíthat a nyilvánvalóan igaz \( a_r - 1 < a_s \), egyenlőtlenség adódik.

Végül, az (A) esethez hasonlóan igazolható, hogy az új számaink is szigorúan növekedő pozitív sorozatot alkotnak.

Az eljárásból világos, hogy a fenti lépéseket véges sokszor alkalmazva elérjük, hogy (19)-ben már \( \hat{r} = \tau \) mellett is egyenlőség teljesüljön. Ezután megismételjük az egészet az első olyan (\( \tau \)-nél már nagyobb) \( \hat{r} \) értékre, amelyre (19)-ben szigorú egyenlőtlenség van, mindaddig, amíg már ott is egyenlőséget kapunk stb. Ezzel igazoltuk, hogy véges sok lépésben eljutunk ahhoz az állapotohoz, amikor (19)-ben mindenütt egyenlőség szerepel, amint állítottuk.

Feladatok

A feladatokban \( 1 \leq a_1 < a_2 < \cdots < a_k \leq r \) egész számok, amelyekre különféle feltételeket írunk elő.
12.1.1 (a) Mennyi $k$ maximuma ($n$ függvényében), ha egyik $a_i$ sem áll elő csupa különböző (és egynél több) $a_j$ összegeként.
(b) Legyen $a_1 < a_2 < \ldots$ pozitív egészeknek olyan végteslen sorozata, amelyben egyik $a_i$ sem áll elő csupa különböző (és egynél több) $a_j$ összegeként. Jelölje $A(n)$ a sorozat $n$-nél nem nagyobb elemeinek a számát. Lássuk be, hogy $\lim_{n \to \infty} A(n)/n = 0$.

12.1.2 Tegyük fel, hogy egyik $a_i$ sem írható fel $a_j + a_{j+1}$ alakban. Jelöljük ezen feltétel mellet $k$ maximumát $f(n)$-nel. Mutassuk meg, hogy $\lim_{n \to \infty} f(n)/n = 2/3$.

12.1.3 (M [626]) Azt vizsgáljuk, hogy egy $t$ szám hányféleképpen állhat elő egymás után következő $a_i$-k összegeként, azaz $t = a_i + a_{i+1} + \cdots + a_j$ alakban (a tagszámot nem korlátozzuk és $i = j$ is megengedett). Legyen $L(k)$ a $t = a_i + a_{i+1} + \cdots + a_j$ egyenlet megoldásszámának maximuma, ahol a maximumot az összes lehetséges $O_i$ rendszerre és $k$-re vesszük ($n$ is tetszőleges lehet). Igazoljuk, hogy $L(k) = \lceil k/2 \rceil$.

12.1.4 Tegyük fel, hogy bármely $i \neq j$ -re $\left[ a_i, a_j \right] > n$. Bizonyítsuk be, hogy az $a_i$ számok reciprokösszege kisebb, mint (a) $2$; (b) $3/2$.

Megjegyzés: Schinzel és Szekeres megmutatták, hogy a reciprokösszeg maximuma 31/30, és ez csak a 2, 3, 5 számok és $n = 5$ esetén lép fel.

12.1.5 Lássuk be, hogy (tetszőleges $a_i$-kre)$\prod_{i=1}^{k} \frac{1}{|a_i| a_i} \leq 1$.

12.1.6 Tegyük fel, hogy $a_i + a_j$ sohasem négyzetszám. Jelöljük ezen feltétel mellet $k$ maximumát $g(n)$-nel.
(a) Igazoljuk, hogy $\frac{1}{3} \leq \liminf_{n \to \infty} \frac{g(n)}{n} \leq \limsup_{n \to \infty} \frac{g(n)}{n} \leq \frac{1}{2}$
(b) Javítsuk az előző egyenlőtlenségben az alsó becslést 11/32-re.

Megjegyzés: 2002-ben Szemerédi Endre bebizonyította, hogy $\lim_{n \to \infty} g(n)/n = 11/32$.

12.1.7 (*) Tegyük fel, hogy $a_i - a_j$ (i.e. j-re) sohasem négyzetszám. Jelöljük ezen feltétel mellet $k$ maximumát $h(n)$-nel. Igazoljuk, hogy $h(n) \geq n^{0.7}$

Megjegyzés: A fenti eredmény Ruzsától származik. Sárközy és Fürstenberg megmutatták, hogy (az összegre vonatkozó kérdéssel ellentétben) $\lim_{n \to \infty} h(n)/n = 0$, azonban $h(n)$ pontos nagyságrendje nem ismert.

12.1.8 (*) Tegyük fel, hogy $a_i$ számok közül akárhány különbözőnek a szorzata mind különböző értéket ad. Jelöljük ezen feltétel mellet $k$ maximumát $\sigma(n)$-nel. Mutassuk meg, hogy $|\sigma(n) - \tau(n)| < 2n^{2/3}$

(ahol $\tau(n)$ az $n$-nél nem nagyobb primék száma).

Megjegyzés: Erdős bebizonyította, hogy alkalmas $c_1$ és $c_2$ pozitív konstansokkal minden elég nagy $n$-re
12.1.9 Mennyi $k$: maximuma ($n$ függvényében), ha egyik $a_i$ sem osztója tőle különböző $a_j$ -k szorzatának?

12.1.10 Tegyük fel, hogy $6 \mid n$ . Mennyi $k$: maximuma ($n$ függvényében), ha bármely három között található kettő olyan, amelyek nem relatív prímek?

12.1.11 Lássuk be, hogy ha $k_0$ prim, akkor van olyan $i, j$, melyre $\frac{a_i - a_j}{a_i a_j} \geq k$ .

Megjegyzés: Az állítás tetszőleges $k$: esetén is igaz. R. L. Grahamnek ezt a sokáig megoldatlan sejtését (elég nagy $k$:ra) Szegedy Márton bizonyította be 1985-ben, még egyetemi hallgatóként.

12.1.12 Tegyük fel, hogy $\nu = \nu_0$: -re $1$ és $n$ között megadható $k = 2 \cdot \log_2 n$ olyan $a_i$, amelyek közül akár hány (különböző az) összege különböző értéket ad. Lássuk be, hogy akkor ugyanez igaz minden $\nu \geq \nu_0$: esetén is.

12.1.13 A T 12.1.1 Tétel bizonyításában a Csebisev-egyenlőséget optimális $C$ -vel alkalmazva mennyire javítható a tételben a (2) felső becslés?

12.2 Sidon-sorozatok

Erdős egy másik „kedvenc” területe a Sidon-problémakör volt. Sidon-sorozatoknak a természetes számok olyan véges vagy végtelen részsorozatait nevezzük, amelyeknél az $a_i + a_j$, $i \leq j$ összegek (vagy ami ugyanaz: az $a_i - a_j$, $i \neq j$ különbségek) mind különbözők. Ezek először Sidon Simonnak a Fourier-sorokra vonatkozó vizsgálatai közben merültek fel az 1930-as években.

Az alábbiakban először véges Sidon-sorozatokkal foglalkozunk.

Maximálisan hány eleme lehet egy Sidon-sorozatnak az $[1, n]$ intervallumban? Bebizonyítjuk, hogy ez a maximum „körülbelül” $\sqrt{n}$ . Ez két állítást jelent: egyrészt azt, hogy $1$ és $n$ között valóban található körülbelül $\sqrt{n}$ elemes Szegő-Sidon-sorozat (alsó becslés a maximális elemszámnak), másrésztt azt, hogy az adott határok között ennél lényegesen hosszabb Sidon-sorozat már nem létezik (felső becslés a maximális elemszámnak).

Erdős és Turán Pál 1941-ben megmutatták, hogy a keresett maximum legfeljebb $n^{1/2} + 2n^{1/4}$ .

Ezt később B. Lindström más módszerrel $n^{1/2} + n^{1/4} + 1$ -re javította, de ugyanaz az eredmény az Erdős–Turán-bizonyítás pontosabb végigszámolásával is kiadódik (T 12.2.4 Tétel). J. Singer egy eredményének felhasználásával Erdős és tőle függetlenül S. Chowla 1944-ben azt is igazolták, hogy elég nagy $n$ -re $n^{1/2} - n^{\epsilon}$ elemes Szegő-Sidon-sorozat valóban meg is adható $n$ -ig, ahol $\epsilon$ egy alkalmas, $1/2$ -nél kisebb pozitív állandó (T 12.2.3 Tétel). Ez a két eredmény együtt azt jelenti, hogy az $[1, n]$ intervallumban a Sidon-sorozatok maximális elemszáma nagyon pontos aszimptotikával.
Máig is megoldatlan azonban a még jobb hibatagok kérdése. Az sejttható, hogy a maximális elemszámnak $\sqrt{n}$-től való eltérése egy $\sqrt{2}$-től független korlát alatt marad. Ennek igazolásáért vagy cáfolásáért korábban Erdős összesen 1000 dollárt ajánlott fel.

Jelöljük $s = \varepsilon(n)$-nel az $n$-ig megadható leghosszabb Sidon-sorozat elemszámát. Próbáljunk először egyszerű felső becslést keresni $s$-re. Mivel egy 1 és $n$ közötti Sidon-sorozatban az $a_i + e_j$ összegek mind különbözők, 2 és $2n$ közé esnek és számuk $\binom{n}{2}$, így $\binom{n}{2} < 2n$, azaz $s < 2\sqrt{n}$. Jobb becslést kapunk, ha az $a_i - a_j > 0$ különbségeket vizsgáljuk; ezek is mind különbözők, $n$-nél kisebbek és számuk $\binom{n}{2}$, így $\binom{n}{2} < n$, azaz $s < \sqrt{2n} + 1$. A felső becslésnél tehát azonnal adódott a $\sqrt{n}$-es nagyságrend, „csak” a $\sqrt{2}$ együtthatóját kell 1-re leszorítni.

„Alulról nézve” sokkal kevésbé világos, hogyan érhető el a $\sqrt{n}$-es nagyságrend. A kettőhatványok példája csak $\log n$-et ad, és a mohó algoritmust is csak $\sqrt{n}$ biztosítható (lásd a 12.2.1 feladatot [404]). Egy szintén Erdős-tól származó nagyon szép elemi konstrukcióval már $\sqrt{n}/2$ hosszú Sidon-sorozatot kapunk (lásd a 12.2.2 feladatot [404]), és mint említtetük, a $\sqrt{n}$ együtthatójához „felformázható” 1-re.

Lássunk akkor hozzá nagy elemszámú Sidon-sorozatok konstrukciójához. Ezt először bizonyos típusú $n$-ekre végezzük el, és ezek segítségével térünk majd át tetszőleges $n$-re.

**12.2.1 Tétel.**  
Legyen $p$ tetszőleges prímszám. Ekkor $n = p^2 + p + 1$-re létezik olyan Sidon-sorozat az $[1, n]$ intervallumban, amelynek $\sqrt{n}$ eleme van.

A T 12.2.1 Tétel helyett egy jóval élessebb és önmagában is nagyon érdekes és meglepő állítást igazolunk.

**12.2.2 Tétel.**  
Legyen $p$ tetszőleges prímszám. Ekkor létezik $p + 1$ darab olyan $a_i$, amelyekre az $a_i - a_j: i \neq j$ különbségek (nemcsak hogy különbözők, hanem ráadásul) páronként inkongruensek modulo $p^2 + p + 1$.

Megjegyzés: A T 12.2.2 Tételben szereplő különbségek száma $p^2 + p$, és modulo $p^2 + p + 1$ éppen ennyi nem nulla maradék van. Vagyis az $a_i - a_j$ különbségek minden maradéktól előállítanak, éspedig mindegyiket pontosan egyszer.

Nyilvánvaló, hogy a T 12.2.2 Tételben az $a_i$-k maguk is páronként inkongruensek kell hogy legyenek, tehát választhatók 1 és $n = p^2 + p + 1$ közöttieknek, és így valóban azonnal adódik a T 12.2.1 Tétel.

A T 12.2.2 Tétel bizonyítása: A bizonyítás a véges testek segítségével történik, az ezek szerkezetére vonatkozó alapvető tételiek és egy kevés lineáris algebra felhasználásával.

Tekintsük a $p^3$ elemű $T_3$ véges testet és ebben a $p$ elemű $T_1$ résztestet. Legyen $\Delta$ a $T_3$ test multiplikatív csoportjának (egyik) generátor eleme, azaz

$$ T_3 = \{0, \Delta, \Delta^2, \ldots, \Delta^{p^3-1} - 1\}. \quad (1) $$

A $T_1$ -beli nem nulla elemek $T_3$ multiplikatív csoportjának részcsoportját alkotják, amelynek generátoreleme nyilván $\Delta^\alpha$, ahol $\alpha = (p^3 - 1)/(p-1) - p^2 + p + 1$. 

397
Vagyis

\[ T_1 = \{0, \Delta^a, \Delta^{2a}, \ldots, \Delta^{(p-1)a} = \Delta^{b \cdot 1 - 1} \}. \]

Tekintsük most \( T_1 \)-at mint \( T_1 \) feletti vektorteret. Az előzőek alapján kapjuk, hogy \( T_1 \) két eleme, \( \Delta^i \) és \( \Delta^j \) pontosan akkor lineárisan összefüggő \( T_1 \) felett, ha

\[ i \equiv j \pmod{n}. \tag{2} \]

A keresett \( a_i \) egészket ezután a következőképpen adjuk meg. Vegyünk egy tetszőleges \( \Theta \in T_3 \setminus T_1 \) elemet, és legyenek \( T_1 \) elemei \( \gamma_1, \ldots, \gamma_p \). Írjuk fel a \( \Theta + \gamma_i \) elemeket

\[ \Theta + \gamma_i = \Delta^{a_i} \tag{3} \]

alakban. Ez (1) alapján megtethető, és így kijelöltünk \( \Psi \) darab \( a_i \) egész számot, a \( p + 1 \) -ik pedig legyen \( a_{p+1} = 0 \).

Megmutatjuk, hogy ezek eleget tesznek a feltételeknek, azaz az \( a_i - a_j \) különbségek, vagy ami ugyanaz, az \( a_i + a_j \) összegek páronként különböző maradékot adnak modulo \( n^2 - p + 1 \).

Tegyük fel, hogy \( a_i + a_j = a_k + a_l \pmod{n^2 - p + 1} \). Ekkor (2) és (3) alapján

\[ (\Theta + \gamma_i)(\Theta + \gamma_j) - \gamma(\Theta + \gamma_k)(\Theta + \gamma_l) = 0 \]

adódik valamely \( \gamma \in T_1 \) elemmel. Mivel \( \Theta \) harmadfokú a \( T_1 \) test felett, ezért nem lehet gyöke egy legfeljebb másodfokú polinomnak. Vagyis csak \( \gamma = 1 \) és \( \{\gamma, \gamma_j\} = \{\gamma, \gamma_l\} \) lehetséges, így a megfelelő \( a_i \)-k is egyenlők, ami éppen a bizonyítandó állítás volt.

A bizonyítás ugyanúgy megy akkor is, ha \( a_{p+1} = 0 \) is szerepel a négy \( a_i \)- között. □

Megjegyzés: A T 12.2.2 Tétel és a bizonyítás ugyanúgy érvényes akkor is, ha \( \Psi \) egy primszám hatvánnyá. Mindez szoros kapcsolatban áll a véges projektív síkokkal.

12.2.3 Tétel . T 12.2.3

Minden elég nagy \( n \) -re megadható olyan Sidon-sorozat az \([1, u]\) intervallumban, amelynek legalább \( \frac{n^{1/2}}{2} - n^{0.27} \) eleme van. ♡

Bizonyítás: Vegyük azt a legnagyobb \( P \) primszámot, amelyre \( p^2 + 1 \leq u \), és \( p^2 + p + 1 \) -re készítsük el az előző ( \( P + 1 \) elemű) konstrukciót. Mivel az 5.5.4/(A) Tétel alapján \( u^{1/2} - n^{0.27} \) és \( n^{1/2} \) között elég nagy \( u \) -re mindig van primszám, ezért \( p > n^{1/2} - n^{0.27} \), amivel a tételt tetszőleges \( u \)-re igazoljuk. □

Megjegyzés: A tetszőleges \( n \) -re történő átérésnél azt használtuk fel, hogy a primek elég „sűrűn” helyezkednek el. Ha tudjuk, hogy \( na \) és \( na + n^2 \) között elég nagy \( n \) -re mindig van primszám, akkor a tételünkben a hibatag \( n^{1/2} \) nagyságrendűnek vehető. Mint az 5.5 pontban láttuk, a szomszédos primek közötti hézag vizsgálata igen nehéz kerdés.

A T 12.2.3 Tétel más bizonyításaira nézve lásd a 12.2.3 [404] és 12.2.4 feladatot [404].

Most rártérünk a Sidon-sorozatok elemszámának \( a(z \ éles) \) felső becslesére.
12.2.4 Tétel. \( T \) 12.2.4

Az \( [1, n] \) intervallumban eső bármely Sidon-sorozatnak legfeljebb \( n^{1/2} + n^{1/4} + 1 \) eleme van.

Első bizonyítás: Legyen \( t \) később alkalmazani megválasztandó egész szám, és toljunk végig egy \( t - 1 \) hosszúságú szakaszt a \( [0, n] \) intervallumon, azaz tekintsük a \( [t - 1, 0], [t - 2, 1], \ldots, [n, n + t - 1] \) intervallumokat. Tegyük fel, hogy az \( s \) elemű Sidon-sorozat elemszáma az egyes intervallumokban \( A_1, A_2, \ldots, A_{n+1} \). Ekkor nyilván

\[
\sum_{i=1}^{n+t} A_i = ts. \tag{4}
\]

Számoljuk össze multiplicitással azokat az \( \{a_i, a_j\}, i > j \) elempárokat, amelyek egy-egy ilyen intervallumba esnek, azaz mindegyik elempárt annyiszor vegyük, ahány intervallum azt tartalmazza. Legyen \( D \) ezek együttes száma. Ekkor nyilván

\[
D = \sum_{i=1}^{n+t} \binom{A_i}{2} = \sum_{i=1}^{n+t} \frac{A_i^2}{2} - \sum_{i=1}^{n+t} \frac{A_i}{2}. \tag{5}
\]

Másrészt, ha egy ilyen elempárból az \( a_i - a_j \) különbség \( d \) különbözség \( d \), akkor ez az elempár pontosan \( t - d \) intervallumba esik bele. A Sidon-tulajdonság miatt minden \( d \) legfeljebb egyszer fordulhat elő, így

\[
D \leq \sum_{d=1}^{t-1} (t - d) = \frac{t(t - 1)}{2}. \tag{6}
\]

(5) és (6) alapján

\[
\sum_{i=1}^{n+t} A_i^2 - \sum_{i=1}^{n+t} A_i \leq t(i - 1) \tag{7}
\]

adódik. A számtonyi és négyzetes közép közötti egyenlőtlenség, valamint (4) felhasználásával (7) bal oldalát a következőképpen becüszhetjük alulról:

\[
\sum_{i=1}^{n+t} A_i^2 - \sum_{i=1}^{n+t} A_i \geq \left( \frac{\sum_{i=1}^{n-t} A_i}{n - t} \right)^2 - ts = \frac{n^2 s^2}{n + t} - ts. \tag{8}
\]

Így (7) és (8) összekapcsolásával azt nyerjük, hogy

\[
s^2 - s \left( \frac{n}{t} - 1 \right) - \left( \frac{n}{t} + 1 \right) (t - 1) \leq 0.
\]

Ezt a másodfokú egyenlőtlenséget megoldva

\[
s \leq \frac{\left( \frac{n}{t} + 1 \right)}{2} - \frac{1}{2} + \sqrt{\left( \frac{n}{t} + 1 \right)^2 - \frac{n}{t} - \frac{3}{4}}
\]

adódik. Ha most \( t \)-nek a \( t = \left[ n^{5/4} \right] + 1 \) értéket választjuk, akkor a tétel állítását kapjuk.

Második bizonyítás: Most bizonyos \( a_i - a_j \) különbségek összegét fogjuk két oldalról megbecsülni. Legyen

\[
s \leq \frac{\left( \frac{n}{n^{5/4}} + 1 \right)}{2} - \frac{1}{2} + \sqrt{\left( \frac{n}{n^{5/4}} + 1 \right)^2 - \frac{n}{n^{5/4}} - \frac{3}{4}}
\]

adódik. Ha most \( t \)-nek a \( t = \left[ n^{5/4} \right] + 1 \) értéket választjuk, akkor a tétel állítását kapjuk.
ahol \( r \)-et később alkalmazásban megválasztjuk. A Sidon-tulajdonság miatt a (9)-beli összeg tagjai között nincs két azonos különbség, számuk

\[
(s - 1) + (s - 2) + \cdots + (s - r) = r\left(\frac{r + 1}{2}\right) = rw,
\]

ahol

\[
w = s - \frac{r + 1}{2},
\]

így \( K' \) legalább akkora, mint az első \( rw \) darab pozitív egész összege, azaz

\[
K' \geq \frac{rw(rw + 1)}{2} \geq \frac{r^2w^2}{2}.
\]

Másrészt a (9)-beli összegnek része pl.

\[
(a_{n-r} - a_{n-r} - 1) + (a_{n-r-1} - a_{n-r} - 2) + \cdots + (a_2 - a_1) < n, \quad n \leq i
\]

és számos más teleszkopikus összeg, amelyek hasonlóképpen becsülhetők felülről. Ezek általános alakja

\[
(a_{n-r} - a_{n-r} - \mu) + (a_{n-r-\mu} - a_{n-r-\mu-2}) + \cdots + a_{n-r} \leq n, \quad 0 \leq \mu < \nu \leq \tau.
\]

Sőt az egész \( K' \) ilyen teleszkopikus részösszegekre bontható, amelyeket úgy kapunk, hogy az indexek befutják az összes olyan 1 és \( s \) közötti (tovább már nem bővíthető) számtani sorozatot, amelynek differenciája legfeljebb \( r \). Mivel \( \mu \) differenciájú számtani sorozat éppen \( \mu \) darab van, így a teleszkopikus részösszegek száma \( 1 + 2 + \cdots + r = r(r + 1)/2 \), és mindegyik részösszeg értéke legfeljebb \( n \), tehát

\[
K' \leq \frac{nr(r + 1)}{2}.
\]

Egybevetve (11)-et és (12)-t, \( 2/r^2 \)-tel történő szorzás után a \( rw^2 < \nu + n/r \) egyenlőtlenséget nyerjük. Innen gyököntással és (10) felhasználásával kapjuk, hogy

\[
s < \frac{r + 1}{2} + \sqrt{\frac{n + \nu}{r}}.
\]

Ha most \( r \)-nek az \( r = \lceil n^{1/4}/4 \rceil + 1 \) értéket választjuk, akkor a téttel állítását kapjuk.

Most rátérünk a végtelen Sidon-sorozatok vizsgálatára. Erdős 1955-ben megmutatta, hogy egy végtelen Sidon-sorozat már szükségképpen „ritkább”: nem fordulhat elő, hogy a sorozatnak az \( [1, \nu] \) intervallumba eső része minden \( n \)-re a véges maximum, vagyis \( \sqrt{\nu} \) körüli elemszámot adjon.

**12.2.5 Tétel.** T 12.2.5

Ha \( A(n) \) jelöli egy végtelen \( A \) sorozat elemszámát \( n \)-ig, akkor bármely \( A \) végtelen Sidon-sorozatra szükségképpen
**KOMBINATORIKUS**  
**SZÁMELMÉLET**

\[
\liminf_{n \to \infty} \frac{A(n)}{\sqrt{n}} = 0, \quad \text{és} \quad \limsup_{n \to \infty} \frac{A(n)}{\sqrt{n / \log n}} < \infty. \quad \star 
\]

**Bizonyítás:** Tekintsünk egy tetszőleges \( A \) végleten Sidon–sorozatot, és legyen \( N \) egy nagy természetes szám. Jelöljük \( A_{i} \)-vel, hány eleme esik a sorozatnak az \([i(i-1)N+1,iN]\) intervallumba, azaz

\[
A_{i} = A(iN) - A((i-1)N), \quad i = 1,2,\ldots, N.
\]

Mivel egy–egy ilyen intervallumon belül a pontpárok különbsége \(< N \), így a Sidon–tulajdonság miatt

\[
\sum_{i=1}^{N} \binom{A_{i}}{2} < N.
\]

Innen

\[
2N > \sum_{i=1}^{N} A_{i}(A_{i} - 1) \geq \frac{1}{2} \sum_{i=1}^{N} (A_{i}^{2} - 1),
\]

vagyis

\[
\sum_{i=1}^{N} A_{i}^{2} < 5N. \quad (13)
\]

Most két oldalról meg fogjuk becsülni az

\[
S = \sum_{i=1}^{N} \frac{A_{i}}{\sqrt{i}}
\]

összeget. Egyrészt a Cauchy–Bunyakovszkij-egyenlőtlenség és (13) felhasználásával azt kapjuk, hogy

\[
S \leq \sqrt{\left( \sum_{i=1}^{N} A_{i}^{2} \right) \left( \sum_{i=1}^{N} \frac{1}{i} \right)} \approx \sqrt{5N \log N}. \quad (14)
\]

Másrészt alakítsuk át \( S \)-et (az ún. Abel-féle átrendezés szerint) a következőképpen:

\[
S = \sum_{i=1}^{N-1} \frac{A(iN) - A((i-1)N)}{\sqrt{i}} > \sum_{i=1}^{N-1} \frac{A(iN)}{\sqrt{i} \sqrt{\log(iN)}} > \sum_{i=1}^{N-1} \frac{A(iN)}{\sqrt{i} \sqrt{\log(iN)}}.
\]

Ha most feltegzük, hogy

\[
A(iN) > c \sqrt{\frac{iN}{\log(iN)}}, \quad i = 1,2,\ldots, N, \quad (16)
\]

akkor (15) alapján

\[
S > c \sum_{i=1}^{N-1} \frac{\sqrt{\log(iN)}}{2(i+1) \sqrt{\log(iN)}} = \frac{c \sqrt{N}}{8 \log N} \sum_{i=1}^{N-1} \frac{1}{i+1} \approx \frac{c}{8 \sqrt{5N \log N}}. \quad (17)
\]

következik.
Mivel \( c > \sqrt{40} \) esetén (17) ellentmond (14)-nek, így \( c > \sqrt{41} \) mellett (16) nem teljesülhet, ami igazolja a tétel állítását.

A T 12.2.5 Tétel nem jelenti azt, hogy egy végölen Sidon-sorozat ne lehetne „időnként” olyan sűrű, mint egy véges: Erdős, majd F. Krückeberg konstruált olyan végölen Sidon-sorozatot, amelynek végölen sok \( n \)-re az \( \lfloor 1.5l \rfloor \) intervallumba eső szelete „közel” \( \sqrt{n} \) elemet tartalmaz (lásd a 12.2.5 feladatot [404]).

Ha most egy minden véges szeleteben „elég” sűrű Sidon-sorozatot szeretnénk megadni, akkor az ún. mohó algoritmuszal készíthetünk egy olyant, amelynek \( n \)-ig legalább \( \sqrt{n} \) elemje van (lásd a 12.2.1 feladatot [404]). Meglepő, hogy ezt a nagyságrendet nagyon hosszú ideig egyáltalán nem sikerült megjavítani. Csak 1981-ben igazolták Ajtai Miklós, Komlós János és Szemerédi Endre, hogy létezzen olyan végölen Sidon-sorozat, amelynek minden (elég nagy) \( n \)-re \( n \)-ig legalább \( e^{\sqrt{n}\log n} \) elemje van, ahol \( c \) alkalmas pozitív konstans. Amint látjuk, ez is csak „alig” volt jobb, mint a mohó algoritmuszal adódó \( \sqrt{n} \) . 1997-ben Ruzsa Imre ezt jelentősen megjavította \( e^{\sqrt{-\frac{1}{2}\log n}} \)-ra, azonban még ez az eredmény is igen messze van az Erdős által sejtett \( n^{1/2} \) -os nagyságrendtől (ahol \( \varepsilon \) tetszőlegesen kicsi pozitív valós szám).

Végül tekintsünk olyan végölen sorozatokat, amelyekre a Sidon-tulajdonság helyett csak azt a gyengébb kikötést tesszük, hogy a pozitív egészeknek az \( a_1 + a_j \) alakban történő előállítászára maradjon korlátos (a Sidon-sorozatoknál ez a korlát 1). Megmutatjuk, hogy az ilyen sorozatokra az \( n^{1/2} \) -os nagyságrend valóban elérhető:

12.2.6 Tétel .  T 12.2.6

Minden \( \varepsilon > 0 \)-hoz létezik olyan \( m \) egész és olyan \( A = \{1 \leq a_1 < a_2 < \ldots \} \) végölen sorozat, amelyre

\[
\liminf_{n \to \infty} \inf_{l > 2} \frac{A(n)}{\sqrt{n^{1/2} - \varepsilon}} > 0,
\]

és bármely benn belüli \( m \)-féléképpen áll elő \( a_i + a_j \) alakban.

A T 12.2.6 Tétel Erdős és Rényi eredménye, bizonyításuk az ún. véletlen módszerek egyik első szármeléleti megjelenése volt: a természetes számok sorozatainak halmazán alkalmaz valószínűségi mezőt bevezette azt mutatott meg, hogy (ezen valószínűség szerint) „majdnem minden” számsorozat megfelel a követelményeknek. Ezt a módszert használjuk majd a T 12.6.3 Tétel bizonyításánál.

A T 12.2.6 Tételre adott alábbi elemi bizonyítás Ruzsa Imrétől származik.

Bizonyítás: Változó alapú szármrendszert fogunk használni, azaz a számokat

\[
c_1 + c_1 k_1 + c_2 k_1 k_2 + \cdots + c_k k_1 \cdots k_i + \cdots
\]

alakban írjuk fel, ahol \( k_1, k_2, \ldots \) rögzített 1-nél nagyobb egészek (a „változó alap”) és \( 0 \leq c_i < k_{i+1} \) a számjegyek. Az alapokat most lassan növő sorozatként úgy választjuk meg, hogy valamilyen kis rögzített pozitív \( \delta \) -val

\[
k_{i+1} \approx k_{i+1}^{1-\delta}
\]

teljesüljön. Lerögzítünk továbbá minden \( i \)-re \( 0 \) és \( \delta \)-között egy-egy maximális elemszámú (véges) \( S_i \) Sidon-sorozatot.
A tétel előírásainak megfelelő sorozatot ezután a következőképpen konstruálunk. Azokat a számokat vesszük, amelyek minden számjegye a megfelelő Sidon-sorozatból való, azaz \( c_i \in S_{i+1} \), és ráadásul legfeljebb \( t \) kivétellel valamennyi számjegy 0.

Az ilyen számok összeadásakor nem keletkezik átvitel, és így a Sidon-tulajdonság miatt bármely természetes szám legfeljebb \( 2^t \)-féléképpen áll elő két ilyen szám összegeként (a jegyek az egyes helyértékekében felcserélődhetnek), tehát \( m = 2^t \). A megfelelő sűrűséget \( \delta \) és \( \epsilon \) alkalmaz megválasztásával fogjuk biztosítani.

Legyen \( n \) tetszőleges, ekkor alkalmaz \( j \)-re

\[
\begin{align*}
k_1 k_2 \ldots k_j \leq n < k_1 k_2 \ldots k_j k_{j+1}. 
\end{align*}
\]

A sorozatban biztosan szerepelnek azok az egészek, amelyek számjegyeire

\[
\begin{align*}
c_0 = c_1 = \cdots = c_{j-\tau-1} = 0 \quad \text{és} \quad c_i \in S_{i+1}, i = j - \tau, \ldots, j - 1
\end{align*}
\]

teljesül. Megmutatjuk, hogy már ezek száma is \( > n^{1/2-\epsilon} \), ha a \( \delta \)-t elég kicsinek, \( t \) értékét pedig elég nagynak választjuk.

Nézzük a részleteket. Legyen \( k_1 = r \) és (18)-nak megfelelően

\[
\begin{align*}
k_i = \left\lfloor r^{(1 + \delta)^{j-1}} \right\rfloor,
\end{align*}
\]

és így

\[
\begin{align*}
|S_j| > \sqrt[k_2]{k_2^2} > r^{k_2}, \quad \text{ahol} \quad k_2 = \frac{(1 + \delta)^{j-1} - \log r}{2}, \quad (22)
\end{align*}
\]

A (20)-nak eleget tevő számok számát \( K \)-val jelölve, elég belátnunk, hogy minden elég nagy \( n \)-re

\[
\begin{align*}
K > n^{1/2-\epsilon}, \quad \text{azaz} \quad \log r, K > \left( \frac{1}{2} - \epsilon \right) \log r, n. \quad (23)
\end{align*}
\]

Először felülről becsüljük \( \log r, \tau \)-et (19) és (21) alapján:

\[
\begin{align*}
\log r, n < \log r, (k_1 k_2 \ldots k_{j+1}) \leq 1 + (1 + \delta) + \cdots + (1 + \delta)^j < \frac{(1 + \delta)^{j+1}}{\delta}. \quad (24)
\end{align*}
\]

Most alulról becsüljük \( \log r, K \)-t. Mivel \( K = |S_{j-\tau-1}| \cdots |S_j| \), így (22) alapján

\[
\begin{align*}
\log r, K > \frac{(1 + \delta)^{j-\tau-1} + \cdots + (1 + \delta)^{j-2} - \tau \log r}{2} - \log r, \tau = \frac{(1 + \delta)^{j-2} - \tau \log r}{2} = \frac{(1 + \delta)^{j-1} - (1 + \delta)^{-t}}{2} \left( 1 - \frac{(1 + \delta)^{-t}}{2} \right). \quad (25)
\end{align*}
\]

Végül (24) és (25) alapján

\[
\begin{align*}
\frac{2 \log r, K}{\log r, n} > \frac{(1 + \delta)^{j(1 + \delta)^{j-1}} - \tau \log r, \tau}{(1 + \delta)^{j+1}} = \frac{(1 + \delta)^{j(1 + \delta)^{j-1}} - (1 + \delta)^{-t}}{1 + \delta - (1 + \delta)^{-t}} \log r, \frac{1}{(1 + \delta)^{j+1}}. \quad (26)
\end{align*}
\]
Feladatok

12.2.1 Mutassuk meg, hogy a mohó algoritmust 1 és \( n \) között egy legalább \( \sqrt[3]{n} \) elemű Sidon-sorozatot kapunk.

12.2.2 Legyen \( P \) primszám és \( a_i = 1 + 2ip + (i^2 \text{ mod } p) \) \( i = 0, 1, \ldots, p-1 \), ahol \( i^2 \text{ mod } p \) az \( i^2 \) legkisebb nemnegatív maradékáját jelöli modul-7 módon. Lássuk be, hogy így \( a_1 = 2p^2 \) és egy \( \sqrt{n/2} \) elemzámú Sidon-sorozatot kapunk az \([1 : n]\) intervallumban.

12.2.3 (M [627]*) Legyen \( P \) tetszőleges primszám. Ekkor létezik \( P \) darab olyan \( a_1 \), amelyre az \( a_i + a_j \) összegek (nemcsak hogy különbözők, hanem ráadásul) páronként inkongruensek modulo \( p^2 - 1 \).

Megjegyzés: Az előzővel nyilván ekvivalens, hogy
\[
- \text{az } i \neq j \text{-re az } a_i - a_j \text{ különbösségek (nemcsak hogy különbözők, hanem ráadásul) páronként inkongruensek modulo } p^2 - 1. \]
A szereplő különbösségek száma \( p^2 - p \), és modulo \( p^2 - 1 \) összesen csak \( p^2 - 2 \) darab nemnulla maradék van. Vagyis az \( a_i - a_j \) különbösségek majdnem minden maradékot előállítanak. A bizonyításból leolvasható, hogy
\[
\text{éppen a } p + 1 \text{-gyel osztható maradékok maradnak ki. } \]
A feladatból a T 12.2.3 Tétel hasonló módon vezethető le, mint ahogyan a T 12.2.2 Tételből következett (ugyanez érvényes a következő feladatra is).

12.2.4 (M [627]*) Legyen \( P \) tetszőleges primszám. Ekkor létezik \( p - 1 \) darab olyan \( a_1 \), amelyre az \( a_i - a_j \) különbösségek (nemcsak hogy különbözők, hanem ráadásul) páronként inkongruensek modulo \( p^2 - p \).

12.2.5 Konstruáljunk olyan \( A \) végletes Sidon-sorozatot, amelyre bármely \( \varepsilon > 0 \) esetén végletes sok \( n \) -re \( A(n) > \left(1/\sqrt[3]{2} - \varepsilon\right)\sqrt{n} \) (azaz \( \limsup_{n \to \infty} A(n)/\sqrt{n} \geq 1/\sqrt[3]{2} \)).

Megjegyzés: Megoldatlan, hogy ugyanaz \( 1/\sqrt[3]{2} \) helyett 1-gyel is igaz-e.

12.2.6 Többtagú összegek. Legyen \( h \geq 2 \) rögzített természetes szám, és az \([1, n]\) intervallumban tekintsünk most olyan sorozatokat, ahol az elemekből képezett \( h \) -tagú összegek mind különbözők.

(a) * Mutassuk meg, hogy van olyan sorozat, amelynek „körülbél” \( n^{1/h} \) eleme van.

(b) Lássuk be, hogy van olyan csak a \( h \) -tól függő \( c = c(h) \) konstans, hogy minden ilyen sorozatnak legfeljebb \( c(h)n^{1/h} \) eleméje van.

Megjegyzés: Megoldatlan probléma, hogy \( c(h) \) vajon \( 1 + \varepsilon \) -ra csökkenhető-e, azaz bármely \( h \) -ra igaz-e, hogy a \( h = 2 \) esetben hasonlóan a maximális elemzám aszimptotikusan \( n^{1/h} \). A T 12.2.4 Tétel bizonyítása azért nem vihető át, mert \( h 
eq 2 \) -re a feltétel nem lehet összegekről különbösségekre átjátszani.
12.2.7 Mutassuk meg, hogy létezik egészeknek olyan $a_1 < a_2 < \ldots$ végként sorozata, hogy a 0-n kívül minden egész szám egyértelműen írható fel $a_i - a_j$ alakban.

12.2.8 A természetes számok két (végként) részesorozatát, $A$ és $B$-t nevezzük jó sorozatpárnak, ha az $a + b$ ($a \in A, b \in B$) összegek mind különbözők. Jó sorozatpárt kapunk például, ha egy Sidon-sorozatot két részre vágunk. Mutassuk meg, hogy létezzen ennél „sűrűbb” jó sorozatpárok is: adjunk meg olyat, amelynél minden $n$-re $A(n) > c\sqrt{n}$, $B(n) > c\sqrt{n}$, $c > 0$ konstansnál.

12.3 Összeghalmazok

Ebben a pontban $A + A = \{a_i + a_j \mid a_i, a_j \in A\}$ típusú halmazokkal foglalkozunk, ahol $A$ elemei a $\{0, n - 1\}$ intervallumba eső egészek vagy pedig modulo $p$ maradékosztályok, ahol $p$ prím. Jelölje $A$ elemszámát $|A| = k$.

$A + A$ elemszáma akkor a lehető legnagyobb, ha $A$ Sidon-sorozat, ekkor $|A + A| = \binom{k+1}{2}$. Most először az ellenkező végletet vizsgáljuk meg: mekkora lehet $|A + A|$ lehető legkisebb értéke. Ha $A$ elemei egész számok, akkor e a várákokéznak megfelelően akkor lép fel, ha $A$ elemei egy számjegyos sorozat egymást követő tagjai, és így $\min |A + A| = 2k - 1$ (lásd a 12.3.1 feladatot [413]).

A Sidon-sorozat adódik $A + A$ minimumára akkor is, ha $A \subseteq \mathbb{Z}_p$ (azaz $A$ elemei modulo $p$ maradékosztályok), ezt a (már egyáltalán nem nyilvánvaló) tényt a T 12.3.1 Tételben igazoljuk. Ezt a tételeit már Cauchy is bebizonyította, majd 120 évvel később két kiváló matematikus, Davenport és Chowla, egymástól függetlenül újra felfedezte. A tételre két bizonyítást adunk, és a feladatok között a tételnek, illetve a bizonyítási módszereknek több érdekes alkalmazását mutatjuk be (lásd a 12.3.3–12.3.8 feladatokat [414]).

Az összeghalmazokkal kapcsolatos másik vizsgálatunk is valamilyen értelmeben a Sidon-tulajdonság duálisának tekinthető. A véges Sidon-sorozatok esetén lőjol, minél nagyobb elemszámú $A$ halmazok előállítása volt azt egyik cél, hogy minden egész szám legfeljebb egyféléképpen legyen felírható $a_i + a_j$ alakban. Most olyan, minél kisebb elemszámú $A$ halmazokat keressünk, hogy minden, a $\{0, n - 1\}$ intervallumba eső egész szám legfeljebb egyféléképpen legyen felírható $a_i + a_j$ alakban. Az ilyen tulajdonságú $A$ halmazokat (másodrendű additív) bázisoknak nevezzük. A bázisok elemszámának minimumára a T 12.3.3 Tételben adunk alsó és felső becslést.

Térjünk rá $|A + A|$ minimumának a meghatározására, ha $A \subseteq \mathbb{Z}_p$. Kicsit általánosabban, az $A + B = \{a + b \mid a \in A, b \in B\}$ halmaz elemszámának minimumát fogjuk meghatároznii $|A|$ és $|B|$ függvényében. Ezt nemcsak azért teszünk, hogy minél általánosabb eredményt nyerjünk, hanem — mint a matematikában oly sokszor — az általánosítás adja a kulcsot magának az eredeti állításnak az igazolásához is.

12.3.1 Tétel (Cauchy–Davenport–Chowla-tétel) . T 12.3.1

Legyen $p$ prím, $A, B \subseteq \mathbb{Z}_p$, $|A| = k(> 0)$, $|B| = r(> 0)$. Ekkor

$|A + B| \geq \min(p, k + r - 1)$. \hspace{1cm} (1)

A $p$ -re mint korlátz kimenő a (1)-ben azért van szükség, mert $A + B \subseteq \mathbb{Z}_p$, és így nyilván $|A + B| \leq p$ .

Az egyenlőtlenség éles: ha $A = \{0, 1, \ldots , k - 1\}$, $B = \{0, 1, \ldots , r - 1\}$, akkor $|A + B| = k + r - 1$, tehát $|A + B| = k + r - 1$, azaz (1)-ben egyenlőség teljesül.
Az $A = B$ speciális esetben kapjuk, hogy $|A + A| \geq \min\{p, 2k - 1\}$, és egyenlőség teljesül, ha (például) $A = \{0, 1, \ldots, k - 1\}$.

Első bizonyítás: Tegyük fel indirekt, hogy (valamilyen rögzített $P$ mellett) van olyan $A$ és $B$, amelyre (1) nem igaz, és nevezzük (házi használatra) csúnyanak az ilyen halmazpárokat.

Tekintsünk egy olyan $A, B$ csúnya halmazpárt, $|A| = k$, $|B| = r$, amelyre $r$ a lehető legkisebb. Konstruáljunk függünk olyan $A'$, $B'$ csúnya halmazpárt, $|A'| = k'$, $|B'| = r'$, ahol $r' < r$, ami ellentmond $r$ minimalitásának. Ez azt jelenti, hogy az indirekt feltéveink (ti. hogy léteznek csúnya halmazpárok) ellentmondásra vezetett, amivel a tétel állítását bebizonyítottuk.

Ha $k + r - 1 > p$, akkor $B$-ből hagyjunk el $k + r - 1 - p' < r'$ elemet, a maradék halmazt jelölje $B'$, és legyen $A' = A$. Nyilván
\[|A' + B'| \leq |A + B| < \min(p, k + r - 1) = p - \min(p, k' + r' - 1),\]

tehát $A'$, $B'$ is csúnya és $(0 <) p' < r'$, ami lehetetlen. Ezért $k + r - 1 \leq p$.

Nyilván $k \geq r \geq 2$, hiszen $k < r$ esetén $A$ és $B$ szerepcseréjéivel ellentmondásra jutunk $r$ minimalitásával, $r = 1$ esetén pedig (1)-ben egyenlőség áll, azaz $A$, $B$ nem lenne csúnya. Mivel $r \geq 2$ és $k + r - 1 \leq p$, ezért $k < p$ is teljesül.

Azt is feltehetjük, hogy $0 \in B$, mivel $B$ minden eleméhez ugyanazt az értéket hozzáadva, $|A|$, $|B|$ és $|A + B|$ egyike sem változik.

Megmutatjuk, hogy ha $b \neq 0$ tetszőleges rögzített eleme $B$-nek, akkor $A + b = \{c + b \mid c \in A\} \not\subseteq A$. Elenkező esetben ugyanis $A + b = A$ teljesülne, és így a két oldalon álló halmazok elemeinek összege megegyezne:
\[\sum_{a \in A} a = \sum_{a \in A} (a + b) = k b + \sum_{a \in A} a,\]

vagyis $k b = 0$, ami $k < p$ és $b \neq 0$ miatt lehetetlen.

Az előzők alapján van olyan $a_1 \in A$ és $b_1 \in B$, amelyre $a_1 + b_1 \not\in A$. Legyen
\[A' = A \cup \{a_1 + b \mid b \in B, a_1 + b \not\in A\} \quad \text{és} \quad B' = \{b \mid a_1 + b \in A\}.
\]

Ekkor nyilván $k' + r' = k + r$ és $0 < r' < r$ (hiszen $0 \in B'$, de $b_1 \not\in B'$). Megmutatjuk, hogy $A' + B' \subseteq A + B$. Legyen $a' + b' \in A' + B'$. Ha $a' \in A$, akkor nyilván $a' + b' \subseteq A + B$ és $a' = a_1 + b$, akkor
\[a' + b' = (a_1 + b) + b' = (a_1 + b') + b \in A + B,
\]

hiszen $B'$ definíciója miatt $a_1 + b' \in A$. Mindez alapján
\[|A' + B'| \leq |A + B| < \min(p, k + r - 1) = k + r - 1 = k' + r' - 1 = \min(p, k' + r' - 1),\]

tehát $A'$, $B'$ is csúnya, továbbá $r' < r$, amivel a kivánt ellentmondásra jutottunk.

A T 12.3.1 Tétel második bizonyításához szükségünk lesz az alábbi egyszerű segítdítelre:
12.3.2 Lemma \( \text{L 12.3.2} \)

Legyen \( T \) tetszőleges kommutatív test, \( A, B \subseteq T \), \( |A| = k \), \( |B| = r \), és \( f(x, y) \) olyan \( T \) feletti kétváltozós polinom, amelynek \( x \), illetve \( y \) szerinti foka \( k \) -nál, illetve \( r \) -nél kisebb (azaz \( f(x, y) = \sum_{i=0}^{k} \sum_{j=0}^{r} \alpha_{i,j} x^i y^j \)). Tegyük fel, hogy minden \( a \in A \) és \( b \in B \) esetén \( f(a, b) = 0 \).

Ekkor \( f \) a nullpolinom (azaz minden együtthatója 0).

**A \text{L 12.3.2 Lemma bizonyítása:}** Írjuk fel \( f(x, y) \cdot t \ y \) polinomjaként, ekkor az együtthatók \( x \) polinomjai lesznek:

\[
f(x, y) = l_0(x) + l_1(x) y + \cdots + l_{r-1}(x) y^{r-1}, \quad \deg l_i \leq k - 1.
\]

Legyen \( a \in A \) -ra

\[
y_a(y) = f(a, y) - l_0(a) + l_1(a) y + \cdots + l_{r-1}(a) y^{r-1}.
\]

Ekkor egyrészt \( \deg y_a \leq r - 1 \), másrészt minden \( b \in B \) -re \( y_a(b) = f(b, b) = 0 \), azaz \( y_a \) -nak legalább \( r \) gyöke van. Ez csak úgy lehetséges, ha \( y_a \) minden együtthatója 0. Ez azt jelenti, hogy a legfeljebb \( k - 1 \) -edfokú \( y_a \) polinomoknak minden \( a \in A \) gyöke, azaz legalább \( k \) gyökük van, és így szükségképpen \( \deg y_a = 0 \) (azaz minden együtthatójuk 0). Ebből (2) alapján kapjuk, hogy \( f = 0 \).

**A \text{T 12.3.1 Tétel második bizonyítása:}** Indirekt tegyük fel, hogy van olyan \( A \) és \( B \), amelyre (1) nem igaz. Az első bizonyításban látottak szerint feltételezhető, hogy \( k + r - 1 \leq p \) (ahol \( |A| = k \), \( |B| = r \)). Legyen \( C = A + B \), ekkor \( |C| \leq k + r - 2 < p \). Legyen

\[
f_t(x, y) = (x + y)^p \prod_{i \in \mathbb{Z}} (x + y - c), \quad \text{ahol} \ n = k + r - 2 - |C|.
\]

Ekkor \( f_t(a, b) = 0 \) minden \( a \in A \), \( b \in B \) esetén.

Az \( f_t(x, y) \) polinomra közvetlenül nem alkalmazhatjuk a L 12.3.2 Lemmát, mert előfordulnak benne olyan \( x^i y^j \) tagok, amelyekben \( i \geq k \) vagy \( j \geq r \). Tekintsük egy tetszőleges \( x^i \cdot t \), ahol \( i \geq k \), és cseréljük ezt ki egy olyan legfeljebb \( k - 1 \) -edfokú \( u_i(x) \) polinomra, amely minden \( a \in A \) helyen ugyanazt az értéket veszi fel, mint \( x^i \), azaz minden \( a \in A \) -ra \( u_i(a) = a^i \). Ilyen \( u_i(x) \) ún. interpolációs polinom (egyértelműen) létezik (lásd például Freud: Lineáris algebra, 3.2.4 Tétel).

Hasonlóan járunk el, ha \( j \geq r \), ekkor \( y^j \) helyére kerül olyan legfeljebb \( r - 1 \) -edfokú \( u_j(y) \), amelynél minden \( b \in B \) -ra \( u_j(b) = b^j \).

Az így kapott \( f_t(x, y) \) polinomra \( f_t(a, b) = 0 \) minden \( a \in A \), \( b \in B \) esetén, továbbá csak olyan \( x^i y^j \) tagok szerepelnek \( f \) -ben, ahol \( i \leq k - 1 \), \( j \leq r - 1 \). A \text{L 12.3.2 Lemma} szerint így \( f_t \) minden együtthatója 0.

**Vizsgáljuk most meg \( f_t \)-ben \( x^{k-1} y^{r-1} \) együtthatóját közvetlenül is.**

Mivel az \( f_t \) polinomban (3) alapján csak \( x^i y^j \) -ből keletkeznek olyan \( x^i y^j \) tagok, ahol \( i + j = k + r - 2 \), minden más tagra \( i + j < k + r - 2 \), továbbá az \( f_t \) -et előállító redukciós eljárás során az \( i \geq k \), illetve \( j \geq r \) típusú \( x^i \), illetve \( y^j \) tényezők kisebb fokszámúakra cserélődnek, így \( f_t \) -ben egyetlen \( x^{k-1} y^{r-1} \) tag képződik, az, amely az \( (x+y)^{k+r-2} \) hatványozás elvégzéséből
közvetlenül adódik; ennek együthattója \( \binom{k+r-2}{k-1} \). Mivel \( k + r - 2 < p \), ezért ez az együthattó (\( \mathbb{Z}_p \)-ben) nem 0. Ez ellentmond annak, hogy \( f \) minden együthattója 0.

Most rátérünk a bázisok elemszámának vizsgálatára. A definíciót megismételve, a \([0, n-1]\) intervallum egy (másodrendű aditív) bázisán nemnegatív egészek olyan \( A \) halmazát értjük, hogy minden \( 0 \leq r \leq n-1 \) egész felírható két \( A \)-beli elem összegeként, azaz \( r = a_i + a_j \) alakban (\( a_i, a_j \in A \)).

Ha \( |A| = k \), akkor az \( a_i + a_j \) összegek száma \( \binom{k+1}{2} \), és ha \( A \) bázis, akkor ezek az összegek legalább \( n \) különböző értéket adnak, tehát

\[
\binom{k+1}{2} \geq n, \quad \text{azaz} \quad k > \sqrt{2n} - 1.
\]

Másrészt, ha \( n \) négyzetszám, \( n = s^2 \), akkor az \( n \)-nél kisebb egészek az \( s \) alapú számrendszerben (legfeljebb) kétjegyűek, vagyis felírhatók \( i + sj \) alakban, ahol \( 0 \leq i, j \leq s - 1 \). Ezt azt jelenti, hogy

\[
A = \{0, 1, \ldots, s-1, s, 2s, \ldots, (s-1)s\}
\]

másodrendű bázis, amelynek elemszáma \( 2s = 2\sqrt{n} \). Ha \( n \) nem négyzetszám, akkor a fentieket \( n \) helyett az \( n \)-et követő legkisebb négyzetszámra lehet elmondani, ekkor tehát \( s = \lceil \sqrt{n} \rceil \).

Az előző meggyondolásokból a bázisok elemszámának minimumára az alábbi becsléseket kapjuk:

\[
\sqrt{2n - 1} < k < 2\sqrt{n} + 2
\]

A következő tételben megmutatjuk, hogy \( \sqrt{n} \) együthattója mindkét becslésben (valamelyest) javítható:

**12.3.3 Tétel.**

Jelölje \( f(n) \) a \([0, n-1]\) intervallumra vonatkozó másodrendű aditív bázisok elemszámának minimumát. Ekkor bármely \( \varepsilon > 0 \) mellett elég nagy \( n \)-re

\[
\frac{\sqrt{2n}}{\sqrt[4]{144}} \sqrt{n} - 2 < f(n) < \sqrt{3,5 + \varepsilon} \sqrt{n}.
\]

A Fried Katalintól származó felső becslés a jelenleg ismert legjobb eredmény, az alsó becslés esetén (Leo Mosertől származó) módszer további finomításával valamivel jobb konstans is elérhető.

**Bizonyítás:** A felső becsléshez vegyük észre, hogy a tétel kimondása előtt megadott számrendszerez konstrukció tulajdonképpen két számtani sorozat egyesítéseként állítja elő a bázist. Ennek a gondolatnak a variálásával most öt számtani sorozat uniójaként készíthetjük el a megfelelő bázist.

Legyen \( l \) tetszőleges pozitív egész, és tekintsük az alábbi öt (diszjunkt) számtani sorozatot:

\[
\begin{align*}
B &= \{a_0, \ldots, a_t\} = \{j \mid 0 \leq j \leq t\}; \\
C &= \{c_0, \ldots, c_{3t}\} = \{2t + 1 + j(t + 1) \mid 0 \leq j \leq 3t - 1\}; \\
D &= \{d_0, \ldots, d_t\} = \{3t^2 + 5t + 1 + j \mid 0 \leq j \leq t\}; \\
E &= \{e_0, \ldots, e_t\} = \{6t^2 + 12t + 3 + jt \mid 0 \leq j \leq t\}; \\
P &= \{f_0, \ldots, f_t\} = \{10t^2 + 18t + 5 + jt \mid 0 \leq j \leq t\}.
\end{align*}
\]
A számtani sorozatok különbsége tehát rendre $1, t + 1, 3t + 1, 7t + 1, 15t + 1$, az elemszámuk pedig $t + 1, 3t + 1, 7t + 1, 15t + 1, 31t + 1$.

Jelölje $A_t$ az öt sorozat egyesítését, ekkor $|A_t| = 7t + 4$. Beláthatjuk, hogy $A_t$ másodrendű bázis $a = 14t^2 + 24t + 7$-re, azaz $14t^2 + 24t + 6$-ig minden egész előáll két $A_t$-beli elem összegeként. Innen a felső becslés már következik: tetszőleges $n$ esetén végyük azt a legkisebb $t$ értéket, amelyre $n \leq 14t^2 + 24t + 7$, ekkor $A_t$ megfelelő bázis $n$-hez és $|A_t| = 7t + 4 \sim \sqrt{3,5n}$, ha $n \to \infty$ (hiszen $t \sim \sqrt{n/14}$).

Most tehát azt igazoljuk, hogy minden $0 \leq r \leq 14t^2 + 24t + 6$ egész felírható két $A_t$-beli elem összegeként. Jelöljük $[[x, y]]$-nal az $[x, y]$ intervallumba eső egészek halmazát. Nyilván

$$B + B = [[0, 2t]] \quad \text{és} \quad B + C = [[2t + 1, 3t^2 + 5t]].$$

Hasonlóan adódik, hogy

$$B + D = [[3t^2 + 5t + 1, 3t^2 + 7t + 1]],$$
$$C + D = [[3t^2 + 7t + 2, 6t^2 + 10t + 1]],$$
$$D + D = [[6t^2 + 10t + 2, 6t^2 + 12t + 2]],$$
$$B + E = [[6t^2 + 12t + 3, 7t^2 + 13t + 3]].$$

Az eddigiak alapján $A_t + A_t \supseteq [[0, 7t^2 + 13t + 3]]$.

Most megmutatjuk, hogy $C + E \supseteq [[7t^2 + 13t + 4, 9t^2 + 17t + 3]]$. Először is

$$c_0 + e_{t-1} = (2t + 1) + (7t^2 + 11t + 3) = 7t^2 + 13t + 4.$$

Mivel a $C$ sorozat differenciája $t + 1$-es, az $E$ é pedig $t$-es, ezért érdemes $C$ egymás után következő elemeihez rendre $E$-nek mindig a megfelelő korábbi elemeit hozzáadni:

$$c_1 + e_{t-2} = c_0 + c_{t-1} + 1,$$
$$c_2 + e_{t-3} = c_0 + c_{t-1} + 2,$$
$$\ldots$$
$$c_{t-1} + e_0 = c_0 + c_{t-1} + (t-1).$$

A következő egész a $c_0 + e_t = c_0 + e_{t-1} + t$ összegként kapjuk meg, majd ismét $C$ elemei előre, $E$ elemei pedig visszafelé haladva a $e_t + e_{t-i}$ összegek minden egész előállítanak $c_t + e_0 = c_0 + e_t + t$-ig. Ezután $c_1 + e_t = c_0 + e_t + (t + 1)$-ig vagyóra, majd a $c_{t+1} + e_{t-i}$ összegeket véve megkapjuk a következő $t + 1$ egész. Az eljárást hasonlóan folytatva egészen a $c_{t+1} + e_1 = 9t^2 + 17t + 3$ összeggig juthatunk el, azaz valóban $C + E \supseteq [[7t^2 + 13t + 4, 9t^2 + 17t + 3]]$.

Továbbhaladva, nyilván $D + E = [[9t^2 + 17t + 4, 10t^2 + 18t + 4]]$.

Végül, az előzőekhez hasonlóan megmutatható, hogy

$$B + F = [[10t^2 + 18t + 5, 11t^2 + 19t + 5]],$$
$$C + F = [[11t^2 + 19t + 6, 13t^2 + 23t + 5]],$$
$$D + F = [[13t^2 + 23t + 6, 11t^2 + 24t + 6]].$$
Ezzel igazoltuk, hogy valóban minden \( 0 \leq r \leq 14t^2 + 24t + 6 \) egész számra \( \tau \in A_t + A_{t'} \), és ezzel a felső becslés bizonyítását befejeztük.

Az alsó becsléshez tekintsünk egy \( A = \{ 0 \leq a_1 < \cdots < a_k \leq n - 1 \} \) tetszőleges másodrendű bázist a \([0, n - 1]\) intervallumon. Legyen

\[
\hat{h}(x) = \sum_{i=1}^{k} x^{a_i} \quad (\theta)
\]

az \( A \) bázishoz tartozó „generatorfüggvény”, ekkor

\[
\hat{h}^2(x) = \left( \sum_{i=1}^{k} x^{a_i} \right) \left( \sum_{j=1}^{k} x^{a_j} \right) = \sum_{i,j=1}^{k} x^{a_i+a_j} - 2 \sum_{1 \leq i < j \leq k} x^{a_i+a_j} + \sum_{i=1}^{k} x^{2a_i} = 2 \sum_{1 \leq i < j \leq k} x^{a_i+a_j} - \sum_{i=1}^{k} x^{2a_i} - \sum_{i=1}^{k} x^{a_i} - 1 \cdot (x^2).
\]

Innen

\[
g(x) = \sum_{1 \leq i < j \leq k} x^{a_i-a_j} - \frac{h^2(x) + h(x^2)}{2}. \quad (\tau)
\]

A \( g(x) \) polinomban \( x^r \) együtthatója éppen azt mutatja, hogy az \( \tau \) hányféleleképpen áll elő \( a_i + a_j \) alakban, ahol \( i \leq j \). Mivel az \( a_i + a_j \) összegek minden \( 0 \leq r \leq n - 1 \) számot előállítanak, ezért ezekre az \( \tau \)-ekre \( x^r \) együtthatója legalább 1, azaz

\[
g(x) = 1 + x + \cdots + x^{a_i-1} + \sum_{n=0}^{2a_i} u_{mn} x^m, \text{ahol } u_{mn} \geq 0. \quad (\phi)
\]

(7) és (8) alapján

\[
y(1) = \frac{l^2(1) + l(1)}{2} = \frac{k^2 - k}{2} = n + \sum_{n=0}^{2a_i} u_{mn}. \quad (\rho)
\]

Mivel \( u_{mn} \geq 0 \), ezért (9)-ből azonnal kapjuk, hogy \( (k^2 - k)/2 \geq n \), ami a tételünk kimondása előtti \( k \geq \sqrt{2n} - (1/2) \) becsélést adja. Ezt akkor tudjuk javítani, ha \( \sum_{n=0}^{2a_i} u_{mn} \) -re a 0-nál (lényegesen) jobb alsó becslést találunk.

Megmutatjuk, hogy

\[
\mathcal{S} = \sum_{n=0}^{2a_i} u_{mn} > nk^2, \quad (\kappa)
\]

ahol \( \nu > 0 \) konstans értékét a bizonyításból explicite meg fogjuk határozní, és azt (9)-be visszahelyettesítve adódik majd a tétel állításában szereplő alsó becslés.

Jelölje \( N = \tau k \), illetve \( P = (1 - \tau)k \) azoknak az \( a_i \)-knek a számát, amelyekre \( a_i > (n - 1)/2 \), illetve \( a_j \leq (n - 1)/2 \) (itt tehát \( N + P = k \) és \( \tau \) a „nagy” \( a_i \) elemek arányát jelöli ebben a konkrét \( A \) bázisban).
Vegyük észre, hogy $S' = \sum_{m=0}^{2n-2} \alpha_m$ éppen az $n-1$-nél nagyobb $\alpha_i + \alpha_j$, $i \leq j$ összegeknek a száma. Ha $\alpha_i$ és $\alpha_j$ is nagyobb, mint $(n-1)/2$, akkor $\alpha_i + \alpha_j > n - 1$, tehát

$$S \geq S' \geq \frac{(N + 1)N}{2} = \frac{\tau k + 1)(\tau k)}{2} \geq \frac{r^2}{2} \cdot k^2. \quad (11)$$

(Ez szemléletesen azt jelenti, hogy ha „sok“ $(n-1)/2$-nél nagyobb $\alpha_i$ van, akkor sok összeg „vész kárba“, és így nagyobb elemzőmű bázis szükséges az $n-1$-ig terjedő számok előállításához. Ehhez a meggondoláshoz nem is lett volna szükség a generátorfüggvényre. Azonban, ha $A$-ban a „pici” $\alpha_s$ elemek dominálnak, akkor már csak így boldogulunk, lásd az alábbiakban.)

Helyettesítsünk most be (8)-ba az $\tau$ helyére egy $\theta \neq 1$ komplex $\tau$-edik egységgyököt. Ekkor a jobb oldal elején szereplő $1 + \theta + \cdots + \theta^{\alpha-1}$ összeg 0, tehát

$$g(\theta) = \sum_{n=0}^{2n-2} \alpha_n \theta^n.$$  

Mindkét oldal abszolút értékét véve

$$|g(\theta)| = \left| \sum_{n=0}^{2n-2} \alpha_n \theta^n \right| \leq \sum_{n=0}^{2n-2} |\alpha_n| \cdot |\theta|^n = \sum_{n=1}^{2n-2} \alpha_n = S,$$

hiszen $\alpha_n \geq 0$ és $|\theta| = 1$. Innen (7) alapján

$$S \geq |g(\theta)| = \left| \frac{\hat{h}^2(\theta) + \bar{h}(\theta^2)}{2} \right| \geq \frac{|\hat{h}(\theta)|^2}{2}, \quad (12)$$

Ezt folytatva a (12) jobb szélén álló különbségre kell alsó becsést adnunk, azaz a kivonandót felülről, a kisebbítendőt pedig alulról kell becsülnünk.

A $\hat{h}(x)$ generátorfüggvény (6) definíciója alapján

$$|\hat{h}(\theta^2)| = \sum_{i=1}^{k} |\theta^2 \alpha_i| \leq \sum_{i=1}^{k} |\theta|^{2 \alpha_i} = k,$$

hiszen $|\theta| = 1$, tehát

$$\frac{|\hat{h}(\theta^2)|}{2} \leq \frac{k}{2}, \quad (13)$$

(ami elhanyagolható lesz a másik kérdéses tag, a $|\hat{h}^2(\theta)|/2$ kisebbítő $k^2$-es nagyságrendjéhez képest).

Alsó becslést keresünk tehát a

$$|\hat{h}(\theta)| = \left| \sum_{i=1}^{k} \theta^{\alpha_i} \right| \quad (14)$$

kifejezésre. Emlékezzünk vissza, hogy lényegében azzal az esettel kell megbirkóznunk, amikor az $(n-1)/2$-nél nem nagyobb $\alpha_i$-k dominálnak, vagyis $P = (1 - \tau)k$ nagy. Ennek megfelelően (14)-ben különválasztjuk a pici és a nagy $\alpha_i$-knek megfelelő részt.
KOMBINATORIKUS
SZÁMELMÉLET

\[ |l_i(q)\| = \sum_{i=1}^{\beta} \theta^{\alpha_i} + \sum_{i=P+1}^{\beta} \theta^{\alpha_i} \geq \left| \sum_{i=1}^{P} \theta^{\alpha_i} \right| - \left| \sum_{i=P+1}^{\beta} \theta^{\alpha_i} \right| \geq \sum_{i=1}^{P} \theta^{\alpha_i} - N. \quad (15) \]

Így elég a

\[ T(\phi) = \left| \sum_{i=1}^{P} \theta^{\alpha_i} \right| \quad (16) \]

kifejezésre jó alsó becslést találnunk.

Legyen \( \omega = \cos(2\pi/n) + i\sin(2\pi/n) \) és \( \beta_j = \omega^j \), \( j = 1, \ldots, P \). Mivel \( 0 \leq \epsilon_j \leq (n-1)/2 \), ezért valamennyi \( \beta_j \) komplex szám képzetes része nemnegatív, azaz a felső félsíkba esnek.

Legyen \( \alpha \) egy később alakulásban megválasztandó hegyesszög, és legyen \( F \) azoknak a \( \beta_j \) -knek a száma, amelyek \( \beta_j \) szögére \( \alpha \leq \beta_j \leq \pi - \alpha \), nevezzük ezeket „felső” \( \beta_j \) -knek. (A többi \( P - F \) darab „alsó” \( \beta_j \) esetén tehát \( 0 \leq \beta_j \leq \epsilon \) vagy \( \pi - \epsilon \leq \beta_j \leq \pi \.)

A felső \( \beta_j \) -k képzetes része \( \text{Im} (\beta_j) \geq \sin \alpha \), az alsóké \( \text{Im} (\beta_j) \geq 0 \), ezért

\[ \left| \sum_{j=1}^{P} \beta_j \right| \geq \text{Im} \left( \sum_{j=1}^{P} \beta_j \right) \geq F \cdot \sin \alpha. \quad (17) \]

Ha most \( \theta \)-t éppen \( \omega \)-nak választjuk, akkor \( \theta^{\alpha_i} = \beta_j \), és így (16) és (17) alapján

\[ T(\omega) \geq F \cdot \sin \alpha. \quad (15) \]

Legyen most \( \theta = \omega^2 \), ekkor \( \theta^{\alpha_i} = \beta_j^2 \). Az alsó \( \beta_j \) -kre \( z^2 \) szöge \( -2\alpha \) és \( 2\alpha \) közé esik, tehát a valós részük \( \text{Re} (\beta_j^2) > \cos(2\alpha) \), a felsők esetén pedig \( \text{Re} (\beta_j^2) \geq -1 \) triviálisan. Ennek alapján

\[ T(\omega^2) = \left| \sum_{j=1}^{P} \beta_j^2 \right| \geq \text{Re} \left( \sum_{j=1}^{P} \beta_j^2 \right) \geq (P - F) \cos(2\alpha) - F \quad (19) \]

Az \( \alpha = \pi/6 \) választással (18)-ből, illetve (19)-ből

\[ T(\omega) \geq F/2 \quad \text{és} \quad T(\omega^2) \geq (P - 3F)/2. \quad (20) \]

Legyen

\[ M = \max (T(\omega), T(\omega^2)), \]

akkor (20) alapján

\[ M \geq \frac{3T(\omega) + T(\omega^2)}{4} \geq \frac{P}{8}, \]

és így azt kaptuk, hogy alkalmas \( \theta \) -val (\( \theta = \omega \) vagy \( \theta = \omega^2 \)) a (16)-beli \( T(\phi) \)-ra \( T(\phi) \geq P/8 \) teljesül. Ezt (15)-be beírva

412
\[ |\lambda(i)| \geq \frac{P}{8} - N = \frac{1 - 9r}{8} k \]  \hspace{1cm} (21) \]

adódik. Így (12), (13) és (21) alapján

\[ S \geq \frac{(1 - 9r)^2}{128} k^2 - \frac{k}{2}. \]  \hspace{1cm} (22) \]

Figyelembe véve (11)-et is kapjuk, hogy

\begin{align*}
S & \geq \max \left\{ \frac{r^2}{2} k^2, \frac{(1 - 9r)^2}{128} k^2 - \frac{k}{2} \right\}. \hspace{1cm} (23)
\end{align*}

A „legrosszabb” eset, ha a két értékben a \( k^2 \) együthatója megegyezik, azaz \( \tau = 1/17 \), és ekkor

\[ S \geq \frac{k^2}{578} - \frac{k}{2}, \]  \hspace{1cm} (24) \]

azaz (10) (a \( k^2/2 \) hibatagtól eltekintve) a \( v = 1/578 \) konstanssal teljesül.

(24)-et (9)-be behelyettesítve kapjuk, hogy

\[ \frac{k^2 - k}{2} \geq n + \frac{k^2}{578} - \frac{k}{2}, \]

ahonnán

\[ \frac{144}{289} k^2 + k \geq n, \]

és így

\[ (k + 2)^2 > \frac{289}{144} n, \]

ami éppen a tételben állított alsó becslést jelenti.  

**Feladatok**

12.3.1 Igazoljuk a valós számok részhalmazaira vonatkozó alábbi állításokat.

(a) Ha \( |A| = k \), akkor \( |A \cup A| \geq 2k - 1 \), és egyenlőség akkor és csak akkor teljesül, ha \( A \) elemei számtani sorozatot alkotnak.

(b) Ha \( |A| = k \), \( |B| = r \), akkor \( |A \cup B| \geq k + r - 1 \), és egyenlőség akkor és csak akkor teljesül, ha \( k = 1 \) vagy \( r = 1 \), vagy pedig \( A \) és \( B \) elemei azonos differenciájú számtani sorozatot alkotnak.

(c) Ha \( |A_i| = k_i \), \( i = 1, 2, \ldots, t \), akkor \( |A_1 + \cdots + A_t| \geq k_1 + \cdots + k_t - 1 \), és ha \( k_i > 1 \), \( i = 1, 2, \ldots, t \), akkor egyenlőség pontosan abban az esetben teljesül, ha minden \( A_i \)-ben az elemek azonos differenciájú számtani sorozatot alkotnak.

12.3.2 Igazoljuk a T 12.3.1 Tétel tetszőleges \( m \) modulusra vonatkozó alábbi általánosítását: Legyen \( A, B \subseteq \mathbb{Z}_m \), \( 0 \in B \). Ekkor \( |A + B| \geq \min \{ |A|, |A| + s \} \), ahol \( s \) a \( B \) elemei között az \( m \)-hez relatív prímek száma. Mutassunk példát olyan összetett \( m \)-re és \( s < |B| - 1 \)-re, amikor egyenlőség teljesül.

12.3.3 Bizonyítsuk be az alábbi állításokat.
(a) Legyen $A, B \subseteq \mathbb{Z}_{m}$, $\emptyset \in A \cap B$, és tegyük fel, hogy $a \in A, b \in B$ mellett $a + b = 0$ csak $a = b = 0$ esetén teljesül. Ekkor $|A + B| \geq |A| + |B| - 1$. (A feltételből most következik, hogy $|A| + |B| - 1 \leq m$, ezért az állításban az egyenlőtlenségnél nincs szükség a T 12.3.1 Tételhez hasonló minimumos megfogalmazásra.)

(b) Az (a)-beli egyenlőtlenség éles.

c) Az (a)-beli állítás $\mathbb{Z}_{m}$ helyett tetszőleges Abel-csoport (véges) részhalmazaira is teljesül.

12.3.4 (*) Legyen $p$ prím, $A \subseteq \mathbb{Z}_{p}$, $|A| = k$ és $A + A = \{a + a' \mid a, a' \in A, a \neq a'\}$, azaz most csak a különböző elemekből képezett kéttágú összegek halmazát vizsgáljuk. Igazoljuk, hogy $|A + A| \geq \max(p, 2k - 3)$.

Megjegyzések: 1. Erdősnek és Heilbronn-nak ezt a sokáig megoldatlan sejtését Hamidoune és Da Silva igazolta először, majd Alon, Ruzsa és Nathanson adott rá egyszerűbb bizonyítást.

2. Az $A = \{0, 1, \ldots, k - 1\}$ példa mutatja, hogy ez a becslés nem javítható.

12.3.5 (a) Legyen $T$ tetszőleges kommutatív test, $A, B \subseteq T$, $|A| = k$, $|B| = r$, továbbá $F(x, y)$ olyan $T$ feletti kétváltozós polinom, amelynek a foka $k + r - 2$, és amelyben az $x^{k - 1}y^{r - 1}$ tag együthatója nem nulla. Lássuk be, hogy van olyan $a \in A$, $b \in B$, amelyre $F(a, b) \neq 0$.

(b) Általánosítsuk az (a) részt 2 helyett $n$ részhalmazra és $n$ -változós $F$ polinomra.

12.3.6 (M [628]*) Legyen $p > 2$ prim, és $C$, ill. $D$ a $\mathbb{Z}_{p}$ -nek két tetszőleges, azonos elemzámú részhalmaza. Mutassuk meg, hogy $C$ és $D$ elemei pára állíthatók úgy, hogy az egyes párok elemeiből képezett kéttágú összegek mind különbözők legyenek.

12.3.7 Fogalmazzuk meg és bizonyítsuk be a T 12.3.1 Tétel megfelelőjét kettőnél több halmaz esetére.

12.3.8 A 3.6.6 feladatot [94] és annak sikbeli, valamint magasabb dimenziós általánosításait vizsgáljuk.

(a) Adjunk új bizonyítást a 3.6.6 feladatra [94] a 12.3.7 feladat [414] felhasználásával.

(b) Igazoljuk, hogy a szokásos sikbeli négyzettrácson 5 tetszőleges ráccs között biztosan van két olyan, amelyeknek a szakaszfelező pontja is ráccs.

(c) Legyen $f(n)$ a legkisebb olyan szám, hogy $f(n)$ darab tetszőleges sikbeli ráccs közül mindig kiválasztható $n$ darab olyan, amelyek súlypontja is ráccs. Mutassuk meg, hogy $f(n) \geq 4n - 3$.

Megjegyzés: 2004-ben igazolták azt a régi sejtést, hogy $f(n) = 4n - 3$.

(d) Legyen $f(n, d)$ a legkisebb olyan szám, hogy a $d$ -dimenziós sokszögnek a $f(n, d)$ darab ráccson közül mindig kiválasztható $n$ darab olyan, amelyeknek a súlypontja is ráccs. Bizonyítsuk be, hogy

(i) $2^{d}(n - 1) + 1 \leq f(n, d) \leq n^{d}(n - 1) + 1$;

(ii) $f(mn, d) \leq f(n, d) + n f(m, d - 1)$.

Megjegyzés: (i)-ben a felső becslés nagymértékben, $Cd^{n}$ -re javítható, ahol $Cd$ csak a $d$ -től függő konstans. Az alsó becslés $d = 1$ és 2 esetén pontos (lásd az (a) részt, illetve a (c) rész utáni megjegyzést). Kiderült azonban, hogy minden $d > 2$ -re és páratlan $n \geq 3$ -ra az alsó becslés
javítható \(( n = 2^k\) esetén az alsó becslés adja a helyes értéket minden \(d\)-re, lásd alább). Az \( f(n, i) \) pontos értéke \( n > 2 \) és \( d > 2 \) mellett csak az alábbi néhány esetben ismert:

\[
f(3, 3) = 19, \ f(3, 4) = 41, \ f(3, 5) = 91, \ f(2^k, d = (2^k - 1)2^d + 1.
\]

12.3.9 Legyen \( p \) prím, \( A \subseteq \mathbb{Z}_p \), és tegyük fel, hogy két különböző \( A \)-beli elem különbsége sohasem négyzetelem \( \mathbb{Z}_p \)-ben (azaz \( a_i - a_j \) semmilyen \( i \neq j \) -re sem kvadratikus maradék mod \( P \)). Lássuk be, hogy \( |A| < \sqrt{p} \).

12.3.10 A \([0, n-1]\) intervallum egy \( h \)-adrendű bázisán nemnegatív egész olyan \( A \) halmazát értjük, hogy minden \( 0 \leq r \leq n - 1 \) egész felirható \( h \) darab \( A \)-beli elem összegeként. Jelölje \( g(h, n) \) az ilyen bázisok elemszámának minimumát. Bizonyítsuk be, hogy  

\[
g(h, n) \leq \sqrt{h} + \frac{h}{2} \leq \sqrt{h^n + h}.
\]

12.4 Schur tétele

A kombinatorikus számelméletnek ez a klasszikus eredménye érdekes módon az ettől igen távolin nőtt Ferma-sejtéssel kapcsolatban született, a bizonyításhoz pedig gráfelméleti módszereket szükséges. A ma is intenzíven vizsgált témakör számos megoldatlan problémával is „büszkélkedhet”.

Először a gráfelméleti háttértérrel foglalkozunk. Kiindulásul tekintsük az alábbi közismert feladványt: 6 ember között biztosan van vagy 3 olyan, akik közül bármelyik kettő ismeri egymást, vagy 3 olyan, akik közül semmilyen kettő sem ismerik egymást (az ismeretséget kölcsönösnek tételezzük fel).

Fogalmazzuk ezt át a gráfelmélet nyelvezetére. Tekintsük azt a 6 szögpontú teljes gráfot, amelynek a csúcsai az emberek, és két csúcsot összekötő él legyen piros, ha a két ember ismeri egymást, és kék, ha nem ismerik egymást. Az állítás ekkor úgy szól, hogy akárhogyan is színezzük ki egy 6 szögpontú teljes gráf éléit pirossal és kékkel, biztosan keletkezik egyszínű háromszög.

Ennek igazolásához vegyük a gráf egy tetszőleges \( A \) csúcst. Az ebből kiinduló 5 él között van (legalább) 3 azonos színű, mondjuk piros. Ha ezen 3 él másik végpontja, \( B \) és \( C \) között vezet piros él, pl. a \( BC \) él piros, akkor \( ABC \) piros háromszög, ellenkező esetben pedig \( BC \) kék háromszög.

A feladványt a következőéppen általánosíthatjuk: az \( n \) szögpontú teljes gráf éleit \( k \) színnel színezzük, és egyszínű háromszög helyett olyan \( k \) szögpontú teljes részgráfot akarunk találni, amelynek minden éle azonos színű (az eredeti probléma a \( t = 3 \), \( k = 3 \) speciális eset jelenti). Ramsey alapvető tétele azt mondja ki, hogy (\( k \)-tól és \( t \)-től függően) elég nagy \( n \) esetén mindig van ilyen részgráf:

12.4.1 Tétele (Ramsey tétele). T 12.4.1

Bármely \( i \) és \( k \) esetén létezik olyan \( n = R(k, i) \), hogy ha egy \( n \) szögpontú teljes gráf éléit akárhogyan színezzük ki \( t \) színnel, lesz olyan \( k \) szögpontú teljes részgráf, amelynek minden éle azonos színű.

A továbbiakban \( R(k, i) \) -vel a legkisebb ilyen tulajdonságú \( n \) -et fogjuk jelölni.

Az előzőkben beláttuk, hogy \( R(3, 2) = 6 \), és könnyen adódik, hogy itt valójában egyenlőség áll (lásd a 12.4.1 feladatot [419]). A tétel bizonyításából leolvasható, hogy \( R(3, 3) \leq 30 \), sőt az is kihozható, hogy \( R(3, t) \leq \lceil cT \rceil \), ahol \( c = 2, 71 \ldots \) a természetes logaritmus alapszáma (lásd
KOMBINATORIKUS
SZÁMELMÉLET

416

a 12.4.2 feladatot [419]). Finomabb módszerekkel a konstans szorzó e−1/24-re javítható, ennél jobb felső becslés nem ismeretes, bár ez minden bizonytal igaz messze van a tényleges R(3, l) Ramsey-számok pontos értéke csak nagyon kevés esetben ismert, pl. R(3, 3) = 17, és az alós és felső becslések is igaz messze esnek egymástól.

Bizonyítás: A jobb áttekinthetőség kedvéért először a k − 3 esetet igazoljuk t szerinti teljes indukcióval, és utána térünk át általános k -ra. (Megjegyezzük, hogy a Schur-tétel bizonyításánál majd csak a k − 3 esetre lesz szükség.)

I. Az indukció kezdő esete lehet akár t = 1 (nyilván R(3, 1) = 3 ), akár t = 2, a már igazolt R(3, 2) ≤ 6 összefüggés alapján. Az utóbbi bizonyításához használt gondolatmenetből leolvashatjuk az általános indukciós lépést is.

Tegyük fel, hogy n = R(3, 1) t-letezik, és színezzük ki egy N szögpontú teljes gráf éleit most t színnel. Ha N ≥ 1 + t(n − 1) + 1, akkor egy tetszőleges A csúcsból induló életet nézve, ezen t(n − 1) + 1 él között a skatulyaelv alapján lesz (legalább) nπ egyszínű, pl. piros. Ha ezen élnek másik végpontjai, pl. B és C között vezet piros él, akkor AπBC piros háromszög. Ellenkező esetben pedig ezek a végpontok egy olyan nπ szögpontú teljes gráf csúcsai, amelynek éleinek életi csak t − 1 színnel vannak színezve, és így az indukciós feltétel szerint van benne egyszínű háromszög.

II. Az általános eset bizonyításához az alábbi módon érdemes finomítani a feladatot. Az egyszerűbb megfogalmazás kedvéért a gráf mérete jelentse a csúcsok számát, a színek legyenek az 1, 2, ..., t számon, és j színű gráfon értsünk olyan (teljes) grá福特, amelyben minden él színe j . Ekkor a módosított állítás a következő.

Bármely t és k₁, ..., k₉ esetén létezik olyan n = R*(k₁, k₂, ..., k₉ ) , hogy ha egy n szögpontú teljes gráf éleit akárhogyan színezzük ki az 1, 2, ..., t színekkel, lesz olyan j , hogy a gráf tartalmaz egy k₉ méretű j színű teljes részgráfot. ( R*(k₁, k₂, ..., k₉ ) most is jelentse a legkisebb ilyen tulajdonságú n -et.)

A két probléma könnyen átjátszható egymásra: egyrészt nyilván R(k, t) = R*(k, ..., k), másrész R*(k₁, ..., k₉ ) ≤ R(k, t) , ahol k = max(k₁, ..., k₉ ) .

A módosított állításnál a minden kᵢ = 1 vagy 2 kiindulási eset triviális, az indukció pedig az alábbi formában működik:

\[ R^*(k₁, ..., k₉) \leq 1 + \sum_{j=1}^{t}[R^*(k₁, ..., kᵢ - 1, ..., k₉)] - 1] + 1 \tag{1} \]

Valóban, színezzük ki egy N szögpontú teljes gráf éleit l színnel, ahol N az (1) jobb oldalán álló érték. Ekkor egy tetszőleges A csúcsot véve, az innen induló élek között a skatulyaelv miatt valamelyik j-re lesz (legalább) R*(k₁, ..., kᵢ - 1, ..., k₉ ) darab j színű. Az ezen élek másik végpontjai alkotta teljes gráfban van egy, az indukciós feltétel által biztosított méretű egyszínű részgráf. Ha ennek színe i ≠ j , akkor egy kᵢ méretű i színű részgráfot kaptunk, tehát készen vagyunk. A j szín esetén pedig kᵢ − 1 csúcsú részgráf adódott, ami az A csúcsból együtt már egy kᵢ méretű j színű részgráfot jelent.

Schur tétele számok színezésére vonatkozik:

12.4.2 Tétel (Schur tétele) . T 12.4.2
Bármely \( t \) esetén létezik olyan \( \alpha = S(t) \), hogy ha az \( 1, 2, \ldots, \alpha + 1 \) számokat akárhogyan színezzük ki \( t \) színnel, lesz olyan azonos színű \( a \) és \( b \), amelyek \( a + b \) összege is ugyanilyen színű (\( a = b \) is megengedett).

A továbbiakban \( S(t) \) -vel a legkisebb ilyen tulajdonságú \( n \) -et fogjuk jelölni, vagyis \( S(t) \) a legnagyobb „rossz” szám: \( 1, 2, \ldots, S(t) \) még kiszínezhető \( t \) színnel úgy, hogy az \( x + y = z \) egyenletnek ne legyen egyszínű megoldása. (A Ramsey-tételnél \( R(k, t) \) a legkisebb „jó” számot jelentette; a két kissé eltérő szellemű jelölés hagyományosan így alakult ki, ezért mi is ezekekhez tartjuk magunkat.)

Nyilván \( S(1) = 1 \) és könnyen adódik, hogy \( S(2) = 4 \). Ezeken kívül pontos értékként csak \( S(3) = 13 \) és \( S(4) = 44 \) ismert. Az \( S(t) \) Schur-számok alsó és felső becsleseire vonatkozóan lásd a 12.4.3 feladatot [419].

**Bizonyítás:** Megmutatjuk, hogy \( S(3) < R(3, t) \), azaz az \( 1, 2, \ldots, R(3, t) \) számokat akárhogyan színezzük ki \( t \) színnel, teljesül az előírt tulajdonság. Tekintsük azt a teljes gráfot, amelynek csúcsai a fenti számok, és az \( \langle i, j \rangle \) él (gráf)színe legyen az \( |i - j| \) (szám)színe. Ekkor a Ramsey-tétel alapján keletkezik a gráfban egyszínű háromszög, azaz van olyan \( i \), és így \( a = j - i \) és \( a + b = m - i \) (szám)színe azonos.

Most rátérünk a Schur-tételnek a Fermat-sejtéssel való kapcsolatára.

Tekintsük az \( x^t + y^t \equiv x^t \pmod{p} \) kongruenciát. Ha végtelen sok \( P \) primre csak triviális, azaz \( xyz \equiv 0 \pmod{p} \) megoldás létezik, akkor abbről következik a Fermat-sejtés a \( t \) kitevőre: ha ugyanis indirekt az \( a, b, c \) nem nulla számokra \( a^t + b^t = c^t \), akkor ezek a kongruenciának is nemtriviális megoldását adják minden \( p > \max(|a|, |b|, |c|) \) primre, és ez ellentmond annak, hogy végtelen sok primre csak triviális megoldás létezik. Megmutatjuk azonban, hogy ez az ötlet sajnos nem vezethet el a Fermat-sejtés bizonyításához:

12.4.3 Tétel .  T 12.4.3

Az \( x^t + y^t \equiv x^t \pmod{p} \) kongruenciának minden \( \langle t \rangle -től függően \) elég nagy \( P \) primre van nemtriviális, azaz \( xyz \not\equiv 0 \pmod{p} \) megoldása.

**Bizonyítás:** Legyen \( P > 1 > S(t) \), \( g \) primitív gyök mod \( P \), és színezzük ki az \( 1, 2, \ldots, P - 1 \) számokat a \( 0, 1, \ldots, t - 1 \) színekkal a következőképpen: \( t \) színekt legyenek azok a számok, amelyek \( g\alpha, g\alpha + t, g\alpha + 2t, \ldots \)-vel kongruensek mod \( P \).

Ekkor a Schur-tétel szerint keletkezik azonos színű \( a, b, c + b \), azaz valamilyen \( r \)-rel

\[
\alpha = g^{\alpha t}, \quad b = g^{\alpha t - r}, \quad a + b = g^{\alpha t + r} \pmod{p},
\]

és így

\[
g^{\alpha t - r} - g^{\alpha t - r} \equiv g^{\alpha t + r} \pmod{p}.
\]

Ezt a \( P \)-hez relatív prim \( g^a \)-rel egyszerűsíve

\[
(g^a)^t + (g^a)^t \equiv (g^a)^t \pmod{p}
\]

417
adódik, vagyis $z = g^s, y = g^r, x = g^s - y$ egy nemtriviális megoldását adja a kongruenciának. □

A természetes számok színezésével kapcsolatban Schur egy másik problémát is felvetett, amelyet először Van der Waerden oldott meg, ezt bizonyítás nélkül közelítjük:

12.4.4 Tétel (Van der Waerden tétele). T 12.4.4

A természetes számokat tetszőlegesen színezve két színrel, biztosan keletkezik akár milyen hosszú (véges) egyszínű számtani sorozat.

Van der Waerden valójában a tételeln az alábbi végessített és több szint szerepeltető változatát igazolta egy ravasz teljes indukcióval:

12.4.4A Tétel (Van der Waerden tétele). T 12.4.4A

Bár mely $t$ és $k$ esetén létezik olyan $n = w(k, t)$, hogy az $1, 2, \ldots, n$ számokat $t$ színrel tetszőlegesen kiszínezve biztosan keletkezik $k$-tagú egyszínű számtani sorozat.

Az $R(k, t)$ Ramsey- és $S(t)$ Schur-számokhoz hasonlóan a (minimalis) $w(k, t)$ Van der Waerden-számok alsó és felső becsleléi is nagyon messze esnek egymástól, és csak nagyon kevés pontos érték ismert:

\[ w(3, 2) = 9, w(4, 2) = 35, w(5, 2) = 178, w(3, 3) = 27, w(3, 4) = 76, \]

valamint triviálisan $w(k, 1) = k$ és $w(2, 1) = 1$. A két szin esetére a $w(k) = w(k, 2)$-re vonatkozó alsó becslesekéről lásd a 12.4.11 feladatot [419].

Können adódik, hogy a természetes számokat két színre színezve nem feltétlenül kapunk végletlen hosszú egyszínű számtani sorozatot, sőt még az is elérhető, hogy pirosból végletlen hosszú, kékrel pedig még hőrungy számtani sorozat se keletkezzék (lásd a 12.4.7 feladatot [419]).

Befejezésül a Van der Waerden-tétel egy nagyfokú általánosítását említtjük meg. Erdősnek és Turánnak ezt a nevezetes, sok évtizeden át megoldatlan sejtését végül Szemerédi Endre igazolta, és ezzel elnyerte a legnagyobb díjat (1000 dollárt), amelyet Erdős matematikai problémák megoldásáért kitűzött, és amelyet tényleg ki is kellett fizetnie, mert a problémát valóban megoldották.

Van der Waerden tétele „csak” azt állítja, hogy a természetes számsort, illetve annak elég nagy kezdőszintét kiszínezve biztosan keletkezik előírt hosszúságú egyszínű számtani sorozat, de nem mondja meg, melyik színből. Természetesen azt érezzük, hogy bizonyára a leggyakrabban előfordulóbb. Ennek kapcsán vetette fel Erdős és Turán, hogy ha a természetes számoknak egy tetszőleges, elég sürű részsorozatát vesszük, akkor ennek is kell tartalmaznia előírt hosszúságú számtani sorozatot. Sejtésük pontos megfogalmazása a következő.

12.4.5 Tétel (Szemerédi-tétele). T 12.4.5

Tekintsük az $\{1, 2, \ldots, n\}$ legnagyobb elemszámú olyan részhalmazát, amely még nem tartalmaz $k$ hosszúságú számtani sorozatot, ennek elemszámát jelölje $\tau(k)$. Ekkor bármielőre rögzített $k$-ra\[\lim_{n \to \infty} \tau(k)/n = 0.\]

Ebből van der Waerden tétele valóban következik, ugyanis ha az $1, 2, \ldots, n$ számokat $\ell$ színrel színezünk, akkor van olyan szín, ami legalább $n^{1/\ell}$-szer fordul elő, és elég nagy $n$-re $\ell/n > \tau(k)$ (hiszen $1/\ell$ nagyobb lesz, mint a $0$-hoz tartó $\tau(k)/n$), vagyis ebből a színből biztosan kapunk $k$ hosszúságú számtani sorozatot.

A Szemerédi-tétel más megfogalmazásban azt mondja ki, hogy a természetes számoknak bármielőre pozitív felső sűrűségű részsorozata tartalmaz akár milyen hosszú (véges) számtani sorozatot. Erdős
ezután azt sejtette, hogy ez a tulajdonság ennél ritkább sorozatokra is igaz: elég az, hogy az elemek reciprokösszege divergens legyen. Nagy meglepetést kellett, amikor ezt a sejtést a prímszámok sorozatára 2004-ben igazolták (vagyis a prímszámok között előfordul tetszőlegesen hosszú számtani sorozat, lásd az 5.1. pontot is), az általános sejtés azonban továbbra is megoldatlan.

### Feladatok

12.4.1 Lássuk be, hogy $R(3, 2) = 6$, $R(k, 1) = k$, $R(1, t) = 1$ és $R(2, t) = 2$.

12.4.2 Mutassuk meg, hogy (a) $R(3, t) \leq 3t!$; (b) $R(3, t) \leq [3t!]$.

12.4.3 Igazoljuk a Schur-számokra vonatkozó alábbi egyenlőtlenségeket:

(a) $S(t) < t^t!$;

(b) $S(t + 1) \geq 3S(t) + 1$;

(c) $S(t) \geq (3^t - 1)/2$;

(d) $S(t + v) \geq 2S(t)S(v) + S(t) + S(v)$.

Megjegyzések: A (b) rész a (d)-nek speciális esete. A (d) rész és $a$ felhasználásával a (c)-beli alsó becslés kicsit javítható.

12.4.4 Adott $n$-hez adjuk meg azt a legnagyobb $r = f(n)$-et, amelyre az $a_1, \ldots, a_n, a_1, \ldots, a_r$ számok kiszínezhetők két színnel úgy, hogy az $a_j + a_r = a_j$ egyenletnek ne legyen egyszínű megoldása.

12.4.5 Bizonyítsuk be, hogy bármely $t$ esetén létezik olyan $a$, hogy ha az $1, 2, \ldots, n + 1$ számokat akárhogyan színezünk ki $t$ színnel, lesz $3$ olyan azonos színű, de nem feltétlenül különböző szám, amelyek összege is ugyanilyen színű.

12.4.6 Legyen $t$. rögzített. Mutassuk meg, hogy minden elég nagy $\mathcal{P}$ primre létezik két szomszédos $t$-edik hatványmaradék mod $\mathcal{P}$, azaz olyan $a \equiv 0, 1 (\mathcal{P})$-ra, hogy az $x + y = 0$ egyenletnek ne legyen egyszínű megoldata.

12.4.7 Bizonyítsuk be, hogy a természetes számokat ki lehet úgy színezni pirossal és kékkel, hogy ne jöjjön létre

(a) végtelen hosszú egyszínű számtani sorozat;

(b) $*$ se végtelen hosszú piros, se pedig 3-tagú kék számtani sorozat.

12.4.8 Lássuk be, hogy a természetes számokat akárhogyan színezünk ki véges sok színnel, bármely $k$-ra végtelen sok olyan $k$-tagú számtani sorozat keletkezik, amelyek mind azonos színűek.

12.4.9 Igazoljuk, hogy a természetes számokat tetszőlegesen kiszínezve véges sok színnel, biztosan keletkezik akármilyen hosszú (véges) egyszínű mértani sorozat.

12.4.10 Lássuk be, hogy $w^r(3, 2) = 9$.

12.4.11 (***) Igazoljuk a $w^r(k)$-re vonatkozó alábbi alsó becsléseket:

(a) $w(k) \geq 2^{k/2} \sqrt{k - 1}$.
KOMBINATORIKUS
SZÁMELMÉLET

(9)(M [629]) \( \mu(n) + 1 > \frac{3}{2} \), ha \( \mu \) prim.

12.4.12 (M [629]*s) Lássuk be az \( \tau_2(n) \)-re vonatkozó alábbi alsó becsültet: minden elég nagy \( n \)-re megadható \( l \) és \( n \) között \( \tau_2(n)/e^{\log n} \) olyan egész szám (ahol \( c > 0 \) alkalmas konstans), amelyek között nem fordul elő háromtagú számtani sorozat.

12.5 Fedőrendszerek

Ismét Erdős egyik „kedvence” problémája következik: a nemnegatív egész számokat véges sok, különböző differenciájú számtani sorozat egyesítéseként állíthatjuk elő:

\[
\{0, 1, \ldots, n, \ldots\} = \\
= \{a_1, a_1 + m_1, a_1 + 2m_1, \ldots\} \cup \cdots \cup \{a_k, a_k + m_k, a_k + 2m_k, \ldots\},
\]

ahol \( 1 < m_1 < \cdots < m_k \). \( \text{(1)} \)

Ennek (ekvivalens) átfogalmazása, hogy az egész számokat különböző modulusok szerinti maradékosztályokkal fedjük le: minden \( t \) egész szám eleme az

\[
a_1 \mod m_1, \ldots, a_k \mod m_k, \quad 1 < m_1 < \cdots < m_k
\]

maradékosztályok közül legalább az egyiknek, azaz van olyan \( \hat{t} \), amelyre \( \hat{t} = a_i \mod m_k \).

A számtani sorozatok, illetve maradékosztályok ilyen rendszerét (kongruencia) fedőrendszerek tekinthetjük.

Példa fedőrendszerre:

\[
\emptyset \mod 2, \quad \emptyset \mod 3, \quad 1 \mod 4, \quad 1 \mod 6, \quad 11 \mod 12.
\]

Ennél kevesebb modulusú fedőrendszer nem létezik, és 5 modulussal is ez az egyetlen lehetséges (lásd a 12.5.4 feladatot [423]).

Erdős a fedőrendszereket egy látszólag távoli probléma megoldásához találta ki, lásd a T 12.5.2 Tételt.

Számos nyitott kérdés kapcsolódik a fedőrendszerekhez, ezek közül a két legrégibb és egyben legérdekesebb a következő:

- Van-e fedőrendszer csupa páratlan modulusból?
- Van-e minden \( I \)-hez olyan fedőrendszer, amelynek minden modulusa nagyobb \( I \)-nél? (A jelenlegi rekord \( I = 20 \).

Természetesen merül fel az egzakt vagy diszjunkt fedés, vagyis amikor az (1)-beli számtani sorozatok, illetve a (2)-beli maradékosztályok diszjunktak, azaz minden egész szám pontosan egy (2)-beli kongruenciát elégti ki.

Az alábbi tételek mutatja, hogy ez nem lehetséges:

12.5.1 Tétel.

A nemnegatív egészek nem állíthatók elő véges sok, különböző differenciájú számtani sorozat diszjunkt egyesítéseként.

A tételekre két bizonyítást adunk, az első a komplex számakra vonatkozó elemi analízisre támaszkodik, a második az állítást egy önmagában is érdekes geometriai problémára átfogalmazva igazolja.

**Első bizonyítás:** Generátorfüggvényt használunk, \( z \) komplex számot jelöl, ahol \( |z| < 1 \).
Tegyük fel indirekt, hogy (1)-ben diszjunkt egyesítés szerepel. Ekkor minden $\alpha \geq 0$ egyértelműen áll elő $\alpha = \alpha_1 + \ldots + \alpha_k$ alakban, ahol $1 \leq i < k$ és $\tau > 0$. Ezért a $|x| < 1$-re érvényes abszolút konvergencia és az ebből adódó átrendezhetőség miatt

$$\left( z^{\alpha_1} + z^{\alpha_1 + \alpha_2} + z^{\alpha_1 + 2\alpha_2} + \ldots \right) + \ldots + \left( z^{\alpha_{k-1}} + z^{\alpha_{k-1} + \alpha_k} + \ldots \right) =$$

$$= 1 + z^\tau + \ldots + z^{\tau k} + \ldots.$$

A mértani sorokat összegezve kapjuk, hogy

$$\sum_{i=1}^{k} \frac{z^{\alpha_i}}{1 - z^{\tau \alpha_i}} = \frac{1}{1 - z}. \quad (4)$$

Ha a $z$ komplekx változó (egy $|z| < 1$ tartománybeli úton) tart egy $n_k$-edik egységgyököhöz, akkor (4) bal oldalán az ennek megfelelő $z^{\alpha_i} / (1 - z^{\tau \alpha_i})$ tag nem lesz korlátos. Ha tehát $z \to \omega = \cos(2\pi/m_k) + i\sin(2\pi/m_k)$, akkor a bal oldal utolsó tagja nem korlátos, a többi tag és a jobb oldal viszont igen, hiszen $n_k$ maximalitása miatt $\omega$ nem lesz $n_k$-edik egységgyökö $i < k$-ra. Így ellentmondásra jutottuk. □

Második bizonyítás: Tegyük fel most is indirekt, hogy (1)-ben diszjunkt egyesítés szerepel. Mivel a számítható sorozatok periodikusak a differenciák legkisebb közös többszöröse $M = [m_1, \ldots, m_k]$ szerint, ezért az indirekt feltevés ekvivalens azzal, hogy az $1, 2, \ldots, M$ számok mindegyike pontosan egy lefedő számított sorozatnak eleme.

Rajzoljunk egy szabályos $M$-szög, a csúccsal számozzuk meg sorban $1, 2, \ldots, M$-mel. Minden lefedő számítható sorozathoz válasszunk egy-egy (különböző) szint, és az adott számítható sorozat által lefedett csúccsal fessük az ehhez tartozó színűre. Pl. ha $M = 12$, és az $1$ számítható sorozathoz a piros tartozik, akkor az 1, 5 és 9 csúccsal lesznek piros színűek.

Nyilván az $u_i \mod n_k$ számítható sorozat által lefedett csúccsal egy $n_k = M/m_k$ oldalú szabályos sokszöget alkotnak (megengedve a szakasszal, illetve ponttal elfajuló), és így

$$u_1 > u_2 > \cdots > u_M.$$ 

Az indirekt feltevés ebben a geometriai átfogalmazásban azt jelenti, hogy van olyan szabályos $M$-szög, amelynek a csúcsai kiszínezhetők néhány ($k \geq 1$) színűen úgy, hogy az egyszínű csúccsal különböző oldalszámú (esetleg elfajuló) szabályos sokszögeket alkossanak.

Azt az egyszerű geometriai tényt figyeljük felhasználni, hogy egy szabályos $u$-szög középpontjából a csúcsokba mutató vektorok összege nulla, ha $u > 1$ (beleértve az $u = 2$ elfajuló esetet is). Ez azért igaz, mert az összvektor a középpont körüli $2\pi/m$ szögű elforgatáskor egyrészt nem változik, hiszen a sokszög önmagába megy át, másrészt viszont maga is elfordul az adott szöggel, és így csak a nullvektor lehet.

A gondolatmenet jobb megvilágítása céljából tegyük fel először, hogy $u_k = 1$. Legyen $\sigma$, illetve $\xi_i \, i = 1, \ldots, k$, a szabályos $M$-szög középpontjából az $M$-szög, illetve az $i$-edik színű csúcsok alkotta $u_i$-szögből mutató vektorok összege. Ekkor nyilván $\sigma = \sum_{i=1}^{k} \xi_i$, másrészt az előbbi megjegyzés alapján $\xi = \xi_1 = \ldots = \xi - 1 = \sigma$, de $\xi \neq 0$, ami ellentmondás.

Az általános esetet erre a következőképpen tudjuk visszavezetni. Legyen $i$ rögzített, és tekintsük a szabályos $M$-szög csúcsainak azt a transzformációját, amely a $j$ csúcsot a $i$ (mod $M$) csúcsba viszi át ($j = 1, \ldots, M$). Megmutatjuk, hogy ekkor az eredetileg egyszínű csúcsok képei továbbra is
egy szabályos sokszög csúcsait fedik le azonos multiplicitással. Például, ha \( M = 12 \), \( t = 2 \), akkor az \( 1 \pmod{4} \) számtani sorozatnak megfelelő 1, 5, 9 csúcsok képe rendre 2, 10, 6, vagyis a 2, 6, 10 szabályos háromszöget kapjuk; a \( 2 \pmod{3} \) kongruencia esetén a 2, 5, 8, 11 csúcsok képe rendre 4, 10, 4, 10, tehát a 4, 10 szabályos kétszög csúcsait nyerjük, mindegyiket kétszer; és végül a \( 4 \pmod{6} \) -ből adódó 4, 10 csúcsok képe 8, 8, tehát ez az „egyszög” jött létre kétszeres multiplicitással.

Általában is, az \( u_i \pmod{m_i} \) -nek megfelelő \( a_i + j m_i \), \( j = 0, 1, \ldots, n_i - 1 \) csúcsok képe \( u(a_i + j m_i) \pmod{M} \). Ezt a \( t \times n \) differenciájú számtani sorozatot mod \( M \) nézve kapjuk, hogy a képek (alkalmas sorrendben) \( u(a_0) \) -ból indulva az egymástól \( \left\langle t m_i, M \right\rangle = \langle t, m_i \rangle m_i \)-távolságra levő csúcsokat adják, mindegyiket ugyanannyniszor, éspedig \( \left\langle t, m_i \right\rangle \)-szer. Vagyis a képek valóban egy szabályos sokszög csúcsait fedik le azonos multiplicitással, és pontosan akkor kapunk „egyszöget”, ha \( u_i \mid t \).

Ennek alapján válasszuk \( k \) értéket \( u_k \) -nak. Ekkor a képekhez megismételve a középpontból a csúcsokba mutató vektorok összegét vizsgáló gondolatmenetünket, minden \( i < k \) -ra az \( ii \) -szögek, valamint az erek \( M \) -sőg képénel ez az összegvektor nulla, az \( ii \) -sőg képénel viszont nem, és ezzel ugyanúgy ellentmondásra jutottunk, mint az \( ii \) speciális esetben.

Most rá térünk Romanov problémájára, amelynek megoldásához Erdős a fedőrendszereket felhasználta.

**12.5.2 Tétel.**

Végtelen sok olyan páratlan szám van, amely nem írható fel egy kettőhatvány és egy prímszám összegeként.

*Bizonyítás:* Azt a jóval erősebb állítást igazoljuk, hogy létezik olyan, páratlan számokból álló végtelen számtani sorozat, amelynek egyik eleme sem írható fel a fenti alakban.

Induljunk ki az alábbi \( u_i \pmod{m_i} \), \( i = 1, 2, \ldots, 6 \) fedőrendszerből:

\[
0 \pmod{2}, 0 \pmod{3}, 1 \pmod{4}, 3 \pmod{8}, 7 \pmod{12}, 23 \pmod{24}.
\]

Felhasználjuk, hogy minden \( \mathfrak{m} \) -hez létezik olyan \( \mathfrak{p} \) prím, amelyre a 2 rendje mod \( \mathfrak{p} \) éppen \( \mathfrak{m} \), azaz \( \mathfrak{a}(2) = \mathfrak{m} \); ilyen \( \mathfrak{p} \) prímek rendre a 3, 7, 5, 17, 13, illetve 241:

\[
\mathfrak{a}(2) = 2, \mathfrak{a}(2) = 3, \mathfrak{a}(2) = 4, \mathfrak{a}(2) = 8, \mathfrak{a}(2) = 12, \mathfrak{a}(2) = 24.
\]

(Megjegyezzük, hogy minden \( \mathfrak{m} \neq \mathfrak{p} \) esetén létezik olyan \( \mathfrak{p} \) prím, amelyre a 2 rendje mod \( \mathfrak{p} \) éppen \( \mathfrak{m} \), ezért a céljainkra a (3) fedőrendszer nem lett volna alkalmas, de minden olyan fedőrendszer megfelelt volna, amelyben a modulusok között a 6 nem szerepel. Az nyilvánvaló, hogy különböző \( \mathfrak{m} \)-ekhez mindig különböző \( \mathfrak{p} \) prímek tartoznak.)

Tekintsük a fenti \( a_1, m_1, p_1 \) értékeket és válasszuk \( s \) -et úgy, hogy \( 2^{s-1} > \text{max}_s p_1 \) teljesüljön, tehát az (5)–(6) fedőrendszer esetén pl. \( s = 9 \) megfelel.

Megmutatjuk, hogy az

\[
x = 2^{n_i} \pmod{p_i^i}, i = 1, \ldots, k, \quad x = 1 \pmod{2^n}
\]

szimultan kongruenciarendszer tetszőleges \( a = c \) megoldását véve \( c \) nem írható fel egy kettőhatvány és egy prímszám összegeként. Mivel (7)-ben a modulusok páronként relatív prímek, ezért a kongruenciarendszer megoldható, és a megoldások egy páratlan számokból álló végtelen számtani sorozatot alkotnak, tehát ezzel a tétel állítása igazolva lesz.
Indirekt tegyük fel, hogy egy \( c \) megoldásra \( c = 2^c + p \), ahol \( p \) prim. Mivel \( a_i \mod m_i \) fedőrendszer, ezért van olyan \( i \), amelyre \( r_i = a_i \mod m_i \). Tudjuk, hogy a 2 rendje mod \( p_i \) éppen \( m_i \), továbbá \( c \) kielégíti (7)-et, tehát
\[
2^c \equiv 2^{a_i} \equiv c \mod p_i.
\]
Ebből következik, hogy \( p = c - 2^c \equiv 0 \mod p_i \), vagyis csak \( p = p_i \) lehetséges.

Így az ellentmondáshoz elég azt igazolnunk, hogy \( c = 2^i + p_i \) nem teljesíti a (7)-beli utolsó kongruenciát, azaz \( 2^c + p_i = 1 \mod 2^a \). Ha \( n = s - 1 \), akkor ezt \( 1 < 2^a + p_i < 2^{a-1} + 2^{a-1} - 2^a \) biztosítja. Ha pedig \( n \geq s \), akkor azonnal adódik, hogy \( 2^a + p_i \equiv p_i \not\equiv 1 \mod 2^a \).

**Feladatok**

(Az (1), illetve (2)-beli jelöléseket használjuk.)

12.5.1 Lássuk be, hogy bármely fedőrendszerre \( \sum_{i=1}^{k} 1/m_i \geq 1 \).

12.5.2 Mutassuk meg, hogy ha egy fedőrendszerben egy \( m_i \) modulust egy (a többi modulustól különböző) osztójára cserélünk ki, akkor továbbra is fedőrendszert kapunk.

12.5.3 Tekintsünk egy minimális fedőrendszer, azaz olyat, amelyből akármelyik maradékosztályát hagyni is el, már nem marad fedőrendszer. Igazoljuk, hogy ekkor bármelyik \( m_i \) osztója a többi \( m_j \) legkisebb közös többszörössének.

12.5.4 Bizonyítsuk be, hogy nincs 2, 3 vagy 4 maradékosztályból álló fedőrendszer, és 5 maradékosztály esetén is csak a (3)-beli modulusok lehetségesek.

12.5.5 Konstruáljunk olyan fedőrendszert, amelyben 3 a legkisebb modulus.

12.5.6 Ahhoz, hogy a diszjunkt fedőrendszer (DFR) fogalma ne legyen üres, engedjük meg, hogy a modulusok között azonosak is előfordulhassanak: \( a_i \mod m_i \), \( i = 1, \ldots, k \), ahol \( 1 < \tau_1 < \cdots < \tau_k \), és minden egész szám pontosan egy maradékosztálynak az eleme. Igazoljuk az ilyen DFR-ekre az alábbiakat:

(a) \( \sum_{i=1}^{k} 1/m_i - 1 \);

(b) \( \tau_k = \tau_{k-1} \);

(c) minden \( k \) -höz van olyan DFR, ahol \( \tau_1 < \tau_2 < \cdots < \tau_{k-1} \).

12.5.7 Bizonyítsuk be, hogy végleten sok páros szám nem írható fel egy háromhatvány és egy prímszám összegeként. Sőt, általánosan, bármely rögzített \( a > 1 \) páratlan számhoz, illetve \( b > 2 \) páros számhoz van végleten sok olyan páros, illetve páratlan szám, amely nem írható fel \( a^n + b \), illetve \( b^a + p \) alakban, ahol \( p \) prim.

### 12.6 Additív komplementumok

A nemnegatív egészek \( A \) és \( B \) végleten részhalmazai egymás additív komplementumai, ha minden elég nagy természetes szám előáll \( a + b \) alakban, ahol \( a \in A \), \( b \in B \).
Például, legyenek $A$, illetve $B$ elemei a 0, valamint azok a pozitív egészek, amelyek tizes számrendszerbeli alakjában az egyesektől számítva minden páratlan, illetve páros helyértéken csakis 0 számjegy szerepel (tehát pl. $3010 \in A$, $70005 \in B$). Ekkor nyilván minden nemnegatív egész (egyértelműen) felírható $a + b$ alakban, tehát $A$ és $B$ egymás additív komplementumai (a továbbiakban a rövidség kedvéért az additív jelzöt általában elhagyjuk).

Először egy egyszerű szükségessé feltétele adunk $A$ és $B$ sűrűségére ahhoz, hogy $A$ és $B$ egymás komplementumai lehessenek, majd megállapítsuk, mennyire éles ez a sűrűségi feltétel. Ezután konkrét halmazok, nevezetesen a kettőhatványok és a primek esetén megvizsgáljuk, mennyire ritka komplementum található hozzájuk.

Jelölje $A(n)$, illetve $B(n)$ az $A$, illetve $B$ halmaz $n$-nél nem nagyobb elemeinek a számát. Legyen $f(n)$ azoknak a $0 \leq t \leq n$ egészeknek a száma, amelyek előállnak $t - a + b$ alakban. Ekkor $f(n) \leq A(n) B(n)$, hiszen az ilyen $t$-k felírásában $a \leq t \leq n$, $b \leq t \leq n$. (Ez két szempontból is durva becslés, ugyanis egyes $t$-től többféle képpen is előállhatnak $a + b$ alakban, továbbá az ilyen $a$, $b$ számokból képzett $a + b$ összegek egy része $n$-nél nagyobb lesz.) Ha $A$ és $B$ egymás komplementumai, akkor minden $t > t_0$ felírható $t = a + b$ alakban, vagyis $f(n) \geq n - t_0$. Az $f(n)$-re adott alsó és felső becslést összevetve kapjuk, hogy bármely $n$-re $A(n) B(n) \geq n - t_0$. Ezt $n$-nell osztva, majd $n \to \infty$ mellett adódnak, hogy additív komplementumok esetén

$$\liminf_{n \to \infty} \frac{A(n) B(n)}{n} \geq 1. \quad (1)$$

A gondolatmenetben alkalmazott durva becslések miatt azt gondolhatnánk, hogy (1)-ben nem állhat egyenlőség, az pedig végképp kizárható, hogy a $\liminf$ helyett a $\limsup$ értéke is lehet 1 (azzal ekkor az (1)-beli hányados határértéke 1). Meglepő módon ez mégis megvalósulhat, sőt igen sok ilyen konstrukció is született, ezekből a legelsőt, Danzer példáját mutatjuk be.

12.6.1 Tétel. T 12.6.1

Léteznek olyan $A$ és $B$ additív komplementumok, amelyekre

$$\lim_{n \to \infty} A(n) B(n) /n = 1. \quad (2)$$

Bizonyítás: Az $A$ egy igen gyorsan növő, és bizonyos oszthatósági tulajdonságokkal is rendelkező sorozat lesz:

$$a_k = (k^2) + k. \quad (3)$$

Nyilván $a_k \equiv k \mod d$, ha $d \leq k^2$. Ebből következik, hogy

$$a_k, a_{k-1}, \ldots, a_{k-d_k+1} \text{ teljes maradéktáblázósz} \mod d_k, \quad (4)$$

ha $d_k \leq (k - d_k - 1)^2$. Minden $k$-höz válasszunk egy ilyen tulajdonságú, viszonylag nagy $d_k$-t, amelyre

$$d_k \leq d_{k+1} \quad (5)$$

és

$$\lim_{\epsilon \to \infty} d_k / \kappa = 1, \quad (6)$$

pl. $d_k = [\kappa - \sqrt{k}]$ megfelel.
Legyen most $n$ tetszőleges, és $k$ olyan, amelyre

$$ka_k \leq n < (k+1)a_{k+1}. \quad (7)$$

Ekkor (4) alapján van olyan $0 \leq s < d_k$, amelyre $nt = c_{k-s} \pmod{d_k}$, vagyis $n$ felírható

$$n = a_{k-s} + rd_k \quad (8)$$
alakban. Becsüljük meg itt $r$ lehetséges értékeit (7) és $0 < a_{k-s} \leq a_k$ felhasználásával:

$$\frac{(k-1)a_k}{d_k} \leq r = \frac{n}{d_k} - a_{k-s} < \frac{(k+1)a_k}{d_k}. \quad (9)$$

Álljon most $B_c$ azokból az $rd_k$ alakú számokból, ahol $r$ kielégíti (9)-et, és legyen

$$B = \bigcup_{k=1}^{\infty} B_k = \bigcup_{k=1}^{\infty} \left\{ rd_c \mid \frac{(k-1)a_k}{d_k} \leq r < \frac{(k+1)a_k}{d_k} \right\}. \quad (10)$$

Ekkor (8) alapján $A$ és $B$ egymás komplementumai.

Most rátérünk (2) igazolására, ehhez $A(n)$ -et, illetve $B(n)$ -et felülről becsüljük.

Mivel (7), illetve (3) szerint $n < (k+1)a_{k+1} < a_{k+2}$, ezért

$$A(n) \leq k + 1 \quad (11)$$

(valójában $A(n) = k$ vagy $k + 1$).

Mivel (10) miatt $B_{k-2}$ legkisebb eleme is legalább $(k+1)a_{k-2}$, ami (7) miatt nagyobb, mint $n$, ezért $B(n)$ -nél $B_{k+2}$-t már nem kell számításba venni, és így

$$B(n) \leq B_{k+1}(n) + B_k(n) + B_{k-1} + \left| \bigcup_{i=1}^{k-2} B_i \right|. \quad (12)$$

Vizsgáljuk most egyenként a (12) jobb oldalán szereplő tagokat.

(10) szerint $B_{k+1}$ legkisebb eleme legalább $ka_{k-1}$, tehát $B_{k+1}$ eleve csak akkor játszik szerepet $B(n)$ -ben, ha

$$ka_{k+1} \leq n, \quad \Rightarrow \quad a_{k+1} \leq \frac{n}{k}. \quad (15)$$

Ebben az esetben is (7) alapján $n < (k+1)a_{k+1}$, ezért $B_{k+1}(n)$ -hez mindenképpen a $\frac{d_k}{c}$ -nek legfeljebb a $ka_{k-1}$ és $(k+1)a_{k+1}$ közé eső többszöröseit kell figyelembe venni, tehát

$$B_{k+1}(n) \leq \frac{(k+1)a_{k+1} - ka_{k-1}}{d_{k+1}} + 1 = \frac{a_{k+1}}{d_{k+1}} + 1 \leq \frac{n}{kd_{k-1}} + 1 \quad (14)$$

(az utolsó egyenlőtlenségnél (5)-öt és (13)-at használtuk fel).

$B_k(n)$, hasonló módon, a $\frac{d_k}{c}$ -nak a $\frac{(k-1)a_k}{d_k}$ és $n$ közé eső többszöröseit számolja össze, vagyis
$B_k(n) \leq \frac{n - (k - 1)a_k}{d_k} + 1 \leq \frac{n - (k - 1)c_k}{d_k - 1} + 1. \quad (15)$

Ugyanígy

$$|B_{k-1}| \leq \frac{k a_k - (k - 2)a_{k-1}}{d_{k-1}} + 1 \leq \frac{k a_k}{d_{k-1}} + 1. \quad (16)$$

Végül, $i \leq k - 2$ esetén $B_i$ minden eleme kisebb $(k - 1)a_{k-1}$-nél, tehát

$$\bigcup_{i=1}^{k-2} B_i \leq (k - 1)a_{k-1} - 1. \quad (17)$$

A (12), (14), (15), (16) és (17) egyenlőtlenségek alapján

$$B(n) \leq \frac{n}{k} + \frac{n + c_k}{d_k - 1} + (k - 1)a_{k-1} + 2. \quad (15)$$

Mivel $7$ alapján $a_k \leq n/k$, így (18)-ből

$$B(n) \leq n\left(\frac{1 + \frac{2}{\epsilon}}{d_k} + \frac{(k - 1)a_{k-1} + 2}{\epsilon}\right). \quad (19)$$

következik.

Így (11) és (19) szerint

$$\frac{A(n)B(n)}{n} \leq \frac{(k + 1)(1 + \frac{2}{\epsilon})}{d_k - 1} + \frac{(k + 1)((k - 1)a_{k-1} + 2)}{\epsilon}. \quad (20)$$

Ha $n$, és így $k$ is tart a végelenhez, akkor (20) jobb oldalán az első tört (6) szerint 1-hez, a második tört pedig (7) és (3) alapján 0-hoz tart, azaz

$$\limsup_{n \to \infty} \frac{A(n)B(n)}{n} \leq 1. \quad (21)$$

Mivel $A$ és $B$ komplementumok, ezért (1) is teljesül, ami (21)-gyel együtt éppen a kívánt (2) képletet adja.

Nevezzük a $B$ -t az $A$ halmaz teljesen gazdaságos komplementumának (TGK), ha (komplementuma az $A$ -nak és) (2) érvényes. A T 12.6.1 Tétel szerint az $A = \{(k^n)! + k \mid k = 1, 2, \ldots\}$ halmazhoz létezik TGK. Ruzsa Imre megmutatta, hogy minden olyan $A = \{a_1 < a_2 < \cdots\}$ halmazhoz létezik TGK, amelyre $\lim_{k \to \infty} \frac{a_k}{k^{\log_k n}} = \infty$ (azaz a T 12.6.1 Tételben szereplő $A$ -nál kevésbé ritka halmazok is megfelelnek, ráadásul semmiféle oszthatósági tulajdonságra sincs szükség).

A következőkben áttekintjük, hogy a kettőhatványok, illetve a prímszámok halmazához mennyire ritka komplementum található. Kezdjük a kettőhatványokkal. Ruzsa belátta, hogy ezekhez is létezik TGK. Az alábbiakban csak ennél egy kicsit gyengébb eredményt igazolunk.

**12.6.2 Tétel.**

A kettőhatványok $H = \{2, 4, 8, \ldots\}$ halmazához létezik olyan $M$ komplementum, amelyre

$$M(n) < c a_1/\log_5 n \quad (22)$$
Mivel $H(n) = \left\lfloor \log_2 n \right\rfloor$, ezért $H(n)M(n)/n < c$, ami valóban nem sokkal rosszabb (2)-nél.

Megjegyezzük, hogy tetszőleges $s > 1$ egészre is az $s$ hatványaiból álló $H_s = \{s, s^2, s^3, \ldots\}$ halmazhoz létezik TGK.

**Bizonyítás:** Mivel a 2 primitív gyök mod 9, ezért primitív gyök mod $3^v$ is minden $v$-re (lásd a T 3.3.5 Tétel bizonyításában az L2 részt). Ez azt jelenti, hogy ha $(3, n) = 1$, akkor van olyan $0 < k \leq \varphi(3^v) < 3^v$, amelyre $n = 2^k \ (\text{mod} \ 3^v)$. Ha $3 \mid n$, akkor ugyanígy $n - 1 = 2^k \ (\text{mod} \ 3^v)$ . Így minden $n$-hez és $v$-hez van olyan $v$ és $0 < k < 3^v$, hogy

$$n = 2^k + 3^v \quad \text{és} \quad n = 2^k + 3^v + 1.$$  \hspace{1cm} (23)

Ennek megfelelően az $M$ komplementum elemei majd alkalmas $3^vT$ és $3^vT + 1$ alakú számok lesznek.

Adott $n$-hez először $v$-et fogjuk megválasztani, majd megnézzük, milyen $v$-kre van szükség.

Mivel $k < 3^v$ miatt $2^k < 2^{3^v}$, ezért (23)-ban $v$ mindenképpen pozitív, ha $2^{3^v} \leq n$ . Ennek alapján válasszuk $n$-hez $v$-et a következőképpen:

$$2^{3^v} \leq n < 2^{3^v+1}.$$  \hspace{1cm} (24)

Ekkor (23) és (24) szerint

$$v \leq 3^v < n < 2^{3^v+1},$$

és így legyen

$$M = \bigcup_{v=1}^{\infty} M_v, \quad \text{ahol} \quad M_v = \{3^v, 3^v + 1 \mid 0 < v < 2^{3^v+1}\}. \quad (25)$$

Az eddigi megondolások alapján $M$ komplementuma $H$-nak.

Most belátjuk, hogy (22) is teljesül.

Legyen

$$K = \{3^v \mid 0 < v, 0 < n < 2^{3^v+1}\}, \quad (26)$$

ekkor

$$M(n) \leq 2|K|. \quad (27)$$

A $K$ halmaz is kétfelé bontjuk, $K_1$-re és $K_2$-re aszerint, hogy $v \leq T$, illetve $v > T$, ahol a $T$-t (az $n$-től függően) később alkalmazásban megválasztjuk.

$K_1$-ben $v$ értéke $T$-fele, $v$ értéke pedig legfeljebb $\log_3 n$-félé lehet, vagyis

$$|K_1| \leq T \log_3 n. \quad (28)$$

$K_2$-ben (26) szerint $T < v < 2^{3^v+1}$, azaz

$$3^{v+1} > \log_3 T. \quad (29)$$
A $3^r$-hez tartozó $\nu$-k száma legfeljebb $\left\lfloor \frac{n}{3^r} \right\rfloor$, tehát

$$|K_2| < \sum_{r \geq \tau_0} \frac{n}{3^r} = \frac{3}{2} \cdot \frac{\tau_0}{3^r},$$

ahol $\tau_0$ a (29)-nek eleget tevő legkisebb $\tau$ érték. Ebből kapjuk, hogy

$$|K_2| < \frac{3}{2} \cdot \frac{\tau_0}{\log_2 T}. \tag{31}$$

(27), (28) és (30) alapján $M_{\nu}(\tau) < 2T \log_4 \nu + 9\nu^2 / \log_2 T$. Innen (22) például a $T = \left\lfloor \frac{\nu}{(\log_2 \nu)^2} \right\rfloor$ választással adódik. □

Most a prímszámok halmazához keresünk minél ritkább komplementumot. Az ezzel kapcsolatos legjobb eredmény Erdőstől származik:

12.6.3 Tétel . \quad T 12.6.3

A prímszámok $\mathbb{P}$ halmazához létezik olyan $\overline{P}$ komplementum, amelyre

$$R(n) < e \log^2 n \tag{31}$$

(ahol $e$ explicit kiszámolható konstans és $\log$ a természetes alapú logaritmust jelöli). □

Mivel $P(n) = \pi(n) \sim n / \log n$, ezért $P(n)R(n)/n < c' \log n$, ami már lényegesen rosszabb (2) nél. A másik irányból Ruzsa Imre igazolta, hogy itt (2) biztosan nem érhető el, azaz $\mathbb{P}$-hez nem létezik TGK.

A bizonyítás fő gondolatmenete: Egy olyan valószínűségi mezőt konstruálunk, amelynek elemei a pozitív egészek bizonyos $\mathbb{P}$ részsorozatai, és meg fogjuk mutatni, hogy egy ilyen $\mathbb{P}$ sorozat 1 valószínűséggel komplementuma a $\mathbb{P}$-nek, és $R(n) \sim e \log^2 n$ ugyancsak 1 valószínűséggel teljesül. Ebből következik, hogy van a tétel állításának eleget tevő $\mathbb{P}$. (Figyeljük meg, hogy ez a gondolatmenet konkrét konstrukció megadása nélkül igazolja a kívánt tulajdonságú sorozat létezését, sőt azt is, hogy „majdnem minden” $\mathbb{P}$ sorozat ilyen, ez utóbbi persze a megadott valószínűség mértéke szerint kell érteni.)

Legyenek $0 \leq \alpha_i \leq 1$, $i = 1, 2, \ldots$ tetszőleges valós számok. Ekkor létezik olyan valószínűségi mező, amely a pozitív egészek bizonyos részsorozataiból áll, és bármely $n$ pozitív egészre $\alpha_i$ annak a valószínűsége, hogy $n \in \mathbb{P}$, továbbá az $n \in \mathbb{P}$ és $m \in \mathbb{P}$ események bármely $n \neq m$ esetén függetlenek. Szemléletesen ezt úgy lehet elképzelni, hogy a sorozatok képzésénél az $1, 2, \ldots$ számokat egymástól függetlenül és rendre $\alpha_1, \alpha_2, \ldots$ valószínűséggel választjuk be a sorozatba.

Legyen most

$$\alpha_i = \min(1, d(\log i)^{\delta}), \tag{32}$$

ahol $d > 0$ később alkalmasan megválasztandó konstans.

Először azt vázoljuk, hogy egy $\mathbb{P}$ sorozat ekkor 1 valószínűséggel komplementuma $\mathbb{P}$-nek.

Legyen $Q_\nu$ az az esemény, hogy az $n$ nem írható fel $\nu^r = \mathbb{P} + \nu^r$ alakban, ahol $\mathbb{P}$ prímszám, $\nu \in \mathbb{P}$, és jelöljük $Q_\nu$ valószínűségét $Q_\nu$-nel. Az $\mathbb{P}$ akkor lesz komplementuma $\mathbb{P}$-nek, ha a $Q_\nu$ események közül csak véges sok következik be. A Borel–Cantelli-lemma szerint ennek 1 a valószínűsége, ha a $Q_\nu$-ek összege konvergens, azaz

428
Számoljuk ki \( q_n \)-et. Egy \( P \) prímre \( n \neq r + p \) azt jelenti, hogy \( u - p \not\in P \), és ennek \( 1 - \alpha_{n-p} \) a valószínűsége. A \( Q_n \) esemény az, hogy \( n \) semmilyen \( P \) prímmel sem írható fel \( n = r + p \) alakban, és így

\[
q_n = \prod_{p < n}(1 - \alpha_{n-p}). \tag{34}
\]

(34)-et és \( 1 - \omega \leq e^{-\omega} \)-et felhasználva, a (33)-beli \( S \)-re

\[
S = \sum_{n=1}^{\infty} q_n = \sum_{n=1}^{\infty} \prod_{p < n}(1 - \alpha_{n-p}) \leq \sum_{n=1}^{\infty} e^{-\sum_{p < n}\alpha_{n-p}} \tag{35}
\]

adódik. Itt a jobb oldalon az \( e \) kifejezése (32) alapján „lényegében”

\[
-d! \sum_{p < n} \frac{\log(n - p)}{n - p} > h \log n, \tag{36}
\]

Belátható, hogy alkalmas \( h \) konstansnal

\[
\sum_{p < n} \frac{\log(n - p)}{n - p} > h \log n, \tag{37}
\]

ha \( u \) elég nagy, tehát a (36)-beli kifejezés kisebb, mint \( -d! \log n \), és így (35) alapján

\[
S < \sum_{n=1}^{\infty} e^{-d! \log n} = \sum_{n=1}^{\infty} n^{-d!},
\]

ami valóban konvergens, ha \( d! -u \)-úgy választjuk, hogy \( d! > 1 \) teljesüljön.

A (37) állítás kicsit hasonlít az T 5.6.3 Tételbeli \( \sum_{p < n}(\log p)/p \sim \log n \) összefüggéshez, mindkettőben \( (\log k)/k \) típusú tagok szerepelnek, azonban a prímek fokozatos ritkulása miatt ez utóbbi összegben a kis \( k \) értékekhez tartozik, és így nagyobb \( (\log k)/k \) tagok dominálnak, míg (37)-ben fordított a helyzet. (37) igazolásához éppen azt kell felhasználni, hogy a prímek későbbi „viszonylag rövid” intervallumokban is „elég sűrű” helyezkednek el.

Most rátérünk annak vázolására, hogy 1 valószínűséggel \( R(n) \sim c \log^2 n \). \( R(n) = \sum_{i=1}^{n} \xi_i \), ahol a \( \xi_i \) valószínűségi változó értéke 1, ha \( i \in \mathbb{R} \), és 0, ha \( i \not\in \mathbb{R} \). Ekkor

\[
\sum_{i=1}^{n} \frac{E(\xi_i)}{\mu_i} = \sum_{i=1}^{n} \frac{\log \mu_i}{\mu_i} \sim \log x \int_{1}^{x} \frac{\mu_i}{\mu_i} \log x dx = \frac{d \log^2 n}{2},
\]

Így elég azt igazolni, hogy 1 valószínűséggel \( \sum_{i=1}^{n} \xi_i \sim \sum_{i=1}^{n} E(\xi_i) \). Ez általánosan igaz, ha \( E(\xi_i) \)-re és \( D(\xi_i) \)-re megfelelő feltételek teljesülnek, amelyek a jelen esetben könnyen ellenőrizhetően valóban fennállnak.

Végül bizonyítás nélkül megemlíthetjük Lorentznek általános halmazok komplementumára vonatkozó alábbi eredményét:

\[
S = \sum_{n=1}^{\infty} q_n < \infty. \tag{33}
\]
12.6.4 Tétel. \[ T \ 12.6.4 \]
Tetszőleges \( A \)-hoz létezik olyan \( B \) komplementum, amelyre
\[
B(n) < 10 \sum_{i=1}^{a} \frac{\log A(i)}{A(i)} \quad \star
\]

Feladatok

12.6.1 Általánosítsuk a pont legelején szereplő példát 10 helyett tetszőleges \( c > 1 \) alapú számrendszerre és a helyértékeknek a páros-páratlan helyett tetszőleges más csoportosítására. Mutassuk meg, hogy az így kapott \( A \) és \( B \) halmazok egymás komplementumai, és határozzuk meg \( \lim_{n \to \infty} A(n)B(n)/n \) értékét.

12.6.2 Legyen \( H \) a kettőhatványok halmaza és \( P_1 = \{ p, p + 1 | p \text{ prím} \} \), azaz a primek mellé vegyük be a \( p + 1 \) alakú számkat is. Igaz-e, hogy \( H \) és \( P_1 \) egy más komplementumai?

12.6.3 Az alábbi feltételek mindegyikéről döntsük el, hogy szükséges-e, illetve elégséges-e ahhoz, hogy az \( A = \{a_1 < a_2 < \ldots \} \) halmaznak létezen véges komplementum, azaz alkalmas véges \( B \) halmazt véve minden elégg negy pozitív egész selőálljon egy \( A \)-beli és egy \( B \)-beli elem összegeként.

(a) \( a_{i+1} - a_i \) korlátos.
(b) \( A \) tartalmaz végtesen számtoni sorozatot.
(c) \( \lim_{n \to \infty} A(n)/n > 0 \)
(d) \( \lim_{n \to \infty} A(n)/n = 1 \)

12.6.4 (*) Legyenek \( A \) elemei \( a_k = 6^k + k \), \( B \) elemei pedig a \( 6^k(1 - 1/k) \) és \( 6^k-1 \) között a \( d_k \)-val oszthatók, ahol \( d_k \) egy olyan \( 2^i3^j \) alakú szám, amelyre \( d_k < k - 5 \log_2 k \), de \( d_k \sim k \) és \( d_{k+1} \leq d_k \). Igazoljuk, hogy \( A \) és \( B \) egymás teljesen gazdaságos komplementumai.

12.6.5 Mutassuk meg, hogy a primekhez a \( T \ 12.6.4 \) Tétel egy olyan \( S \) komplementumot biztosít, amelyre \( S(n) < c \log^2 n \) (vagyis így a \( T \ 12.6.3 \) Téthel gyengébb eredményt kapunk).

12.6.6 Lássuk be, hogy tetszőleges \( A \) (végtesen) halmaznak van olyan \( B \) komplementuma, amelyre \( B(n)/n \to 0 \), ha \( n \to \infty \) (azaz \( B \) nulla sűrűségű).
13. fejezet - EREDMÉNYEK ÉS ÚTMUTATÁSOK

13.1 Számelméleti alapfogalmak

13.1.1. 

1.1.1 A hatjegyű szám a háromjegyű szám 1001-szere, és 1001 osztható 91-gyel.

1.1.2 Mutassuk meg, hogy az \( a^2 - b^2 = (a - b)(a + b) \) szorzatban mindkét tényező páros és (pontosan) az egyik osztható 4-gyel.

Másik lehetőség: \( (2k + 1)^2 - (2m + 1)^2 = 4k(k + 1) - 4m(m + 1) \) jobb oldalán mindkét tag osztható 8-cal.

1.1.3 \( \overline{35a} = 100b + 10c + a = 10 \cdot a + b - 999c \).

1.1.4 Szorozzuk be \( 5a + 9b \) -t alkalmas egész számmal úgy, hogy ehhez a 23 megfelelő többszörössét hozzáadva éppen \( 3a + 10b \) -t kapjunk.

1.1.5 Igaz: (b), (d), (f).

1.1.6

(i) Használjuk az \( a^n - b^n = (a - b)(a^{n-1} - a^{n-2}b + \cdots + b^{n-1}) \) azonosságot.

(ii)–(iii) Alkalmazzuk (i)-et helyett \( -b \)-vel.

1.1.7 \( c = \pm 3 \).

1.1.8 \( 11^a + 2 + 12^a - 1 = 12(144 - 11^a) + 133 \cdot 11^a \).

Bizonyíthatunk teljes indukcióval is.

1.1.9 \( n = 4k + 2 \). (Belátható, hogy ez az összes megfelelő \( n \).

1.1.10 A \( (b - 1)^2 \ | b^k - 1 \) oszthatóság ekvivalens \( b - 1 \ | b^{k-1} + b^{k-2} + \cdots + 1 \) teljesülésével. Itt a jobb oldalt írjuk át

\[
(\overline{b^{k-1} - 1}) + (\overline{b^{k-2} - 1}) + \cdots + (1 - 1) + k
\]
alakba, ekkor az első \( k \) tag mindig osztható \( b - 1 \)-gyel.

1.1.11 Ha \( a \geq b \), akkor \( 2^a + 1 = 2^a - b^b - b + 2^a - 1 + 1 \). Az eljárást folytatva kapjuk, hogy van olyan \( d < c \), amelyre \( 2^b - 1 \mid 2^d + 1 \). Innen \( 2^d - 1 < 2^d + 1 < 2^{d-1} + 1 \), amiből a kívánt \( b < 2 \) adódik. — Egy másik út: Ha \( b \) -nek van egy \( c > 1 \) páratlan osztója, akkor \( 2^c - 1 \mid 2^{ac} - 1 \), továbbá \( 2^c - 1 \mid 2^b - 1 \mid 2^a + 1 \mid 2^{ac} + 1 \), ahonnan \( 2^c - 1 \mid 2 \), ami ellentmondás. Ha \( b \) osztható 4-gyel, akkor \( 15 = 2^1 - 1 \mid 2^b - 1 \mid 2^c + 1 \), ez azonban lehetetlen, ugyanis \( 3 \mid 2^c + 1 \iff c \) páratlan és \( 5 \mid 2^c + 1 \iff a = 4k + 2 \).
1.1.12

(a) $a = b \sigma$ alapján $|a| = |b| \cdot |\sigma| \geq |b| \cdot 1$, ha $q \neq 0$.

(b) Az (a) rész alapján $\sigma$ osztóinak a száma legfeljebb $2 \cdot |\sigma|$.

1.1.13 Használjuk fel, hogy egy pozitív egész számnak önmagán kívül a legnagyobb pozitív osztója legfeljebb a szám fele, a következő pedig legfeljebb a szám harmada lehet. — Válasz:

(a) a pozitív páros számok;

(b) a 3-mal, illetve a 4-gyel osztható pozitív számok (csak $3k = k + k + k$, $4k = 2k + k + k$ és $6k = 3k + 2k + k$ lehetséges).

1.1.14 Jelölje a szám számjegyeit az egyes helyi értéktől (azaz „hátulról”) kezdve $a_0, \ldots, a_n$, ekkor a szám

$$a_n a_{n-1} \cdots a_1 a_0 = a_{n-1} 10^n + a_{n-2} 10^{n-1} + \cdots + a_1 10 + a_0.$$ Használjuk fel a következők:

(a) $10^k - 1$ mindig osztható 9-cel.

(b) $\hat{k} \geq 2$ esetén $10^\hat{k}$ osztható 4-gyel, illetve 25-tel.

(c) $\hat{k} \geq 3$ esetén $10^\hat{k}$ osztható 8-cal, illetve 125-tel.

(d) Ha $\hat{k}$ páratlan, akkor $10^\hat{k} + 1$, ha pedig $\hat{k}$ páros, akkor $10^\hat{k} - 1$ osztható 11-gyel.

1.1.15 Nem létezik, vizsgáljuk a 3-mal való oszthatóságot.

1.1.16 Létezik: bizonyítsuk be teljes indukcióval, hogy bármely $k$-ra létezik (pontosan egy) olyan $k$-jegyű szám, amelyben csak az 1 és 2 számjegyek fordulnak elő, és amely osztható $2^k$-val.

1.1.17 (b) $\binom{n}{k}$ egész szám.

1.1.18 Minden $n > 1$-re az első játékosnak van nyerő stratégiája.

1.1.19 írjuk fel a számokat egy kettőhatvány és egy páratlan szám szorzataként, és használjuk a skatulyaelvet. — Okoskodhatunk teljes indukcióval is.

1.1.20 $0 = \emptyset \cdot q$ fellépésnek $\emptyset$ nem egyértelmű.

1.1.21 (a) $u = 4k + 2$.

(b) $u = \pm 4$.

1.1.22

(a) Osztható; a hányadosuk (a nevező gyökéntelenítése után) ilyen alakra hozható.

(b) $1 + \sqrt{2} \mid 1$.

(c) $1 + \sqrt{2}$ hatványai megfelelnek.
(d) Vég tele sok.

(e) Ha \( \pm 1 = c^2 - 2d^2 = (c + d\sqrt{2})(c - d\sqrt{2}) \), akkor \( c + d\sqrt{2} \mid 1 \).

A megfordításhoz mutassuk meg, hogy ha \( c + d\sqrt{2} \mid r + s\sqrt{2} \), akkor \( s^2 - 2d^2 \mid r^2 - 2s^2 \).

(f) Ha lenne ezeken kívül is egység, akkor azt alkalmasszak \( \pm (1 + \sqrt{2})^k \)-val beszorozva egy olyan \( u + v\sqrt{2} \) egységet is kapnánk, amelyre

\[
1 < u + v\sqrt{2} < 1 + \sqrt{2}.
\]

Itt (e)-el felhasználásával \( u \) és \( v \) előjelének mind a négy lehetséges értékkészletéből ellentmondásból jutunk.

(g) Mindkét lehetőség végtele sokszor előfordul: ez lényegében (e)-ből következik.

1.1.23 (d) (ii) és (iv) bármely integrálatási tartományban igaz, (i) és (iii) pedig pontosan akkor, ha létezik egységelem. (Ha nincs egységelem, akkor \( a \mid b \land c \iff a = b - 0 \).)

13.1.2.

1.2.1 Válasz: 97.

Útmutatás: A háromjegyű szám osztója a két szám különbségének.

1.2.2 Mivel csak \( \equiv n \)-féle osztási maradék lehet, ezért lesz végtele sok olyan kettőhatvány, amelyek azonos maradékokat adnak \( n \)-mel osztva.

1.2.3 Tekintsük a \( a_1, a_2, \ldots, a_k \) számok \( n \)-nel való osztási maradékkait.

1.2.4 Ha \( \equiv n \) az adott szám, akkor vegyük azokat a legfeljebb \( n + 1 \)-jegyű számokat, amelyeknek minden számjegye 1-es: 1, 11, 111, … Ezek között biztosan lesz két olyan, amelyek azonos maradékokat adnak \( n \)-mel osztva, így a különbségük osztható \( n \)-mel és a kívánt alakú.

1.2.5 Jelöljük \( \equiv n \)-nak \( n \)-mel való osztási maradékát \( r_{n-1} \)-val. Az \( \{r_{n}, r_{n+1}\} \) párok csak \( n^2 \)- különbségő értéket vehetnek fel, ezért lesz olyan \( t > s \), amelyre \( \{r_t, r_{t+1}\} = (r_s, r_{s+1}) \). Lássuk be, hogy ekkor bármely \( \overline{k} \)-ra \( \{r_{t}, r_{t+1}\} \) \( \{r_{t+s}, r_{t+s+1}\} \), azaz az \( r_n \) maradékok periodikusan ismétlődnek (\( t < s \) periodus szerint). Mivel \( r_0 = 0 \), ezért bármely \( j \)-re \( r_j(0-s) = 0 \), azaz \( n\mid r_j(0-s) \).

1.2.6

(a) Minden szám \( 3k \) vagy \( 3k \pm 1 \) alakú, ezek négyzete \( 3r \), illetve \( 3s + 1 \) alakú, azaz egy négyzeteszám 3-mal osztva 0 vagy 1 maradékat adhat.

(b) 0, 1.

(c) 0, \pm 1.

(d) 0, 1, 4.

1.2.7 Vizsgáljuk az összeg maradékát 3-mal vagy 4-gyel osztva.

1.2.8
(a) Nincs. Vizsgáljuk a 4-gyel és az 5-tel való osztási maradékot.

(b) Az (a) részhez hasonlóan megmutatható, hogy a nyolc- vagy többjegyű számok között nincs ilyen négyzeteszám, továbbá a négy- vagy hatjegyű ilyen számok utolsó jegye csak 4 lehet. Ez utóbbiaknál vizsgáljuk a 11-gyel, illetve a $\frac{111}{3} = 3\overline{7}$ -tel való oszthatóságot. — Válasz: az egyetlen ilyen négyzeteszám a 7744.

1.2.9 Mutassuk meg, hogy egy számnak és bármely páratlan párhuzamot hatványának ugyanaz a maradéka 3-mal osztva.

1.2.10 Válasz: 16 (azaz a szorzat minden esetben osztható $2^{10}$-nal, és vannak olyan számok, amikor $2^{17}$ -nel már nem).

1.2.11 $A \lfloor \sqrt{n} \rfloor = k$ egyenlőség pontosan a $k^2 \leq n < (k + 1)^2$ számokra teljesül. Ezek közül éppen a $k^2$, $k^2 + k$ és $k^2 + 2k$ osztható $k$ -val. — Válasz: $3(19^2 - 1) = 290997$.

1.2.12 $|a + b| - (|a| + |b|) = 9$ vagy 1.

1.2.13 Nem. Például $1^2 = 2q + r$ esetén $r \geq 4$.

1.2.14 Legyen a számrendszer alapszáma $t$. Ha $d \mid t - 1$, akkor egy szám $d$ -vel való osztási maradéka megegyezik a számjegyei összegének az osztási maradékával. Ha $d \mid t^k$, akkor az osztási maradék megegyezik az utolsó $k$ számjegyből álló szám osztási maradékával. Ha $d \mid t + 1$, akkor az osztási maradék megegyezik a számjegyek váltakozó előjelű összegének az osztási maradékával (az egyesek helyén álló számjegyet pozitív előjellel kell venni).

1.2.15 Ez tulajdonképpen az előző feladatnak a speciális esete.

1.2.16 Vizsgáljuk a 9-cell való osztási maradékot. — Válasz: 8.

1.2.17 A 9-es számrendszerbeli jegyeket egyenként átírjuk 3-as számrendszerbeli (esetleg 0-val kezdődő) kétjegyű számokká. — Hasonló meggondolás alkalmazható minden olyan esetben, amikor az egyik alap a másiknak (positív egész kívüleinés) hatvanya.

1.2.18 Válasz: $u = 8$.

Útmutatás: $A \lfloor t^3 \rfloor \leq v \leq (t + 1)^2 - 1$ feltételből $t = 2$ adódik.

1.2.19 A feltételekből rögtön adódik, hogy a jobb oldali szorzótényező 1102. A részletszorzatok összefoglalásából látszik, hogy a számrendszer alapszáma $t \leq 4$, a szorzat utolsó jegye miatt viszont $t$ páratlan, így $t = 3$. Hasonló meggondolásokból kapjuk, hogy az első szorzótényező 2102.

1.2.20 A $t \mid 7355$, $t \geq 5$ és $t < 10$ feltételekből $t = 7$.

1.2.21

(a) $A 1, 2, 4, \ldots, 2^9$ súlyokkal $2^{10} - 1 = 1023$ gramm beállítatlan minden egész gramm lemérhető. Ez a lehető legtöbb: egy mérés során minden egyes súlynál két lehetőség között választhatunk: betesszük a serpenyőbe vagy nem tesszük be. Így tíz súlyval legfeljebb $2^{10} - 1$ -féle értékét lehet lemérni (az 1-et azon eset miatt kell levonni, amikor egyik súlyt sem tesszük be a serpenyőbe).

(b) $A 1, 3, 9, \ldots, 3^9$ súlyokkal $(3^{10} - 1)/2$ grammig minden egész gramm lemérhető: a hármas számrendszerbeli felírásnál a 2-es számjegyeket „$-1$ -esekre” kell átváltani. Ennél jobb súlykészlet
nincs: a méréseknél minden súlyra 3 lehetőség van (egyik serpenyő — másik serpenyő — egyik sem), azonban a két serpenyő szimmetriája miatt az így kapott számot 2-vel el kell osztani.

1.2.22 A keresett határérték \( \log_{2} 10 = 3.3219 \ldots \)

1.2.23 Az T 1.2.2 Tétel bizonyítását kell értelemszerűen módosítani.

13.1.3.

1.3.1 \( 14 = 3794 \cdot (-44) + 2226 \cdot 75 \).

1.3.2

(a) \( A \left(3n + 5, 7n + 12\right) = d \) jelöléssel \( d \mid -7(3n + 5) + 3(7n + 12) = 1 \), és így \( d = 1 \).

(b) \( A \left(3n^2 - 1, 4n^2 + 3\right) = d \) jelöléssel \( d \mid -4(3n^2 + 1) + 3(4n^2 + 3) = 5 \), továbbá \( 5 \mid 3n^2 + 1 \), és így \( d = 1 \).

(c) Az \( (\nu! - 1, (\nu + 1)!, 1)\) jelöléssel \( d \mid (\nu + 1)! - 1 \) és így \( d \mid \nu! - (\nu! - 1) = 1 \).

(d) \( A \left(7^n - 2, 7^{n+1} - 5\right) = d \) jelöléssel \( d \mid (7^{n+1} - 5) - 7(7^n - 2) = 9 \), továbbá \( 7^n - 2 = (2 \cdot \nu + 3 + 1)\nu - 2 = 3k + 1 - 2 = 3k - 1 \), tehát \( d \) nem lehet osztható 3-mal.

1.3.3 ha \( \nu \) páratlan, és 2, ha \( \nu \) páros.

1.3.4 (a) 5 vagy 10.

(b) 5, 15 vagy 45.

1.3.5 6, 10, 15 vagy 21, 66, 77 stb.

1.3.6 Igaz: (a), (c).

1.3.7 Válasz: \( (a, b) \). — Útmutatás: \( b \mid k \leftrightarrow \frac{b}{(a, b)} \mid k \).

1.3.8

(a) Igaz: mivel \( (\nu + a, b + \nu) \mid (\nu + \nu) - (b + \nu) = a - b \), biztosan megfelelnek azok az \( n \) -ek, amelyekre \( a + \nu = k(a - b) + 1 \) alakú.

(b) Igaz.

(c) Hamis, ellenpélda \( a = 1, b = 4 \).

1.3.9

(a) Végtelen sok; ha \( a, b \) ilyen számpár, akkor bármely \( t \) egésszel az \( a + t, b - ta \) számpár is megfelel.

(b) 1.

(c) \( (a, b) \).

1.3.10 (b) Használjuk fel, hogy \( \delta \) és \( \delta_1 \) kölcsönösen osztják egymást.
1.3.11 Először lássuk be, hogy \( e(a,b) \mid \{ae, cb\} \). Ezután a \( e(a,b)g = (ca, cb) \) egyenlőségben mutassuk meg, hogy \( q \) egység.

1.3.12

(a) Pontosan azoknak, amelyek a 10-hez relatív prímek (azaz nem oszthatók sem 2-vel, sem 5-tel). — Útmutatás: Használjuk az 1.2.4 feladat [7] gondolatmenetét, majd az T 1.3.9 Tételt.

(b) A legkisebb ilyen a \( 3^{1000} \) darab 1-esből álló csupaegy. — Útmutatás: Igazoljuk \( k \) szerinti teljes indukcióval, hogy a \( 3^k \) -nal osztható legkisebb csupaegy éppen \( 3^k \) darab 1-esből áll.

1.3.13 Használjuk fel többször az \( r \mid s \Rightarrow r^{2} - 1 | r^a - 1 \) összefüggést, valamint az \( (a, k) = n \alpha + k \nu \) előállítást.

1.3.14

(a) Mutassuk meg, hogy ha \( (n, k \) kettőhatványok és például) \( k < n \), akkor \( a^k + 1 | a^n - 1 \).

(b) \( d^{(n,k)} + 1 \), ha \( \alpha / (n, k) \) és \( k^j (n, k) \) páratlan, egyébként pedig 1, illetve 2, aszerint, hogy \( a \) páros, illetve páratlan.

1.3.15 A másodszomszédok is relatív prímek. A harmadszomszédok közül a 3-nal osztható indexek legnagyobb közös osztója 2, a többiek relatív prímek.

1.3.16 Használjuk fel a \( \varphi_{3^{n+k} = \varphi_{3^{n+k-1} + \varphi_{3^n + 1}} \) azonosságot. Ebből a \( k | \alpha \Rightarrow \varphi_k | \varphi_{3^n} \) állítást az \( n/k \) szerinti teljes indukcióval igazolhatjuk. A megfordításhoz és a legnagyobb közös osztóra vonatkozó állításhoz lássuk be, hogy ha \( a = bq + r \), akkor \( (\varphi_a, \varphi_r) = (\varphi_q, \varphi_r) \). — Egy másik lehetőség: Mutassuk meg, hogy bármely \( m \) -re az \( m \) -mel osztható Fibonacci-számok indexei éppen a legkisebb ilyen tulajdonságú nemnulla Fibonacci-szám indexének a többszörösei.

1.3.17 A két szakasz hosszát \( a \) -val és \( b \) -vel jelöljük, \( k \) és \( n \) pedig alkalmas pozitív egészeket jelentenek.

(a) Ha \( a/b = k/n \), akkor \( a/k = b/n \) közös mérték. Megfordítva, ha \( c \) közös mérték, azaz \( a = kc \), \( b = uc \) (ahol \( c \) közös mérték), akkor az \( a \) -val és \( b \) -vel végzett euklideszi algoritmus tulajdonképpen ugyanaz, mint a \( k \) és \( n \) egész számokkal végzett euklideszi algoritmus, tehát véget ér. Megfordítva, ha a szakaszokkal végzett euklideszi algoritmus véget ér, akkor az utolsó nemnulla maradék közös mérték lesz.

(b) Végelen sok; bármely \( nt \) -re egy közös mérték \( nt \) -edrésze is közös mérték.

(c) A maradékos osztás megfelelője: annyiszor felmérjük a kisebbik szakaszt a nagyobbikra, ahányszor csak lehet, azaz \( a = bq + r \), ahol \( q \) pozitív egész, \( r \) valós, és \( 0 \leq r < b \). Ha a két szakasz összemérhető, \( a = kc \), \( b = uc \) (ahol \( c \) közös mérték), akkor az \( a \) -val és \( b \) -vel végzett euklideszi algoritmus tulajdonképpen ugyanaz, mint a \( k \) és \( n \) egész számokkal végzett euklideszi algoritmus, tehát véget ér. Megfordítva, ha a szakaszokkal végzett euklideszi algoritmus véget ér, akkor az utolsó nemnulla maradék közös mérték lesz.

(d) Ilyen „kitüntetett” közös mérték létezése az euklideszi algoritmusból következik.

(e) Az \( A \mathcal{B} \mathcal{C} \mathcal{D} \) négyzet \( b \) hosszúsága oldalát mérjük fel \( A \) -ból az \( a \) hosszúságú \( A \mathcal{C} \) átlóra. Az így kapott \( F \) pontra \( A F = b \) és \( F C = r \). Állítsunk \( E \) -ből merőleges az átlóra, ez mesze a \( B \mathcal{C} \) oldalt \( F \)-ben. Ekkor \( r = F \mathcal{C} = F F = F B \). Ha most az algoritmus következő lépésében \( b \)-t osztjuk maradékosan \( r \)-nel, akkor először \( B F \)-et felmérve \( B \mathcal{C} \)-re, ezután az \( E \mathcal{C} \) egyenlőszárú derékszögű háromszög \( \mathcal{C} \mathcal{B} \) átfogóját és \( C \mathcal{E} \) oldalát kell maradékosan elosztanunk. Ezzel azonban a kiindulási helyzet ismétlődött meg kisebb méretekben: egy (kisebb) négyzet átlóját és oldalát kell összehasonlítanunk. Ez azt mutatja, hogy az euklideszi algoritmus a vég telenségig folytatódik.

436
13.1.4.

1.4.1 Eredmény: (a) és (b) 3.
(c) 5.
(d) 7.

Útmutatás: Vizsgáljuk a 3-mal, 5-tel, illetve 7-tel való osztási maradékot.

1.4.2 Nem létezik; ha a $c$ differencia pozitív, és $c > 1$ a számtoni sorozat tetszőleges eleme, akkor például a $c + 6c$ elem biztosan összetett.


1.4.4
(a) Alkalmazzuk az $a - 1 | a^k - 1$, illetve $k = rs$ esetén az $a^r - 1 | a^s - 1$ oszthatóságokat.
(b) Ha $\hat{k} = rs$, ahol $s$ páratlan, akkor $a^r + 1 | a^k + 1$.

1.4.5 Eredmény: $t = 2, k = 1$.

Útmutatás: Vizsgáljuk a $t + 1$-gyel vagy $t$ -vel való oszthatóságot.

1.4.6 Eredmény: (a), (d) és (e) $u = 1$.
(b) $u = 2, 4$.
(c) Nincs ilyen $u$.

Útmutatás: (a)-nál vizsgáljuk a 3-mal való oszthatóságot, a másik négy kifejezést pedig bontsuk szorzattá.

1.4.7
(a) Ha $a = ab$, ahol $0 < a \leq b$, akkor $a \leq \sqrt{n}$, így csak $a = 1$ lehet.
(b) Ha ennek a legkisebb $d$ osztónak lenne egy nemtriviális pozitív $s$ osztója, akkor $s | n$ is igaz és $1 < s < d$, ami ellentmondás.
(c) Ha $a = dk$, ahol $d$ az 1-nél nagyobb osztó közül a legkisebb, akkor a (b) rész szerint $d$ prim, és az (a) rész felhasználásával kapjuk, hogy $k$ is prim.

1.4.8 Használjuk ki a $17$ prim tulajdonságát.

1.4.9 A felbontatlanok a $4k + 2$ alakú számok, primek pedig nincsenek.

1.4.10
(a) Vizsgáljuk a $p | p^2$ oszthatóságot (és használjuk fel az 1.1.23a feladat [5] megoldásánál látott gondolatmenetet is).

437
**13.1.5.**

1.5.1 Ha \( a = p_1 \cdots p_v \), akkor \( |p_k| \geq 2 \) miatt \( a \geq 2^v \).

1.5.2

(a) A \( 2^t \), \( \pm 2^k \) és \( 2^k p \) alakú elemek, ahol \( t \) tetszőleges páratlan szám és \( P \) tetszőleges páratlan, az egészek körében felbonthatatlan szám.

(b) Példa: \( 2^2 \cdot 3^{1096} \).

1.5.3 Első bizonyítás: nem igaz a páros számok körében, hogy egy felbonthatatlan szükségképpen prim (sőt, egyáltalán nincsenek prímek).

 Második bizonyítás: a legutolsó lépésben szereplő \( p_1 \mid q_1 - p_1 \Rightarrow p_1 \mid q_1 \) következtetés a páros számok körében nem érvényes, hiszen itt \( p_1 \nmid p_1 \).

1.5.4 \( 1000 = 20 \cdot 50 = 10 \cdot 10 \cdot 10 \).

1.5.5 Felhasználjuk, hogy \( V \) nemnulka elemei egyértelműen felírhatók \( 2^k 5^m \) alakban, ahol a \( k \) és \( m \) kitevők tetszőleges egészek és \( t \) a 10-hez relatív prim egész.

(a) Egységek: \( \pm 2^k 5^m \). — Felbonthatatlanok: \( 2^k 5^m p \), ahol \( p \neq \pm 2, \pm 5 \) az egészek körében felbonthatatlan szám.

(b) A \( 2^k 5^m t \) felbontása \( V \)-ben tulajdonképpen \( t \) felbontását jelenti az egész számok körében.

(c) Legyen \( f(2^k5^m t) = |t| \) és \( f(0) = 0 \).

1.5.6 Az utolsó lépésben \( p_1 \mid q_1 q_2 \cdots q_s \) adódik, és ennek lehetetlenségéhez még egyszer fel kell használni az indukciós feltevést \( a = q_1 q_2 \cdots q_s \)-re.

1.5.7 Legyen \( a = \pm p_1^{b_1} \cdots p_v^{b_v} \), ahol a \( P \) számok páronként különböző pozitív felbonthatatlanok és \( k_i > 0 \), továbbá \( k = k_1 + \cdots + k_v \). Ekkor a felbontások száma \( 2^{k-1} \left| f(1, \ldots, k, t) \right| \).

1.5.8 Az \( c \neq 0 \) felbonthatatlan tényezőkre bontását állítsuk elő \( a \) és \( b \) felbontásából, és használjuk fel, hogy az \( ab \) felbontásában szerepelnie kell a \( P \) egységszerezének is.

1.5.9 A megfelelő \( \{ p_1, p_2, p_3 \} \) értékhármasok: \( 5, 2, 2; -5, -2, -2; 5, 2; 3, 5; -3, 2; -5, 3, -2 \). — Útmutatás: Az átalakítás után kapott \( 2^x p_2 = (p_1 - p_2 - p_3) (p_2 + p_3) \) egyenlőség a szármelélet alaptelete szerint csak úgy teljesülhet, ha \( p_2 + p_3 = \pm p_2, \pm p_3 \neq -1 \) vagy \( \pm p_2 p_4 \).

1.5.10 Válasz: 2 és 3. — Útmutatás: Legyen \( z^x + y^3 = x^a \). Itt feltehető, hogy \( x \) és \( y \) relatív prímek. Bontsuk a bal oldalt szorzattá, ekkor mindkét tényező szükségképpen a \( P \)-nek hatványa. Fejezzük ki innen \( xy \)-t.

**13.1.6.**

1.6.1 Akkor és csak akkor \( k \)-adik hatvány, ha a kanonikus alakjában minden prim kitevője osztható \( k \)-val.
1.6.2
(a) Legyen \( P \) az \( ab \) szorzat \( a \) ténylezőjének egy tetszőleges prímosztója. Mivel \( \{a, b\} = 1 \), ezért \( P \mid b \), vagyis a \( P \) ugyanakkora kitevővel szerepel az \( a \) és az \( ab \) kanonikus alakjában. Ezután használjuk fel az 1.6.1 feladatot [27].

(b) Ha a szorzat nem nulla, akkor a két ténylező egy-egy \( k \)-adik hatvány egységszerese lesz.

(c) A ténylezőkről azt kell feltenni, hogy páronként relatív primek.

1.6.3 Az 1.6.2a feladatra [27] támaszkodjunk.

1.6.4 Válasz: 3 és 7. — Útmutatás: A számolálot bontsuk szorzattá, majd alkalmazzunk az 1.6.2a feladathoz [27] hasonló gondolatmenetet.

1.6.5
(a) Ha \( a_1 \mid \gamma \) és \( b_1 \mid \beta \), akkor az oszthatóság elemi tulajdonságai alapján \( a_1b_1 \mid \alpha \beta \). A megfordításhoz az T 1.6.2 Tételt használjuk fel. Tekintsük az \( ab \) egy tetszőleges \( P \) prímosztóját, és legyen a \( P \) kitevője \( a, b \), illetve \( c \) kanonikus alakjában rendre \( \alpha, \beta \), illetve \( \gamma \) (ezek között a 0 is előfordulhat). A \( c \mid ab \) feltétel szerint \( \gamma \leq \alpha + \beta \), és azt kell megmutatni, hogy \( \gamma \) előáll \( \gamma = \alpha' + \beta' \) alakban, ahol \( 0 \leq \alpha' \leq \alpha \), és \( 0 \leq \beta' \leq \beta \).

(b) Alkalmazzuk az (a)-ban láttott gondolatmenetet, és használjuk fel, hogy \( \alpha \) és \( \beta \) közül az egyik 0. — Egy másik lehetőség: Legyen \( a_1b_1 = a_2b_2 \), ahol \( a_1 \mid a \) és \( b_1 \mid b \). Ekkor \( a_1 \mid a_2b_2 \), továbbá \( (a_1, b_2) = 1 \), tehát \( a_1 \mid a_2 \). Ugyanígy a fordított oszthatóság is teljesül, ezért (a pozitivitás miatt) \( a_1 = a_2 \).

(c) Például \( a \) és \( b \) tetszőleges \( c \geq 1 \) közös osztója előáll \( c = 1 \cdot c = c \cdot 1 \) alakban.

(d) Használjuk az (a), illetve (b) részben láttott gondolatmenetet.

(e) \( (a, b) \mid c \mid [a, b] \).

1.6.6 Használjuk az T 1.6.2 Tételt.

1.6.7 (a) \( 2^{30} \).

(b) \( 2^{10} \cdot 3^2 \).

(c) \( 2^5 \cdot 3 \cdot 5 \cdot 7 = 840 \).

1.6.8 A keresett \( n \) -ek a négyzetszámok. — Útmutatás: Használjuk fel a \( d(n) \) képletét és az 1.6.1 feladatot [27]. — Egy másik lehetőség: Képezzünk osztópárokat; minden \( d \mid n \) osztóhoz párosítsuk az \( \nu/\hat{\nu} \) komplementer osztót, és vizsgáljuk meg, mely esetben fordul elő, hogy egy osztó és a komplementer osztója megegyeznek.

1.6.9 Válasz: 20. — Útmutatás: Vizsgáljuk meg, hogy egy adott sorszámú zárhoz mely örökö nyúltak hozzá, és alkalmazzuk az előző feladatot.

1.6.10 (b) Egyenlőség akkor és csak akkor teljesül, ha \( \omega \) kanonikus alakjában minden prim kitevője páratlan.

1.6.11
(a)–(b) Vizsgáljuk meg, hány olyan osztója lehet \( n \) -nek, amely nagyobb, mint \( n/2 \), illetve \( n/3 \).

(c) Képezzünk osztópárokat, amelyek szorzata \( n \), ezekben a kisebbik (pontosabban a nem-nagyobbik) elem legfeljebb \( \sqrt{n} \). — Egy másik lehetőség: Alkalmazzuk az (a) és (b) részben láttott gondolatmenetet általában \( n/k \)-ra, és válasszuk meg \( k \) értékét optimálisan.

1.6.12 Válasz: \( n^{k(n)/2} \). — Útmutatás: Képezzünk osztópárokat.

1.6.13 Válasz: \( n + 1 \). — Útmutatás: (i) \( n + 1 \) darab osztó valóban megadható, mert \( 2 \cdot 5^{n-i} \), \( i = 0, 1, \ldots, n \) (az egyetlen) megfelelő választás. (ii) Több osztó már nem lehet jó, ugyanis bármely \( n + 2 \) osztó között a skatulyaelv alapján található (legalább) kettő olyan, amelyekben az 5 kitevője azonos, és így ezek valamelyike osztója lesz a másiknak.

1.6.14

(a) \( a \mid b \).

(b) 8.

(c) \( 2^r \), ahol \( r \) a \( b/n \) különböző prímosztóinak a száma.

(A (b) és (c) résznel az \( x \cdot y \) és \( y \cdot x \) szampárokat \( x \neq y \) esetén különbözőknek tekintettük.)

1.6.15 Az \( [a, b]/[a, b] = ab \) azonosság (1.6.6/III. Tétel) bizonyításához hasonló gondolatmenetet lehet alkalmazni.

1.6.16 Igaz: (b), (d).

1.6.17

(a) \( a \mid [a, b] , \ a + b \Longrightarrow b \mid a \).

(b), (d) Osszunk le \( [a, b] \)-vel, és használjuk fel az 1.6.16b feladatot [29].

(c) Például \( a = 10k , \ b = 15k \), vagy \( a = n(n+v) , \ b = v(n+v) \).

1.6.18 Mind a feltétel, mind pedig az állítás azzal ekvivalens, hogy \( a \) és \( b \) bármely közös prímosztója ugyanakkora kitevővel szerepel \( a \) és \( b \) kanonikus alakjában.

1.6.19 Legyen egy tetszőleges \( P \) prim kitevője \( a , \ b \), illetve \( c \) kanonikus alakjában rendre \( \alpha , \beta \), illetve \( \gamma \) (ezek között a 0 is előfordulhat). Ekkor az (a)-beli azonossághoz azt kell igazolni, hogy \( \max(\alpha , \min(n, \beta , \gamma)) = \min(n, \max(\alpha , \beta , \max(\alpha , \gamma)) \). Ennek helyességét külön-külön ellen- őrizzük le abban a három esetben, amikor \( \alpha \) a három kitevő közül a legkisebb, a középső, illetve a legnagyobb. Hasonlóan bizonyíthatunk a (b) résznel is.

1.6.20

(a) Az előző feladat jelöléseivel élve, mindkét feltétel azzal ekvivalens, hogy \( \alpha , \beta \) és \( \gamma \) közül kettő egyenlő, és a harmadik ezeknél nem kisebb.

(b) Végtelen sok.

(c) Az (a)-beli állítás megfelelője igaz marad, ha a legnagyobb közös osztót mindenhol legkisebb közös többszörössel cseréljük. A kitevőkre ez azt jelenti, hogy \( \alpha , \beta \) és \( \gamma \) közül kettő egyenlő, és a harmadik
EREDMÉNYEK ÉS ÚTMUTATÁSOK

1.6.21 Bontsuk minél jobban szorzattá \( p^4 - 1 \) -et, és külön-külön igazoljuk a 16-tal, a 3-mal és az 5-tel való oszthatóságot.

1.6.22 Bontsuk szorzattá \( a^b - b^a \) -t, és külön-külön igazoljuk a 8-cal, a 7-tel és a 9-cel való oszthatóságot.

1.6.23 A kifejezést bontsuk szorzattá, és a 360 prímethatvány tényezőire külön-külön mutassuk meg az oszthatóságot.

1.6.24 Az osztó kanonikus alakjában a megfelelő tényezőkre külön-külön igazoljuk az oszthatóságot.

Használjuk fel az \( \text{c} - \text{b} | a^\text{c} - b^\text{b} \) típusú oszthatóságokat, valamint a 101-gyel való oszthatósághoz a binomiális tételeit.

1.6.25 (a) 275.

(b) Nem végződik nullára.

1.6.26 (a) Az \( n! \) kanonikus alakjában bármely \( p \) prim kitevője kisebb, mint \( n \) : ha \( p^k \leq n < p^{k+1} \).

\[
\alpha_p = \sum_{k=1}^{\infty} \frac{r_k}{p^k} = \sum_{k=1}^{n} \frac{n}{p^k} \leq \sum_{k=1}^{n} \frac{1}{p^k} = \frac{n(p^k - 1)}{p^k - 1} < \frac{n}{p^k - 1} \leq r_k.
\]

(b) \( c = 2, n = 2^i \).

1.6.27

(a) \( \binom{n}{k} = \binom{r_k}{k} \binom{r_k - 1}{k - 1} \). Innen \( k | \binom{r_k - 1}{k - 1} \), és mivel \( k, n = 1 \), ezért \( k | \binom{r_k - 1}{k - 1} \). Ez azt jelenti, hogy \( \binom{n}{k} / k = \binom{r_k - 1}{k - 1} / k \) egész szám.

(b) Nem igaz, ellenpélda \( \binom{10}{4} \).

(c) (c1) \( n = \text{prim} \).

(c2) \( n = 2^i \).

(c3) \( n = 2^i - 1 \).

(d) Nincs: \( k | \binom{r_k}{k} \binom{r_k - 1}{k - 1} \). Innen \( r_k | k \binom{r_k}{k} \). Ha \( \binom{r_k}{k} \binom{r_k - 1}{k - 1} \) lenne, akkor ebből \( r_k | k \) következné, ami lehetetlen.

1.6.28 A megfelelő rozmárlétszámok éppen a kettőhatványok.

1.6.29 Első megoldás: Megfelel egy olyan prim, amely az adott \( n! + k \) szám kanonikus alakjában magasabb hatványon szerepel, mint a \( k \)-ban.

 Második megoldás: Minden gyökök számok van \( n! / 2 \) -nél nagyobb primosztója, és ez semelyik másik számok sem osztója.

1.6.30 9.
1.6.31 A négyzetmentes számok (azaz amelyek nem oszthatók semmilyen egynél nagyobb egész szám négyzetével).

1.6.32 Bizonyítsunk indirekt. Vezessük vissza a feladatot arra az esetre, amikor a két \( k \)-adik hatvány relatív prim, majd mutassuk meg, hogy a különbségük osztója mindkét \( k \)-adik hatvány 2-szeresének, és így a 2-nek is, ami lehetetlen.

1.6.33

(a) Indirekt: \( (\frac{a}{b})^2 = 100 \Rightarrow a^2 = 100b^2 \), majd vizsgáljuk a két oldal kanonikus alakjában az 5 (vagy a 2) kitevőjét.

(b) Indirekt: \( 6^{a/b} = 18 \Rightarrow 6^a = 18b \), itt feltehető \( a, b > 0 \). Vizsgáljuk a két oldal kanonikus alakjában a 2 és a 3 kitevőjét.

1.6.35 (a) Nem létezik.
(b) Létezik.

### 13.2 Kongruenciák

#### 13.2.1

2.1.1 Alkalmazzuk a P1 példánál láttott módszert.

2.1.2 Válasz: 999. — Útmutatás: \( 999 \equiv -1 \pmod{1000} \).

2.1.3 A 11-gyel való oszthatósági szabály bizonyítása:

\[ 10 \equiv -1 \pmod{11} \implies 10^k \equiv (-1)^k \pmod{11}, \]

és így

\[
a_r a_{r-1} \ldots a_1 a_0 = a_r 10^k + a_{r-1} 10^{k-1} + \ldots + a_1 10 + a_0 \equiv \\
= a_0 - a_1 + a_2 + \ldots + (-1)^r a_r \pmod{11}.
\]

2.1.4 Igaz: (a), (d), (e), (h).

2.1.5 Válasz: 50. — Útmutatás: A négyzetszámok lehetséges utolsó számjegyeit a 101-féle számjegy, azaz a 101 szerinti összes maradék négyzetre emeléséből kapjuk meg. Határozzuk meg, hogy így hány páronként inkongruens érték keletkezik, ehhez vizsgáljuk meg, hogy a négyzetre emeléskor milyen egybeeséseket történnek. Használjuk fel a 2.1.4h feladatot [35].

2.1.6 A „tétel” hamis, például \( \left( \frac{3}{7} \right) \neq \left( \frac{5}{7} \right) \). A bizonyításban ott a hiba, hogy egy (egész értékű) tört számlálójába nem szabad azzal kongruens értéket helyettesíteni, még akkor sem, ha az új tört is egész szám lesz.

2.1.7 Az \( a \equiv b \pmod{r} \) kongruencia felhasználásával lássuk be, hogy az

\[ (a^m - b^m)/(a - b) = a^{m-1} + a^{m-2} b + \ldots + b^{m-1} \]

kifejezés is osztható \( r \)-mel.

2.1.8 Mutassuk meg, hogy \( a \equiv b \pmod{3} \), majd ennek felhasználásával lássuk be, hogy

\[ (a^n - b^n)/(a - b) \]

relatív prim a 3-hoz.
EREDMÉNYEK ÉS ÚTMUTATÁSOK

2.1.9

(b) A legegyszerűbb, ha $k$ szerinti indukcióval bizonyítunk, felhasználva (a)-t és az \( \binom{n}{2} = \binom{n}{n-1} + \binom{n-1}{1} \) azonosságot. — Egy másik lehetőség: a törtekkel kapcsolatos problémák elkerülése érdekében érdemes átszorozni a $k!$ nevezővel; mivel \( (k!, p^j - 1) \), ezért így a bizonyítandóval ekvivalens kongruenciához jutunk, változatlan modulus mellett. A „törtmentes” alak a $p - j \equiv -j \pmod{\phi(p)}$ kongruenciák összeszorzásával igazolható.

(c) A (b) résznél jelzett bármelyik módszer értelemszerű módosítása célhoz vezet.

2.1.10 Válasz: $p = 5$. — Útmutatás: Lássuk be, hogy \( \binom{3p}{p} \equiv 3 \pmod{p} \).

2.1.11

(a) A $\phi$-vel történő egyszerűsítés után a nevezőben $(p - 1)!$ marad, ami relatív prim a $p$-hez, tehát a vele történő beszorzás ekvivalens kongruenciához vezet. Ez utóbbi helyességét az előző két feladat mintájára igazolhatjuk.

(b)–(c) Hasonló módszerrel bizonyíthatunk, mint az (a) résznél.

13.2.2.

2.2.1 (a) 3.

(b) 5.

(c) 2.

Útmutatás: A modulus relatív prim a megadott elemekhez, és osztója azok különbségének.

2.2.2 (a) $6^2 \cdot 5^{m-2} \cdot 3^n!$

(b) $6 \cdot 5^{\phi(m)} - 1 \cdot \varphi(m)!$

(Két maradékkrendszert akkor is különbözöen tekintettünk, ha csak az elemek sorrendjében különböznek.)

2.2.3 Mindkét tulajdonság csak a számítani sorozat differenciájától függ, jelöljük ezt $d$ -vel.

(a) $d \mid m$.

(b) $\langle d, \sigma \rangle = 1$.

2.2.4

(a) $\tau n$ páratlan.

(b) Minden $\tau n$ jó.

(c) $\tau n = 2$.

(d) $\langle \tau n, 10 \rangle = 1$.

(e) $\tau n = 2$.

(f) $\tau n = 3^k$.
444

(g) $\gamma n$ négyzetmentes.

(Az (a) és (d) kérdés a 2.2.3b feladat [40] speciális esetének is tekinthető.)

2.2.5

(a) $(\gamma n, 15) = 1$.

(b) Minden $m$ jó.

(c) $\gamma n = 2$.

(d) $(\gamma n, 20) \leq 2$.

(e) Minden $m$ jó. — Ez a 2.2.4g bizonyításában szereplő gondolatmenethez hasonlóan, de annál jóval egyszerűbben igazolható.

2.2.6 Igaz: (b).

2.2.7

(a) A maradék 0, ha $\gamma n$ páratlan, és $m/2$, ha $\gamma n$ páros. — Útmutatás: Lássuk be, hogy a maradék nem függ attól, hogy melyik teljes maradékrendszer választottuk, ezután vizsgáljuk meg például a legkisebb nemnegatív vagy a legkisebb abszolút értékű maradékok rendszerét. — Egy másik lehetőség: állítsuk úgyesen pára a teljes maradékrendszer elemeit.

(b) Használjuk fel az (a) részt. — Páratlan $\gamma n$ esetén mindig tudunk példát mutatni arra is, hogy az $a_i + b_i$ elemek teljes maradékrendszerzert alkotnak, és arra is, hogy nem alkotnak teljes maradékrendszerzert.

(c) Egy redukált maradékrendszer elemeinek az összege 0 maradékok ad, ha $\gamma n > 2$. — Az $a_i + b_i$ összegekre ugyanaz a válasz, mint teljes maradékrendszere esetén.

2.2.8 (a) $\gamma n$ páratlan vagy osztható 4-gyel.

(b) $\gamma n$ páratlan.

2.2.9

(a) $\gamma n = 2^k$. — Útmutatás: Pontosan akkor kapunk teljes maradékrendszerzert, ha a megadott számok páronként inkongruensek, azaz $i + j - (i + 2) + \cdots + j - (i + j + 1)(j - 2)/2$ semmilyen $0 \leq i < j \leq m - 1$ esetén sem lehet osztható $\gamma m$-mel. Ha $\gamma n = 2^k$, akkor a két tényező ellentétes paritását kihasználva lássuk be, hogy ilyen oszthatóság sohasem áll fenn. Ha viszont az $\gamma n$ nem kettőhatvány, azaz $\gamma n = 2^k(2^k - 1)$, ahol $s > 0$ (a $k$ kitevő lehet 0 is), akkor $(2^k - s) + (2^k - s + 1) + \cdots + (2^k - s)$ osztható (sőt egyenlő) $\gamma m$-mel. Itt a legnagyobb tagra biztosan teljesül az előírt $2^k + s < m$ feltétel, azonban a legkisebb tagnál $2^k - s \leq 0$ előfordulhat. Ebben az esetben az előző összeg tagjai közül hagyjuk el az összes negatív, a $(2^k - s)$ szereseit és a 0-t; ekkor már egy, a megfelelő határok közé eső, és továbbra is $\gamma n$-mel osztható „tiltott” összeget kapunk.

(b) $\gamma n$ páros.

2.2.10 Igaz: (a), (c), (e).

Útmutatás (c)-hez és (e)-hez: Mutassuk meg, hogy mindkét állítás következik az alábbiból:

Ha $(r, k) = 1$, akkor létezik olyan $s$, hogy $s \equiv r (\text{max} k)$ és $(s, m) = 1$. 

444
Ennek igazolása: Ha az \( m \) minden prímosztója osztója a \( k \)-nak is, akkor \( \langle r, k \rangle = 1 \Rightarrow \langle r, m \rangle = 1 \), és ekkor \( s = r \) megfelel. Egyébként legyenek \( q_1, \ldots, q_t \) az \( m \) olyan prímosztói, amelyek nem osztói a \( k \)-nak, és tegyük fel, hogy ezek közül éppen \( q_1, \ldots, q_j \) osztója az \( r \)-nek (\( j = 0 \) és \( j = t \) is lehetséges). Ekkor \( s = r + q_{j+1} \cdots q_t \) megfelel.

2.2.11 (b) Válasz: \( m/\langle a, m \rangle \).

Útmutatás: \( ar_i + b \equiv ar_j + b \pmod{m} \iff r_i \equiv r_j \pmod{m/\langle a, m \rangle} \).

2.2.12

(a) \( (a, m) = 1 \) vagy \( 2, ha \ m = 4k + 2 \) alakú, és \( (a, m) = 1 \), egyébként.

(b) \( \mathcal{P}_1 \cdot \ldots \cdot \mathcal{P}_s \mid b \), ahol \( \mathcal{P}_1, \ldots, \mathcal{P}_s \) az \( m \) összes különböző prímosztója.

2.2.13 \( \langle k, ma \rangle = 1 \).

2.2.14 (c) Használjuk fel a (b) részt.

13.2.3.

2.3.1 Állítsuk pára egy (ügyesen választott) redukált maradékrendszer elemeit, vagy használjuk \( \varphi(n) \) képletét.

2.3.2

(a) 3, 4, 6.

(b) 5, 8, 10, 12.

(c) Nincs ilyen \( n \).

(d) 61, 77, 93, 99, 122, 124, 154, 186, 198.

2.3.3

(a) 1785 = 5 \cdot 257. Útmutatás: \( \varphi(2^{11}) = 2^{10} \), ezért a keresett szám legfeljebb \( 2^{11} \). Ennél kisebb megfelelő tulajdonságú számot csak \( 2^k + 1 \) alakú prímek szorzata adhat.

(b) 3^{11}. Útmutatás: Használjuk fel, hogy (i) \( 2 \cdot 3^{10} + 1 \) nem prim (osztható 17-tel), továbbá (ii) ha egy \( \mathcal{P}(>2) \) prímre \( 3^j \mid p - 1 \), akkor \( \mathcal{P} \geq 2 \cdot 3^j + 1 \).

2.3.4 100, 80, 50, 40.

2.3.5

(a) Használjuk fel \( \mathcal{P} \) és \( \mathcal{N} \) kanonikus alakját és a \( \varphi \) -függvény képletét. Vigyázzunk arra, hogy mindkét szám kanonikus alakjában csak pozitív kitevők szerepeljenek.

(b) Következik az (a) részből.

(c) A legkevesebb számolással úgy érünk célhoz, ha a

\[ \varphi((a, b)) \varphi([a, b]) = (\varphi(a), \varphi(b)) \cdot \varphi(a), \varphi(b) \]

azonosságot igazoljuk.
2.3.6 A \( \frac{\varphi(a)}{\varphi(b)} = \frac{a}{b} \) egyenlőség átírható a következő alakba:

\[
\prod_{\substack{p \mid a \atop p \text{ prím}}} \left(1 - \frac{1}{p}\right) \cdot \prod_{\substack{q \mid b \atop q \text{ prím}}} \left(1 - \frac{1}{q}\right),
\]

(1)

Ha \( a \) és \( b \) prímosztói megegyeznek, akkor (1) nyilván teljesül. A megfordítás igazolásához indirekt tegyük fel, hogy (1) valamely más esetben is teljesülne. Hagyjuk el a közös \( 1 - 1/p = 1 - 1/q \) tényezőket, majd szorozzuk be mindkét oldalt a közös nevezővel (azaz a megmaradt \( p \) -k és \( q \) -k szorzatával). Ekkor a \( p \) -k és \( q \) -k közül a legnagyobbb csak az egyik oldalnak lesz osztója, ami ellentmondás.

2.3.7 Igaz: (a).

2.3.8 Legyen a \( k \) kanonikus alakja \( k = \prod_{i=1}^{r} p_i^{\beta_i} \), \( \beta_i > 0 \). Ekkor megfelel

\[
n = \prod_{i=1}^{r} p_i^{\alpha_i}, \quad \text{ahol } \alpha_i = \begin{cases} \beta_i, & \text{ha } p_i \mid \prod_{j=1}^{r} (p_i - 1); \\ \beta_i + 1, & \text{egyéb} \end{cases}
\]

2.3.9 Használjuk fel, hogy ha \( r > 1 \), akkor az \( \tau \mid n \) és \( \{r, n\} = 1 \) feltételek kizárják egymást. — Egyenlőség akkor és csak akkor teljesül, ha \( r = 1 \), 4 vagy prim. — Útmutatás: Minden más esetben található olyan \( 1 < r < n \), amelyre \( \{r, n\} > 1 \), de \( r \mid n \); például \( n = p \) megfelel, ahol \( P \) az \( n \) legkisebb prímosztója.

2.3.10

(a), (c) Használjuk \( \varphi\alpha\) képletét.

(b) Ekkor az (1) táblázat oszlopai nem alkotnak teljes maradékrendszert modulo \( b \).

2.3.11

(a) Az \( n \) legkisebb prímosztójának a többszörösei biztosan nem relatív prímek az \( n \) -hez. — Egyenlőség akkor és csak akkor teljesül, ha \( n \) egy prímszám négyzete.

(b) (b1) \( n \) prim.

(b2) 10.

(b3) 15, 49.

(b4) Nincs ilyen \( n \) .

2.3.12 1, 2 és 3. — Útmutatás: Mutassuk meg, hogy \( \varphi\alpha\mid n \leftrightarrow n = 2^\alpha 3^\beta \), ahol \( \alpha \geq 0 \) és \( \beta = 0 \), vagy \( \alpha > 0 \) és \( \beta > 0 \).

2.3.13 Bizonyításunk indirekt; használjuk a \( \varphi\ )-függvény képletét, ekkor az egyszerűsítések után megmaradó legnagyobb prímosztó csak az egyik oldalnak lesz osztója.

2.3.14 Egyszerűsítsük az \( \sqrt{n}, \sqrt{n}/2, \ldots, n/\sqrt{n} \) törteket, és számoljuk össze, hogy egy adott nevező hányszor fordul elő.

2.3.15 A \( \varphi\alpha\) képletének felhasználásával lássuk be, hogy \( \varphi\alpha \geq \sqrt{n}/2 \).

Egy másik lehetőség: az \( n \) prímosztóin kívül minden prímszám relatív prim az \( n \) -hez, és \( n \) -ig „sok” prímszám van (lád az 5.4 pontot).
2.3.16 Jelölje $2 = p_1 < p_2 < \cdots$ a (pozitív) prímszámok sorozatát, és legyen $p_j$ a legkisebb olyan prim, amely nem osztója a $k$-nak. Ekkor $n = (p_j - 1)k$ megfelel.

2.3.17 Legyen $2 = p_1 < p_2 < \cdots < p_{1000}$ az első 1000 prímszám, és jelölje $P$ ezek szorzatát. Ekkor az $u_t = P(p_t - 1)/p_t$ számok megfelelnek.

2.3.18 Válassz: $u \leq 3$. — Útmutatás: Hasonlítsuk össze a 2 kitevőjét $\varphi(n!)$ és $k!$ kanonikus alakjában.

2.3.19 $m = 2^k$ vagy $p$ vagy $2p$, ahol $p > 2$ prim.

13.2.4.

2.4.1 Használjuk fel, hogy $\varphi(n) \leq n$ miatt $\varphi(n) \mid n!$. — A feladatot megoldhatjuk az Euler–Fermat-tétel nélkül is. Az $1, 2, 2^2, \ldots, 2^n$ számok között a skatulyaelv alapján található két olyan, amelyek kongruensek modulo $n$: $2^i \equiv 2^j \pmod{n}$, ahol $0 \leq i < j \leq \varphi(n)$. Mivel $(2, n) = 1$, ezért $2^j$-vel egyszerűsíthetünk, és így $2^{j-i} \equiv 1 \pmod{n}$, ahol $1 \leq j-i \leq n$. Innen $j-i \mid n!$ alapján következik a feladat állítása.

2.4.2 Válasz: 49.

Útmutatás: $(1793, 10^2) = 1$ miatt $1793^{\varphi(100)} \equiv 1 \pmod{100}$. Számítsuk ki $\varphi(100)$-at és használjuk fel, hogy $1793 = -7 \pmod{100}$.

2.4.3 Alkalmazzuk (többször) a kis Fermat-tételt $p = 13$-ra.

2.4.4 Lássuk be, hogy a két szám közül az egyik osztható 7-tel.

2.4.5 Határozzuk meg az osztó kanonikus alakját, és minden primhatványtényezőre külön igazoljuk az oszthatóságot az Euler–Fermat-tétel felhasználásával. Ne felejtsük el azokat az eseteket is megvizsgálni, amikor ez a primhatvány az $u$-hoz nem relatív prim.

2.4.6 Lássuk be, hogy egy 30-adik hatvány csak 0 vagy 1 maradékot adhat 11-gyel, illetve 9-cel osztva.

2.4.7 Mutassuk meg, hogy egy 88-adik hatvány csak 0 vagy 1 maradékot adhat 23-mal osztva.

2.4.8 Ha $r_i$ és $r_j$ egyike sem kongruens 0-val mod $p$, akkor az $r_i^{2p-5} \equiv r_j^{2p-5} \pmod{p}$ kongruenciát $r_ir_j$-vel beszorozva, a kis Fermat-tétel felhasználásával $r_i \equiv r_j \pmod{p}$, azaz $i = j$ következik.

2.4.9
(a) A T 2.4.1B Tétel bizonyításának a mintájára válasszuk külön a $p$ és $p \mid \omega$ eseteket.

(b) Jelölje $k$ az $m$-re kanonikus alakjában előforduló kitevők maximálumát. Ekkor $i, j \geq k$, $i = j \pmod{\varphi(m)} \implies a^i \equiv a^j \pmod{m}$. — Útmutatás: Lássuk be, hogy az $m$-re kanonikus alakjában szereplő minden egyes $\varphi^\alpha$ primhatványtényezőre $a^\alpha \equiv a^\alpha \pmod{\varphi^{\alpha}}$. Ehhez használjuk fel, hogy $\varphi^\alpha \mid \varphi(m)$ (lásd a 2.3.5a feladatot [44]).

2.4.10 Igaz: (a), (c).

(a) Használjuk az Euler–Fermat-tételt ($n = 133$, $m = 1000$), vagy alkalmazzuk a 2.4.1 feladatnál [47] vázolt módszer megfelelő módosítását.
(b) Vizsgáljuk a 4-gyel való oszthatóságot.

(c) Induljunk ki a $136^k \equiv 136 \mod 10000$ \iff $136^{k-1} \equiv 1 \mod 125$ összefüggésből.

2.4.11 Útmutatás: $a^k = a \mod d$ \iff $a^{k-1} = 1 \mod d/(a,d)$.

2.4.12 A csoportok a $(10^k - 1)/9$ alakú számok, tehát azokat az $\mathfrak{n}$ -eket kell meghatározní, amelyekre $10^k \equiv 1 \mod 9m$ teljesül alkalmas (pozitív) $k$ -val.

2.4.13 Elég azt megmutatni, hogy $n^2 + 1$ -nek bármely $\mathfrak{p}$ páratlan, pozitív primosztója $4k + 1$ alakú. Ennek belátságához az $x^k \equiv -1 \mod p$ kongruenciát emeljük $(p - 1)/2$ -edik hatványra, és használjuk a kis Fermat-tételt.

A feladatot megoldhatjuk a kis Fermat-tétel nélkül is. Tegyük fel indirekt, hogy létezne egy $4k - 1$ alakú $a$ pozitív egész és egy olyan $n$, amelyre $a \mid n^2 + 1$. Vegyük a legkisebb ilyen $a$ -t. Az ellentmondást úgy fogjuk kihozni, hogy találunk egy $a$ -nél kisebb pozitív egész, amely szintén $4k - 1$ alakú és osztója egy $a^2 + 1$ alakú számnak.

Mivel az $a \mid n^2 + 1$ oszthatóság csak az $n$ -nak az $a$ -val vett osztási maradékától függ, ezért feltehető, hogy $0 \leq r \leq a - 1$ (sőt azt is előirhatnánk, hogy $n \leq c/2$ teljesüljön). Legyen $n^2 + 1 = a^2$. Ekkor $a^2 = n^2 + 1 \leq (a - 1)^2 + 1 < c^2$, tehát $(0 < q < c$.

Ha $a$ páros, akkor $n^2 = 1$ szám $4k + 1$ alakú, és így a $q$ szám $4k - 1$ alakú.

Ha $a$ páratlan, akkor $n^2 + 1$ szám $8k + 2 = 2(4k + 1)$ alakú, és így a $q/2$ szám $4k - 1$ alakú.

Azt kaptuk, hogy az $a$ -nél kisebb pozitív szám is osztója $n^2 + 1$ -nek, ami ellentmondás.

2.4.14 A kis Fermat-tétel alapján $\mathfrak{n}^{19} = n^4 \mod 19$, így a feltétel $a^4 = -1 \mod 19$ alakba írható. Ezt a kongruenciát emeljük 9-edik hatványra.

2.4.15 Az (a) és (b) állításból az $\mathfrak{n} = \mathfrak{p}$ speciális esetben éppen a kis Fermat-tétel második alakját kapjuk. A (c) állítás azt mutatja, hogy van olyan összetett $\mathfrak{n}$ is, amelynél $a^{\mathfrak{n}} \equiv a \mod m$ teljesül minden $a$ -ra. (Az ilyen összetett számokat univerzális alprimeknak vagy Carmichael-számonak hívjuk, és ezekkel részletesen a 5.7 pontban foglalkozunk.) — Útmutatások:

(a) Négyszormentes $\mathfrak{n}$ esetén az $\mathfrak{n}$ minden $\mathfrak{p}$ primosztójára lássuk be, hogy $a^{\mathfrak{n}(\mathfrak{p}) + 1} = a \mod \mathfrak{p}$. Ha az $\mathfrak{n}$ nem négyzetmentes, azaz osztható egy $\mathfrak{p}$ primszám négzetzével, akkor például $a = \mathfrak{p}$ -re nem teljesül a szóban forgó kongruencia.

(b) Használjunk fel a 2.4.9b feladat [47] eredményét.

(c) Vizsgáljuk az $a^{1729} = a \mod k$ kongruenciákat, ahol $k$ az 1729 egy tetszőleges prím(hatvány)osztója.

2.4.16 T 2.4.1B: Nyilván elegendő $a^p \equiv a \mod \mathfrak{p}$ teljesülését egy teljes maradékrrendszer elemeire, azaz például $a = 1, 2, \ldots, \mathfrak{p}$-re belátni. Tegyük fel, hogy a kongruencia valamely $a = k$ -ra teljesül, ekkor $(k + 1)^p$ -t a binomiális tétel szerint kifejtve kapjuk, hogy a kongruencia $a = k + 1$ -re is érvényes.
Megjegyzés

T 2.4.1 A 2.4.1 A

: Legyen \((a, p) = 1\). Ekkor az (imént igazolt) \(a^p = a \pmod{p}\) kongruenciát szabad -val egyszerűsíteni, azaz \(a^{p-1} \equiv 1 \pmod{p}\) is fennáll.

**13.2.5.**

2.5.2

(a) \(x \equiv 11, 28, 45 \pmod{51}\).

(b) \(x \equiv 9, 38, 67, 96 \pmod{116}\).

(c) \(x \equiv 1011 + 1111k \pmod{5555}, 0 \leq k \leq 4\).

(d) \(x \equiv (2^{k+5} + 4)/3 \pmod{2^{k+2} + 1}\), ha \(k\) páros, és nincs megoldás, ha \(k\) páratlan.

(e) \(x \equiv 0, 11 \pmod{19}\). — Útmutatás: A kis Fermat-tétel alapján az \(x(8x + 7) \equiv 0 \pmod{19}\) kongruenciához jutunk. Ezután ismét használjuk fel, hogy a 19 prim.

(f) \(x \equiv 73 \pmod{100}\). — Útmutatás: Mivel \(\left(\frac{27}{100}\right) = 1\), ezért csak olyan megoldás jöhet szóba, amely relatív prim a 100-hoz. Így használhatjuk az Euler–Fermat-tételt.

2.5.3 A \(12x \equiv 31 \pmod{49}\) kongruenciából 25 és 74 adódik.

2.5.4 Válasz: 67.

Útmutatás: Az Euler–Fermat-tételből \(3^{260} \equiv 1 \pmod{100}\), így a \(3x \equiv 1 \pmod{100}\) kongruenciát kell megoldani.

2.5.5 Elégséges: (a), (c), (f).

2.5.6 Igaz: (a), (b).

2.5.7 \(m\).

**13.2.6.**

2.6.1

(a) 93.

(b) Az \(x = 4 \pmod{12}\), \(x = 8 \pmod{15}\) kongruenciarendszer nem oldható meg.

2.6.2 (a) Akármiről lehet.

(b) 3 vagy 7.

2.6.3 Alkalmazzuk a P1 példánál bemutatott eljárást: Alakítsuk át mindegyik kongruenciát olyan szimultán kongruenciarendszerré, amelyben a modulusk a modulusok az eredeti modulus kanonikus alakjában szereplő primhatványok. Ne felejtsük el, hogy az egyes primhatvány modulusú kongruenciák vizsgálata során általában két esetet érdemes megkülönböztetni aszerint, hogy a keresett \(x\) megoldás relatív prim-e a modulushoz, vagy sem. — Eredmények:
EREDMÉNYEK ÉS ÚTMUTATÁSOK

(a) \( x \equiv 20 \pmod{176} \).

(b) \( x \equiv 60 \pmod{333} \) és \( x \equiv 208 \pmod{333} \).

(c) \( x \equiv 91 \pmod{105} \).

2.6.4 (a) 1.

(b) 2.

2.6.5 A kérdéses modulo 1000 kongruencia helyett vizsgáljuk a modulo 125 és modulo 8 adódó szimultán kongruenciarendszert. — Válasz: 016.

2.6.6 1166.

2.6.7 (a) 25, 76.

(b) 376, 625.

2.6.8

(a) Válasz: 36. — Útmutatás: Az \( x^2 \equiv x \pmod{10^{20}} \) kongruencia helyett vizsgáljuk a megfelelő prímhatvány modulusok szerinti szimultán kongruenciarendszert. Mutassuk meg, hogy egy prímhatvány modulusra nézve az \( x(x - 1) \equiv 0 \) kongruencia megoldásszáma 2.

(b) Válasz: 135. — Útmutatás: Határozzuk meg az \( x^2 \equiv x \pmod{10^{20}} \) kongruencia megoldásszámát az (a)-beli eljáráshez hasonló módon.

2.6.9 Mivel egy napban \( 24 \cdot 60 = 1440 \) perc van, tehát az \( x \equiv 39^{5857} \pmod{1440} \) kongruenciát kell vizsgálnunk. \( 1440 = 2^4 \cdot 3^2 \cdot 5 \) alapján elhelyezi a \( 2^5 \), \( 3^2 \) és 5 modulusokra nézzük a kongruenciát. — Válasz: 13 óra 21 perc.

2.6.10 A 2.2.14b-c feladat [41] megoldásához hasonlóan járhatunk el.

2.6.11 Legyenek \( p_1, \ldots, p_k \) különböző prímszámok, és tekintsük az \( x + i \equiv 0 \pmod{p_i^2} \), \( i = 1, 2, \ldots, k \) szimultán kongruenciarendszert.

2.6.12

(a) Egy-egy megoldás \( x = a + b + c \), illetve \( x = ab + bc + ac \).

(b) Szükségesség: Alkalmazzuk a T 2.6.1 Tételt a két kongruenciából álló részrendszerekre. — Elégésségesség: Legyen \( \alpha = d_1a_1 + d_2b_1 + d_3c_1 \), ahol \( a_1, b_1 \) és \( c_1 \) páronként relatív prímek, és \( x = d_1x_1 \). Osszuk el valamennyi kongruenciát \( d \)-vel (a modulusokat is beleértve). Az így kapott szimultán kongruenciarendszerben \( x_1 \) az ismeretlen és \( a_1, b_1 \) és \( c_1 \) a modulusok. Mivel a modulusok páronként relatív prímek, ezért ez a kongruenciarendszer megoldható, és így megoldható az eredeti rendszer is.

2.6.13 Szükségesség: Alkalmazzuk a T 2.6.1 Tételt a két kongruenciából álló részrendszerekre. — Elégésségesség: Bizonyítsuk \( k \) szerinti teljes indukcióval. A \( k - 1 \)-re vonatkozó indukciós feltevés szerint az első \( k - 1 \) kongruenciából álló részrendszer megoldható, legyen \( c \) egy megoldás. Ekkor elég az
\[ x \equiv c \pmod{m_1, \ldots, m_{k-1}}, \quad x \equiv c_k \pmod{m_k} \]
kongruenciarendszer megoldhatóságát igazolni. A T 2.6.1 Tétel kritériumának az ellenőrzéséhez 
használjuk fel az 1.6.19b feladat több tagra vonatkozó általánosítását, valamint $1 \leq i \leq k - 1$-re az 
$(e_k, m_i) = 1$ feltételek teljesülését.

2.6.14 Nincs. — Utmutatás: A kongruencia megoldásszáma megegyezik a prim(hatvány)tényezők 
szerinti szimultán kongruenciarendszerben szereplő kongruenciák megoldásszámainak a szorzatával.

2.6.15

(a) Szükségesség: A rendszer elemszáma $\varphi(k) = n$. A 0 (mod $u$) előállításához használt $c$ számra 
$u \mid c$, továbbá $(c, k) = 1$, ezért $(k, m_i) = 1$.

Elégségesség: Legyen $r_1, \ldots, r_n$ tetszőleges teljes maradékrendszer modulo $u$, $s_1, \ldots, s_n$ 
tetszőleges redukált maradékrendszer modulo $k$ (a feltétel szerint $\varphi(k) = n$). Ekkor $(k, m_i) = 1$ miatt az 
$x = x_i \pmod{n}$, $x = x_i \pmod{k}$, $i = 1, 2, \ldots, n$ szimultán kongruenciarendszerek megoldhatók, és ezek egy-egy megoldása a kívánt tulajdonságú számhalmazt szolgáltat.

(b) A szükségesség nyilvánvaló. Az elégségesség bizonyítása $(k, n) = 1$ esetén az (a) rész 
mintájára történhet, az általános esetben azonban úgy kell a két redukált maradékrendszer elemeit összepárosítani, hogy az így létrejövő szimultán kongruenciarendszerek megoldhatók legyenek. 
Annak igazolásához, hogy az ilyen párosítás tényeg megvalósítható, a következő állítást kell belátni: 
ha $d \mid n$, akkor egy modulo $n$ redukált maradékrendszer elemeiből minden modulo $d$ redukált 
maradékosztályba ugyanannyi elem esik.

2.6.16

(a) Először mutassuk meg, hogy bármely $n$ -re és $i \neq j$ -re $(a_i + n, a_j + n)$ csak az 
$S = (a_1 - a_2)(a_1 - a_3)(a_2 - a_3)$ osztói közül kerülhet ki. Legyen ezután $P$ az $S$ tetszőleges 
prímosztója, és válasszuk meg $n$ -et modulo $P$ úgy, hogy az $a_i \not\equiv n$ számok közül legfeljebb egy le legyen osztható $P$ -vel ($P > 3$ -ra akár az is elérhető, hogy $a_1 \not\equiv n$, $a_2 \not\equiv n$ és $e_4 \equiv n$ egyike se legyen osztható $P$ -vel). Az $S$ különböző prímosztóira így adódó kongruenciák egy 
szimultán kongruenciarendszert alkotnak, amely a modulusok páronként relatív prim volta miatt 
biztosan megoldható.

(b) Például 1, 2, 3, 4 megfelel.

(c) Finomítsuk az (a)-beli eljárást úgy, hogy az $S = \prod_{1 \leq i < j \leq 4}(a_i - a_j)$ szorzat páratlan prímosztóit 
ez a 4-et tekintjük modulusoknak.

(d) Most olyan $n$ -et kell választani, hogy az $S$ bármely $P$ prímosztójával az $a_i + n$ számok közül 
legfeljebb kettő legyen osztható.

(e) Öt szám esetén mindkét állítás igaz, hat számra viszont már mindkettő hamis.

13.2.7.

2.7.1

(a) Válasz: 2, ha $m = 4$, és 0, ha $m > 4$. — Utmutatás: Ha az $m$ felirható két különböző, 1-nél 
nagyobb egész szám szorzataként, akkor ezek mindkettő szerepelnek tényezőként $(m - 1)!$-ban,
tehát \( m \mid (m-1)! \). Hátravan még az \( m = p^2 \) eset, ahol \( P \) prim. Ha \( P > 2 \), akkor \( P \) és \( 2P \) is szerepel tényezőként \( (m-1)! \)-ban.

(b) Válasz: 2, ha \( m = 4 \), \( p - 1 \), ha \( m = 2p \), ahol \( P > 2 \), prim és 0 egyébként. — Útmutatás: Először lássuk be, hogy ha \( m = P^2 \), ahol \( P \mid \frac{1}{2} \) és \( \frac{1}{2} > 2 \), akkor \( P^2 \mid m \). Ebből következik, hogy az \( m = 2^\alpha \), \( 2^\alpha \) és \( 2^\alpha \) (ahol \( P > 2 \) prim) esetek kivételével a keresett maradék 0. Ha \( m = P^2 \) vagy \( 2P^2 \), ahol \( \alpha > 2 \), akkor a \( \left( \frac{p}{m} \right) \) szorozatban \( P^2 - 1 \) és \( 2P^2 - 1 \) is szerepel, ezért \( m \mid \left( \frac{p}{m} \right) \).

Hasonlóan, ha \( m = 2^\alpha \), ahol \( \alpha \geq 3 \), akkor \( 2^\alpha - 1 \) és \( 2 \) is szerepel tényezőként \( \left( \frac{p}{m} \right) \)-ben. Végül az \( m = 2P \) esetben a \( \left( \frac{p}{m} \right) = (P - 1)! \) szorzat maradéktáját vizsgáljuk külön modulo \( P \) és modulo 2.

(c) Válasz: -1, ha \( m = 4 \), \( P^2 \) vagy \( 2P^2 \), ahol \( P > 2 \) prim, és 1 egyébként. — Útmutatás: A Wilson-tételre adott párból állításos bonyolítás módosításánál a fő nehézséget az jelenti, hogy (a legtöbb) összefügg \( m \) eseteken \( c^2 \equiv 1 \pmod{m} \) nem csak \( c \equiv \pm 1 \pmod{m} \) esetén teljesül. A \( F \) állításnál a redukált maradéktérendszert azon \( c \) elemei okoznak problémát, amelyeknek „ónnagja a párja”, azaz \( c^2 \equiv 1 \pmod{m} \). Jelöljük ezek halmazát \( H \)-val. Ekkor a keresett \( P \) maradék megegyezik a \( H \) -beli elemek szorzatának a maradékával. Ha \( m = 4 \), \( P^2 \) vagy \( 2P^2 \), akkor \( H \) -ban csak \( c \equiv \pm 1 \pmod{m} \) szerepel, és így \( \gamma \equiv -1 \pmod{m} \). A többi esetben a kínai maradéktéttel segítségével lássuk be, hogy \( H \) -nak több, mint két eleme van. Legyen \( d \equiv 1 \pmod{m} \) a \( H \) tetszőleges eleme, és állítsuk pára (csak) \( H \) elemeit a \( c \rightarrow \gamma \pmod{m} \) megfeleltetéssel. Innen \( \gamma \equiv d \) vagy 1 (mod \( m \)) adódik. A \( H \) -beli pára állítást most egy másik \( \gamma \equiv 1 \pmod{m} \) elem szerint elvégezve kapjuk, hogy csak \( \gamma \equiv 1 \pmod{m} \) lehetséges.

2.7.2 Válasz: 7 és 17. — Útmutatás: Ha \( m \) prim, akkor használjuk fel a Wilson-tételt. Ha \( m \) \vline \( m \) esetben \( m = 6 \geq m/2 \), akkor \( (m - 6)! \) nem lehet relatív prim az \( m \)-hez.

2.7.3 Azt kell igazolni, hogy az \( a_1 b_1, \ldots, a_n b_n \) szorzatok nem alkotnak teljes maradéktérendszert modulo \( m \).

(a) Legyen \( m \) prim, \( m = p \). Ha a \( P = a_i = b_i \) előállításnál \( i \neq j \), akkor \( a_i b_i = a_j b_j = 0 \pmod{p} \). Ha \( P = a_i = b_i \), akkor a többi \( a_j \) elem, illetve a többi \( b_j \) elem redukált maradéktérendszert alkot modulo \( P \), és megmutatjuk, hogy az \( a_j b_j \) szorzatok viszont nem alkotnak azt. A Wilson-tétel alapján

\[
\prod_{j \neq i} a_j b_j = \prod_{j \neq i} a_j \prod_{j \neq i} b_j = (-1)(-1) = 1 \neq -1 \pmod{p},
\]

teját az \( a_j b_j \) (\( j \neq i \)) szorzatok nem alkotnak redukált maradéktérendszert modulo \( P \).

(b) Először mutassuk meg, hogy ha \( k \mid m \), akkor a \( k \)-val osztható \( a \)-kat és \( b \)-ket eleve „egymással kell összeszoroznai”. Ha \( m \) nem négyszorosos, azaz van olyan \( p \) prim, amelyre \( p^2 \mid m \), akkor az előző észrevetel alapján bármely \( a_i b_i \) szorzat vagy relatív prim a \( P \) -hez, vagy pedig osztható \( p^2 \)-tel, tehát például a \( \{p\} \) maradékosztály nem lesz reprezentává. Ha \( m \) négyszorosos, és \( P \) az \( m \) egy páratlan primszöjtje, akkor lássuk be, hogy az \( m/P \)-vel osztható \( a \) és \( b \) elemek egy-egy teljes maradéktérendszert alkotnak modulo \( P \), és vezessük vissza a feladatot az (a) részre.

2.7.4 A \( \left( \frac{p - 1}{2} \right) \equiv -1 \pmod{p} \) kongruenciáiban a \( p - c > (p - 1)/2 \) tényezők helyére írjunk \(-c\)-t, majd a „négyzetgyökvonásnál” használjuk ki \( P \) prim tulajdonságát.
2.7.5 A \((p^2 - 1)!\) -ból \(p^r - 1\) -et kiemelve \(p + 1\) darab modulo \(p\) reduált maradéknegyedszorzat marad (a \(p + 1\) -edik a \(p\) -vel osztható számok együtthatóiiból keletkezik).

2.7.6 \((p^2 - 3)/2\).

2.7.7 Válasz: 10000. — Útmutatás: Vizsgáljuk külön a maradéket modulo 101 és modulo 100, majd oldjuk meg a kapott szimultán kongruenciarendszert.

2.7.8 Válasz: 3, 4, 5, 9. — Útmutatás: Először „ejtsük ki a faktoriális”; az első szám alkalmaz többszörösségét a másodikból levozva kapjuk, hogy a keresett \(d\) legnagyobb közös osztó osztója \(3^{\xi(n+3)}\) -nak. Ennek alapján mutassuk meg, hogy ha \(n \geq 4\), akkor \(d = 3\). Használjuk fel, hogy \((n + 2)!\) maradéka 0 vagy \(-1\) modulo \(n + 3\).

2.7.9 Mindkét kérdésre \(m \leq 3\) a válasz. — Útmutatás: Nyilván elég meghatározni, hogy \(m > 3\) -ra nem létezik ilyen alakú reduált maradéknegyedszorzat. Ha \(n = p > 3\) prim, akkor csak \(1, 2, \ldots, (p - 1)!\) jóhete szóba, de a Wilson-tétel alapján \((p^2 - 2)! \equiv 1\) \(\mod (p - 1)!\). Ha \(m\) összetett és \(p\) a legkisebb primosztója, akkor egyéb \(p \leq k\) esetén \((k, m)! \neq 1\), másrészt egyszerűen igazolható, hogy \(p \leq \varphi(m)\), tehát a faktoriálisok között csak \(\varphi(m)\) -nél kevesebb olyan van, amely relatív prim az \(m\) -hez.

2.7.10 A 31-gyel való oszthatóságot nem befolyásolja, ha az összeget a 31-hez relatív prim \(\{a_1, a_2, \ldots, a_3\}\) számmal beszorozzuk. Ezután használjuk fel a Wilson- és a kis Fermat-tételt.

2.7.11 Válasz: \(0, \pm 1\). — Útmutatás: Lássuk be, hogy ha a számú sorozat egyik eleme sem osztható \(p^r\)-vel, akkor az elemek vagy reduált maradéknegyedszorzat alkotnak modulo \(p\), vagy pedig mind azonos maradéket adnak \(p^r\) -vel osztva. Ennek megfelelően használjuk fel a Wilson-, illetve a kis Fermat-tételt.

2.7.12 Válasz: \(x = 1, y = 2\). — Útmutatás: Az \(x!\) -ban minden \(1 \leq i \leq x - 1\) tényleg helyére írjuk a vele kongruens \(- (x - i)\) számot, ekkor

\[x! (x - x)! \equiv (-1)^{x-1} x (x - 1)! \mod (x + 1)\]

adódik. Ezután használjuk fel a Wilson-tételt, illetve a 2.7.1a feladatot [64].

2.7.13 Válasz: \(p \leq 5\). — Útmutatás: Tegyük fel indirekt, hogy egy \(p > 3\) primre \((p^2 - 1)! + 1 - p^k\) teljesül. Ezt átalakítva a

\[\frac{(p^2 - 2)!}{p - 1} = \frac{p^k - 1}{p - 1} - p^{k - 1} + p^{k - 2} - \cdots + 1\] (1)

eyenőséget nyerjük. Vizsgáljuk (1)-et modulo \((p - 1)!\) : a 2.7.1a feladat [64], illetve \(p - 1 \mod p - 1\!\!\left(p - 1\right)\) alapján \(0 = \frac{k}{p!}\) \(\mod p - 1\) adódik. Innen azt kapjuk, hogy \(k \geq p - 1\), azonban ekkor \(p^k \geq p^{p-1} > (p - 1)! + 1\), ami ellentmondás.

13.2.8.

2.8.1 Páros \(m\) -ek esetén.

2.8.2

(a) \(13x = 1 (\mod 100)\) kongruenciát kell megoldani. — Válasz: (77).
(b) \[100 - \varphi(100) - 1 = 59.\]

c) 19.

d) Van.

2.8.3 Válaszok:

(a) 2.

(b) 4.

(c) 8.

(d) Legyen \(m = p^t \cdot q \), ahol \(t\) páratlan, és jelölje \(t\) különböző prímosztóinak a számát \(k\). Ekkor a keresett érték \(2^k\), ha \(\alpha \leq 1\); \(2^{k+1}\), ha \(\alpha = 2\); és \(2^{4+k^2}\), ha \(\alpha \geq 3\).

Útmutatás: Az \(\frac{x^2}{m} \equiv 1 \pmod{m}\) kongruencia megoldásszámát kell meghatározni. Vizsgáljuk először azt a speciális esetet, amikor \(m\) egy páratlan prim hatványa, illetve kettőhatvány, majd általános esetén térjünk át az \(m\) kanonikus alakjában szereplő primhatvány tényezők szerinti szimultán kongruenciarendszerre.

2.8.4

(a)–(b) Használjuk a nullosztó definícióját vagy a T 2.8.5 Tételt.

c) Ezek az \(m\) -ek a primhatványok.

(d) Az összeg \((0)\), ha \(m\) páratlan, és \((m/2)\), ha \(m\) páros. A szorzat \((2)\), ha \(m = 4\), és \((0)\), ha \(m > 4\).

e) Pontosan a nem négyzetmentes számok ilyenek, azaz amelyek legalább egy prímszám négyzetével oszthatók.

2.8.5

(a) Először be kell látni, hogy a műveletek „jól vannak definiálva”, azaz két ilyen maradékosztály összege és szorzata megint ilyen típusú maradékosztály. A műveleti azonosságok az összes modulo 20 maradékosztály körében érvényesek, tehát a \(\mathbb{Z}/20\) részhalmazon is „automatikusan” teljesülnek. Nullelem a \((0)\) a, a \((45)\) ellentettje a \((-45)\) a. Egységelem a \((1)\), a \((15)\) és a \((4)\) inverze önmaga, a \((8)\) és \((12)\) pedig egymás inverze.

(b) Bármely \((a) \in K\) -ra \((a) = (1)\), tehát valóban minden elem nullosztó. Ebből következik, hogy nem létezhet egységelem, és \(K\) nem lehet test. (Az, hogy \(K\) kommutatív gyűrű, az (a) részhöz hasonlóan igazolható.)

c) Legyen \(1 < k < m\) és \(k \mid m\).

(i) Ekkor a modulo \(m\) maradékosztályok közül a „\(k\) -val oszthatók” a maradékosztályok közötti összeadásra és szorzásra egy \(R\) kommutatív gyűrűt alkotnak.

(ii) Ha \((k, \frac{m}{k}) = 1\), akkor ez az \(R\) gyűrű egységleme.

(iii) Ha \((k, \frac{m}{k}) = 1\) és \(m/k\) prim, akkor \(R\) test.

(iv) Ha \((k, \frac{m}{k}) \neq 1\), akkor \(R\) minden nemnulla eleme nullosztó, és így már egységleme sem létezik.
2.8.6 Csak a köbre emeléssel nincs semmi probléma. Részletesen az alábbiakat mondhatjuk:

(a) Lnk: a jobb oldalon álló maradékosztály általában függ attól, hogy az \((a)\) és \((b)\) maradékosztályból melyik reprezentást választottuk.

(b) Köbre emelés: értelmes a definíció.

(c) Köbgyökön: a jobb oldalon álló maradékosztály általában függ attól, hogy az \((a)\) maradékosztályból melyik reprezentánsat választottunk, sőt további problémát jelent, hogy egy adott maradékosztálynál már az is függhet a reprezentáns választásától, hogy \(\sqrt[3]{\text{egyáltalán egész szám-e.}}

(d) Számjegy közép: hasonló a helyzet, mint (c)-nél. — Ha finomabb vizsgálatot akarunk végezni, akkor érdemes a páros és páratlan \(n\) esetet megkülönböztetni. Ha \(n\) páratlan és a két maradékosztályból olyan reprezentánsokat veszünk, amelyekre \((a + b)/2\) egész szám (ilyen reprezentánsok mindig vannak), akkor ez egyértelműen meghatározza a \((a + b)/2\) maradékosztályt, tehát ily módon (kissé erőltetetten) értelmezhetjük bármely két maradékosztály számtani középét. Ha \(n\) páros, akkor a két maradékosztály bármely két reprezentánsára egyformán igaz, hogy \((a + b)/2\) egész szám-e vagy sem, azonban \((a + b)/2\) az első esetben sem lesz egyértelmű. Ez azt jelenti, hogy páros \(n\) esetén semhogyan sem tudjuk két maradékosztály számtani középét a fenti módon értelmeznii.

(e) Hatványozás: a jobb oldalon álló maradékosztály általában függ attól, hogy a \((b)\) maradékosztályból melyik reprezentánsat választottuk.

2.8.7 Kövessük — értelemszerű módosításokkal — a 2.4.1 Tételre adott bizonyítás gondolatmenetét. Legyen \(G\) összes eleme \(\gamma_1, \gamma_2, \ldots, \gamma_k\). Először mutassuk meg, hogy ekkor \(a\gamma_1, \ldots, a\gamma_k\) is kiadj a csoport összes elemét. Ebből következik, hogy \((e + \gamma_1) \cdot (e + \gamma_2) \cdots (e + \gamma_k) = \gamma_1\gamma_2 \cdots \gamma_k\). Ezt az egyenlőséget \(\gamma_1\gamma_2 \cdots \gamma_k\) inverzével beszorozva a feladat állítását kapjuk.

2.8.8 A Wilson-tétel bizonyításának a mintájára párosítsunk minden elemet az inverzével. Ebből azonnal következik az állítás, ha \((e\cdot\text{-vel együtt})\) legfeljebb két olyan elem van, amelynek a négyszete az egységelem. Ha kettőnél több ilyen elem van, akkor ezen körében csináljunk egy másféle párosítást.

13.3 Magasabb fokú kongruenciák

13.3.1.

3.1.1 (a) 2.

(b) 4.

(c) 0.

(d) 60.

3.1.2 Alkalmazzuk a \(\mathbb{Z}_n\) gyűrűre azt a tételt, hogy egy (kommutatív) gyűrű feletti polinom akkor és csak akkor osztható \(x^2\) -val, ha a megfelelő polinomfüggvények az \(x\) gyöke.

3.1.3 Csak (c) igaz.

3.1.4 (a) Pl. \(f = x(x-1) \cdots (x-11)\).

(b) \(37 \cdot 36 \cdot (36)\).
3.1.5 Ha \( i \) megoldás, akkor \( f(i)^{p-1} \equiv 0 \pmod{p} \), ha pedig nem megoldás, akkor a kis Fermat-tétel miatt \( f(i)^{p-1} \equiv 1 \pmod{p} \).

3.1.6 Használjuk fel a Wilson-tételle ebben a pontban adott bizonyítást: a keresett szorzat \( (-1)^{i+1}a_{p-1-j} \), ahol \( a_{p-1-j} \) a bizonyításban szereplő \( f \) polinom megfelelő együtthatója.

3.1.7 Írjunk \( x^{p-1} \) helyére mindaddig 1-et, amíg ez csak lehetséges.

3.1.8 Kezeljük a kérést a \( \mathbb{Z}_p \) test feletti polinomok körében. Itt az \( f \) polinomhoz tartozó polinomfüggvények \( p \) helyettesítési értéke van. A Lagrange- vagy Newton-féle interpoláció egy olyan \( g \) polinom létezését garantálja, amelynek a foka legfeljebb \( p-1 \) vagy \( g \) a nullpolinom, és a \( g \) -hez tartozó polinomfüggvény az adott helyeken az előre megadott értékeket veszi fel, vagyis jelen esetben minden helyettesítési értéke ugyanaz, mint az \( f \) -hez tartozó megfelelő helyettesítési érték.

— Az interpolációs polinom előállítására többféle eljárás ismert, azonban minden esetben van hozzá az \( f \) összes helyettesítési értékére, tehát eleve ismernünk kell magukat a gyököt és így a megoldásszámot is. Ennek megfelelően az interpolációs polinom nem használható a megoldásszám megkereséséhez.

3.1.9 Tegyük fel, hogy a \( g_1 \) és \( g_2 \) polinom is megfelel, és tekintsük a \( h \) = \( g_1 \) - \( g_2 \) polinomot. A feltételek alapján a \( h \) modulo \( P \) vett foka legfeljebb \( p-1 \) lehet, ugyanakkor a \( h(x) = 0 \pmod{p} \) kongruenciának minden \( x \) megoldása, azaz a megoldásszám \( P \). Az ellentmondás csak úgy oldható fel, hogy \( h \) -nak modulo \( P \) nincs foka, azaz \( h \) minden együtthatója osztható \( P \)-vel.

3.1.10 A T 3.1.3 Tételre adott első bizonyítást módosítsuk a 2.4.15b feladat [48] felhasználásával.

13.3.2.

3.2.1 (a) 1.

(b) 2.

(c) 12.

(d) 46. (Azt, hogy nem 23 a rend, minden számolás nélkül is megmutathatjuk \( 43 \equiv -2^2 \pmod{47} \) és a kis Fermat-tétel felhasználásával.)

3.2.2 Csak a (c) esetben van ilyen \( c \) szám.

3.2.3 9, 21 és 63.

3.2.4 Használjuk az \( (a^i)^{t} = a^{it} \) összefüggést és a T 3.2.2 Tétel (i) állítását. Ennek alapján a legnehezebb (c) rész (amelynek (a) és (b) speciális esete) a következőképpen igazolható:

\[
1 \equiv (a^i)^{t} = a^{it} \pmod{m} \iff k \mid i, i \equiv k \pmod{t}(\text{irányítás szerűen} k \mid (i, k)) \iff k \mid (i, k) \iff k \mid (i, k). \]

3.2.5

(a) 10 és 30 (mutassunk példát is arra, hogy mindkettő valóban előfordul).

(b) 36.

3.2.7 16.

3.2.8
EREDMÉNYEK ÉS ÚTMUTATÁSOK

(a) $\varphi \mid a^3 - 1 = (a - 1)(a^2 + a + 1)$, de $\varphi \mid a - 1$.

(b) Válasz: 6. — Útmutatás: Az (a) rész alapján $(1 + a)^2 \equiv a \pmod{p}$.

3.2.9 16.

3.2.10

(a) (A kongruenciák az $m$ modulusra vonatkoznak):

$$a^n \equiv 1 \iff \alpha_m(a) \mid n$$

$$a^k \equiv 1 \iff \alpha_m(a) \mid k$$

$b) Az (a) rész alapján $a^n - 1$ és $a^k - 1$ közös osztói ugyanazok, mint $\alpha_{\langle a, k \rangle} = 1$ osztói.

3.2.11 Indirekt tegyük fel, hogy $mn > 2$-re $a^n - 1$ és $a^k - 1$ teljesül. Ekkor $\alpha_m(a) \mid n$ és $\alpha_n(a) \mid k$ páratlan, továbbá $a^{2k} \equiv 1 \pmod{m}$ alapján $\alpha_m(a) \mid 2k$. Innen $\alpha_n(a) \mid k$, azaz $a^k \equiv 1 \pmod{m}$ következik, ami ellentmondás.

3.2.12 Ha $a^n \equiv -1 \pmod{p}$, akkor az előző feladat útmutatásához hasonló módon kapjuk, hogy $\alpha_p(a) = 2$. Ez az állítás $P$ helyett tetszőleges $m > 2$ modulusra is igaz. A megfordításnál legyén $a^n \equiv 1 \pmod{m}$, ekkor $a^k \equiv -1 \pmod{p}$. Ez a rész összetett modulusra általában nem igaz, legyen például $m = 15$ és $a = 4$.

3.2.13 (b) Használjuk fel, hogy $a^k \equiv 1 \pmod{[m, n]}$ akkor és csak akkor igaz, ha az $a^k \equiv 1 \pmod{m}$ és $a^k \equiv 1 \pmod{n}$ kongruenciák egyszerre teljesülnek.

3.2.14 Válasz: 7. — Útmutatás: Az $x^2 \equiv 1 \pmod{1000}$ kongruencia $x \neq 1 \pmod{125}$ megoldásainak a számát keressük. A mod 1000 kongruencia helyett vizsgáljuk az $x^2 \equiv 1 \pmod{125}$ és $x^2 \equiv 1 \pmod{8}$ szimultan kongruenciarendszert.

3.2.15

(a) Mivel $(ab)^{u,v} = a^{u,v} b^{u,v} \equiv 1 \cdot 1 \equiv 1 \pmod{m}$, ezért $\alpha(m) \mid [u,v]$. Ebből következik, hogy ha $\alpha(\tau) - uv$, akkor $(u,v) = 1$. A megfordításhoz tegyük fel, hogy $(ab)^{u,v} \equiv 1 \pmod{m}$; azt kell belátni, hogy ekkor $\tau \mid m$. A kongruenciát $\alpha -$adik hatványra emelve kapjuk, hogy $1 \equiv a^{u,v} b^{u,v} \equiv b^{u,v} \pmod{m}$. Innen $\alpha(b) = v \mid b^2$, és $(u,v) = 1$ miatt így $v \mid m$. Hasonlóan adódik, hogy $\alpha(u) \mid [u,v]$ tehet $\alpha(u) = [u,v] \mid \tau$.

(b) Az (a) részbén már megmutattuk, hogy $\alpha(\tau) \mid [u,v]$. A másik oszthatóságot az (a) rész második felében látott gondolatmenet mintájára igazolhatjuk.

3.2.16 Legyen $d = (\alpha(a), \alpha(b))$, és emeljük a kongruenciát $\alpha(d)/d$ -edik, illetve $\alpha(b)/d$ -edik hatványra.

3.2.17 Vegyük észre, hogy modulo $a^n - 1$ az $a$ rendje épen $n$.

3.2.18 Mutassuk meg, hogy ha $ab \equiv 1 \pmod{m}$, akkor $\alpha_m(a) \equiv \alpha_m(b)$, és így $\alpha_m(a) + \alpha_m(b)$ páros szám. Külön kell kezelni, ha itt $a \equiv b \pmod{m}$, vagyis $a^2 \equiv 1 \pmod{m}$; ez azt jelenti, hogy $\alpha_m(a) = 2$ (ami páros szám) vagy $a \equiv 1 \pmod{m}$ (amelynek a rendje 1).


3.2.19

(a) A maradék 1, ha \(a = 1 \pmod{p} \), és 0 egyébként.

(b) A maradék 1, ha \(o(a) = p-1 \), és \(-1 = o(a) \pmod{p} \).

3.2.20

(a) Legyen az \(a/b \) racionális szám tizedestört-alakja \(a/b = 0, c_1 c_2 c_3 \ldots \), ekkor a \(c_i \) tizedesjegyeket a következő maradékos osztásokból kapjuk:

\[
\begin{align*}
10r_1 &= c_1 b + r_1, & \text{ahol} \quad 0 &\leq r_1 < b, \\
10r_2 &= c_2 b + r_2, & \text{ahol} \quad 0 &\leq r_2 < b, \\
10r_3 &= c_3 b + r_3, & \text{ahol} \quad 0 &\leq r_3 < b, \\
& & & \quad \vdots \\
\end{align*}
\]

Ha itt valamelyik \(r_i = 0 \), akkor az eljárás véget ér, és véges tizedes törtet kapunk. A többi esetben, mivel mindegyik \(r_i \) csak az \(1, 2, \ldots, b-1 \) értékeket veszi fel, ezért lesz olyan \(\hat{h} < \hat{j} \), amelyre \(r_h = r_j \). Ekkor (1) alapján \(c_{h+1} = c_{j+1}, r_{h+1} = r_{j+1} \), és így \(c_{h+2} = c_{j+2}, r_{h+2} = r_{j+2} \) stb., vagyis ekkor végtelen szakaszos tizedes törtet kapunk.

A megfordításhoz tegyük fel, hogy a \(0 < c_1 < 1 \) valós szám tizedestört-alakja véges:

\[
\alpha = 0, u_1 u_2 \ldots u_k, \quad u_k \neq 0
\]

illetve végében szakaszos:

\[
\alpha = 0, v_1 v_2 \ldots v_k \nu_1 \ldots \nu_n \ldots ,
\]

ahol \(v_1 v_2 \ldots v_k \) a nem ismétlődő rész (a tiszta szakaszos esetben ez hiányzik, azaz \(\hat{k} = 0 \), \(v_1 \ldots v_k \) pedig a (legkisebb ismétlődő) szakasz.

A (2a) esetben \(\alpha = \frac{v_1 \ldots v_k}{10^k} \), a (2b) esetben pedig \(\alpha(10^{n+1} \hat{h} - 1)^{10^k} \) lesz egész szám.

(b) Ezt lényegében már az (a) részben beláttuk.

(c) Egy tiszta szakaszos tizedes tört az (a)-ban látott eljárással egy \(10^a - 1\) nevezőjű (közönséges) törté alakítható, a \(b \) az ennek (esetleges) egyszerűsítésével kapott tört nevezője, tehát \((b, 10) = 1 \).

A megfordításhoz tekintsük az (1)-beli eljárást, legyen \(\gamma_0 = a \), ekkor

\[
\begin{align*}
\gamma_0 &= a \pmod{b}, \\
\gamma_1 &= 10a \pmod{b}, \\
\gamma_2 &= 10r_1 = 10^2a \pmod{b}, \\
\end{align*}
\]

és ugyanily általában \(\gamma_i \equiv 10^i a \pmod{b} \).

Az \(\gamma_i \equiv \gamma_j \pmod{b} \) egyenlőség a \(10^i a \equiv 10^j a \pmod{b} \) kongruenciát jelenti, ami \((10a, b) = 1 \) miatt ekvivalens \(10^{i-h} a \equiv 1 \pmod{b} \) teljesülésével. Ez azt jelenti, hogy lesz olyan \(i > 0 \), amelyre \(\gamma_i = \gamma_h = a \), vagyis a szakasz rögtön a tizedesvessző után kezdődik, a szakasz hossza pedig annyi, ahány modulo \(b \) páronként inkongruens hatványa van a 10-nek, azaz \(v_0(10) \).

(d) Az ekvivalencia az előző két részből a „maradékkel” szerint következik, hiszen a kimaradt racionális számok adják a kimaradt vegyes szakaszos esetet. Itt a nem ismétlődő rész, illetve a szakasz hosszára vonatkozó állítást a (c) részénél látottak mintájára igazolhatjuk.
3.3.3.

3.3.1 Azoknak a redukált maradékosztályoknak az elemei, amelyek egy-egy reprezentása:
(a) 3, 5;
(b) 3, 7;
(c) 5, 11.

3.3.2 Megfelel például az

3.3.3

(a) Kövessük a T 3.3.5 Tétel bizonyításában az (L1) és (L2) rész gondolatmenetét. Először keressünk egy primitív gyököt modulo 5, ilyen például a 2. Ezután nézzük meg, hogy a 2 primitív gyök-e modulo 25; ehhez elég \( 2^{5-1} \neq 1 \pmod{25} \) teljesülését ellenőrizni, ami valóban fennáll. Mivel a 2 primitív gyök modulo 5², ezért primitív gyök minden 5-hatványra is.

(b) Keressük a számot \( a = 2 + 5t \) alakban. Az \( a \) akkor nem lesz primitív gyök mod 25, ha

3.3.4 Igaz: (b), (d), (e), (f).

3.3.5

(a) Ha \( g \) primitív gyök, akkor \( g^{(p-1)/2} \equiv -1 \pmod{p} \), és így

\[
(\bar{g}_1 \bar{g}_2)^{(p-1)/2} \equiv (-1)(-1) = 1 \pmod{p}.
\]

(b) Mutassuk meg, hogy ha \( g \) primitív gyök és \( gh \equiv 1 \pmod{p} \), akkor \( h \) is primitív gyök. Ennek alapján megfelel egy ilyen \( g \) és \( h \) pár, valamint egy \( t \) tetszőleges primitív gyök, hiszen \( ght \equiv t \pmod{p} \).

3.3.6 Legyen \( p > 2 \) prim, \( g \) primitív gyök mod \( p \). Ekkor az \( 1, g, \ldots, g^{p-2} \) elemek redukált maradékként alkotnak mod \( p \), és így

\[
(p-1)! \equiv 1 \cdot g \cdot \cdots \cdot g^{p-2} \equiv (g^{(p-1)/2})^{p-2} = (-1)^{p-2} = -1 \pmod{p}.
\]

3.3.7 Az összeg maradéka 0, ha \( p \) primitív gyök mod \( p \), akkor az összeg maradéka nyilván \( p - 1 \), egyébként pedig használjuk fel a (véges) mértani sorozat összegképletét.

3.3.8 Válasz: 1, ha \( p > 3 \), és 2, ha \( p = 3 \).
3.3.9

(a) Használjuk fel a 3.2.4c feladatot [75].

(b) Tekintsük az (a) részben szereplő \( j = \frac{t(p - 1)}{d} \) értékeket a \( 0 \leq j < p - 1 \) feltétel mellett: ekkor \( 0 \leq i < d \) és \( (i, d) = 1 \) miatt ezek száma \( \varphi(d) \).

3.3.10 Az egyik irány könnyen következik a 3.2.4a feladatból. A megfordításhoz induljunk ki abból, hogy \( a \) és \( b \) egy \( \theta \) primitív gyök alkalmazott hatvanyaival kongruensek modulo \( \mathcal{P} \), és használjuk fel a 3.2.4c feladatot [75]. — Másik lehetőség: \( (c, \mathcal{P}) = 1 \) esetén az összes \( \varphi(c) \)-edrendű elem száma megegyezik a \( c \) hatványai között előforduló \( \varphi(c) \)-edrendű elemek számával.

3.3.11 Minden állítás érvényben marad, ha \( \mathcal{P} - 1 \) helyére \( \varphi(m) \)-et írunk.

3.3.12

(a) Vegyük észre, hogy elég a következő összefüggést igazolni:
\[
5^{2^{\alpha-3}} = 1 + t2^{\alpha-1},
\]
ahol \( t \) páratlan (és \( \alpha \geq 3 \)), és ezt bizonyítsuk be \( \alpha \) szerinti teljes indukcióval.

(b) A kongruencia már mod 4 sem teljesül.

(c) A megadott számok relatív prímek \( mn \)-hez, számuk \( \varphi(mn) \), továbbá a feladat (a) és (b) részéből könnyen adódik, hogy páronként inkongruensek modulo \( mn \).

3.3.13 Legyen \( g \) primitív gyök mod \( \mathcal{P}^{2^\alpha} \), \( \alpha = 1, 2, \ldots, r \). Ekkor megfelel, ha \( u_t \) az \( x = g_t \) (mod \( \mathcal{P}^{2^\alpha} \)), \( x = 1 \) (mod \( \mathcal{P}/\mathcal{P}^{2^\alpha} \)) szimultán kongruenciarendszer megoldása. — Páros \( mn \) esetén használjuk fel a 3.3.12c feladatot [83] is. Legyen az \( mn \) kanonikus alakjában a 2 kitevője \( \alpha \). Ha \( \alpha = 1 \), akkor a képleten semmit sem kell változtatni. Ha \( \alpha = 2 \), akkor a képleten a hatványok szorzatát egy \( u^j \) tényezővel kell kiegészíteni, ahol \( 0 \leq j < 2 - \varphi(4) \). Ha \( \alpha \geq 3 \), akkor egy \( u^j \) kiegészítő tényező kell, ahol \( 0 \leq j < 2 \) és \( 0 \leq k < 2^{\alpha-2} \). Itt az \( u \), illetve \( v \) értékeket az \( x \equiv -1 \) (mod \( 2^\alpha \)), \( x \equiv 1 \) (mod \( m/2^\alpha \)), illetve az \( x \equiv 5 \) (mod \( 2^\alpha \)), \( x \equiv 1 \) (mod \( m/2^\alpha \)) szimultán kongruenciarendszerek megoldásaként kaphatjuk meg.

3.3.14

(a) Egy tetszőleges \( F \) egész együtthatós polinom esetén jelölje \( \deg F \) az \( F \) fokszámát, \( N(F) \) pedig az \( F(x) \equiv 0 \) (mod \( p \)) kongruencia megoldásszámát. A T 3.1.2 Tételből következik, hogy \( N(F) \leq \deg F \). Ha \( x^{p-1} - 1 = f \) , akkor a kis Fermat-tétel és \( p \) prim volta miatt egy redukált maradékkrendszer minden eleme kielégíti az \( f(x) \equiv 0 \) (mod \( p \)) és \( h(x) \equiv 0 \) (mod \( p \)) kongruenciák közül (legalább) az egyiket, ezért
\[
p - 1 \leq N(f) + N(h) \leq \deg f + \deg h = p - 1,
\]
igy mindenhol egyenlőség teljesül. Tehát valóban \( N(f) = \deg f \).

(b) Alkalmazzuk az \( f_1 \) polinomokra az (a) részt.

(c) Egy \( c \) elemre akkor és csak akkor teljesül \( \varphi(c) = q^\theta \), ha \( f_1(c) \equiv 0 \) (mod \( p \)), de \( f_2(c) \equiv 0 \) (mod \( p \)). Ilyen \( c \) létezése a (b) rész alapján következik.
(d) Legyen a $d$ kanonikus alakja $d = q_1^{d_1} \cdots q_r^{d_r}$. A (c) rész alapján létezik olyan $c_i$, amelyre $\alpha_p(c_i) = q_i^{d_i}(i = 1, 2, \ldots, r)$. Ekkor a 3.2.15a feladat [76] szerint $\alpha_p(c_1 \cdots c_r) = d$.

13.3.4.

3.4.1 A feltétel szerint $p | \tau^5 - 2 = 11 \cdot 31$, azaz csak $p = 11$ és $p = 31$ jöhet szóba. A 7 primitív gyök mod 11, de nem primitív gyök mod 31, és így egyedül $p = 11$ felel meg a feltételeknek.

3.4.2 (a) $0$.

(b) $(p-1)/2$.

(c) $(p+1)/2$.

3.4.3

(a) Kétféleképpen is előállíthatunk olyan $\varrho$-hatványokat, amelyek az $ab$ szorzattal kongruensek mod $\varpi$:

$$g^{\text{ind}(ab)} \equiv ab \equiv g^{\text{ind}a} \cdot g^{\text{ind}b} = g^{\text{ind}a + \text{ind}b} (\text{mod } \varpi),$$

és így az első és utolsó tagban a $\varrho$ kivevői kongruensek mod $\varpi - 1$.

(b) Az (a) részhez hasonló gondolatmenetet alkalmazunk:

$$g^{\text{ind}(a^x)} = a^k \equiv (g^{\text{ind}a})^k = g^{k \cdot \text{ind}a} (\text{mod } \varpi).$$

3.4.4 Az előző feladatnál látott módon bizonyíthatunk.

3.4.5 $\alpha_p(c)$. 

3.4.6 Ez a T 3.3.4 Tétel (i) állításának az átfogalmazása.

3.4.7

(a) Az előző feladat alapján mindkét feltétel azzal ekvivalens, hogy $a$ primitív gyök mod $\varpi$.

(b) A 3.2.4c feladat [75] alapján $\alpha_p(a) = (p-1)'(\text{ind }a, p-1)$, bármelyik primitív gyök szerint képeztük is az indexet.

3.4.8 Használjuk fel a 3.4.6 feladatot [86].

3.4.9 Induljunk ki a 3.4.7b feladathoz [86] adott útmutatásból.

3.4.10 Egy-egy táblázat felső sorában a mod $\varpi$ redukált maradékosztályok legkisebb pozitív reprezentánsait soroljuk fel növekvő sorrendben, az alsó sorban pedig rendre ezeknek az elemeknek a $\varrho$ alapú indexei szerepelnek.

(a) $\varpi = 7$, $\varrho = 3$:

$$\begin{array}{ccccccc}
1 & 2 & 3 & 4 & 5 & 6 \\
0 & 2 & 1 & 4 & 5 & 3
\end{array}$$

(b) $\varpi = 11$, $\varrho = 2$:

$$\begin{array}{cccccccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\
0 & 1 & 8 & 2 & 4 & 9 & 7 & 3 & 6 & 5
\end{array}$$
3.4.11 Ha \( P \mid a \), akkor a megfelelő \( k \) számok a \( P \) többszörösei. Legyen most \( (a, p) = 1 \) és \( g \) egy primitív gyök mod \( p \). Ekkor az \( x \equiv g \mod p \), \( x \equiv 1 \mod (p - 1) \) szimultán kongruenciarendszer megoldásait vehetjük \( k \)-nak. — A feladat megoldható primitív gyök nélkül is, csak a kis Fermat-tételre támaszkodva: az \( x \equiv a \mod p \), \( x \equiv 1 \mod (p - 1) \) szimultán kongruenciarendszer megoldásai megfelelnek \( k \)-nak.

13.3.5.

3.5.1

(a) Nincs megoldása.

(b) \( x \equiv 51 \mod 101 \), — Útmutatás: Használjuk fel a kis Fermat-tételt.

(c) \( x \equiv \pm 2 \mod 23 \), — Útmutatás: A szokásos redukció után az \( x^2 \equiv 4 \mod 23 \) kongruencia adódik.

(d) \( x \equiv 0, \pm 6, \pm 7 \mod 17 \).

(e) \( x = 0, 2, 5, 6 \mod 13 \).

(f) \( x \equiv \pm 3 \mod 11 \), — Útmutatás: Mivel \( x \equiv 0 \mod 11 \) nem megoldás, ezért a redukcióról

3.5.2

(a) Válasz: 12. — Útmutatás: Az \( x^{20} \equiv 1 \mod 73 \) és \( x^{15} \equiv 1 \mod 73 \) kongruenciák megoldásszámának összegéből le kell vonni a közös megoldások számát, azaz az \( x^{(6, 15)} = 1 \mod 73 \) kongruencia megoldásszámát.

(b) Válasz: \((k + 1, 30)\), ha 31 \( \mid k + 1 \), és \((k + 1, 30) - 1\), egyébként.

Útmutatás: A bal oldal \( (x^{k+1} - 1)/((x - 1)) \) alakba írható. Így a kér déses kongruencia megoldásai \( x \equiv 1 \) -től esetleg eltekintve azonosak az \( x^{k+1} \equiv 1 \mod 31 \) kongruencia megoldásaival. Külön meg kell vizsgálni, hogy az \( x \equiv 1 \mod 31 \) milyen \( k \) esetén lesz megoldása az eredeti kongruenciának.

3.5.3 \( a \equiv 0, \pm 1 \mod p \).

3.5.4 A megoldhatóság feltétele: \((k, p - 1) \mid \text{ind}_g g = 1 \). Ekkor a megoldásszám \((k, p - 1) = 1 \).

3.5.5 \( x \equiv \phi_i \mod p \), \( i = 1, \ldots, r \).

3.5.6 (a) 1.

(b) \( \pm 1 \).
3.5.10 $\left(\frac{k_1}{p_1} - 1\right) = 2$.

3.5.11

(a) Válasz: 1, ha $p - 1\mid k$, és 0 egyébként. — Útmutatás: Legyen $d = (k, p - 1)$. A $k$ -adik hatványmaradékok $g^{\frac{d}{d}}$ alakban írhatók, ahol $0 \leq r < (p - 1)/d$. Használjuk ezután a véges mértani sorozat összegképletét. — Egy másik lehetőség: A 3.3.7 feladatban [83] szereplő összegben minden $k$ -adik hatványmaradék $(k, p - 1)$-szer fordul elő. —

Egy harmadik út: Vegyük észre, hogy a $k$ -adik hatványmaradékok éppen a $\mathbb{Z}_p$ feletti $x^{\frac{k - 1}{p - 1}} - 1$ polinom (egyszeres) gyökei, és használjuk fel a gyökök és együtthatók közötti összefüggést.

(b) Válasz: $-1$, illetve 1, aszerint, hogy $(k - 1)$ páros, illetve páratlan.

Útmutatás: Állitsuk pára a $k$ -adik hatványmaradékokat úgy, hogy az egy pára tartozó elemek szorzata 1 maradékot adjon. — További lehetőségek: Írjuk fel a $k$ -adik hatványmaradékokat az (a) részhez adott első útmutatás szerint, illetve alkalmazzuk az (a) részhez adott harmadik útmutatást.

3.5.12 Lásd a 3.5.9 feladathoz [90] adott útmutatást. — Általánosítás: $a$ akkor és csak akkor lesz egyszerre $k$ -adik és $\eta$ -edik hatványmaradék, ha $\left[\frac{k}{\eta}\right]$ -edik hatványmaradék.

13.3.6.

3.6.1 Egy olyan homogén lineáris egyenletrendszernek, amelyben az ismeretlenek száma nagyobb az egyenletek számánál, mindig van nemtriviális megoldása. (Ez nemcsak modulo $P$, hanem bármely más test felett is érvényes.)

3.6.2 Alkalmazzuk a Chevalley-tételt.

3.6.3

(a) A kínai maradéktétel szerint elegánt a problémát egy $P^\alpha$ primhatvány modulusra megoldani. Ha $\alpha > 1$, akkor az $x_1 = p^{(\alpha^2-1)/2}$, $x_2 = x_3 = 0$ választás megfelelő. Ha $\alpha = 1$, akkor (pl. a Chevalley-tétel alapján) az $x_1^2 + x_2^2 + x_3^2 = 0 \pmod{p}$ kongruenciának van nemtriviális megoldása. Itt feltehető $|x_1| \leq p/2$, ezért $0 < x_1^2 + x_2^2 + x_3^2 < p^2$, tehát az $x_1^2 + x_2^2 + x_3^2$ összeg (amely a feltétel szerint $P$ -vel osztható) $P^\alpha$ -tel már nem lehet osztható.

(b) Az (a)-beli eljárást kell egyetlen esetben finomítani: ha $\alpha > 1$ és páratlan, akkor legyen $x_2 = p^{(\alpha - 1)/2}u_1$, és az $\eta_1$ -kre alkalmazzuk az előbb $\alpha = 1$ -re látott gondolatmenetet.

3.6.4 A $P = 2$ eset nyilvánvaló. Ha $P > 2$, akkor a Chevalley-tétel szerint léteznek olyan $\nu_i$ egészek, $1 \leq i \leq 5$, amelyek a $\sum_{i=1}^{5} x_i^2 = 0 \pmod{p}$ kongruencia egy nemtriviális megoldását adják. Ha itt pl. $u_1 \neq 0 \pmod{p}$, akkor $\nu_i = v_i^{(p - 2)}u_i$ is megoldás és $v_i \equiv 1 \pmod{p}$. A több $v_i$ -ről is feltehető $|v_i| \leq (p - 1)/2$. Ennek megfelelően $\sum_{i=1}^{5} v_i^4$ osztható $P$ -vel és
3.6.5

(a) A \( c_{ij} \) számban a \( a_i \) prim kitevője legyen \( \gamma_i \) \((1 \leq i \leq k, 1 \leq j \leq r)\). Az \( f_i(x_1, \ldots, x_t) = \sum_{j=1}^r \gamma_i x_j^2 \) polinomokra és \( p = 3 \)-ra alkalmazzuk a Chevalley-tételt.

(b) Itt \( i \geq (m-1)k + 1 \) a megfelelő feltétel.

3.6.6 Először azt igazoljuk, hogy ha az állítás igaz \( \omega = r \)-re és \( s = s \)-re, akkor teljesül \( u = rs \)-re is. A \( 2rs - 1 \) számból vegyünk tetszőleges \( 2r - 1 \)-et, ekkor az \( r \)-re vonatkozó állítás szerint kiválaszthatunk \( \tau \) olyat, amelyek összege osztható \( r \)-rel. A maradék \( 2rs - 1 - r \) számból ismét vegyünk tetszőleges \( 2r - 1 \)-et, ezek között is van \( r \) darab olyan, amelyek összege osztható \( r \)-rel. Lássuk be, hogy ily módon \( 2s-1 \) darab olyan \( r \)-es csoport keletkezik, ahol minden csoport elemeinek az összege osztható \( r \)-rel. Alkalmazzuk ezután az \( s \)-re vonatkozó állítást ezen összegek \( r \)-edrészére.

Ennek alapján elég az \( n = p \) prim esettel foglalkozni. Legyen \( f_1 = \sum_{j=1}^{2p-1} c_j x_j^{p-1} \), \( f_2 = \sum_{j=1}^{2p-1} x_j^{p-1} \), és alkalmazzuk a Chevalley-tételt.

3.6.7

(a) Indirekt tegyük fel, hogy az egyetlen megoldás \( x_j = a_j \), \( j = 1, 2, \ldots, t \). Ekkor a Chevalley-tételre adott bizonyításban csak a \( G \) polinom definícióját kell módosítani: legyen most

\[
G(x_1, \ldots, x_t) = \prod_{j=1}^t (1 - (x_j - a_j)^{p-1}).
\]

(b) Legyen a megoldásszám \( s \), a megoldások \( u_1; \ldots; u_s \). Minden \( u_v \) megoldáshoz készítsük el az (a) résznak megfelelően megadott \( G_v \) polinomot (\( v = 1, \ldots, s \)). Legyen \( G = \sum_{v=1}^s G_v \). Ekkor a Chevalley-tétel bizonyítását követve \( F^* = G \) adódik. A fokszámokat összehasonlítként ebből azt kapjuk, hogy \( G \)-ben az \((x_1 \cdots x_t)^{p-1} \) tag együtthatója csak 0 lehet modulo \( p \), azaz \( s(-1)^t \equiv 0 \mod p \).

3.6.8

(a) Az \( A \) mátrix determinánsa

\[
\begin{vmatrix}
-a & 0 & \cdots & 0 \\
0 & -b & a & \cdots & 0 \\
0 & 0 & -b & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
a & 0 & 0 & \cdots & -b
\end{vmatrix} = (-b)^{p-1} + (-1)^{p-2} q^{p-1} = 0 \quad (\mod p),
\]

tehát \( \tau(A) \leq p - 2 \). Másrésztt a bal felső elemhez tartozó aldedményszám \((-1)^{p-2} \not\equiv 0 \mod p\)

(b) A kérdéses mátrix minden eleme 1, tehát a rangja 1, és így a megoldásszám \( p - 2 \) (vö. a 3.5.3 feladattal [89]).
3.6.9 Azt kell belátnunk, hogy a mátrix determinánsa $0 \pmod{p}$.
(a) A sorok összege $0$.
(b) Az $i$-edik sort $s_i$-vel jelölve $s_1 + s_2 - s_3 - s_4 + s_5 + \cdots = 0$.

3.6.10 Jelölje a König–Rados-tételben a három polinomhoz tartozó mátrixokat $A_f$, $A_g$, illetve $A_h$.
Az $A_f$ mátrixból a sorok permutálásával úgy kapjuk meg $A_g$-t, hogy az utolsó sorból lesz az első, miközben a többi sor egymáshoz viszonyított helyzete nem változik. Az $A_f$-ből úgy jutunk el $A_h$-hoz, hogy tükrözzünk a főátlóra, majd az utolsó sorból első sort csinálunk. Mivel ezek az átalakítások a mátrix rangját nem változtatták meg, a három kongruencia megoldásszáma azonos. — Könnyen megoldhatjuk a feladatot a König–Rados-tétel nélkül is. Ha $f(j, p) = 1$, akkor $f(j) \equiv g(j)^h \pmod{p}$, és így az első két kongruenciának ugyanazok a megoldásai. Hasonlóan igazolható, hogy

$$f(i) = 0 \pmod{p} \iff h(a^{-1}) = 0 \pmod{p},$$

ahol $a^{-1}$ az $a$ multiplikatív inverzét jelenti: $a a^{-1} \equiv 1 \pmod{p}$.

3.6.11 A T 3.1.3 Tételben leírt redukciós eljárással kiküszöbölhetjük a $p-1$-nél magasabb fokú tagokat. Továbbá könnyen eldönthető, hogy $x \equiv 0 \pmod{p}$ mikor megoldás, ezért elég a $p$-hez relatív prim megoldások keresésére szorítkozni. Ebben az esetben a kis Fermat-tétel alapján $x^{p-1} \equiv 1 \pmod{p}$ helyére $1$-et írhatunk. Ha a kapott $h_i = d_0 + d_1 x + \cdots + d_{p-2} x^{p-2}$ polinomban minden $d_j$ osztható $p$-vel, akkor $h_i(x) \equiv 0 \pmod{p}$ nyilván minden $x$-re teljesül. Végül, ha $d_0 = \cdots = d_{i-1} = 0 \pmod{p}$, de $d_i \neq 0 \pmod{p}$, akkor a $h_i = h_i x^i$ polinomra már alkalmazhatjuk a König–Rados-tételt, és a $h_i(x) \equiv 0 \pmod{p}$, íll. $h_i(x) \equiv 0 \pmod{p}$ kongruenciának ugyanazok a redukált maradékosztályok lesznek a megoldásai.

13.3.7.

3.7.1 (a) 1.
(b) 0.
(c) 12.
(d) 73.
(e) 15.

3.7.2 Használjuk a T 3.7.1 Tételt.

3.7.3
(a) A megoldhatóság feltétele $a \equiv 1 \pmod{11}$, a megoldásszám 10.

Útmutatás: Használjuk a kis Fermat-tételt és a T 3.7.1 Tételt.
(b) A megoldhatóság feltétele $a \equiv 1 \pmod{8}$, a megoldásszám 4.

3.7.4 Az állítás leolvasható a T 3.7.1 Tételre adott bizonyításból.

3.7.5
(a) \[ x \equiv 32 \pmod{7^3} \].
(b) Nem oldható meg.
(c) \[ x \equiv 2 + 40j \pmod{7^3} \].

13.4 Legendre- és Jacobi-szimbólum

13.4.1.

4.1.1 Első bizonyítás: Az \[ x^2 \equiv c^2 \pmod{p} \] kongruencia megoldható; az egyik megoldás \[ x \equiv c \pmod{p} \].

Második bizonyítás: \[ (c^2)^{(p-1)/2} = c^{p-1} \equiv 1 \pmod{p} \].

Harmadik bizonyítás: \[ \binom{c^2}{p} = \binom{c}{p}^2 = 1 \].

4.1.2 (a) 1.
(b) \(-1\).
(c) \(-1\).

4.1.3 Az összeg 0, a szorzat 1, ha \( p \equiv 1 \pmod{4} \), és \(-1\), ha \( p = -1 \pmod{4} \).

4.1.4 Az \[ x^2 = a \pmod{p} \] kongruencia megoldása szükségképpen kongruens a \( \pm 1, \pm 2, \ldots, \pm \left( \frac{p-1}{2} \right)^2 \) redukált maradékrendszer valamelyik \( j \) elemével, és így valóban \( a = \left| j \right|^2 \pmod{p} \). Továbbá mind a megadott elemek, mind pedig a kvadratikus maradékok száma \( \left( \frac{p-1}{2} \right)^2 \), ezért a megadott elemek között már nem lehetnek kongruensek. Ez utóbbi közvetlenül is bizonyítható: Indirekt, ha valamely \( 1 \leq n < u \leq \left( \frac{p-1}{2} \right)^2 \) esetén \( u^2 = v^2 \pmod{p} \), akkor \( v \mid (v - u)(v + u) \), de itt \( 1 \leq v - u < v + u \leq \left( \frac{p-1}{2} \right) \), tehát egyik tényező sem osztható \( P \)-vel, ami ellentmond \( P \) prim voltának.

4.1.5 Megmutatjuk, hogy \( a = b = 0 \pmod{77} \), és így \( 30 \cdot 20 = 77^2 \mid a^2 + b^2 \). Indirekt okoskodva, ha például \( a \) nem osztható (mondjuk) 7-tel, akkor 7 prim volta és \( 7 \mid a^2 + b^2 \) miatt \( b \) sem osztható 7-tel. Ekkor \( a^2 \equiv -b^2 \pmod{7} \) és \( \left( \frac{-1}{7} \right) = -1 \) felhasználásával az alábbi módon jutunk ellentmondásra:

\[
1 = \left( \frac{a}{7} \right)^2 \left( \frac{b}{7} \right)^2 = \left( \frac{a^2}{7} \right) \left( \frac{-b^2}{7} \right) = \left( \frac{-1}{7} \right) \left( \frac{b}{7} \right)^2 = -1.
\]

4.1.6 Használjuk fel a Wilson-tételt.

4.1.7 \( \left( \pm a^{(p+1)/4} \right)^2 = a^{(p+1)/2} = a \cdot a^{(p-1)/2} \equiv a \cdot 1 = a \pmod{p} \).

4.1.8 (a) Ha \( a_p(a) = 2k + 1 \), akkor \( (a^p)^2 \equiv a \pmod{p} \).
(b) \( p = 4k + 3 \).

4.1.9
EREDMÉNYEK ÉS ÚTMUTATÁSOK

(a) Ha \( a_p(g) = \rho - 1 \), akkor \( g^{(\rho - 1)/2} \neq 1 \) (n.c.d. \( p \)).

(b) \( \rho = 2^k + 1 \) (ezek az ún. Fermat-prímek, lásd az 1.4.4 feladatot [17] és az 5.2 pontot).

4.1.10 32.

4.1.11

(a) Mivel \( \rho + 1 = 4k \), így \( 1 = \left( \frac{1}{\rho} \right) = \left( \frac{\rho + 1}{\rho} \right) = \left( \frac{4k}{\rho} \right) = \left( \frac{2}{\rho} \right)^2 \left( \frac{k}{\rho} \right). \)

(b) Bizonyítsunk az (a) részhez hasonlóan.

4.1.12 Ha \( \rho \leq 11 \), akkor legalább az egyik kongruencia \( x^2 \equiv 0 \) (n.c.d. \( p \)) típusú. Egyébként használjuk ki, hogy a jobb oldalak sorzata négyzeteszám, és így a megfelelő öt Legendre-szimbólum szorzata szükségképpen 1.

4.1.13

(a) \( a \equiv 1 \) és 6 (mod 13). — Útmutatás: Alkalmazzuk a teljes négyzeté kiegészítést.

(b) \( a \equiv -3 \) (mod 17). 

(c) \( a \equiv 0 \), \( \pm 8 \) (mod 23). — Útmutatás: Az \( x \equiv 35 \) helyére a kis Fermat-tétel alapján \( a^3 \) írható. Az \( x \) kiemelése után egy másodfokú visszavezethető negyedfokú kongruencia adódik.

(d) Nincs megoldás. — Útmutatás: \( x \equiv 0 \) (n.c.d. 19) nem megoldás, így ekvivalens lépést végzünk, ha \( x \) -szel szorzunk és \( x^{18} \) helyére 1-et írunk.

4.1.14

(a) Alkalmazzuk a Legendre-szimbólum multiplikativitását.

(b) Legyen \( a_1(p) = \gamma \) és \( a \) a legkisebb olyan egész, amelyre \( r^n > p \). Ekkor \( 0 < r^n - p < n \), ezért \( \left( \frac{r}{p} \right) = -1 \), és így \( r > n \). Ezt felhasználva \( (r - 1)n < p \) -ből adódik az állítás.

4.1.15

(a) \( \left( \frac{\gamma}{p} \right) = 1 \), ha \( (i, p) = 1 \), és 0, ha \( \gamma \equiv i \).

(b) Mutassuk meg, hogy ha \( S(u, p) \) -ben \( \gamma \) helyére mindenütt \( a^\gamma \) -t írunk, akkor egyrészt az összeg nem változik, másrészt \( \left( \frac{\gamma}{p} \right) = 1 \) kiemelése után az új összeg éppen \( S(1, p) \) -vel egyenlő.

(c) Rögzített \( \gamma \) -re az \( i + \alpha \) értékek teljes maradékkrendszert alkotnak mod \( P \), és így az ezekhez tartozó Legendre-szimbólumok összege a 4.1.3 feladat [102] alapján 0.

(d) Az előző három részből következik.

4.1.16

(a) Vegyük észre, hogy \( \left( \frac{\gamma}{p} \right) + 1 \) értéke aszerint 2, 0, illetve 1, hogy \( c \) kvadratikus maradék, kvadratikus nemmaradék, illetve osztható \( P \) -vel.

(b) Az (a) részből következik a 4.1.3 [102] és 4.1.15d feladatok [103], valamint a \( \left( \frac{\gamma}{p} \right) \) -re tanultak felhasználásával.
13.4.2.

4.2.1 Megoldható: (c), (e), (f). — A (c)-nél használjuk fel a Wilson-tételt, az összetett modulusok esetén pedig akkor és csak akkor oldható meg a kongruencia, ha a modulusok minden primhatvány osztójára nézve létezik megoldás.

4.2.2

(a) \( p = 5k + 1 \) vagy \( 8k + 3 \). — Útmutatás: \( \left( \frac{-2}{p} \right) = \left( \frac{-1}{p} \right) \left( \frac{2}{p} \right) \).

(b) \( p = 12k \pm 1 \) vagy \( p = 3 \). — Útmutatás: A reciprocitási tétel alkalmazásánál az számít, hogy \( p > 3 \) mivel kongruens mod 4, utána pedig az, hogy \( p \) mivel kongruens mod 3. Ezért aszerint érdemes az eseteket megkülönböztetni, hogy \( p \) mivel kongruens mod 12.

(c) \( p = 6k + 1 \) vagy \( p = 3 \).

(d) \( p = 5k \pm 1 \) vagy \( p = 5 \).

(e) \( p = 8k \pm 1 \) vagy \( 8k + 3 \). — Útmutatás: Bontsuk szorzattá \( x^4 - 4 \)-et.

(f) \( p = 4k + 1 \). — Útmutatás: Alkalmazzuk a T 3.5.1 Tételt, vizsgáljuk az eseteket a \( p \)-nek a 8-cal való osztási maradéka szerint, és használjuk fel a \( \left( \frac{-1}{p} \right) \) és \( \left( \frac{2}{p} \right) \) képletét.

(g) Minden \( p \) -re. — Útmutatás: Használjuk fel az (e) és (f) részt, vagy alkalmazzuk a T 3.5.1 Tételt.

(h) A \( 24k + 17 \) alakú prímek kivételével minden primre.

4.2.3 Kövessük a 4.1.5 feladatra [102] adott útmutatást, felhasználva, hogy az 1999 prim és \( \left( \frac{-2}{1999} \right) = -1 \).

4.2.4 A feltétel ekvivalens azzal, hogy \( \left( 2c \right)^8 \equiv -2^7 \pmod{43^{100}} \). Az \( x^k \equiv -2^7 \pmod{43} \) kongruencia megoldhatóságához használjuk fel a T 3.5.1 Tételt, valamint, hogy \( \left( \frac{-2}{43} \right) = 1 \). A 43^{100} modulsra a 3.7.2 feladat [98] (vagy a T 3.7.1 Tétel) alapján térhetünk át. Végül a kapott maradékosztályoknak a modulus páratlansága miatt biztosan van páros eleme is.

4.2.5

(a) Ha \( 8c^2 \equiv 1 \pmod{p} \), akkor

\[ 1 = \left( \frac{1}{p} \right) = \left( \frac{8c^2}{p} \right) = \left( \frac{2}{p} \right)^8 \left( \frac{c}{p} \right)^2 = \left( \frac{2}{p} \right)^8 \left( \frac{c}{p} \right)^2. \]

A második állítást indirekt bizonyítjuk: Ha \( 8c^2 - 1 \) minden primitívkezője \( 8k + 1 \) alakú volna, akkor ezek (megfelelő multiplicitással vett) szorzata, azaz maga a \( 8c^2 - 1 \) is \( 8k + 1 \) alakú lenne, ami ellentmondás.

(b) Az (a) részhez hasonlóan okoskodhatunk (most \( \left( \frac{2}{p} \right) = -1 \) adódik).

(c) A \( \left( \frac{-1}{p} \right) \) felhasználásával kapjuk, hogy \( c^2 + 4 \) minden (páratlan) \( p \) primosztójára \( p \equiv 1 \pmod{4} \). Ez azt jelenti, hogy \( p \equiv 1 \) vagy \( 5 \pmod{8} \) és (mod 12) is. Mivel \( c^2 + 4 \equiv 5 \pmod{8} \) és (mod 12), ezért nem teljesülhet minden primosztóra \( p \equiv 1 \pmod{8} \), illetve (mod 12).
4.2.6
(a) A reciprocitási tétel alapján
\[ \prod_{i=r}^{k} \left( \frac{a_i}{r_i} \right) = (-1)^{\left( \frac{r}{2} \right)}, \]
ahol \( r \) a \( 4k - 1 \) alakú \( P_i \) -k száma, továbbá \( \left( \frac{r}{2} \right) \) pontosan akkor páratlan, ha \( r = 2 \) vagy 3.

(b) A feltétel szerint minden \( i \neq j \) -re \( \left( \frac{P_i}{P_j} \right) = 1 \). Így a reciprocitási tétel miatt a \( P_i \) prímek között legfeljebb egy lehet \( 4k - 1 \) alakú.

4.2.7
(a) A középső számot \( c \) -vel jelölve, az összeg
\[ S = (c - 9)^2 + (c - 8)^2 + \cdots + (c + 9)^2 = 19(c^2 + 30) \]
alakba írható. Mivel \( \left( \frac{-29}{19} \right) = -1 \), ezért \( S \) a 19-nek pontosan az első hatványával osztható, és így nem lehet teljes hatvány.

(b) Az (a) részhez hasonlóan elég belátunk, hogy \( a = \left( \frac{1 - y^2}{12} \right) \) kvadratikus nemmaradék mod \( P \). Vegyük észre, hogy \( \left( \frac{y}{P} \right) = \left( \frac{16a}{P} \right) = \left( \frac{y}{P} \right) \).

4.2.8 Például \( f = (x^2 + 1)(x^2 - 17)(x^2 + 17) \) megfelel.

13.4.3.

4.3.1 (a) 1.
(b) - 1.
(c) - 1.
(d) 1.

4.3.2
(a) Legyen \( m = p_1 \cdots p_r \). Ha az \( x^2 \equiv a \pmod{m} \) kongruencia megoldható, akkor minden \( i \) -re az \( x^2 \equiv a \pmod{p_i} \) kongruencia is megoldható, tehát minden \( i \) -re \( \left( \frac{a}{p_i} \right) = 1 \), és így \( \left( \frac{a}{m} \right) = \left( \frac{a}{p_1} \right) \cdots \left( \frac{a}{p_r} \right) = 1 \).

(b) Például \( m = 9, a = 2 \), vagy \( m = 15, a = 8 \) stb.
(c) \( m = p^{2k+1} \) (ahol \( p \) prim, \( k \geq 0 \)).

4.3.3 A \( P = 2 \) eset nyilvánvaló. Egyébként \( P \equiv 1 \pmod{4} \), ekkor \( \left( \frac{-1}{P} \right) = 1 \), tehát elég az \( a, b > 0 \) esetet nézni. Legyen (mondjuk) az \( a \) páratlan, ekkor (\( a > 1 \) esetén)
\[ \left( \frac{a}{P} \right) = \left( \frac{k}{a} \right) \left( \frac{c^2 + b^2}{a} \right) \left( \frac{b^2}{a} \right) = 1. \]
4.3.4 Mindkét összeg − 1.

Útmutatás (b)-hez: Lássuk be, hogy \( \left( \frac{2}{2k+1} \right) = \left( \frac{-2}{2k+1} \right) \).

4.3.5

(a) Ha \( a \equiv 1 \pmod{4} \), akkor \( \left( \frac{a}{m} \right) = \left( \frac{m}{a} \right) = \left( \frac{a}{a} \right) \). Ha \( a = 2^k t \), ahol \( k \geq 2 \) és \( t \) páratlan, akkor \( m = n \pmod{4} \) miatt a reciprocitás egyformán működik a \( t, m \) és \( t, n \) párra, továbbá \( k > 3 \) esetén \( m = n \pmod{8} \) miatt \( \left( \frac{2}{m} \right) = \left( \frac{2}{n} \right) \), ha pedig \( k = 2 \) (vagy tetszőleges páros szám), akkor nincs szükség \( \left( \frac{2}{m} \right) \)-re, illetve \( \left( \frac{2}{n} \right) \)-re.

(b) Mindkét esetben megfelel tetszőleges (az \( a \)-hoz relatív prim, 1-nél nagyobb, páratlan) \( m \) és \( n = m + 2a \).

4.3.6

(a) \( 0 \) vagy \( \varphi(m) \). — Útmutatás: Ha minden \( \left( \frac{a}{m} \right) = 1 \), akkor az \( S \) összeg nyilván \( \varphi(m) \). Egyébként legyen \( c \) tetszőleges olyan szám, amelyre \( \left( \frac{c}{m} \right) = -1 \), és írjunk \( r \) helyére mindenhová \( cr^{-1} \)-et. Az így keletkező \( S' \) összegről lássuk be, hogy egyrészt \( S' = S \), másrészt \( S' = -S \).

(b) \( -1 \), ha \( n \) egy \( 4k + 3 \) alakú prim páratlan hatványa, és \( 1 \) minden más esetben.

4.3.7

(a) \( n \) négyzetszám. — Útmutatás: A négyzetszámok nyilván megfelelnek. Ha \( n \) nem négyzetszám, akkor van olyan \( P \) prímosztója, amely páratlan hatványon szerepel az \( n \) kanonikus alakjában, azaz \( n = p^k t \), ahol \( \left( \frac{t}{p} \right) = 1 \) és \( k \) páratlan. Legyen \( c \) egy kvadratikus nemmaradék mod \( P \). Ekkor az \( x \equiv c \pmod{p} \), \( x \equiv 1 \pmod{t} \) szimultán kongruenciarendszer egy \( a \) megoldására \( \left( \frac{c}{P} \right) = -1 \).

(b) \( a \) négyzetszám. — Útmutatás: Az (a) részhez hasonlóan bizonyíthatunk, használjuk fel a reciprocitást is. Ne felejtse el, hogy \( a \) lehet páros és/vagy negatív szám is.

### 13.5 Prímszámok

#### 13.5.1.

5.1.1 Ha valamilyen \( n > 1 \) modulusra (például) \( \nu_1, \ldots, \nu_j \) teljes maradéktrendszer modulo \( n \), akkor bármely \( n \)-re az \( \nu_1 + \nu_2 + \cdots + \nu_j \) számok is teljes maradéktrendszert alkotnak modulo \( n \), és így biztosan van közöttük \( n \)-mel osztható. Ha \( n | \nu_1 + \nu_2 + \cdots + \nu_j \), akkor \( n \equiv r_i \) nem lehet prim.

5.1.2

(a) Legyen \( u \geq 7 \) páratlan. Ekkor \( u - 3 > 4 \) páros, és így \( u - 3 = p_1 + p_2 \), tehát \( u = 3 + p_1 + p_2 \).

(b) Ha egy páros szám három prim összege, akkor az egyik prim szükségképpen a 2, továbbá \( u - 2 = p_1 + p_2 \iff u = 2 + p_1 + p_2 \).

5.1.3 Minden \( u \geq 8 \). — Minden \( u \geq 40 \), valamint \( u = 18, 24, 30, 34 \) és 36.

5.1.4 Csak az 5 és 2 pár ilyen.
5.1.5 (c) Használjuk fel, hogy ha \( (a, d) = 1 \), akkor a számtani sorozat első \( p \) tagja teljes maradékkrendszerről modulo \( p \).

5.1.6 Mersenne és Fermat: Az 1.4.4 feladatban [17] láttuk, hogy ha \( k \) összetett, akkor \( 2^k - 1 \) , ha pedig \( k \) nem kettőhatvány, akkor \( 2^k - 1 \) biztosan összetett.

\[ u^2 + 1 : \text{Ha } u > 1 \text{ páratlan, akkor } u^2 + 1 > 2 \text{ páros, és általában, ha } k < u \equiv k \pmod{2^2 + 1}, \]
akkor \( u^2 + 1 \equiv k^2 + 1 \equiv 0 \pmod{2^2 + 1} \), tehát ekkor \( u^2 + 1 \) összetett.

Csupaegy: A \( k \) darab 1-esből álló szám is biztosan összetett, ha \( k \) összetett.

\[ 333...31 : \text{Ezek a számok } (10^k - 7)/3 \text{ alakúak, és } 2 < k < 8 \text{ esetén primek. Azonban ha } \]
\[ \kappa = 2 + 30r, \text{ akkor a kis Fermat-étel alapján } 10^k - 7 \equiv 10^2 - 7 \pmod{31}, \text{ és így } (3, 31) = 1 \]
miatt

\[
\frac{10^k - 7}{3} = \frac{10^2 - 7}{3} = 31 \pmod{31},
\]

tehát ilyenkor mindig 31-gyel osztható számot kapunk. Ugyanígy adódik, hogy például végig sok 17-tel osztható van közöttük: a 10 primitív gyök modulo 17, tehát létezik olyan \( s \), amelyre \( 10^s \equiv 7 \pmod{17} \), és ekkor \( \kappa = s + 156r \) esetén \( 17 \| (10^k - 7)/3 \).

Fibonacci: Minden harmadik elem páros, sőt tetszőleges \( m \)-re végig sok \( m \)-mel osztható van közöttük (lásd az 1.2.5 feladatot [7]).

5.1.7 Használjuk fel az ún. interpolációs polinomokra vonatkozó tételt: Bárivel k helyen tetszőlegesen előirva a helyettesítési értékeket, pontosan egy legfeljebb \( k - 1 \) -edfokú megfelelő polinom létezik (amelynek együthatói az adott testből valók).

5.1.8

(a) Ha \( a \equiv b \pmod{f(b)} \), akkor \( f(a) \equiv 0 \pmod{f(b)} \).

(b) Az állítás átfogalmazható arra, hogy ha \( g \) egész együthathós polinom, akkor \( g(n^r) \) nem lehet minden \( n \)-re egy primszám rögzített konstanssoros. Ennek bizonyítása az (a)-hoz hasonlóan történhet.

(b2) Ha egy komplex együthathós polinom a főszámánál több racionális helyen racionális értéket vesz fel, akkor szükségképpen racionális együthathós. Ez például az interpolációs polinomok segítségével igazolható.

(b3) Egy kivételével minden változónak adjunk rögzített egész értéket, ezzel a feladatot visszavezetünk az egyváltozós esetre.

5.1.9

(a) Az T 5.1.1 Tétel bizonyításának gondolatmenetéből \( n \) szerinti teljes indukcióval következik.

(b) \[ \left[ 10^{2^{2^r}} \right] \] egész szám „végén” éppen \( P_1 \) áll.

(c) A \( c \) számot (valószínűleg) csak úgy tudjuk megadni, ha már előre ismerjük (az éppen a \( c \) segítségével meghatározni remélő) primszámokat.

5.1.10 Pl. \( K = (10^4)! \) megfelel.
13.5.2.

5.2.1

(a) A könnyen adódó $F_{n+1} = F_n(F_n - 2) + 2$ összefüggést felhasználva bizonyítsunk teljes indukcióval.

(b) Támaszkodjunk az (a) részre.

(c) Mindegyik Fermat-szám van olyan primitíven, amely elemiának másik Fermat-számnak sem lehet osztója.

(d) Az $n$ -edik primszám nem lehet nagyobb $F_{n-1}$ -nél.

5.2.2 Ha $F_n$ prim, akkor mutassuk meg, hogy $\left(\frac{2}{F_n}\right)$, illetve $\left(\frac{10}{F_n}\right)$ értéke $-1$. A megfordítás pontosan ugyanúgy igazolható, mint az T 5.2.2 Tételben.

5.2.3 A feltétel szükségességet ugyanúgy igazolhatjuk, mint az T 5.2.2 Tételben. A megfordításnál okoskodjunk indirekt; ekkor feltételezhető, hogy $K_n$ -nek létezik egy $q \leq \sqrt{K_n}$ prímosztója. Mutassuk meg, hogy $\alpha p(3) = 2^n$ vagy $5 \cdot 2^n$. Innen kapjuk, hogy $2^n \equiv 1 \pmod{q}$. Ezt a $q \leq \sqrt{K_n}$ feltétellel összefuttatva elfogadható a kettő hatványok.

5.2.4 Használjuk fel a $\varphi(N)$ képletét.

5.2.5 Válassz: 5. — Utmutatás: Először mutassuk meg, hogy $k$ szükségképpen kettőhatvány. Ezután használjuk fel az 5.2.1a feladatot [124] és azt a tényt, hogy $F_5$ osztható 641-gyel.

5.2.6 Az T 5.2.3 Tétel alapján a legkisebb szóba jövő primek 47, a 233, a 223, illetve a 431, és az ismételt négyzetre emelők módszerével ellenőrizhetjük, hogy ezek valóban osztói a megadott Mersenne-számoknak.

5.2.8 Ha $2^{2^k} \equiv -1 \pmod{q^2}$, akkor az T 5.2.1 Tétel bizonyításához hasonló módon $\alpha p(2) \equiv q^2 + 1 \pmod{2^k}$ adódik. Ebből kapjuk, hogy $\alpha p(2) \equiv q^2 \equiv q \equiv -1 \pmod{q^2}$. A Mersenne-számkra vonatkozó állítás hasonlóan igazolható.

5.2.9 A $(8, 9)$ páron kívül csak azok a párok megfelelők, amelyek egyik tagja egy Fermat-vagy Mersenne-prím, a másik tag pedig a megfelelő kettőhatvány.

5.2.10 Ha $k \mid n$ teljesül $H_k$ -ban, akkor egyrésztt alakul át $a \equiv b \pmod{k}$, másrészt $a/k$ iratura rendellenessé válik. Innen $\sqrt{3}$ irracionális. Az állítás másik irányra nyilvánvaló.

5.2.11 Elég belátni, hogy ha $F_n$ prim, akkor alakul $\alpha p(6) \equiv 0 \pmod{2^j}$ alakú. Ekkor $F_n \equiv H_{1-j} \pmod{2^j}$.

13.5.3.

5.3.1 Válassz: 6003. (A redukált maradékosztályokban végzeten sok, a 9999 primosztói által reprezentált maradékosztályokból pedig egy-egy (positív) prim található.)

5.3.2 A problémát az jelenti, hogy az $4 \equiv 4p_1 \cdots p_n + 1$ számnak nem feltétlenül van $4k + 1$ alakú primosztója, mert lehet, hogy páros sok $4k + 3$ alakú prim szorzata.
5.3.3
(a) Kövessük az T 5.3.2 Tétel bizonyításának a gondolatmenetét.
(b)–(h) Járjunk el az T 5.3.3 Tétel bizonyításának a mintájára. Az egyes esetekben mindig vizsgáljuk meg, milyen alakú primosztó lehetnek a következő alakú számoknak [(a) (c), (d), (f) és (h) résznél használjuk fel a 4.2.5 feladatot [108]]:

\( u^2 + 2 \); (c) \( u^2 + 4 \); (d) \( u^2 - 2 \) vagy \( 8u^2 - 1 \);
\( 5n^2 - 1 \); (f) \( u^2 + 4 \); (g) \( (2u)^2 + 3 \); (h) \( 12n^2 - 1 \).

5.3.4 Végtelen sok; a \( 10000k + 4321 \) számok sorozatról van szó.

5.3.5 Indirekt tegyük fel, hogy a szóban forgó tizedes tört szakaszos lenne, \( k \) hosszúságú szakasz. Azonban végtelen sok prim van, amelynek az utolsó \( 2k \) jegye 1-es, és olyan prim is végtelen sok van, amelynek az utolsó \( 2k \) jegye 3-as, ezért a szakasznak egyrészt csupa 1-esből, másrészt csupa 3-asból kellene állnia, ami lehetetlen.

5.3.6 A feltétel: \( (a, b, c) = 1 \). A szükségesség nyilvánvaló. Útmutatás az elégségességhez: Legyen \( (a, b) = s \), ekkor \( (a, c) = 1 \). A Dirichlet-tétel alapján van olyan \( k \), amelyre \( a + bk = sp \), ahol \( P \) egy \( c \)-nel nagyobb prim. Ezután alkalmazzuk ismét a Dirichlet-tételt az \( sp + cx \), \( a = 0, 1, \ldots \) számok sorozatra.

5.3.7
(a) Például a \( p = 8 \cdot |k| \cdot k + 1 \) alakú prímekre \( (c^k) = 1 \). Ennek igazolásához felhasználhatjuk \( |k| \) kanonikus alakját és a Legendre-szimbólum (vagy a Jacobi-szimbólum) tulajdonságait. (Gondoljunk arra az esetre is, amikor \( c \) páros és/vagy negatív szám.)

(b) Válassz: \( c \) nem négyzeteszám. — Útmutatás: használjuk fel a 4.3.7b feladatot [112] (vagy az ott láttott megoldás gondolatmenetét).

5.3.8 Legyenek \( p_1, \ldots, p_{n-1} \) különböző prímek. Ekkor alkalmas \( k \) egész számról az
\[ f = x^{a_1} + k(x - p_1) \ldots (x - p_{n-1}) \]
polinom megfelel: \( a_1 = p_1, \ldots, a_{n-1} = p_{n-1}, a_n = 1 \).

5.3.9 Legyenek \( a \) és \( d \) rögzített relatív prim pozitív egészek. Válasszunk olyan \( r \) nemnegatív egész, amelyre \( a_1 = a + r \cdot d \) összetett szám. Ekkor bármely \( s \) pozitív egészre \( (a_1, d^s) = 1 \), és így a feltétel szerint létezik olyan \( k_s \), amelyre \( s = a_1 + k_s \cdot d^s \) prim. Ezek a \( P_s \) prímek valamennyi egyben \( a + k_s \cdot d^s \) alakúak is, és (\( k_s \neq 0 \) miatt) szükségképpen végtelen sok különböző van közöttük.

13.5.4.

5.4.1 Írjuk fel az \( a \) és \( b \) számot \( a = \lfloor a \rfloor + \lfloor a \rfloor \), illetve \( b = \lfloor b \rfloor + \lfloor b \rfloor \) alakban, ahol \( 0 \leq \{ a \}, \{ b \} < 1 \). Ekkor \( a + b = \lfloor a \rfloor + \lfloor b \rfloor + \{ a \} + \{ b \} \). Ha itt az utolsó két tag összege 1-nél kisebb, akkor \( \lfloor a + b \rfloor = \lfloor a \rfloor + \lfloor b \rfloor \), ha pedig 1 és 2 közé esik, akkor \( \lfloor a + b \rfloor = \lfloor a \rfloor + \lfloor b \rfloor + 1 \).

5.4.2 Lássuk be, hogy elég \( x \) egész értékeire szorítkozzunk, majd használjuk fel, hogy csak véges sok olyan pozitív egész van, amely kisebb, mint (az T 5.4.3 Tétel által garantált) \( x^0 \).

5.4.3 Alkalmazzuk az T 5.4.2 Tétel bizonyításához hasonló gondolatmenetet. A \( \pi(p_n) = \gamma_1 \) összefüggésből és a \( \pi(\alpha) \) -re adott felső becslésből azonnal adódik, hogy \( \gamma_1 > \left(1/c_2 \right) \cdot n \cdot \log n \).
EREDMÉNYEK ÉS ÚTMUTATÁSOK

\( \tau \) elég nagy. A másik irányú becslés kicsit bonyolultabb, itt szükségünk van a \( \log_{\mathcal{E}} n < (1 + \varepsilon) \log \tau \)
egyenlőtlenség igazolására is. Eredmény: bármely \( \varepsilon > 0 \) esetén minden ( \( \varepsilon \)-től is függen) elég nagy \( \tau \)-re \( \phi_n < (1/(c+\varepsilon) \cdot n \cdot \log \tau \).

5.4.4 A feladat két része könnyen következik egymásból: az (a) rész a (b) rész logaritmusált változata. Az (a) rész igazolásához támaszkodhatunk a

\[
\log_{\mathcal{E}} \tau_n \cdot \pi({\tau}_n) \geq \sum_{\tau \leq \tau} \log_{\mathcal{E}} \tau \geq \log \int_{\tau} (f(\tau) - f(f(\tau)))
\]
egyenlőtlenségekre, ahol például az \( f(\tau) = \tau^2/(\log \tau)^2 \) választás célhoz vezet.

5.4.5 A (iii) a (iv)-nek logaritmusált alakja. Az (i) \( \Rightarrow \) (ii), illetve (i) \( \Rightarrow \) (iii) következtetés ugyanúgy igazolható, mint az T 5.4.2 Tétel, illetve az 5.4.4 feladat [134]. A megfordításoknál is hasonló gondolatmenetet érdemes követni.

5.4.6

(a) A felső becslés azonnal adódik az \( \hat{S}(n) \leq n \cdot \pi(n) \) összefüggésből és \( \pi(x) \) felső becsléséből.
Az alsó becslés igazolásához induljunk ki az \( \hat{S}(\tau) \geq (\pi(n) - \pi(\tau)) \cdot (n-\tau) \) egyenlőtlenségből, ahol \( 0 < c < 1 \), és a primszámtétel segítségével mutassuk meg, hogy található olyan \( \epsilon' > 0 \), amelyre \( \pi(x) - \pi(\tau_1) > \epsilon' \cdot n/(\log \tau) \).

(b) A \( \hat{S}(n) \sim n \cdot \log \log k \) összefüggés alapján mutassuk meg, hogy

\[
\hat{S}(\tau) \sim \sum_{k=\tau}^{n(\tau)} k \log \log k \sim \int_{\tau}^{n(\tau)} t \log t dt.
\]

Használjuk fel, hogy

\[
\int t \log t dt = \frac{2t^2 \log t - t^2}{4} \quad \text{és} \quad \pi(\tau) \sim \frac{n}{\log \tau}.
\]

5.4.7 Használjuk fel, hogy egy adott \( \mathcal{N} \)-ig „sok” prímszám van, és így ezekből sok kétszárú összeg, illetve különbség képezhető, ugyanakkor az így keletkező páros számok „kevesen” vannak, ezért a skatulyaelv alapján legalább az egyik páros szám sokfélekeppen áll elő ilyen összegként, illetve különbségként.

Nézzük mindezt részletesebben az összegekre, a különbségek is hasonlóan tárgyalhatók. Bármely két, \( \mathcal{N} \)-nél nem nagyobb páratlan prímszám összege egy \( 2\mathcal{N} \)-nél nem nagyobb páros számnak. Az ilyen összegek száma

\[
\left( \pi(N) - 1 + 1 \right) \sim \frac{N^2}{2(\log N)^2}
\]
a \( 2\mathcal{N} \)-nél nem nagyobb páros számok száma pedig \( \mathcal{N} \). Ezért (elég nagy \( \mathcal{N} \) esetén) van olyan páros szám, amely legalább

\[
\frac{\mathcal{N}}{3(\log N)^2} > K
\]
-félelekeppen áll elő két prímszám összegeként.
5.4.8 A képlet alapja a Wilson-tétel és a megfordítása: $j > 1$ esetén $j \mid (j-1)! + 1 \iff j \text{ prim.}$
— A $\pi(n)$ gyakorlati kiszámítására ez a formula nem használható, mert már a faktoriálisok, illetve ezek osztási maradékaiknak meghatározására sem ismerünk gyors algoritmust.

13.5.5.

5.5.1 Használjuk fel a Csebisev-tételt.

5.5.2 Írjuk fel a nagyobbik számtartomány $n = p + (n − p)$ alakban, ahol $p$ a legnagyobb prim $n$ -ig, majd ismételjük meg ugyanezt $n$ helyett $n − p$ -vel stb. Az eljárás addig folytatódik, amíg a "maradék" 0 vagy 1 lesz. Az $n$ -et vagy $n − 1$ -et ily módon előállító prímek a Csebisev-tétel alapján mind különbözők.

5.5.3

(a) Az 1-es számjeggyel kezdődő $k + 1$-jegyű számok $10^k \leq n < 2 \cdot 10^k$ alakúak, és ezek között a Csebisev-tétel szerint minden $k$ -ra található prím szám.

(b) A Csebisev-tétel helyett támaszkodjunk az T 5.5.5 Tétel (A) részére.

5.5.4

(a) Legyen $P$ olyan prim, amelyre $n/2 < p \leq n$. A törteket közös nevezőre hozva a közös nevező is, és pontosan egy tag kivételével az összes számláló is osztható $P$-vel. Ezért az összeg nem lehet egész (csak olyan törtként írható fel, amelynek a nevezője osztható $P$-vel). — Az állítás bizonyítható a Csebisev-tétel felhasználása nélkül is, ha az $\Pi_{k=1}^n (k, 2, \ldots, n)$ közös nevezőben és az így adódó számlálókban a 2 kitevőjét vizsgáljuk.

(b) Ha $n > 2k, 1$ , akkor az (a) részre adott (bármelyik) bizonyítás átvihető. Ha $n < 2k, 1$ , akkor az összeg kisebb, mint 1.

5.5.5 Mivel $\binom{2n}{k} = \binom{2n}{2n-k}$, ezért feltehető, hogy $k < n$. Ekkor

$$\binom{2n}{k} = \frac{(2n)!}{k! \cdot (n + 1)!}.$$ 

A jobb oldali törtnél a számláló és a nevező is $n-k$ darab tényező szorzata, és a számláló bármely tényezője nagyobb, mint a nevező bármely tényezője. Ennél fogva a tört nagyobb, mint 1.

5.5.6 A modulusok páronként relatív prímek, ezért a kongruenciarendszer megoldható. A megoldások egy redukált maradékosztályt alkotnak modulo $\Pi = p_1 \cdot p_2 \cdot \ldots$ , amelyben a Dirichlet-tétel szerint található (végint sok) $p \leq m$ prim szám. A kongruenciarendszer konstrukciójának megfelelően $p \mid j$ osztható $Pj$ -vel, $p \nmid j$ pedig $q_i$ -vel, továbbá $p \mid j \leq p_i$ , $p \nmid j \geq q_i$ , tehát valamennyi $p \pm j$ összetett szám.

5.5.7

(a) $\binom{2n}{n}$ számlálójának a $P$ az egyik tényezője, viszont a nevező és a számláló többi tényezője nem osztható $P$-vel.

(b) Mind a számláló, mind a nevező a $P$-nek pontosan a második hatványával osztható (a számlálóban a $p^2$ és $4p$ , a nevezőben a $p$ és $2p$ tényezőkben szerepel a $P$). — Általánossítás: Ha $2n/(2k + 1) < p \leq n/k$ és $p > 2k$ , akkor $\binom{2n}{n}$ nem osztható $P$-vel.
5.5.8 Jelöljük $L$-lel az $u$ és $2u$ közötti primerek számát. Az T 5.5.3 Tétel bizonyításában szereplő $C$ az 5.5.7a feladat szerint a $u$ és $2u$ közötti primerek szorzata, ennél nagyobb $C < (2u)^L$. Másrészt a bizonyításban szereplő (6) egyenlőségből elég nagy $u$-re $C > 4^{\alpha_5/4}$ következik, hiszen az ottani (7) jobb oldalán szereplő különbségi kivonandó elhanyagolható a kisebbitendőhöz képest. A $C$-re most felért két egyenlőségből kapjuk, hogy $4^{\alpha_5/4} < (2u)^L$, ahonnan logaritmalással adódik a feladat állítása elég nagy $u$-re, majd az 5.4.2 feladat mintájára minden $u \geq 2$-re.

5.5.9

(a) Használjuk fel, hogy elég nagy $u$ esetén az $(u,n + u^{2/3})$ intervallum tartalmaz prímszámot.

(b) A $\theta_n = |\alpha\nu|^{\nu}$ feltétel ekvivalens

$$\sqrt[\nu]{\theta_n} \leq \alpha < \sqrt[\nu]{\theta_n} + 1 \tag{1}$$

teljesülésével. Válasszuk meg a $\theta_n$ priméket rendre úgy, hogy (1) azt jelentse, hogy $\alpha$ egy egymáshoz skatulyázott intervallumsorozat minden intervallumának eleme. Ez megtető, mert az egymásba skatulyázottsga ekvivalens $\theta_n^{1/\nu} \leq \theta_{n+1} < (\theta_n + 1)^{1/\nu} - 1$ egyenlőséggel.

(c) A (b)-beli képletben $\nu$ pontos értéke nem ismert, csak $\alpha$ létezését tudtuk igazolni.

5.5.10

(a) Az T 5.5.5 Tétel (B) részének bizonyítását követve azt kapjuk, hogy alkalmas $c > 0$ mellett az $(u,n + c \log n)$ intervallum végétlen sok $u$-ra nem tartalmaz prímszámot.

(b) Az T 5.5.1 Tétel bizonyítása szerint $u = (K + 1)! + 1$ esetén az $(u,n + K)$ intervallum prímszámos. Fejezzük ki a $K$-t az $n$ segítségével. Ehhez használjuk fel az $m!$-ra vonatkozó alábbi becsléseket:

$$\left(\frac{m}{e} \right)^m < m! \leq m^m.$$ (A felső becslés nyilvánvaló, az alsó becslés pedig könnyen igazolható teljes indukcióval.) Ezeket az egyenlőségeket (vagy a Stirling-formulát) logaritmalával $\log m! \sim m \log m$ adódik. A jelen esetben ez azt jelenti, hogy $\log \nu \sim K \log K$, ahonnan azt nyerjük, hogy $K \sim \nu \log \nu/\log \log \nu$.

Ezzel azt igazoltuk, hogy bármely $\varepsilon > 0$ esetén végétlen sok olyan $n$: pozitív egész létezik, amelyre az $(n, n + (1 - \varepsilon) \log n/\log \log n)$ intervallum nem tartalmaz prímszámot.

(c) A jelzett megfigyelés szerint, ha $u - 1$ a $K + 1$-nél nem nagyobb primek szorozata, akkor az $(u,n + K)$ intervallum prímszámos. Az L 5.4.5 Lemma szerint $u \leq 4^{K + 1}$, az 5.4.4b feladat [134] szerint pedig $u < c^{(1 + \varepsilon)K + 1}$ is igaz (ez utóbbihoz felhasználtuk a prímszámüket). Innen $K > c \log \nu$ adódik, vagyis az (a)-beli eredményt kapjuk, illetve az élesebb becslést felhasználva az T 5.5.5 Tétel (B) részének állítása adódik.

5.5.11 Alkalmazzuk az T 5.5.5 Tétel (B) részének bizonyításához hasonló gondolatmenetet (természetesen most fordított irányú egyenlőségekről van szó). Az egyetlen lényeges eltérést az jelenti, hogy $\nu < N$ miatt $\log \nu < \log N$ nem teljesül (erre az (15) megfeleléjénél lenne szükség). Ezen például az alábbi módon segíthetünk: Ha $N > p_1 > N/(\log N)^2$, akkor elég nagy $N$-re
\[ \log p_i > (1 - \varepsilon') \log N \]. Ezért a (13)-nak megfelelő egyenlőtlenségeket ezekre a primekre érdemes felírni és összegezni.

13.5.6.

5.6.1 Divergens: (a), (c), (e).

Az egyes sorozatokat jelölje rendre \( A, B, \ldots, F \), az \( n \) -nél nem nagyobb elemek számát pedig rendre \( A(n), B(n), \ldots, F(n) \). Ekkor
\[
A(n) \sim c_1 \eta; \quad B(n) \sim \sqrt{n}; \quad E(n) \sim c_2 \eta; \quad F(n) \sim c_3 \sqrt{n},
\]
ahol a \( c_i \) -k alkalmas pozitív konstansok (amelyek a \( c_3 \) kivételével függnek \( L \) -től). A \( D \) sorozatra
\[
D(n) \sim c_4 (\log n)^k
\]
teljesül, ahol \( k \) az \( L \) -nél kisebb primek száma; itt lényegesen egyszerűbb annak a gyengébb eredménynek az igazolása, hogy
\[
c_5 (\log n)^k < D(n) < c_6 (\log n)^k.
\]

5.6.2 Csak (c) divergens. — A megfelelő integrálók:
(a) \[ \int \frac{dx}{x \log x} = \frac{\log \log x}{\log x} ; \]
(b) \[ \int \frac{dx}{x \log (\log x)^2} = \frac{1}{\log x} ; \]
(c) \[ \int \frac{dx}{\log x \log (\log x)^2} = \log \log \log x . \]

5.6.3 Divergens: (b). — Az T 5.6.1 Tétel első bizonyításához hasonló gondolatmenetet érdemes alkalmazni.

5.6.4

(a) Konvergens: rendezzük át a számokat a legkisebb prímosztóik szerint (ezek a feltétel szerint mind különbözők), ekkor \( u_n \geq \frac{n^2}{\ln n} \), tehát
\[
\sum_{n=1}^{\infty} \frac{1}{\omega_n} < \sum_{n=1}^{\infty} \frac{1}{n^2} < \infty.
\]

(b) Konvergens: A feltétel alapján \( u_n \geq \frac{2^{\omega_n - 2}}{\omega_n} = n^{2^{\omega_n - 2}} \). Mivel \( \alpha = 2 \log 2 > 1 \), ezért
\[
\sum_{n=1}^{\infty} \frac{1}{\omega_n} < \sum_{n=1}^{\infty} \frac{1}{n^\alpha} < \infty.
\]

(c) Divergens: elég nagy \( u \) -re \( u_n < e^v \), ahol \( c = 10^{100} \).

(d) Lehet konvergens, és lehet divergens.

(e) Konvergens: Rendezzük át a számokat az osztóik száma szerint, ekkor a feltétel szerint \( d(\omega_n) \geq n \)
. Az 1.6.11c feladat [28] alapján ebből \( \omega_n \leq \sqrt[n]{\log n} \), azaz \( u_n \geq n^{2}/4 \) következik. Ezután használjuk fel, hogy a négyzetszámok reciprokösszege konvergens.
5.6.5 Nem érdemes; az összeg nagyságát aránytalanul befolyásolhatja az első néhány tag. Például, ha a kőbszámokhoz hozzávesszük a 2-t és a 3-at, akkor a reciprokösszeg már nagyobb lesz a négyzetszámok reciprokösszegénél, ugyanakkor a kőbszámok lényegesen gyorsabban nőnek, mint a négyzetszámok, tehát a kőbszámok(nak a 2-vel és a 3-mal kibővített) sorozata ritkább a négyzetszámokénél.

5.6.6 Az T 5.6.1 Tétel harmadik bizonyításához hasonló gondolatmenetet érdemes alkalmazni.

5.6.7 Ha az \(a_j\) sorozat nem tart 0-hoz, akkor könnyen adódik, hogy a végteles sor divergens, a végteles sorozat pedig 0. Ezért a továbbiakban feltehetjük, hogy az \(a_j\) sorozat 0-hoz tart. A végteles sorozat logaritmusát véve kapjuk, hogy

\[
\prod_{j=1}^{\infty} (1 - a_j) = 0 \iff \sum_{j=1}^{\infty} - \log(1 - a_j) = \infty.
\]

Használjuk fel, hogy \(0 < a_j < 1/2\) esetén \(a_j < -\log(1 - a_j) < 2a_j\).

5.6.8 A bizonyítandó egyenlőtlenséggel ekvivalens, ha a két oldal logaritmusára igazoljuk a megfelelő egyenlőtlenséget. Ehhez használjuk fel az T 5.6.2 Tételt és azt, hogy \(0 < 2 < 1/2\) esetén \(- \log(1 - a)\) jól közelíthető \(a\) -val.

5.6.9
(a) Divergens: az \(n = 2p\) alakú számokra \(u_p''(i) = 4p\), és már a \(\sum_{p=1}^{\infty} 1/(4p)\) sor is divergens.

(b) Konvergens. — Legyen \(q\) rögzített prímszám és \(S_q\) azon \(n\) egészek reciprokösszege, amelyekre \(P(q) = q\). Mutassuk meg, hogy

\[
S_q = \frac{1}{e} \prod_{p \leq q} \frac{1}{1 - \frac{1}{p}}.
\]

Az 5.6.8 feladat [150] alapján ekkor \(S_q < e^{(\log q)/q}\). Innen kapjuk, hogy

\[
\sum_{n=2}^{\infty} \frac{1}{n P(n)} = \sum_q S_q < e \sum_{q} \frac{\log q}{q^2} < \infty.
\]

13.5.7.

5.7.1
(a) Az algoritmusban szerepel az \(r_k = r_{k-1} q_k + 2 \uparrow r_{k-2}\) lépés. Itt a jobb oldal első tagjában szereplő szorzatot \(r_{k+1} \geq r_{k+2}\ és \(r_k \geq 1\) felhasználásával csökkentve a kívánt \(r_k > 2r_{k+2}\) egyenlőtlenség adódik.

(b) \(2 \log_2 b\).

(c) A legkisebb \(b\) -hez akkor jutunk, ha \((a, b) = r_{s-1} = 1\ és a \(q_i\) hányadosok a lehető legkisebbek, azaz \(q_s = 2\), a többi \(q_i\) pedig 1. Ekkor az algoritmus egyenlőségei a végéről kezdve a következő alakot öltik:

\[
r_{s-1} = 1, r_{s-2} = 2, r_{s-3} = r_{s-2} + r_{s-1}, \ldots, b = r_1 + r_2,
\]

ahonnan a Fibonacci-számok képzési szabálya szerint \(r_{j+1} = \varphi_{j+1}\), és \(b = \varphi_k + 1\).
Az eljárás során a „számláló” és a „nevező” legnagyobb közös osztója nem változik (még a „számláló” felezésekor sem, hiszen a „nevező” és így a legnagyobb közös osztó is páratlan). Az eljárás euklideszi algoritmus jellege miatt végül el kell jutnunk \( d \)-hez. Ez a \( d \) érték a „számlálóba” kerül, hiszen az egységes lépések végén ott jelennek meg az új számok. Ekkor a \( v ", nevezőre" \( (d, v) = (a, b) = d \) teljesül, tehát \( d \mid v \).

5.7.3 \( 341 = 11 \cdot 31 \). Ekkor

\[
\varphi(11) \mid 340 \Rightarrow 2^{340} \equiv 1 \pmod{11}, \quad \text{és} \quad 2^5 \equiv 1 \pmod{31} \Rightarrow 2^{340} \equiv 1 \pmod{31}.
\]

Ebből következik, hogy \( 2^{340} \equiv 1 \pmod{11 \cdot 31} \), vagyis a 341 kettes alapú álprím. Ugyanakkor

\[
3^{340} \equiv 3^{10} \not\equiv 1 \pmod{31} \Rightarrow 3^{510} \not\equiv 1 \pmod{31},
\]

tehát a 341 nem hármas alapú álprím.

5.7.5 Mivel \( p \) páratlan, ezért

\[
a = \frac{a^p - 1}{a - 1} \cdot \frac{a^p + 1}{a + 1} = (a^{p-1} + a^{p-2} + \cdots + 1)(a^{p-1} - a^{p-2} - \cdots + 1),
\]

ahonnan kapjuk, hogy \( n \) páratlan és összetett. Az \( 9^{n-1} \equiv 1 \pmod{n} \) kongruencia abból következik, hogy \( a^{2^p} \equiv 1 \pmod{n} \) és \( n \equiv 1 \pmod{2^p} \); ez utóbbi az \( n(a^2 - 1) = a^{2^p} - 1 \) egyenlőség modulo \( p \) vizsgálatából és \( n \) páratlanságából adódik.

5.7.6 \( 561 = 3 \cdot 11 \cdot 17 \). Így \( (a, 561) = 1 \Rightarrow a^{560} = 1 \pmod{561} \) igazolásához elég belátni a kongruencia fennállását a 3, a 11 és a 17 modulusokra, ez pedig a kis Fermat-tétel felhasználásával könnyen adódik.

5.7.7 (a) \( \Rightarrow \) (b): Ha \( n \) nem négyzetmentes, akkor az T 5.7.4 Tétel bizonyításának idevágó részét követte (de az ottani (2) képletet értelmszerűen kihagyva) ellentmondásra jutunk. Ha \( p \mid \sigma \), akkor végünk egy olyan \( \vartheta \) primitív gyököt mod \( p \), amely relatív prím \( n \) -hez (ez utóbbi feltétel teljesülését az T 5.7.4 Tétel bizonyításában többször alkalmazott szimultán kongruenciarendszeres eljárással biztosíthatjuk). Ekkor

\[
(g, \nu) = 1 \Rightarrow g^{n-1} \equiv 1 \pmod{n} \Rightarrow g^{\frac{n-1}{p}} - 1 \equiv 1 \pmod{p} \Rightarrow a_p(g) = p - 1 \mid \nu - 1.
\]

(b) \( \Rightarrow \) (c): Mivel \( n \) négyzetmentes, ezért elég az \( n \) minden \( p \) prímosztójára igazolni az \( a^n \equiv c \pmod{p} \) kongruenciát. Ha \( p \mid c \), akkor ez nyilvánvalóan teljesül, ha pedig \( (p, a) = 1 \), akkor a kis Fermat-tétel és \( p - 1 \mid n - 1 \) alapján \( a^{n-1} \equiv 1 \pmod{p} \), amiből a bizonyítandó kongruencia \( a^n \)-val való szorzással adódik.

(c) \( \Rightarrow \) (a): Ha \( (a, n) = 1 \), akkor az \( a^n \equiv c \pmod{n} \) kongruenciát \( c \)-val egyszerűsítve kapjuk, hogy \( a^{n-1} \equiv 1 \pmod{n} \).

5.7.8 Használjuk fel az 5.7.7 feladat [160] (b) feltételét.

5.7.9
(a) Ha véletlenül \( 1 < (\nu, n) < \tau \) adódik, akkor ezzel nemcsak \( n \) összetettségét igazoltuk, hanem sikerült az \( n \) egy nemtriviális osztóját is előállítanunk. (Ennek azonban igen kicsi az esélye, lásd a (b) részt.)

(b) Nagyjából \( 10^{-100} \).

5.7.10 Ekkor \((u - 1, \tau)\) [illetve \((u + 1, n)\)] egy nemtriviális osztó.

5.7.11 Először egy primeszettel megállapítjuk, hogy az \( n \) prim-e. Nyilván elég azzal az esettel foglalkoznunk, amikor \( n \) páratlan összetett szám.

Először egy gyors algoritmusmal meg tudjuk állapítani, hogy \( n \) teljes hatvány-e: megvizsgáljuk, hogy \( \sqrt[n]{n} \) egész szám-e, ahol \( 2 \leq k \leq \log_2 n \). Ha \( n = m^k \), akkor elég \( nk \)-et faktorizálnunk. A feladat feltétele \( m \)-re is teljesül, hiszen \( \varphi(m) \) \( \varphi(n) \) miatt a \( \varphi(n) \) általunk ismert többszöröse a \( \varphi(n) \)-nek is többszöröse. Így a továbbiakban feltehetjük, hogy az \( n \) nem teljes hatvány.

Válasszunk (mondjuk) 1000 véletlen \( \tau \)-et értéket, és számítsuk ki \((a, \tau)\)-et. Ha \((u, n) > 1\), akkor az 5.7.9 feladat [160] alapján az \( n \)-et két nemtriviális osztója szorzatára tudjuk bontani.

5.7.12 Nem alkalmas, ugyanis nem ismerünk gyors algoritmust a faktoriálisok, illetve ezek osztási maradékainak meghatározására.

5.7.13
(a) Kövessük az 5.7.4 Tétel bizonyításának azt a részét, amikor azt igazoltuk, hogy ha van tanú, akkor legalább annyi tanú van, mint cinkos.

(b) Legyen \( u > 1 \) páratlan szám. Válasszunk (mondjuk) 1000 véletlen \( \nu \neq 0 \) \((m \geq n)\) értéket, és mindegyikre vizsgáljuk meg, hogy \( a^{n-1} \equiv 1 \mod n \) teljesül-e. Ha legalább egy esetben nem teljesül, akkor az \( u \) biztosan összetett. Ha mind az 1000 esetben teljesül, akkor \( 2^{-1000} \)-nel kisebb annak a valószínűsége, hogy az \( n \) nem prim és nem univerzális álprím.

5.7.14 Jelölje \( R \) a kipróbált \( u \)-k számát. Ha \( u \) prim, akkor mindig \( \pm 1 \) maradéket kapunk, és \( 2^{-R} \) a valószínűsége annak, hogy minden maradék 1. (Ennél a tesztmél tehát a „másik irányban” is tévedhetünk, azaz egy primet is tévesen összetett számmnak vélnénk.) Ha \( u \) összetett, akkor az 5.7.4 és 5.7.5 Tételek bizonyításához hasonlóan járhatunk el.
5.7.15 Módosítsuk értelemszerűen az 5.2.3 feladat [124] útmutatásánál szereplő gondolatmenetet.

5.7.16

(a) Lássuk be, hogy \( \alpha_i(a) = n - 1 \).

(b) Legyen \( n - 1 \) kanonikus alakja

\[
n - 1 = p_1^{\hat{a}_1} \ldots p_r^{\hat{a}_r}.
\]

A feltétel alapján \( p_i^{\hat{a}_i} \mid \alpha_i(a_i) \). Ekkor (pl. a 3.2.4c feladat [75] szerint) léteznek olyan \( b_i \) számok, amelyekre \( \alpha_i(b_i) = p_i^{\hat{a}_i} \), ahonnan a 3.2.15a feladat [76] alapján kapjuk, hogy \( \alpha_i(b_1 \ldots b_r) = n - 1 \).

(c) Tegyük fel indirekt, hogy \( n \) összetett, ekkor létezik egy \( q \leq \sqrt{n} \) prímosztója. Ezután ismételjük meg a (b) rész gondolatmenetét az \( n \) helyett a \( q \) modulusra. Azt kapjuk, hogy van olyan \( b \), amelyre \( \alpha_i(b) = c > \sqrt{n} \), ami ellentmondás.

5.7.17 Azt kell igazolni, hogy ha egy \( a \) -ra jó sorozatot kapunk, akkor

\[
a^{(n-1)/2} \equiv \left( \frac{a}{n} \right)(n) \quad (*)
\]

is teljesül.

Ha \( a^r = 1 \mod{n} \), akkor könnyen adódik, hogy (*) mindkét oldalán 1 áll.

Rátérve az \( a^{2^r} \equiv -1 \mod{n} \) esetére, az \( a^{(n-1)/2} \) maradékának a meghatározása most sem jelent nehézséget. Ezután mutassuk meg, hogy ha \( q \) az \( n \) prímosztója, akkor \( \alpha_q(a) \) a \( 2^{j+1} \) -nek pártalan többszöröse, és így \( 2^{j+1} \mid q - 1 \) is teljesül. Ezek alapján bizonyítsuk be, hogy \( \left( \frac{a}{q} \right) \) értéke \( (a - 1)/2^{j+1} \) paritásától függ, majd az \( n \) kanonikus alakjának segítségével írjuk fel \( \left( \frac{a}{q} \right) \) értékét.

Végül, ha az \( n \) kanonikus alakjában a \( q \) primek helyére beírjuk a \( 2^{j+1} \mid q - 1 \) feltételből adódó alakot, akkor a beszorzást elvégezve és egy alkalmas kettőhatvány szerinti oszthatóságot vizsgálva megkapjuk, hogy \( \left( \frac{a}{q} \right) \) valóban a (*)-nak megfelelő értéket veszi fel.

13.5.8.

5.8.1 Ekkor ez egy aláírás nélküli, névtelen levél, amelyet akár egy harmadik fél is hamisíthatott \( A \) nevében.

5.8.2 \( T\)- invertálhatósága azt jelenti, hogy az \( e^r = \varepsilon \mod{N} \) kongruenciának bármely \( s \) esetén ( \( r \)-ben) pontosan egy megoldása van. Ez a kongruencia ekvivalens az

\[
e^r = \varepsilon \mod{p_i}, \quad r^s = s \mod{q} \quad (1)
\]

szimultan kongruenciarendszerrel. Az (1)-beli két kongruenciának a 3.5.7 feladat [90] szerint akkor és csak akkor van minden \( s \) -re pontosan egy megoldása, ha \( (s, p - 1) = (t, q - 1) = 1 \), azaz ha \( (s, \varphi(N)) = 1 \).

5.8.3
(a) Elég megmutatni, hogy a szóban forgó kongruencia mod \( P \) és mod \( Q \) is fennáll. Nézzük például mod \( P \) . Ha \( P \mid r \), akkor mindkét oldal 0-val kongruens, ha pedig \((p,r) = 1\), akkor

\[ r^{1+k \phi(N)} \equiv r^{(q-1)} \equiv r \pmod{p}, \]

(b) \( y \equiv 1 \pmod{p-1,q-1} \).

5.8.4 Nem okoz gondot, hiszen csak azt használjuk fel, hogy az \( r^P \equiv r \pmod{\phi(N)} \) kongruencia minden \( r = \text{mod} \) -rel teljesül (lásd az 5.8.3a feladatot [164]). Természetesen ekkor a \( \phi(N) \)-nek vélt \((p-1)(q-1)\) szorzat valójában nem \( \phi(N) \).

5.8.5 Legyen \( s \equiv r^t \pmod{N} \), ahol \( s \) és \( t \) ismert, és \( r \) értékét szeretnénk meghatározni. Emeljük \( s \)-et a \( t \)-edik hatványra, majd az eredményt megint a \( t \)-edik hatványra stb., amíg ismét \( s \)-sel kongruens számot nem kapunk:

\[ s^{k \cdot t} \equiv s \pmod{N}. \quad (2) \]

Mivel \((t,\phi(N)) = 1\), ezért az 5.8.2 feladat [164] szerint a (2) kongruenciából lehet \( t \)-edik gyököt vonni, azaz

\[ s^{k \cdot t} \equiv r \pmod{N}. \]

Ez azt jelenti, hogy ha (2) elég kis \( k \)-ra bekövetkezik, akkor \( r \)-et meg tudjuk határozni. Ha \( \frac{1}{t} \equiv 1 \pmod{\phi(N)} \), akkor az 5.8.3a feladat [164] szerint (2) biztosan teljesül, ezért nem szabad, hogy a \( t \) modulo \( \phi(N) \) vett rendje kicsi legyen.

5.8.6 Az \( A \), illetve \( B \) a

\[ a b \equiv (a b) \equiv (a b) \pmod{N}. \]

egyenlőségek alapján tudja a megadott értéket kiszámítani. Más ezt (remélhetőleg) nem tudja megcsinálni, hiszen nem ismeri \( \hat{k}_A \) és \( \hat{k}_B \) egyikét sem.

5.8.7 (a) Tegyük fel indirekt, hogy két részösszeg egyenlő. A közös tagokat kiejtve elérhetjük, hogy a két összegben együttvéve is csupa különböző tag szerepeljen. Ekkor az előforduló legnagyobb tag a (6) feltétel szerint egymában is nagyobb már, mint a teljes másik összeg, ami ellentmondás.

(b) Tegyük fel indirekt, hogy bizonyos \( a_i \)-kre és \( d_j \)-kre \( \sum a_i = \sum d_j \). Ekkor (7) alapján \( \sum a_i = \sum d_j \pmod{m} \). Az \((t,m) = 1\) feltétel miatt \( r \)-rel egyszerűsíthetünk, azaz \( \sum c_i = \sum d_j \pmod{m} \). Végül, mivel \( m > \sum_{i=0}^{n-1} c_i \), ezért a kongruencia helyett egyenlőség is írható, ami ellentmond \( C \) összeginjektivitásának.

(c) Közvetlenül következik az összeginjektivitás definíciójából.

(d) Az \( u \) előállításához a \( d_t \) értékekre van szükség, vagyis arra, hogy a megadott \( u \) az összeginjektív sorozat mely tagjainak az összege. A (6) sorozatnál ehhez alkalmazzuk a mahó algoritmust, azaz vegyük mindig a lehető legnagyobb \( c_i \)-t. A (7) sorozatnál az \( r \equiv c_i \pmod{m} \) kongruenciák legkisebb pozitív megoldásai megadják a \( c_i \)-ket és a megfelelő \( c' \)-t, amelyekre már alkalmazhatjuk az előző eljárást.
13.6 Számelméleti függvények

13.6.1.

6.1.1 A multiplikativitás igazolásához alkalmazzuk a $d(n)$ függvény képletét (T 1.6.3 Tétel), vagy használjuk fel az 1.6.5a-b feladatot [28]. A teljes multiplikativitás cáfolásához elég egyetlen olyan $c$, $b$ számpár, amelyre $d(ab) \neq d(a)d(b)$ és $(a,b) \neq 1$.

6.1.2 (a), (c) $f(n)$ és $\hat{h}(n)$ se nem additív, se nem multiplikativ.

(b) $g(n)$ teljesen multiplikativ.

(d) $k(n)$ additív, de nem teljesen additív.

6.1.3 Multiplikatív $h$ nem létezik. A feltételek alapján

$$0 = h(6) = h(2)h(3) \Rightarrow h(10)h(15) = h(2)h(5)h(3)h(5) = 0 \neq 3.$$  

Additív, sőt teljesen additív $h$ viszont végzetesen sok létezik. A feltételekből adódó

$$0 = h(2) + h(3), \quad 1 = h(2) + h(5), \quad 3 = h(3) + h(5).$$

egyenletrendszer megoldva kapjuk, hogy $h(2) = -1$, $h(3) = 1$ és $h(5) = 2$. Válasszuk $h(7)$ értékét egy $c$ paraméternek, a többi $P$ prímre pedig legyen $h(p) = 0$, ekkor egyértelműen meghatározható a $h$ teljesen additív függvény, amely ezeket a feltételeket kielégíti: Ha

$$n = 2^α \cdot 3^β \cdot 5^γ \cdot 7^ω + t, \quad a_{11} (t, 210) = 1 \quad \text{és} \quad α, β, γ ≥ 0, t = 1, 2, 3, 4,$$

akkor

$$h(n) = -α_1 + α_2 + 2α_3 + α_4.$$  

6.1.4 Ha van ilyen $f \neq 0$ multiplikatív függvény, akkor a T 6.1.6 Tétel szerint $f(1) = 1$, és ha az $u$ kanonikus alakjában szereplő primhatványok $q_j, \ldots, q_w$, akkor a T 6.1.7 Tétel alapján csak $f(u) = c_j \cdot \ldots \cdot c_w$ lehetséges. Az ily módon a $c_j$ -k segítségével definíált függvényről mutassuk meg, hogy valóban multiplikatív. Az additív esetben és a (b) résznél is hasonlóan kell eljarni.

6.1.5 Igaz: (a), (d).

6.1.6 (a) A szükséges és elégséges feltétel $f(k) = 0$.

(b) Most is $f(k) = 0$ a szükséges és elégséges feltétel. Az elégségesség bizonyításához vegyük $a$, $b$ és $k$ kanonikus alakját, és a T 6.1.7 Tétel alapján írjuk fel $g(a) = f(ka)$, $g(b) = f(kb)$ és $g(ab) = f(ka'b)$ értékét. Használjuk fel, hogy $(a,b) = 1$ miatt a $k$ bármely prímösztőja az $a$ és $b$ közül legfeljebb az egyiket oszta.
EREDMÉNYEK ÉS ÚTMUTATÁSOK

(c) A teljesen multiplikatív esetben \( f(k) = 1 \) vagy 0 a szükséges és elégéges feltétel. A multiplikatív esetben ez csak szükséges, de nem elégéges: legyen például

\[
f(n) = \begin{cases} 0, & \text{ha } n \equiv 4 \pmod{8}; \\ 1, & \text{egyébként}, \end{cases}
\]

ekkor \( f(k) = 0 \), de \( g \) nem multiplikatív, pl. \( g(3)g(2) = 0 \neq 1 = g(6) \). Szükséges és elégéges feltétel: \( f(k) = 1 \) vagy \( f(kn) = 0 \) minden \( n \) -re (ez utóbbi a \( g = 0 \) függvényt jelenti).

6.1.7

(a) Használjuk fel az \( ab = (a, b)[a, b] \) összefüggést.

(b) Használjuk fel a számok kanonikus alakját.

(c) Azok az \( f \)-ek, amelyek előállnak egy additív és egy konstans függvény összegeként.

(d) A szóban forgó egyenlőséget a multiplikatív függvények konstansszorosai mindig kielégítik. Ha feltevésünk, hogy \( f(1) \neq 0 \), akkor ezek adják az összes megoldást. Az általános esetben az összes megoldást az alábbi függvények szolgáltatják:

\[
f(n) = \begin{cases} 0, & \text{la } K \nmid n; \\ \text{egyenlet}, & \text{la } K \mid n, \end{cases}
\]

ahol \( g(x) \) multiplikatív, \( c \) konstans és \( K \) rögzített pozitív egész.

6.1.8 Az állítás a multiplikativitás és additivitás definíciójának közvetlen következménye.

6.1.9

(a), (e) Azonnal következik a definíciókból.

(b)–(d) Először mutassuk meg, hogy az \( f \) szorzat akkor és csak akkor teljesen additív, illetve additív, ha \( f(a)g(b) + f(b)g(a) = 0 \) minden \( a, b \) , illetve minden relatív prim \( a, b \) esetén teljesül. — Válasz (d)-re: Ha \( f \neq 0 \) és \( g \neq 0 \), akkor \( f \) és \( g \) egy vagy két prim hatványaitól eltérő értéked minden primhatvány helyen 0, és a második esetben az adott két prim hatványain felvett függvényértékekre is szoros szabályszerűség érvényes.

(f) Következik a T 6.1.6 Tételből.

6.1.10

(a) Közvetlenül következik a definíciókból.

(b) A feltétel átalakítható az \( \left( f(c) - g(a) \right) \left( f(b) - g(b) \right) = 0 \) egyenlőségére. A multiplikatív esetben a két függvény egy \( P \) prim hatványain esetleg eltérő értékű lehet, minden más primhatvány helyen viszont azonos értéket kell felvenniük.

6.1.11 Ha \( f = 0 \), akkor a feltétel alapján \( g = 0 \) is igaz, és az állítás triviálisan teljesül. Egyébként az 1 helyen felvett függvényértékek alapján a két függvény összege csak az 1 konstans lehet. Az \( f = 1 - g \) függvényre a multiplikativitást felirva a \( g \) additivitása alapján az adódik, hogy \( (a, b) = 1 \) esetén \( g(a)g(b) = 0 \). Ebből következik, hogy esetleg egy \( P \) prim hatványaitól eltérő értéke minden primhatvány helyen a \( g \) értéke 0, az \( f \) értéke pedig 1, és így \( P \nmid n \) esetén \( g(n) = 0 \) és \( f(n) = 1 \).
Innen azonnal adódik, hogy $P \not| \tau$ esetén $\left( f^{1000} + g^{1000} \right)(\tau) = 1 \implies \left( f^{1000} \right)(\tau) = 0$, amiből a kívánt multiplicatívitás, illetve additivitás könnyen leolvasható.

6.1.12 A 6.1.9d feladat [170] megoldásához hasonló gondolatmenetet érdemes alkalmazni. Most a következő egyenlőségekből lehet kiindulni:

(a) Ha $\hat{\nu} = f - g$, ahol $f$ és $g$ multiplikatív, akkor bármely $(a, b) = 1$ esetén

$$\left( f(a) - 1 \right) \left( f(b) - 1 \right) = \left( g(a) - 1 \right) \left( g(b) - 1 \right).$$

(b) Ha $\hat{\nu} = f \sigma$, ahol $f$ multiplikatív és $\sigma$ additív, akkor bármely $(a, b) = 1$ esetén

$$f(a)g(c) \left( f(b) - 1 \right) = f(b)g(b) \left( f(a) - 1 \right) = 0.$$

6.1.13

(a) Mutassuk meg, hogy végtelen sok páronként relatív prim helyen a függvény értéke 0.

(b) Legyen $f(1) = f(2) = 1$ és $f(\nu) = 0$, ha $\nu > 2$.

(c) Ha létezik végtelen sok különböző $P$ prím és $P \not| \nu$, amelyre $f^{\nu} \not= 0$, akkor ezek segítségével az (a) részhez hasonlóan megmutatható, hogy a függvény minden függvényértéket végtelen sok helyen vesz fel. Ezért csak véges sok ilyen $P$ létezhet, és ekkor ezek maximuma megfelel $K$-nak.

6.1.14

(a) Hamis. Ellenpélda: $f(\nu) = 3$, ha $2 \mid \nu$, de $4 \not| \nu$, és $f(\nu) = 0$ egyébként. Ez az $f$ additív, továbbá $f(4) + f(\hat{\nu}) = f(32)$ is teljesül, de nem teljesen additív, mert pl. $f(2) + f(\hat{\nu}) \neq f(12)$.

(b) Igaz. Ha $(c, \nu b) = 1$, akkor $(\nu a, b) \geq (a, b) > 1$ és

$$f((\nu a)b) = f((\nu a)b) = f(c) + f(\nu b) = f(c) + f(a) + f(b) = f(c) + f(b).$$

(c) Hamis. Ez más megfogalmazásban ugyanaz, mint az (a) állítás.

(d) Igaz. A bizonyítás a (b)-nél látt módon történhet.

(e) Hamis. Ellenpélda: $f(1) = f(2) = 1$ és $f(\nu) = 0$, ha $\nu > 2$.

Érdemes végiggondolni, miért változott meg a válasz a (d)-hez képest: ott az $f(\nu b) \neq f(a) + f(b)$ egyenlőtlenséghez $f(c)$-t hozzáadva az egyenlőtlenség továbbra is érvényes marad, ezzel szemben ha (e)-nél az $f(\nu b) \neq f(a) + f(b)$ egyenlőtlenséget $f(c) = 0$-val szorozzuk meg, akkor már egyenlőséget kapunk.

6.1.15 Eredmény: $\varphi(\nu) = n \prod p \cdot \left( 1 - \frac{1}{p} \right)$ (ahol $P$ prím jelöl). Útmutatás: Bizonyítsuk be, hogy $\varphi(\nu)$ multiplikatív, ehhez szimultán kongruenciarendszereket érdemes felhasználni. Ezután elég a függvény értékét a primhatvány helyeken meghatározni.

6.1.16 Lássuk be, hogy a bal és a jobb oldalon álló függvény egyaránt multiplikatív (a bal oldali összegnél az előző feladathoz hasonló gondolatmenetet érdemes alkalmazni). Ennek alapján elég az egyenlőséget a primhatvány helyeken igazolni.
13.6.2.

6.2.1 Legyen $a$, illetve $b$ összes pozitív osztója $a_1, \ldots, a_r$, illetve $b_1, \ldots, b_s$. Az 1.6.5a-b feladat [28] szerint $(a, b) = 1$ esetén az $a_i b_j$ számok kiadják $a b$ összes pozitív osztóját, és mindegyiket csak egyszer. Így

$$\sigma(ab) = \sum_{i=1}^{r} \sum_{j=1}^{s} a_i b_j = \left( \sum_{i=1}^{r} a_i \right) \left( \sum_{j=1}^{s} b_j \right) = \sigma(a) \sigma(b).$$

Ezután a multiplikativitás alapján előg a $\sigma$-függvény értékeit a primhatvány helyeken meghatározni.

6.2.2 Használjuk fel a függvények képletét, vagy pedig támaszkodjunk az 1.6.5a-c feladatra [28].

6.2.3 Mivel $3 \nmid \varphi(n)$, ezért az $n$ minden $\varphi$ prímosztója $3k - 1$ alakú. Legyen egy ilyen $\varphi$ kitevője az $n$ kanonikus alakjában $\alpha$. Ha $\alpha$ páratlan, akkor $\sigma(p^\alpha)$-ből kiemelhető $1 + p$, és így $\sigma(n)$ osztható 3-mal, ami ellentmond a feltételnek. Ezért minden $\varphi$ kitevője páros, tehát az $n$ négyzeteszám.

6.2.4 Legyen az $n$ kanonikus alakja $n^1 = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Ekkor minden olyan $k$ megfelel, amelyre

$$p_i^{\alpha_i+1} - 1 \mid p_i^{\alpha_i+1} - 1, \quad i = 1, \ldots, r.$$  

Ez teljesül, ha minden $i$-re

$$\alpha_i + 1 \mid k \alpha_i + 1, \quad \text{azaz} \quad \alpha_i + 1 \mid (k-1)\alpha_i.$$

Így biztosan megfelel, ha a $k - 1$ tetszőleges közös többszöröse az $\alpha_i + 1$ számoknak.

6.2.5 Válasz: $u$. — Útmutatás: Az osztók reciprokosszegénél hozzunk közös nevezőre, és használjuk fel, hogy ha $d$ végigfut az $n$ osztóin, akkor $n/d$ is végigfut az $n$ osztóin.

6.2.6 (a) Válasz: A négyzeteszámok és a négyzeteszámok kétszeresei. — Útmutatás: Használjuk fel a $\sigma(n)$ képletének törtmentes alakját. — Másik lehetőség: Legyen $n = 2^{k+1}$, ahol $t$ páratlan. A feladat szempontjából csak $n$ páratlan osztói, azaz $t$ osztói számítanak; azt kell megvizsgálni, mikor lesz $d(t)$ páratlan. Az 1.6.8 feladat [28] szerint ez pontosan akkor teljesül, ha $t$ négyzeteszám.

(b) Válasz: Különböző Mersenne-prímek szorzatai. — Útmutatás a szükségességhez: Legyen az $n$ kanonikus alakja $n^1 = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Ekkor

$$2^k = \sigma(n) = \prod_{i=1}^{r} (1 + p_i + p_i^2 + \cdots + p_i^{\alpha_i}).$$

Itt minden tényező maga is kettőhatvány, és így páros is, tehát minden $p_i > 2$ és mindegyik $\alpha_i$ páratlan. Ekkor $1 + p_i$ kiemelhető:

$$2^k = \prod_{i=1}^{r} (1 + p_i)(1 + p_i^2 + p_i^4 + \cdots + p_i^{\alpha_i - 1}).$$

A jobb oldalon minden tényező kettőhatvány, ezért $2^k$ Mersenne-prím. Azt kell még igazolni, hogy $\alpha_i = 1$. Tegyük fel indirekt, hogy valamelyik $\alpha_i > 1$. Ekkor az $1 + p_i^2 + \cdots + p_i^{\alpha_i - 1}$
tényezőből (annak párossága miatt) \(1 + p^2\) kiemelhető, és \(1 + p^2\) is kettőhatvány. Ez azonban nem lehetséges, mert \(1 + p^2\) már 4-gyel sem osztható.

6.2.7 Első megoldás: \(\sigma(n) \neq 2p\), ahol \(P\) egy \(3k - 1\) alakú páratlan prim.

Második megoldás: \(\sigma(n) \neq 3^s\), ha \(s > 1\).

Harmadik megoldás: Használjuk fel, hogy a \(\sigma\) -függvény „ritkán” vesz fel páratlan értéket.

Negyedik megoldás: Az \(1, 2, \ldots, N\) értékeket a \(\sigma\) -függvény csak az \(1, 2, \ldots, N\) helyek valamelyikén veheti fel. Mutassuk meg, hogy ezen \(x \leq N\) helyek közül is „sokszor”, mondjuk \(r\) esetben \(\sigma(x) > N\). Ekkor a \(\sigma(1), \ldots, \sigma(N)\) függvényértékek közül legfeljebb \(N - r\) darab lehet kisebb vagy egyenlő, mint \(N\), vagyis az \(1, 2, \ldots, N\) számok közül legalább \(r\) darab nem szerepel a \(\sigma\) -függvény értékkészletében.

Ötödik megoldás: Mutassuk meg, hogy „sok” olyan \(x_i \neq x_j\) pár van, amelyre \(\sigma(x_i) = \sigma(x_j)\), majd alkalmazzunk a negyedik megoldáshoz hasonló gondolatmenetet.

6.2.8 Csak \(n = 1\) felé meg.

Útmutatás: Lássuk be, hogy ha \(n \geq 2\), akkor \(n! < \sigma(n!) < (n + 1)!\).

6.2.9 Használjuk fel, hogy \(n = ab\) esetén \(a\) és \(b\) közül az egyik nagyobb vagy egyenlő, mint \(\sqrt{n}\). — Egyenlőség pontosan akkor teljesül, ha az \(n\) egy prímszám négyzete.

6.2.10
(a) (a1) \(n\) prim.

(a2) Nincs megoldás. (a3) \(n = 1\), \(4\).

(a4) \(n = 21\).

(b) Csak \(c = 1\) esetén.

(c) Ha \(c = 2k + 1 > 7\) és \(2k = p \perp q\), ahol \(P\) és \(Q\) különböző primek, akkor \(n = pq\) megfelel.

6.2.11
(a) (a1) \(n\) prim.

(a2) Nincs megoldás. (a3) \(n = 4\).

(a4) \(n = 6\).

(b) Csak \(c = 2\) esetén.

(c) \(c = 4k\), ahol \(k > 3\).

6.2.12

(a) Végtelen sok. — Ha találunk egy megfelelő \(a_0, b_0\) párt, és \(P\) az \(a_0\) és \(b_0\) közös prímosztója, akkor \(a_k = a_0 p^k, b_k = b_0 q^k\) is megfelel. Kiindulásnak vehető például \(a_0 = 6, b_0 = 8\) vagy \(a_0 = 12, b_0 = 14\) stb.
(b) Végteken sok. — Ha \( n \) felírható \( n = p_1 + p_2 = p_3 + p_4 \) alakban, ahol a \( p_i \) számok különböző
prímek, akkor \( a = p_1p_2, b = p_3p_4 \) megfelel. Az 5.4.7 feladathoz [135] hasonlóan igazolható, hogy
végteken sok ilyen \( n \) létezik (azaz amelyik legalább kétféleképpen írható fel két különböző prímek
összegeként). — Megjegyezzük, hogy ugyanez a gondolatmenet az (a) résznél is alkalmazható, ott
azonban egyszerűbben is célhoz értünk.

6.2.13 Használjuk fel, hogy az 1-en és \( n \) -en kívül az \( n \) minden minden osztója legfeljebb \( n/2 \)
, illetve legalább 2.

Egyenlőség: (a) \( n = 1 \) vagy prím; (b) és (c) \( n = 4 \) vagy prím.

6.2.14 Válasz: \( n = 6 \). — Útmutatás: Az előző feladat gondolatmenetét kell finomítani.

6.2.15

(a) Használjuk fel az (a1) egyenlötlen séghez a függvények képletét, az (a2)-höz pedig azt, hogy a \( \varphi(n) \)
az \( n \) bizonyos osztóinak előjelés összege. Mindkét esetben az egyenlőség pontosan akkor teljesül,
ha \( n \) prim.

(b) Mutassuk meg, hogy ha \( n \) kanonikus alakja \( n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \), akkor

\[
\frac{\sigma(n)\varphi(n)}{n^2} = \prod_{i=1}^{r} \left( 1 - \frac{1}{p_i^{\alpha_i+1}} \right) \geq \prod_{i=1}^{r} \left( 1 - \frac{1}{p_i^2} \right).
\]

A (b1) állítás ebből \( p_i \geq i + 1 \) alapján következik.

A (b2) állításhoz igazoljuk, hogy

\[
\inf \frac{\sigma(n)\varphi(n)}{n^2} = \lim_{N \to \infty} \prod_{p \leq N} \left( 1 - \frac{1}{p^2} \right),
\]

majd használjuk fel az 5.6.6 feladatot [149].

6.2.16 Legyen az \( n \) kanonikus alakja \( n = 2^\tau p_1^{\alpha_1} \cdots p_r^{\alpha_r} \), ahol \( p_i > 2 \) (itt \( \alpha = 0 \)
illetve \( \tau = 0 \) is lehet). Mutassuk meg, hogy minden \( \alpha_i - 1 \) , \( \alpha \leq 2 \) és \( \tau \leq 1 \). Ebből következik,
 hogy \( n = 1, 2, 4, p, 2p \) vagy \( 4p \), ahol \( p \) paratlan prim. Ezeket behelyettesítve könnyen igazolható, hogy
csak a megadott \( n \) értékek teljesítik a feltételeit.

6.2.17 Mindkét függvény csak a 0 és \( \pm 1 \) értékeket veszi fel.

6.2.18

(a) 3. — Útmutatás: Négy egymást követő egész szám közül valamelyik osztható 4-gyel.

(b) Akármi lenyok. — Útmutatás: Lásd a 2.6.11 feladatot [61].

6.2.19 Legyen az \( n \) -edik primitív egységyökök összege \( S(n) \). Elég belátni, hogy \( S(n) \)
multiplikatív, továbbá \( S(p^\alpha) = \mu(p^\alpha) \) bármely \( p^\alpha \) primhatványra. Az \( S(n) \)
multiplikativitásához mutassuk meg, hogy \( (a,b) = 1 \) esetén egy \( a \) -adik és egy \( b \) -edik primitív egységyök szorzata \( ab \)
-edik primitív egységyök, és minden \( ab \) -edik primitív egységyök egyértelműen felírható ilyen
szorzat alakban. — A feladat az összegzési és megefordítási függvények segítségével is megoldható,
lásd a 6.5.9a feladatot [194].

6.2.20 0.
6.2.21
(a) Használjuk fel a függvények képletét, vagy pedig azt, hogy az \( \mathfrak{m} \) osztói a multiplicitással számolt prímosztók bizonyos részhalmazainak felelnek meg. — Ha \( \mathfrak{m} \) négyzetmentes, akkor mindkét helyen egyenlőség teljesül, egyébként pedig mindkét helyen szigorú egyenlőtlenség áll.

\[ k^\mathfrak{m}(\mathfrak{n}) \leq d_k(n) \leq k^{\mathfrak{m}(\mathfrak{n})}. \]

6.2.22 Igaz: (a).

6.2.23 Hasonlóan járhatunk el, mint a \( \sigma \)-függvény esetében, lásd a T 6.2.2 Tételt és a T 6.2.8 Tétel \( \sigma \)-ra vonatkozó részének a bizonyítását, vagy pedig a 6.2.1 feladatot [176]. Eredmény: Ha az \( \mathfrak{n} \) kanonikus alakja \( \mathfrak{n} = \mathfrak{p}_1^{\mathfrak{r}_1} \cdots \mathfrak{p}_v^{\mathfrak{r}_v} \) és \( \nu \neq \emptyset \), akkor

\[ \sigma_{\nu}(\mathfrak{n}) = \prod_{i=1}^{\nu} \left( 1 + \mathfrak{p}_i^{\mathfrak{r}_i} + \mathfrak{p}_i^{2\mathfrak{r}_i} + \cdots + \mathfrak{p}_i^{\mathfrak{v}^{\mathfrak{r}_i}} \right) = \prod_{i=1}^{\nu} \frac{\mathfrak{p}_i^{\mathfrak{r}_i+1} - 1}{\mathfrak{p}_i^{\nu} - 1}. \]

13.6.3.

6.3.1 Használjuk fel a T 6.3.2 Tételt.

6.3.2
(a) Ha az \( \mathfrak{n} \) kanonikus alakja \( \mathfrak{n} = \prod_{i=1}^{\nu} \mathfrak{p}_i^{\mathfrak{r}_i} \), akkor a \( 2\mathfrak{n} = \sigma(\mathfrak{n}) \) feltétel a

\[ 2 \prod_{i=1}^{\nu} \mathfrak{p}_i^{\mathfrak{r}_i} = \prod_{i=1}^{\nu} \left( 1 + \mathfrak{p}_i + \cdots + \mathfrak{p}_i^{\mathfrak{v}^{\mathfrak{r}_i}} \right) \]

egyenlőséget jelenti. Az (1) bal oldala a 2-nek pontosan az első hatványával osztható, ezért a jobb oldal tényezői közül az egyik 2-vel osztható, de 4-gyel már nem, a többi tényező pedig páratlan. Ez azt jelenti, hogy egyetlen \( \alpha \)-kitevő lesz páratlan és az ehhez tartozó \( \mathfrak{p}_j \) prim biztosan \( \mathfrak{p}_j \) alakú, a többi \( \alpha \)-kitevő pedig páros.

(b) Az (a) rész szerint \( \mathfrak{n} = \mathfrak{s}^2 \mathfrak{p} \), ahol \( \mathfrak{p} \) egy \( \mathfrak{p}_1 + 1 \) alakú prim. Ebből azonnal következik, hogy \( \mathfrak{n} \equiv 1 \pmod{4} \). Ha \( \mathfrak{p} \equiv 3 \pmod{9} \), akkor \( \mathfrak{n} \equiv 9 \pmod{36} \). Ha \( \mathfrak{p} \equiv 3 \pmod{p} \), akkor \( \mathfrak{n} \equiv \mathfrak{n} \) miatt \( \mathfrak{p} \equiv \mathfrak{n} \). Mivel \( \mathfrak{p} \) kitevője az \( \mathfrak{n} \) kanonikus alakjában páratlan, ezért \( 1 + \mathfrak{p} \mid \sigma(\mathfrak{n}) \), és így \( \mathfrak{p} \equiv 1 \pmod{3} \). Ez azt jelenti, hogy csak \( \mathfrak{p} \equiv 1 \pmod{3} \) lehetséges, tehát \( \mathfrak{n} = \mathfrak{s}^2 \mathfrak{p} \equiv 1 \pmod{3} \). Az \( \mathfrak{n} \equiv 1 \pmod{4} \) kongruenciával együtt ebből azt kapjuk, hogy \( \mathfrak{n} \equiv 1 \pmod{12} \).

6.3.3
(a) A bizonyítandó \( 2\mathfrak{r}^\alpha > \sigma(\mathfrak{r}^\alpha) \) egyenlőtlenség ekvivalens átalakításokkal a \( \mathfrak{r}^\alpha(\mathfrak{r}^2 - 1) > 1 \) alakra hozható.

(b) \[ \frac{\sigma(\mathfrak{r}^\alpha q^\beta)}{\mathfrak{r}^\alpha q^\beta} = \left( 1 + \frac{1}{\mathfrak{p}} + \cdots + \frac{1}{\mathfrak{p}^{\mathfrak{v}}} \right) \left( 1 + \frac{1}{q} + \cdots + \frac{1}{q^{\nu}} \right) < \]

\[ < \frac{\mathfrak{p} - 1}{\mathfrak{p} - 1} \cdot \frac{\mathfrak{q} - 1}{\mathfrak{q} - 1} \leq \frac{3}{2} \cdot \frac{5}{4} < 2. \]

(c) Példák bővelkedőre: legyen \( \mathfrak{n} \) kanonikus alakja \( \prod_{i=1}^{\nu} \mathfrak{p}_i^{\mathfrak{r}_i} \), ahol \( \mathfrak{p}_1 \) az \( i \)-edik prímszám (tehát \( \mathfrak{p}_1 = 3, \mathfrak{p}_2 = 5 \) stb.) és \( \alpha_1 \geq 3 \), a többi \( \alpha_i \) pedig tetszőleges pozitív egész.
Példák hiánynosra: $k$ darab olyan különböző $q_i$ prim szorzata, amelyekre

$$1 + \frac{1}{q_i} < \sqrt[4]{2}.$$  

(d) Mutassuk meg, hogy ha $a > 1$, akkor

$$\frac{\sigma(a^2)}{a^{\frac{1}{2}}} > \frac{\sigma(n)}{n}.$$  

A (2)-t legegyszerűbben annak alapján igazolhatjuk, hogy ha $n$ összes osztója $d_1, \ldots, d_k$, akkor az $a d_i$ számok az $a n$ különböző osztói, és így $\sigma(a n) > a \sigma(n)$. Másik két lehetőség, ha a $\sigma$ képletét használjuk, illetve azt a tényt, hogy $\sigma(n)/n$ az $n$ szám osztóinak a reciprokösszege.

(e) Egy hiánynos számot tetszőleges bővelkedő számmal megszorozva bővelkedő számot, egy elég nagy prímszámmal szorozva pedig hiánynos számot kapunk.

6.3.4 A 6.2.6a feladat [176] alapján egy ilyen szám csak $n = 2^a i^2$ alakú lehet. Azt kell még igazolni, hogy $a = 0$. $\sigma(n) = 2n + 1$ feltételt átalakíthatunk

$$(2^a + 1)(\sigma(i) - i^2) - i^2 + 1$$

adódik. Ha $a \geq 1$, akkor (3) bal oldalának első tényezője $4k - 1$ alakú, és így létezik $4k - 1$ alakú prímosztója. Ez azonban ellentmond annak, hogy egy $i^2 + 1$ alakú számnak nem lehet $4k - 1$ alakú prímosztója.

6.3.5

(a) A T 6.3.2 Tétel bizonyításához hasonló gondolatmenetet lehet alkalmazni.

(b) Azt kell belátni, hogy ekkor $\sigma(n)$ is páratlan. Írjuk fel $\sigma(n)$ alatt $\sigma(i) = 2^v w$ alakban, ahol $w$ páratlan, és mutassuk meg, hogy $v \geq 1$ esetén ellentmondásra jutunk.

(c) Tegyük fel, hogy $p^\alpha$ supertökéletes, és írjuk fel $\sigma(p^\alpha)$ kanonikus alakjának felhasználásával $\sigma(\sigma(p^\alpha))$ értékét.

6.3.6

(a) Az $n$ osztóinak harmonikus közepe

$$\frac{\sum_{d|n} \frac{1}{d}}{\sigma(n)}.$$  

(b) Az (a) rész alapján elég azt igazolni, hogy ha $n$ tökéletes szám, akkor $d(n)$ páros, azaz $n$ nem lehet négyzetszám. Ez valóban igaz, hiszen ha $n$ négyzetszám, akkor $\sigma(n)$ páratlan, és így $\sigma(n) \neq 2v$.

(c) Tegyük fel indirekt, hogy $1 + p + \cdots + p^\alpha | p^\alpha (\alpha + 1)$ . Mivel

$$1 + p + \cdots + p^\alpha | \sigma(\sigma(p^\alpha)),$$

ezért $1 + p + \cdots + p^\alpha | \alpha + 1$. Ez azonban lehetetlen, hiszen $1 + p + \cdots + p^\alpha > \alpha + 1$.

(d) Legyen $n = p_1 p_2 \cdots p_r$, ahol $p_i$ prim és $p_1 < p_2 < \cdots < p_r$. Ha mindegyik $p_i$ páratlan, akkor a
\[ \frac{p_1 - 1}{2} \cdots \frac{p_k - 1}{2} \mid p_1 \cdots p_k \]

oszthatóság azért nem teljesülhet, mert \( (p_i - 1)/2 \) a jobb oldal minden tényezőjéhez relatív prim.

Ha \( p_1 = 2 \), akkor szükségképpen \( p_2 = 3 \). Az \( n = 6 \) harmonikus szám, ha pedig az \( n \) -nek további prim tényezői is vannak, akkor az előző esethez hasonlóan juthatunk ellentmondásra.

6.3.7

(a) Ha \( a < b \) és \( \sigma(a) = \sigma(b) = a + b \), akkor \( \sigma(\sqrt{a}) = \sqrt{a} + \sqrt{b} < 2b \) és \( \sigma(\sqrt{a}) = \sqrt{a} + \sqrt{b} > 2\sqrt{a} \).

(b) Tegyük fel indirekt, hogy \( a = 2^k \) és \( b \) barátságos szám pár. Ekkor

\[ \sigma(2^k) = 2^{k+1} - 1 = \sigma(b) = 2^k + b, \]

ahonnan \( b = 2^k - 1 \), továbbá \( b \) és \( \sigma(b) \) páratlansága miatt \( b = u^2 \). Az így adódó \( 2^k - 1 = u^2 \) egyenlőség azonban már modulo 4 sem teljesülhet, ha \( k \geq 2 \).

13.6.4.

6.4.1 Az \( \Omega(n) \) -re vonatkozó völgytétel szó szerint a T 6.4.1 Tétel mintájára bizonyítható, a \( d_k(n) \) esetén annyit kell változtatni, hogy a szimultán kongruenciarendszer modulusai \( 2^{K+k} \) és \( 2^{K-k} \), az \( \omega(n) \) -hez pedig két olyan relatív prim modulus érdemes választani, amelyek mindegyike \( K+2 \) darab különböző primszám szorzata.

A \( \sigma(n) \) völgytételénél bármely elég nagy prim megfelel \( n \) -nek, hiszen ekkor \( \sigma(n) = n + 1 \), ugyanakkor \( n + 1 \) és \( n - 1 \) párossága miatt

\[ \sigma(n - 1) > (n - 1) + \frac{n - 1}{2} \quad \Rightarrow \quad \sigma(n + 1) > (n + 1) + \frac{n + 1}{2}. \]

Ugyanígy bizonyítható a \( \varphi(n) \) -re vonatkozó hegytétel is.

A többi függvény hegytételénél és \( \varphi(n) \) völgytételénél a T 6.4.2 Tétel bizonyításához hasonlóan \( n \) -et az első \( \tau \) primszám szorzatának érdemes választani.

A \( d_k(n) \) és \( \sigma(n) \) hegytetele, illetve a \( \varphi(n) \) völgytele a T 6.4.2 Tétel bizonyításának értelemszerű módosításával igazolható.

Végül, az \( \Omega(n) \) és \( \omega(n) \) függvények esetén, a T 6.4.2 Tétel bizonyításának a jelöléseivel élve, azt kell megmutatni, hogy \( r - \varepsilon > K \). Ez abból következik, hogy

\[ n \leq p_1 \cdots p_{K+1}^{r - K - 1} < p_r^r K, \]

ha \( r \) elég nagy, ugyanakkor

\[ n - 1 = q_1 \cdots q_s > p_r^s. \]

6.4.2 Kövessük a T 6.4.5 Tétel bizonyításának gondolatmenetét.

6.4.3
(a) Megfelel például, ha \( n \) az első 101 prim szorzatának eléggé nagy hatványa.

(b) Legyen \( n \) az első \( r \) primszám szorzata. Ekkor az 5.4 pont eredményei alapján

\[
\log n \sim p_r \sim r \log r, \quad \text{és így} \quad r \sim \frac{\log n}{\log \log n}
\]

adódik. Ebből \( d(n) = 2^r \) miatt a feladatban megadott becslést kapjuk.

6.4.4 Legyen \( \Omega(n) = s \), azaz \( n = q_1 \cdots q_s \), ahol \( q_i \neq q_j \) is előfordulhat. Ekkor \( q_i \geq 2 \) miatt \( n \geq 2^s \). Egyenlőség pontosan akkor teljesül, ha \( n \) kettőhatvány.

6.4.5 Lássuk be, hogy adott \( r \) esetén az első \( r \) primszám szorzata a legkisebb olyan \( n \), amelyre \( \omega(n) = r \). Ez azt jelenti, hogy \( \omega(n) \) az \( n \) függvényében mért maximális nagyságrendjét az ilyen alakú számokon éri el. Ha \( n \) az első \( r \) prim szorzata, akkor 6.4.3 [188]b-hez hasonlóan kapjuk a feladat állításait.

6.4.6

(a) Alkalmazzuk a T 6.4.6 Tételt az \( n^{0.99}/\varphi(n) \) függvényre, vagy használjuk fel a \( d(n)/\varphi(n) \geq n \) összefüggést és a T 6.4.5 Tételt.

(b) \( \varphi(n) \geq r(n) - \omega(n) \).

(c) Legyen \( n \) tetszőleges olyan egész, amelyre \( \omega(n) = r \), és legyen \( n_r \) az első \( r \) primszám szorzata. Mutassuk meg, hogy

\[
\frac{\varphi(n_r)}{n_r} > \frac{\varphi(n)}{n}, \quad \text{és} \quad \log \log n \geq \log \log n_r.
\]

Ennek alapján az állítást eléggé az \( n_r \)-számokra igazolni.

A primszámok eloszlásáról tanult eredményeket felhasználva kapjuk, hogy

\[
\log \left( \frac{\varphi(n_r)}{n_r} \right) = \log \prod_{i=1}^{r} \left( 1 - \frac{1}{p_i} \right) = \sum_{i=1}^{r} \log \left( 1 - \frac{1}{p_i} \right) \geq
\]

\[
- \sum_{i=1}^{r} \frac{1}{p_i} + \sum_{i=1}^{r} \frac{1}{p_i^2} > - \sum_{p \leq p_r} \frac{1}{p} - 2 > - \log \log p_r - c - 2,
\]

azaz

\[
\frac{\varphi(n_r)}{n_r} > \frac{1}{c' \log p_r}.
\]

Ezután vegyük figyelembe a \( \log \log n_r \sim \log p_r \) összefüggést (ami \( \log n_r \sim p_r \) -ből a mindkét oldal végtehenez tartása miatt jogos "logaritmálással" adódik).

(d) Alkalmazzuk a T 6.4.6 Tételt a \( \sigma(n)/n^{1.01} \) függvényre, vagy használjuk fel a \( \sigma(n) \leq nd(n) \) összefüggést és a T 6.4.5 Tételt.

(e) \( \sigma(n)/n \) az \( n \) osztóinak a reciprokösszege, és így
\[
\frac{\sigma(n)}{n} \leq \sum_{j=1}^{\sigma(n)} \frac{1}{j} \leq 1 + \log n.
\]

(f) A (c) részhez hasonlóan kell bizonyítani.

Megjegyezzük, hogy a 6.2.15a feladat [178] alapján a \(\sigma(n)\) -re vonatkozó állítások közvetlenül is következnek a \(\varphi(n)\) -re vonatkozó megfelelő állításokból (és a 6.2.15b feladat [178] szerint ez fordítva is „majdnem” igaz).

6.4.7 Használjuk fel, hogy

(a) \(\lim_{n \to \infty} \prod_{p \leq n} \left(1 - \frac{1}{p}\right) = 0\); 

(b) \(\lim_{n \to \infty} \prod_{p \leq n} \left(1 + \frac{1}{p}\right) = \infty\).

6.4.8

(a) Legyenek \(\nu_1, \nu_2, \ldots\) azok a prímek, amelyekre \(k \mid \nu - 1\), és legyen \(B_r = v_1 \ldots v_r\).

Ha \(\langle n, B_r \rangle > 1\), akkor az \(n\) osztható valamelyik \(\nu_i\) -vel, és így \(k \mid \nu_i - 1 \mid \varphi(n)\).

Ezek szerint \(k \mid \varphi(n)\) legfeljebb azokra az \(n\) -ekre fordulhat elő, amelyek a \(B_r\) -hez relatív prímek.

Az ilyen \(n\) -ek száma \(N\) -ig nagy \(N\) esetén körülbelül

\[
\frac{\varphi(B_r)}{B_r} N.
\]

Így elég megmutatni, hogy bármely \(\varepsilon > 0\) -hoz található olyan \(r\), hogy

\[
\frac{\varphi(B_r)}{B_r} = \prod_{i=1}^{r} \left(1 - \frac{1}{c_i}\right) < \varepsilon.
\]

Ez az 5.6.7 feladat [149] alapján következik abból, hogy \(\sum_{i=1}^{\infty} 1/\nu_i\) divergens.

(b) Ha \(\omega(n)\) nagy, akkor \(\varphi(n)\) osztható a 2-nek egy nagy hatványával, tehát eleve kevés ilyen \(\varphi(n)\) érték keletkezik. Ha \(\omega(n)\) kicsi, akkor \(\varphi(n) > cn\), ahol \(c\) (kis pozitív) konstans, és így ha \(\varphi(n) \leq N\), akkor \(n < N/c\). De ezekre az \(n\) -ekre (is) az (a) rész szerint \(\varphi(n)\) majdnem mindig osztható egy előre megadott nagy \(k\) -val (ez a \(k\) lehet a már szerepelt kettőhatvány is), azaz ismét csak kevés \(\varphi(n)\) érték keletkezhet.

6.4.9

(a) A 6.4.8a feladathoz [189] hasonlóan bizonyíthatunk. Legyenek \(\omega_1, \omega_2, \ldots\) azok a prímek, amelyekre \(k \mid \omega_i + 1\), és legyen \(C_r = \omega_1 \ldots \omega_r\).

Ha az \(n\) valamelyik \(\omega_i\) -nek pontosan az első hatványával osztható, akkor

\(k \mid \omega_i + 1 \mid \sigma(n)\).
Ezek szerint \( k / \sigma(n) \) legfeljebb azokra az \( n \) -ekre fordulhat elő, amelyek vagy relatív prímek \( C_r \) -hez, vagy pedig \( C_r \) valamelyik primitívgyöjéjének a négyzetével is oszthatók. Ezek az \( n \) -ek bizonyos maradékosztályokba esnek mod \( C_r^2 \). Az ilyen mod \( C_r^2 \) maradékosztályok számának és \( C_r^2 \) -nek az aránya

\[
\prod_{i=1}^{\infty} (1 - \frac{\nu_i}{\nu_i^2})
\]

Mutassuk meg a 6.4.8a feladatban [189] látott módon, hogy ez az arány tetszőlegesen kicsi lehet, ha \( r \) elég nagy.

(b) Itt egyszerűbb a dolgunk, mint a \( \sigma(n) \) -nél volt, ugyanis \( \sigma(n) \leq N \) -ből következik, hogy \( n \leq N \). Ennek megfelelően a \( \varphi(n) \) -nél látott bizonyításnak csak az utolsó lépésére van szükség: mivel \( \sigma(n) \) majdnem mindig osztható egy előre megadott nagy \( k \) -val, ezért csak kevés \( \sigma(n) \) érték keletkezhet.

13.6.5.

6.5.1 A \( d_j(n) \) függvények definíciójából következik.

6.5.2

(a) Tegyük fel, hogy \( f \) multiplikatív, és legyen \( (a, b) = 1 \). Az \( f^+ \) multiplikativitásának igazolásához felhasználjuk, hogy az 1.6.5a-b feladat [28] szerint \( ab \) osztóit egyértelműen előállíthatjuk az \( a \) és a \( b \) egy-egy osztójának szorzataként (amelyek nyilván szintén relatív prímek). Ennek alapján

\[
f^+(ab) = \sum_{d | ab} f(d) = \sum_{a_1, b_1 | a, b} f(a_1 b_1) = \sum_{a_1 | a} f(a_1) \sum_{b_1 | b} f(b_1) = (\sum_{a_1 | a} f(a_1)) (\sum_{b_1 | b} f(b_1)) = f^+(a)f^+(b).
\]

A megfordítást hasonló módon igazolhatjuk \( n = ab \) szerinti teljes indukcióval vagy a Möbius-féle megfordítási formulát felhasználásával.

(b) Ha \( f \) helyére \( f^+ \) -t írunk, akkor éppen az (a)-beli állításhoz jutunk.

6.5.3

(a) \( f = 0 \) és a D 6.5.1 Definíció utáni példáknál definiált \( e(i) \) . — Útmutatás: Mutassuk meg, hogy egy \( p \) prímre \( f^+(p^r) = (f^+(p))^r \) csak \( f(p) = 0 \) esetén teljesülhet.

(b) \( f = 0 \) . — Útmutatás: Vizsgáljuk az \( f^+ \) függvény értékét rendre az alábbi helyeken: \( \mathfrak{p}_1 \mathfrak{p}_2, \mathfrak{p}_1 \mathfrak{p}_3, \mathfrak{p}_2 \mathfrak{p}_3, \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3 \) stb., ahol \( \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3 \) különböző prímek, és olvassuk le ebből, hogy \( f \) értéke minden primhatvány helyen nulla.

6.5.4

(a) Használjuk fel a 6.5.2 feladatot [193].

(b) Következik az (a) részből és \( f^+ \) teljes multiplikativitásából. Az \( f(n) = n \) esetben \( \sigma(n) \) , illetve \( \varphi(n) \) képletét nyerjük.
6.5.6 Legyen \( n \) kanonikus alakja \( n = \prod p_i^{\alpha_i} \). Ekkor

\[
f(n) = \sum_{i=1}^{v} f(p_i^{\alpha_i}) = \sum_{i=1}^{v} \sum_{\beta_i=0}^{\alpha_i} f(p_i^{\beta_i}) = \sum_{p \mid n} f(p).
\]

Innen \( f \) egyértelműségét következik, hogy ha \( k \) nem prímhatvány, akkor \( f(k) = 0 \).

6.5.7 A Möbius-féle megfordítási formula szerint ez az \( f(n) = n \) függvény.

6.5.8 A Möbius-féle megfordítási formula szerint

\[
\varphi(n) = \sum_{d \mid n} \mu(d) \frac{T_d}{d}
\]

6.5.9

(a) Jelöljük az összes \( n \)-edik egységgyög összegét \( T(n) \)-nel, az \( n \)-edik primitív egységgyökök összegét pedig \( S(n) \)-nel. Ekkor \( S(n) = T(n) = \varphi(n) \) miatt \( S(n) = \mu(n) \). (Egy másik bizonyítást a 6.2.19 feladatban [178] vázoltunk.)

(b) Jelöljük az összes \( n \)-edik egységgyög, illetve az \( n \)-edik primitív egységgyökök \( k \)-adik hatványainak összegét \( T_k(n) \)-nel, illetve \( S_k(n) \)-nel. Ekkor \( S_k(n) = T_k(n) \) és

\[
T_k(n) = \begin{cases} n, & \text{ha } n \mid k; \\ 0, & \text{ha } n \not\mid k. \end{cases}
\]

Irjuk fel \( S_k(n) \) -et a Möbius-féle megfordítási formula segítségével, és használjuk fel a 6.5.8 feladatot[194] is. — Másik lehetőség: Mivel \( S_k(n) \) és a feladatban megadott függvény is multiplikatív, ezért elég az egyenlőségeket a primhatvány helyeken igazolni.

(c) Térjünk át a modulo \( p \) testre. Jelöljük az \( x^k \equiv 1 \pmod{p} \) kongruencia megoldásainak összegét \( V(k) \)-val, a \( k \)-adrendű elemek összegét pedig \( U(k) \)-val. Mutassuk meg, hogy \( U^+(n) = V(n) \), továbbá \( d \mid p - 1 \) esetén \( V(d) = \varphi(d) \). Ebből vezessük le, hogy \( d \mid p - 1 \) esetén \( U(d) = \mu(d) \), és így speciálisan \( U(p - 1) = \mu(p - 1) \).

6.5.10 (a) \( \varphi(1), \varphi(2), \ldots, \varphi(n) \).
(b) $\alpha!$.
(c) 1.
(d) 0.

6.5.11 A T 6.5.4 Tétel bizonyítása átvihető erre az általános esetre is.

13.6.6.

6.6.1 $d_k(n)$.

6.6.2 Az összefüggéssel közönségesen minden rendben van, a szorzás szerepét betöltő konvolúcióra az
asszociativitás, a kommutativitás és az egységelem létezése a T 6.6.2 Tételből következik, és az

$$(f + g) * h = (f * h) + (g * h)$$

disztributivitás is könnyen ellenőrizhető (a „szorzás” kommutativitása miatt elég az egyik oldali
disztributivitást igazolni). Nullosztómentesség: Lássuk be, hogy ha $k$, illetve $n$ a legkisebb olyan
positív egész, amelyre $f(k) \neq 0$, illetve $g(n) \neq 0$, akkor $f + g)(k*n) \neq 0$.

6.6.3 Válasz: $k$. — Útmutatás:írjuk fel minden $n$ -re a $(g * g * \cdots * g)(\sigma)$ egyenlőséget, ebből $\sigma = 1$ -re

$$g(1) = \sqrt[n]{f(1)}$$
adódik, majd $\sigma = 2, 3, \ldots$ esetén rendre egyértelműen meghatározhatók a $g(2), g(3), \ldots$
függvényértékek.

6.6.4

(a) A 6.5.2 feladat [193] útmutatásához hasonló gondolatmenetet lehet alkalmazni.

(b) Ha $f = 0$ vagy $g = 0$, akkor az állítás igaz, ezért a továbbiakban feltehetjük, hogy
$f(1) = g(1) = 1$. Ha $f * g$ teljesen multiplikatív, akkor az

$$(f * g)(p^n) = (f(p))^n = (g(p))^n$$

egyenlőségből bármely $p$ primre $f(p)g(p) = 0$, és így $f$ és $g$ teljes multiplikativitása miatt
minden $\sigma > 1$ -re is $f(p^\sigma)g(p^\sigma) = 0$ adódik. A megfordításhoz mutassuk meg, hogy az $f(p)g(p) = 0$
feltételből

$$(f * g)(p^\sigma) = f(p^\sigma) + g(p^\sigma) = (f * g)(p)$$
következik.

6.6.5 Az egyik lehetőség, ha kihasználjuk, hogy az egyenlőség mindkét oldalán multiplikatív függvény
áll, így elég az egyenlőséget a primhatvány helyeken igazolni. Elegánsabb azonban a konvolúció
tulajdonságaira támaszkodni: Legyen $g(n) = n$, ekkor $\alpha * \gamma = (g * 1) * (n * g) = g * g$, tehát

$$\sum_{d|n} \sigma(d)\gamma(d) = (\alpha * \gamma)(n) = (g * g)(n) = \sum_{k|n} k \cdot \frac{n}{k} = n \delta(n).$$
6.6.6
\[ \sum_{n=1}^{\infty} \left| \frac{f(n)}{n^s} \right| = \sum_{n=1}^{\infty} \frac{f(n)}{n^{s-s_0}} \cdot \frac{1}{n^{s-s_0}} < c \sum_{n=1}^{\infty} \frac{1}{n^{s-s_0}} < \infty. \]

6.6.7 Alkalmazzuk a T 6.6.4 Tételt.

6.6.8 Használjuk fel a 6.6.1 feladatot [198] és a T 6.6.4 Tételt.

6.6.9 Írjuk fel a \( \sigma \), illetve \( \mu^t \) függvényt összegzési, illetve megfordítási függvényként, és alkalmazzuk a 6.6.7 feladatot [198].

6.6.10
(a) A jobb oldal definíció szerint a
\[ \prod_{\nu < N} \left( \sum_{k=0}^{\infty} \frac{f(p^k)}{p^{ks}} \right) \]

szorzat határértéke, ha \( N \to \infty \). Az (1)-ben szereplő véges sok abszolút konvergens sor szorzását elvégezve a számelmélet alaptétele és f multiplikativitása miatt azokból az \( f(\nu)/\nu^s \) értékekből álló \( F_N(s) \) végleten sort kapjuk, ahol az \( \nu \) minden prímosztója kisebb vagy egyenlő, mint \( N \). Mivel az
\[ f^*(s) = \sum_{\nu=1}^{\infty} \frac{f(\nu)}{\nu^s} \]
sor abszolút konvergens, ezért
\[ \lim_{N \to \infty} F_N(s) = F(s). \]

(b) Az \( f \) teljes multiplikativitása miatt
\[ \frac{f(p^k)}{p^{ks}} = \left( \frac{f(\nu)}{\nu^s} \right)^k, \]
és így az (a)-beli képlet jobb oldalán most végleten mértani sorok állnak.

6.6.11 Az egyenlőség következik a \( \zeta \) -függvény szorzat-előállításából és abból, hogy a \( \mu^t \) -függvény \( M(s) \) Dirichlet-sora a \( \zeta \) -függvény reciproka. — Másik lehetőség: Alkalmazzuk a 6.6.10a feladatot [199] az \( f = \mu^t \) függvényre.

6.6.12
(a) Válasz: \( \pi^4/36 \). — Útmutatás: Használjuk fel a 6.6.8a feladatot [198].

(b) Válasz: \( 5\pi^4/72 \). — Útmutatás: A \( d^2(\nu) \) függvény \( T(s) \) Dirichlet-sorát a 6.6.10a feladat [199] alapján végleten szorzattá alakítva, majd a szorzat tényezőiként fellépő végleten sorokat kiszámítva lássuk be, hogy
\[ T(s) = \frac{\zeta^4(s)}{\zeta^2(2s)}. \]
6.6.13 Válasz: \(15/\pi^2\). — Útmutatás: Alkalmazzuk a 6.6.10a feladatot \([199]\) az \(f = |u|\) függvényre, majd lássuk be, hogy az így kapott végleten szorzat értéke \(\zeta(s)/\zeta(2s)\).

6.6.14

\[
\sum_{n=1}^{\infty} \frac{f(n)x^n}{1-x^n} = \sum_{n=1}^{\infty} f(n)\left(\sum_{j=1}^{\infty} x^j\right) = \sum_{k=1}^{\infty} x^k\left(\sum_{n=1}^{\infty} f(n)x^n\right) = \sum_{k=1}^{\infty} f(k)x^k.
\]

(b) Alkalmazzuk a feladat (a) részét a \(f^L\), illetve \(\vartheta\) függvényre és \(x = 1/2\) -re. Eredmény: (b1) \(1/2\); (b2) 2.

13.6.7.

6.7.1 Válasz: 1. — Útmutatás: A T 6.7.5 Tétel második bizonyításához hasonló meggondolásokkal kapjuk, hogy ez az összeg az \(1, 2, \ldots, n\) egészek közül azoknak a számát határozza meg a logikai szitaformula segítségével, amelyek egyetlen prímmel sem oszthatók. Nyilván csak egyetlen ilyen pozitív egész van: az 1, tehát az összeg értéke 1. (A „tanulság”: időnként a dolgok elbonyolítása is hasznos lehet; most is az történt, hogy egy nyilvánvaló darabszámot bonyolult képlettel is meghatároztunk, és éppen ez tette lehetővé a bonyolult képlet egyszerű alakjának a megtalálását.) — Másik lehetőség: miután a választ (néhány \(n\) kipróbálása után) megsejtettük, az eredmény helyességét teljes indukcióval is igazolhatjuk.

6.7.2 Válasz: \(6/\pi^2\). — Útmutatás: Jelölje \(K(n)\) az \(1, 2, \ldots, n\) egészek között a négyzetmentsések számát. A feladat ekkor a

\[
\lim_{n \to \infty} \frac{K(n)}{n^2}
\]

határérték vizsgálata. A T 6.7.5 Tétel második bizonyításához hasonlóan a logikai szitaformula segítségével lássuk be, hogy

\[
K(n) = \sum_{j \leq \sqrt{n}} \mu(j) \left\lfloor \frac{n}{j^2} \right\rfloor.
\]

Vegyük észre, hogy az egészoszlophibát megelőző legfeljebb \(\sqrt{n}\) nagyságú „hibatag” keletkezik, ami az

\[
n \sum_{j \leq \sqrt{n}} \frac{\mu(j)}{j^2}
\]

„főtaghoz” képest elhanyagolható.

6.7.3

(a) Válasz: \((\log n)^2/2\). — Útmutatás: A T 6.7.2 Tételt a \(d_s = d_2 = 1\) konvolúcióra alkalmazva

\[
D_s(n) = \sum_{j=1}^{n} d(j) \left\lfloor \frac{n}{j} \right\rfloor
\]

adódik. Az \(n\) -nel való osztási és az egészresz elhagyása után (a keletkező hibatagtól eltekintve) a

\[
\sum_{j=1}^{n} \frac{d(j)}{j}
\]

(1)

498
összeget kell megbecsülni. Ehhez felhasználjuk a $d(n)$ középpontjáére vonatkozó T 6.4.3 Tételt. Az ottani jelölésekkel $d(j) = D(j) - D(j - 1)$. Rendezzük át az (1) összeget ennek megfelelően, majd alkalmazzuk $D(j)$-re a T 6.4.3 Tételt, ekkor hibatagoktól eltekintve a

$$\sum_{k=2}^{n} \log j \sim \int_{2}^{n} \log t \, dt \sim \frac{\log^2 n}{2}$$

eredményhez jutunk. Ne felejtsük el azt is megmutatni, hogy a hibatagok elhanyagolhatók ehhez a főtaghoz képest.

(b) Válasz:

$$\frac{n^\nu \xi(n^\nu + 1)}{\nu + 1}.$$

Útmutatás: Kövessük a T 6.7.3 Tétel bizonyításának gondolatmenetét. Legyen $f_\nu(n) = n^\nu$, és alkalmazzuk a T 6.7.2 Tételt a konvolúcióra, ekkor

$$\sigma_\nu = 1 + f_\nu$$
adóik. Ezután a jobb oldal $k$ szerinti belső összegét becsüljük a szokásos módon az integrálkritériummal (lásd az T 5.6.1 Tétel első bizonyítását, illetve az 5.6.2 feladatot [148]).

6.7.4 Mivel a $\sigma$ középpontkővágvénye „viszonylag kicsi”, ezért az $1, 2, \ldots, \tau$ számok között „sok” olyan $\tilde{i}$ van, amelyre (peldaul) $\sigma(\tilde{i}) \leq 2\tau$. A 6.4.9 feladat [190] alapján „kevés” ilyen $\sigma(\tilde{i})$ érték van, ezért valamelyiket a függvénynek sok helyen fel kell vennie.

6.7.5

(a) Az alsó becsles $\Omega(\tilde{i}) \geq \omega(\tilde{i})$ miatt nyilvánvaló. A felső becsleshez írjuk be $\Omega(\tilde{i})$ és $\omega(\tilde{i})$ előállítását a megfordítási függvények segítségével (lásd a 6.5.5c-d feladatot [193]), ekkor a szokásos összegátervezéssel, majd az egészszorzat elhagyva azt kapjuk, hogy

$$\sum_{\tilde{i}=1}^{\tau} (\Omega(\tilde{i}) - \omega(\tilde{i})) < n \sum_{\tilde{i} \leq \tau} \frac{1}{\tilde{i}^{\nu}},$$

ahol $\sum_{\tilde{i}}$-vel azt jelöljük, hogy csak azokra az $\tau$ értékekre kell az összegzést végezni, amelyek a primek egyenlő nagyobb kitevőjű hatványai. Az 5.6.1b feladat [148] megoldásánál beláttuk, hogy ez az összeg kisebb 1-nél.

(b) Ez az (a) részből és az említett tételekből következik.

6.7.6 Használjuk fel a 6.2.21a feladatot [178], és alkalmazzuk a Hardy–Ramanujan-tételt $\omega$ -ra és (a 6.7.5b feladat [211] alapján) $\Omega$-ra.

6.7.7 A (melepő) válasz: 0. — Útmutatás: Használjuk fel, hogy a Hardy–Ramanujan-tétel megfelelője érvényes $\Omega$-ra is (lásd a 6.7.5b feladatot [211]). Tegyük fel, hogy $\tilde{i} = ab$, ahol $a$ és $b$ kisebb, mint $\sqrt{\tau}$. Ekkor a „legtöbb esetben” $\Omega(a)$ és $\Omega(b)$ is „körülbéliül”

$$\log \log \sqrt{\tau} \sim \log \log n,$$

és így $\Omega(\tilde{i}) \sim 2 \log \log \tau$. Ilyen $\tilde{i}$ azonban (ismét a 6.7.5b feladat [211] szerint) csak kevés van.
6.7.8 A pontos tételt úgy kapjuk, ha a T 6.7.7 Tételben az $\omega$ helyére az (előírt tulajdonságokkal rendelkező) $f$-et, a $\log \log \iota$ helyére pedig a

$$\sum_{p \leq x} \frac{f(p)}{p^\alpha}$$

értéket írjuk. A bizonyítás ugyanúgy történik, mint a T 6.7.7 (és T 6.7.7A) Tétel esetén.

13.6.8.

6.8.1 Rögzített $m$ és $k = 1, 2, \ldots$ mellett az $f(m^k) = k f(m)$ számsorozat csak úgy lehet korlátos, ha $f(m) = 0$.

6.8.2 Legyen $m$ rögzített, és tekintsük azokat a $k$ pozitív egészeket, amelyekre $\{k, m\} = 1$. Ekkor $f(m) = f(km) - f(k)$. A Cauchy-féle konvergenciakritérium szerint bármilyen $\varepsilon > 0$ esetén elég nagy $k$ mellett $|f(km) - f(k)| < \varepsilon$ teljesül, és így csak $f(m) = 0$ lehetséges.

6.8.3 Az alábbi függvények felelnek meg:

$$f = 0; \quad g_r(a) = a^c; \quad h_r(a) = \begin{cases} 1, & \text{ha } a = 1, \\ r, & \text{ha } a = 2, \\ 0, & \text{ha } a > 2, \end{cases}$$

ahol $c$ tetszőleges valós szám és $0 \leq r \leq 1$.

Útmutatás: Ha a függvény mindenhol pozitív értéket vesz fel, akkor a logaritmusára alkalmazhatjuk a T 6.8.1 Tételt, és így a fenti $g$: függvényeket nyerjük. Ha a függvény valahol 0 értéket veszi fel, akkor minden nagyobb helyen is 0-t kell felvenni; ennek alapján mutassuk meg, hogy a legkisebb olyan hely, ahol a 0-t veszi fel, nem lehet nagyobb, mint 3. Ebből az $f = 0$ mellett a fenti $h_r$ függvényeket kapjuk. Végül könnyen adódik, hogy a függvény séhol sem vehet fel negatív értéket.

6.8.4 Ekkor a $-f$ függvény kielégíti a T 6.8.1 Tétel bizonyításában szereplő (1) feltételeit.

6.8.5 Az $f$ valós és képzetes részére külön-külön alkalmazható a T 6.8.1 Tétel.

6.8.6

(a) Megfelel például a

$$k_1, 2k_1, 2k_2, 3k_2, 3k_3, 4k_3, \ldots, jk_j, (j + 1)k_j, \ldots$$

sorozat, ahol $\{k_j, j(1 + 1)\} = 1$ és $k_j$ számok (az előírt $b_a$ elemekhez képest) elegendően nagyok. Ha a sorozat elemein az $f$ például monoton növő, akkor az additivitás miatt

$$f(j) + f(k_j) = f(jk_j) \leq f((j + 1)k_j) = f(j + 1) + f(k_j),$$

ahonnan $f(k_j)$ kivonása után $f(j) \leq f(j + 1)$, azaz $f$ monotonitása adódik. Ezután a T 6.8.1 Tételből következik, hogy $f(a) = c \log \iota$.

(b) Megfelel például a

$$c_1, c_2 d_1, c_2 d_2, c_3 d_3, \ldots, c_j d_j, \ldots$$
sorozat, ahol a \(d_1, d_2, \ldots\) számsorozatban minden 1-nél nagyobb egész végétlen sokszor fordul elő, továbbá \((v_j, d_j) = 1\) és a \(v_j\) számok (az előírt \(b_k\) elemekhez képest) elegendően nagyok. Legyen \(m > 1\) rögzített és \(\varepsilon > 0\) tetszőleges. Ekkor a sorozat konstrukciója, \(f\) additivitása és a feladat feltétele miatt van olyan (nagy) \(j\), amelyre \(m = d_j\) és
\[
|f(m)| = |f(v_jd_j) - f(v_j)| < \varepsilon,
\]
tehát csak \(f(m) = 0\) lehetséges.

### 13.7 Diofantikus egyenletek

#### 13.7.1.

7.1.1 Háromféleképpen. (10000 = 201 \cdot 47 + 7 \cdot 79 = 122 \cdot 47 + 54 \cdot 79 = 43 \cdot 47 + 101 \cdot 79.)

7.1.2 14.

7.1.3 Hétféleképpen. — Útmutatás: A \(7x + 13y + 15z = 500\), \(x, y, z = 50\) egyenletrendszerből például \(x\) -et kiküszöbölve a \(6y + 8z = 150\), majd ezt 2-vel osztva a \(3y + 4z = 75\) diofantikus egyenletethez jutunk. Ennek olyan megoldásait keressük, ahol \(y \geq 0\), \(z \geq 0\), továbbá \(x \geq 0\) miatt \(y + z \leq 50\).

7.1.4 9.

7.1.5 Az \(ax + by + c\) diofantikus egyenletet \(b \neq 0\) esetén egy \(x, y\) egész számpár pontosan akkor elégti ki, ha \(x\) megoldása az \(ax + c(\frac{1}{b})\) lineáris kongruenciának (és \(y\) értéke ekkor egyértelműen adódik az egyenletről). Vegyük észre, hogy a 2.5.4 Tétel bizonyításában szereplő (5) képlet (a jelölések „konverziója” után) éppen a T 7.1.1 Tétel (1) képletének az \(x\)-re vonatkozó részével azonos. (Nem feltétlenül szükséges a bizonyításra támaszkodni, elég csak a T 2.5.4 Tétel állítását felhasználni, ekkor azonban kicsit nehézesebb a gondolatmenet.)

7.1.6 (a) 0 vagy \(\infty\). (b) 0 vagy 1.

7.1.7 \(x = -3 - 5\nu - 10\nu, y = 3\nu + 3\nu + 1, z = 2\nu + 1\). — Útmutatás: A kétismeretlenes esethez hasonlóan az egyik ismeretlen kifejezve, majd a törtből a biztosan egész értékű részt leválasztva és alkalmas új ismeretlenet bevezetve csökkentsük az együttáthatók abszolút értékét mindaddig, amíg a tört nevezője 1 lesz. Ezután az így adódó két egész paraméterrel írjuk fel az eredeti ismeretlenek értékeit.

7.1.8 Egy lehetséges út, ha a T 7.1.1 Tétel után vázolt megoldási algoritmust általánosítjuk (ezt alkalmaztuk az előző feladatnál is), ebből a megoldhatóságra vonatkozó állítás is kihozható. —

Egy másik lehetőség a \(k\) szerinti teljes indukció. A \(k\) ismeretlenes \(a_1x_1 + \cdots + a_kx_k = c\) egyenletet a következőképpen vezethetjük vissza \(k - 1\) ismeretlenesre: Legyen \(d = \gcd(a_k-1, a_k)\), ekkor \(a_{k-1}x_{k-1} + a_kx_k\) alakban éppen \(d\) többszörösei, azaz a \(d\) számok állnak elő. Így az eredeti egyenlet helyett visszahatjuk a \(k - 1\) ismeretlenes \(a_1x_1 + \cdots + a_{k-2}x_{k-2} + dy = c\) egyenleten, amelyre már alkalmazhatjuk az indukciós feltételt.

7.1.9 Ha az egyenlet megoldható, akkor az egyenlet bármely megoldása nyilván megoldása a kongruenciának is tetszőleges \(m\) modulus esetén. Ha az egyenlet nem oldható meg, akkor \(\{a_1, \ldots, a_k\} \nmid c\), és ekkor az \(m = \{a_1, \ldots, a_k\}\) modulusra nyilván a kongruencia sem oldható meg.
7.1.10 Ez pontosan akkor igaz, ha az \( a_i \) számok relatív prímek és található közöttük pozitív. – Útmutatás: A feltétel szükségsessége nyilvánvaló. Az elégségsességhez tegyük fel, hogy például \( a_1 > 0 \). Ha valamely \( a_0 \) -ra sikerül pozitív egészekből álló megoldást találni, akkor \( x_i \) értékét növelve és a többi \( x_i \) értékét változtatlanul tartva, a \( a_i \)-lal reprezentált modulo \( a_0 \) maradékosztály minden \( a_0 \) nál nagyobb elemére is kapunk megfelelő megoldást. Így elég azt megmutatni, hogy minden modulo \( a_1 \) maradékosztálynak van olyan \( c \) eleme, amelyre létezik pozitív egész megoldás. Ehhez használjuk fel, hogy az

\[
a_1x_1 + \cdots + a_kx_k = c
\]

diofantikus egyenlet (a 2.5 pontban pontosan megfogalmazott értelemben) „ekvivalens” az

\[
a_2x_2 + \cdots + a_kx_k \equiv c \pmod{a_1}
\]

kongruenciával. Oldjuk meg a (2) kongruenciát \( c = 1, 2, \ldots, a_1 \) -re. (Biztosan létezik megoldás, mert \((a_1, \ldots, a_k) = 1\) miatt (1) bármely \( c \) -re megoldható az egész számok körében.) Mivel kongruenciáról van szó, nyilván az is feltehető, hogy mind az \( a_1 \) darab kongruencia esetében a kapott \( x_2, \ldots, x_k \) értékek mindegyike pozitív.

7.1.11

(a) Legyen \( a > b \), és alkalmazzuk az előző feladat alapötletét. Eszerint ha egy \( c \) összerakható, akkor nyilván bármely pozitív \( t \) -vel \( c + tb \) is összerakható. Így a feladat megoldásához mindegyik modulo \( b \) maradékosztályban meg kell keresni a legkisebb összerakható elemet. Mivel \((a, b) = 1\), ezért a \( 0, 1, a, 2a, \ldots, (b-1)a \) elemek teljes maradékrendszer alakot alkotnak modulo \( b \), vagyis az egyes maradékosztályok legkisebb összerakható elemei \( b, a, 2a, \ldots, (b-1)a \). Ez azt jelenti, hogy a legnagyobb nem összerakható szám az „utolsóként belépő” \((b-1)a\) -val reprezentált maradékosztály \((b-1)a - b = ab - c - b\) eleme.

(b) Válasz: \((a-1)(b-1)/2\). (Ez biztosan egész szám, hiszen \((a, b) = 1\) miatt \( a \) és \( b \) közül legalább az egyik páratlan.) — Útmutatás: Mutassuk meg, hogy ha két pozitív egész összege \( ab - c - b \), akkor közülük az egyik összerakható, a másik pedig nem.

7.1.12 A megoldásokhoz kényelmesebb a feladatot „fordított” szemlélettel, „összeállítás” helyett „szétvágásra” átfogalmazni: egy adott kocka (a) minden elég nagy \( n \), illetve (b) \( n \geq 48 \) esetén szétvágható pontosan \( n \) darab kockára.

(a) Mivel egy kockából könnyen csinálhatunk 8, illetve 27 kis kockát, ezek egymás utáni alkalmazásával egy kocka \( 1 \div 7x \div 26y \) részre is bontható, ahol \( x \) és \( y \) tetszőleges nemnegatív egészek. A 7 és a 26 relatív prímek, és így valóban minden elég nagy \( n \) előállítható ilyen alakban.

(b) Mivel egy kockát 8 részre vágva, a kis kockák számát mindig tudjuk 7-tel növelni, ezért elég az állítást a 48 és 54 között \( n \) -ekre igazolni.

48: \( 45 = 27 + 3 \cdot 7 \), azaz a kockát vágjuk 27 részre, majd 3 kis kockát 8-8 részre.

49: egy 6 oldalú kocka alsó felét bontsuk 4 darab 3 oldalú kockára, a felső sorát 36 darab egységkockára, a fennmaradó két sor pedig 9 darab 2 oldalú kockára.

50: \( 50 = 7 \cdot 7 + 1 \).

51: egy 6 oldalú kocka alsó felét és még egy nyolcadát bontsuk 5 darab 3 oldalú kockára, a megmaradt részből kiválaszthatunk 5 darab 2 oldalú kockát és marad még 41 darab egységkocka.
52: egy 4 oldalú kockából vegyünk ki egy 3 oldalú részt, ekkor marad 37 egységkocka, ezekből kettőt 8-8 részre osztva összesen 52 kockára bontottuk az eredeti kockát.

53: \[ 50 = 1 \cdot 2 + 19 \cdot 2 + 7 \] alapján eléggő olyan eljárást mutatni, amely 19-cel növeli a kockák darabszámát; egy 3 oldalú kockát bontunk egy 2 oldalúra és a megmaradó 19 egységkockára.

54: egy 8 oldalú kocka háromnegyedét bontsuk 6 darab 4 oldalú kockára, a maradékából leválasztható 2 darab 3 oldalú és 4 darab 2 oldalú kocka, valamint marad 42 darab egységkocka.

13.7.2.

7.2.1 Mutassuk meg, hogy ha \[ x^2 + y^2 = z^2 \], akkor \[ x, y \] és \[ z \] között található 3-mal, 4-gyel, illetve 5-tel osztható. Nézzük például az 5-tel való oszthatóságot. Egy négyszetszám 5-tel osztva 0, 1 vagy −1 maradéket ad. Tegyük fel indirekt, hogy \[ x, y \] és \[ z \] egyike sem osztható 5-tel, ekkor \[ x^2 + y^2 = z^2 \] bal oldala 0-val vagy \[ \pm 2 \] -vel kongruens modulo 5, a jobb oldal viszont \[ \pm 1 \] -gyel, ami ellentmondás. A 4-gyel, illetve 3-mal való oszthatóság is hasonlóan igazolható. (Mindhárom oszthatóságnál az egyenlet helyett a T 7.2.1 Tétel szerinti karakterizációt használva is hasonlóan bizonyíthatunk.)

7.2.2 Válasz: \[ 8, 15, 17 \]. — Útmutatás: Az \[ xy/2 \] területképlet alapján \[ xy = 120 \]. A 120 összes lehetséges felbontását megvizsgálva csak a \[ 8 \cdot 15 \] esetben lesz \[ x^2 + y^2 \] négyszetszám. — Másik lehetőség: A T 7.2.1 Tétel alapján \[ 60 = d^2 + 96mn(m - n)(m + n) \] egyenletet kell megoldani az ott megadott (4) feltételrendszerét is figyelembe véve. Így egyedül a \[ d = 1, m = 4, n = 1 \] eset lehetséges.

7.2.3 Válasz: \[ 6, 8, 10 \] és \[ 5, 12, 13 \]. — Útmutatás: A T 7.2.1 Tétel alapján a terület \[ d^2 + 96mn(m - n) \], a kerület pedig \[ 2d + 96mn(m - n) \] az egyenlet megoldása.

Ezek egyenlősége az egyszerűsítések után a \[ d^2 + 96mn(m - n) = 2 \] egyenletet jelenti. Ennek a T 7.2.1 Tétel (4) feltételét is kielégítő megoldásai \[ d = m - 2, n = 1 \], illetve \[ d = 1, n = 2, m = 3 \]. — Másik lehetőség: Az

\[
\frac{xy}{2} = x - y + z, \quad x^2 - y^2 = z^2
\]
diofantikus egyenletrendszer megoldani. Az első egyenlethből átrendezéssel kapott

\[
\frac{xy}{2} = z = x + y
\]
egyenlőséget emeljük négyzetre, ekkor a második egyenlet felhasználásával és \[ x \cdot y \]-nal történő egyszerűsítés után \[ z = (xy/4) - 2 \] adódik. Ezt az első egyenletbe visszahelyettesítve, átrendezés és szorzattal alakítás után \[ (x - 4)(y - 4) = 8 \] egyenletbe jutunk. Mivel \[ x \] és \[ y \] pozitív, ezért (a tényezők sorrendjétől eltekintve) csak az \[ 1 \cdot 8 \] és \[ 2 \cdot 4 \] előállítás ad megoldást.

7.2.4 Válasz: minden \( k \geq 3 \)-ra. — Útmutatás: Használjuk a T 7.2.1 Tételt. Lássuk be, hogy az 1 és a 2 nem állítható elő az ott megadott \[ x, y \], illetve \[ z \] alakok egyikeként sem. A 2-nél nagyobb számok esetén pedig a képletben szereplő \[ d \] szorzó miatt elég azt igazolni, hogy a 4 és a páratlan számok előállnak ilyen alakban: \( 4 = 2 \cdot 2 \cdot 1 \), illetve \( 2r + 1 = (r + 1)^2 - 2 \).

7.2.5 Ha \[ x, y, z \] primitív pitagoraszi számhármas, akkor \( (y - x)^2 \), \( x^2 \) és \( (x + y)^2 \) relatív primek, és számíthatván sorozatot alkotnak.

Megjegyzés: Az \( x^2 + y^2 = 2u^2 \) diofantikus egyenlet \( 0 < u < w < v \) és az \( x^2 + y^2 = z^2 \) pitagoraszi egyenlet \( 0 < x < y < z \) megoldásai kölcsönösen visszavezethetők egymásra, az
$a = y - x, v = x + y, w = z$, illetve a fordított irányú $x = (v - u)/2, y = (u + v)/2, z = u$ helyettesítéssel ($x$-re és $y$-ra egész számokat kapunk, mivel $u$ és $v$ szükségképpen azonos paritású). Ennek alapján az $d^2 + v^2 = 2u^2$ egyenlet összes megoldását is felirhatjuk három egész paraméter segítségével.

### 13.7.3.

#### 7.3.1
Mivel az $x$ és $y$ előjele most nem számít, ezért az összes egész körében kapott megoldásokat négyesével csoportosítva kapunk egy-egy „lényegesen különböző megoldást”, kivéve az $y = 0$ esetet (amely csak akkor fordul elő, ha $u$ négyzeteszám). Ennek megfelelően a „lényegesen különböző megoldások” száma $\left\lfloor \frac{2^u}{u} \right\rfloor$, ahol $\frac{2^u}{u}$ a T 7.3.1 Tételben megadott megoldásszám.

#### 7.3.2 Két megoldás van: a süteményt a tepsi oldalaival párhuzamosan 6, illetve 8, vagy pedig 5, illetve 12 részre kell vágni (az első esetben 48, a második esetben 60 szelet keletkezik). — Útmutatás: Ha a tepsi oldalaival párhuzamosan $x$, illetve $y$ részre vágunk, akkor $x^2+y^2$ égett és $(x-2)(y-2)$ nem égett szelet keletkezik. Az így kapott egyenlet az $(x-4)^2(y-4) = 8$ alakra hozható. — Másik lehetőség: A tepsi fala mentén körbehaladó „sorban” összesen 8-cal több szelet van, mint a következő (szintén „körbefutó”) sorban. Ez azt jelenti, hogy ennél a két sor nál beljebb is összesen 8 szelet van, amelyek egy $2 \times 4$ -es vagy egy $1 \times 8$ -as téglaalapot alkotnak.

#### 7.3.3 A $2/p = 1/x + 1/y$ egyenlet a $(2x - 2p)/(2y - 2p) = p^2$ alakra hozható. — Ottlik Géza megoldása: Az egyenletet $2p$ -nél beszorozva kapjuk, hogy valamelyik ismeretlen osztható $p$ -vel, mondjuk $x = kp$. Ezt visszahelyettesítve fejezzük ki $y$ -t, és lássuk be, hogy $p = 2k - 1$. Innen $x$ és $y$ is egyértelmű.

#### 7.3.4 Pontosan azok, ahol a nevezőnek van nem $1$ alakú pozitív osztója.

#### 7.3.5 Az $\frac{1}{u} = \frac{1}{2u} + \frac{1}{2u}$ egyenlőség alapján elég megmutatni, hogy a megadott $n$ -ekre $4/n$ felírható két vagy három természetes szám reciprokának az összegeként.

<table>
<thead>
<tr>
<th>$u$</th>
<th>$\frac{4}{u}$</th>
<th>$\frac{1}{u}$</th>
<th>$\frac{1}{2u} + \frac{1}{2u}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2s$</td>
<td>$\frac{1}{s} + \frac{1}{s}$</td>
<td>$\frac{1}{s}$</td>
<td>$\frac{1}{s}$</td>
</tr>
<tr>
<td>$4s - 1$</td>
<td>$\frac{1}{3} + \frac{1}{4s}$</td>
<td>$\frac{1}{4s}$</td>
<td>$\frac{1}{4s}$</td>
</tr>
<tr>
<td>$8s - 3$</td>
<td>$\frac{1}{2u} + \frac{1}{2u}$</td>
<td>$\frac{1}{2u}$</td>
<td>$\frac{1}{2u}$</td>
</tr>
<tr>
<td>$24s - 15$</td>
<td>$\frac{1}{8s - 3} + \frac{1}{24s - 15}$</td>
<td>$\frac{1}{8s - 3}$</td>
<td>$\frac{1}{8s - 3}$</td>
</tr>
<tr>
<td>$24s - 7$</td>
<td>$\frac{1}{8s} + \frac{1}{24s - 7}$</td>
<td>$\frac{1}{8s}$</td>
<td>$\frac{1}{8s}$</td>
</tr>
</tbody>
</table>

#### 7.3.6 Induljunk ki az $a/j = 1/b + 1/b + \cdots + 1/b$ („rossz") előállításból, majd alkalmazzuk elég sokszor például az $\frac{1}{n} = \frac{1}{n + 1} + \frac{1}{n(n + 1)}$
7.3.7 Nincs. — Útmutatás: Az $z^4 - 4 = y^3$ diofantikus egyenlet bal oldalát szorzattá bontva, a két tényező páratlan és hatvány, és így külön-külön is ötödik hatvány, a különbségük 4, ami lehetetlen. Páros $z$-re pedig az egyenlet bal oldala nem osztható 8-cal, a jobb oldal viszont igen.

7.3.8 Az egyetlen megoldás $x = y = s = i = 0$. — Útmutatás: A feladat egyszerűen visszavezethető az egész megoldások keresésére, sőt (az indirekt feltételezett nemtriviális megoldásról) az is feltethető, hogy $(x, y, s, i, t) = 1$. Ekkor a paritást vizsgálva ellentmondásra jutunk. — Másik lehetőség: Egy nemtriviális egész megoldás olyan szabályos háromszög középpont, amelynek mindhárom oldal éle osztható szám. Területi megfontolásokkal mutassuk meg, hogy nincs ilyen háromszög.

7.3.9 Az összeg 3-mal osztható, de 9-nél nem.

7.3.10 $\pm 4$, $\pm 6$.

7.3.11 A feladat „csúnya” megoldása: Legyen a hat szám $n, n+1, \ldots, n+5$, és osszuk ezeket minden lehetséges módon két csoportba. Azt kell igazolni, hogy az így adódó egyenletek egyikének sincs egész megoldása. Mivel egy egész együtthatós polinom egész (sőt racionális) gyökéi könnyen megkereshetők, ezért a feladat megoldása csak némi türelmes számlálást igényel. Természetesen nem kell minden lehetőséget számításba venni, például a tényezőkénti összehasonlításból látszik, hogy $u(n+1)(n+4)$ minden $u>0$ esetén kisebb, mint $(n+2)(n+3)(n+5)$, és más hasonló megfontolások is alkalmazhatók.

7.3.12 Csak páros $m$-re van megoldás: $u = m + 1$ és $x = y = 2^{m/2}$.

Útmutatás: Az egyenlet $\left\{x, y\right\}$ segítségével átírva mutassuk meg, hogy csak $z = y$ lehetséges. Ebben az esetben az egyenlet a

$$\frac{m}{2} = 2^{m/2}$$

alakra hozható. Ekkor nyilván $x = 2^s$. Ezt (3)-ba visszairva lássuk be, hogy $n = 2s$ és $n = m + 1$.
7.3.13

(a) Az \((x + 5)(y + 3) = 22\) alakból könnyen leolvasható a \(2d(22) = 8\) darab megoldás.
(b) Nincs megoldás. Az egyenletet modulo 11 érdemes vizsgálni.
(c)–(e) Csak a triviális \(x = y = z = 0\) megoldás létezik. A „jó” modulusok: (c)-nél 3 vagy 8; (d)-nél 5, 7, 8 vagy 23; (e)-nél 11.
(f) \(x = \pm 1\), \(z = -2\). — Útmutatás: a bal oldal két tényezője bármely \(x\) egész szám esetén relativ prim, ezért külön-külön is köbszámok.
(g) \(x = \pm 1\), \(y = 0\). — Útmutatás: Egyszerű átalakítások után azt kapjuk, hogy két szomszédos szám szorzata „majdnem” negyedik hatvány. Ezen az úton továbbhaladva, alkalmas kongruenciavizsgálatok után még egy szorzattá bontásra van szükség.
(h) \(y = z\), valamint \(x = 2\), \(y = 4\) és \(z = 4\), \(y = 2\). — Útmutatás: írjuk át az egyenletet \((x, y, z)\) segítségével, vagy pedig logaritmálás után használjuk fel az \(f(z) = z/\log z\) (valós) függvény viselkedését.
(i) \(x = 5\), \(y = 1\). — Útmutatás: Vizsgáljuk az egyenletet modulo 31, és használjuk fel a hatványmaradékokról tanultakat.

7.3.14

(a) Nincs ilyen számrendszer. — Útmutatás: \(x > 0\) esetén \(1 + x + x^2\) mindig két szomszédos négyzetszám közé esik.
(b) A 3-as számrendszer az egyetlen megoldás. — Útmutatás: \(x > 3\) esetén \(4(1 + x + x^2 + x^3 + x^4)\) két szomszédos négyzetszám közé esik.
(c) Nincs ilyen számrendszer. — Útmutatás: A megfelelő kifejezés két relativ prim tényező szorzatára bontható, és közelül az egyik nem lehet négyzetszám.

13.7.4.

7.4.1 \(|1 + i| a + bi \iff a \equiv b \pmod{2}\).

7.4.2

(a) \(\alpha = \gamma \rho \iff \overline{\alpha} = \overline{\gamma \rho}\).
(b) Az (a) részből következik.
(c) Következik akár a Gauss-felbontatlan, akár a Gauss-prím definíciójából, vagy pedig a T 7.4.15 Tételből.

7.4.3 A 7.4.2a feladat [234] szerint \(\alpha \mid a \iff \overline{\alpha} \mid a\), vagyis ekkor \(\alpha = \varepsilon \overline{\alpha}\), ahol \(\varepsilon\) egység. Mutassuk meg, hogy itt a két oldal abszolút értéke mindig egyenlő, a szögek összehasonlításából pedig \(\arg(\varepsilon) = k \cdot 45^\circ\) adódik. Ez pontosan azt jelenti, hogy \(\alpha\) a koordinátatengelyek vagy pedig az \(y = \pm x\) egyenesek valamelyikén helyezkedik el. (Az \(\alpha = \varepsilon \overline{\alpha}\) egyenlőségből az \(\varepsilon = \pm 1\) és \(\pm i\) esetek végigpróbálásával is ugyanerre az eredményre jutunk.)

7.4.4

(a) Használjuk fel, hogy az \(a/b\) racionális szám akkor és csak akkor Gauss-egész, ha egész szám.
(b) Ha \((a, b) = d\) az egész számok körében, akkor azt kell igazolni, hogy az \(a_1 = a/d\) és \(b_1 = b/d\) számok a Gauss-egészek körében is relatív primek. Ha egy \(\gamma\) Gauss-egész közös osztója \(a_1\)-nek és \(b_1\)-nek, akkor \(N(\gamma)\) az egész számok körében közös osztója \(N(a_1) = a_1^2\)-nek és \(N(b_1) = b_1^2\)-nek, amiből következik, hogy \(N(\gamma) = 1\), tehát \(\gamma\) egység. (Egy másik lehetőség, hogy alkalmas \(u\) és \(v\) egész számokkal \(1 = a_1u + b_1v\), és így \(\gamma \mid a_1\) és \(\gamma \mid b_1\) esetén szükségképpen \(\gamma \mid 1\).)

7.4.5 Igaz: (a), (c).

7.4.6 (Természetesen a megadott eredmények helyett azok bármelyik egységszerese is helyes.)

(a) \(2 - i\). — Útmutatás: alkalmazzuk az euklideszi algoritmust.

(b) \(2\). — Útmutatás: használjuk fel, hogy \(1 - i\) és \(2 + i\) Gauss-prímek, továbbá \(2 = (1 - i)^2\) és \(2 + i = 39\).

(c) \(1 + i\). — Útmutatás: A keresett \(\delta\) legnagyobb közös osztó osztója a két szám összegének és különbségének is, ahonnan \((1 + i, 2 - i) = 1\) miatt \(\delta \mid 2\) adódik. Innen \(\delta = 1\) vagy \(2\) vagy \(1 + i\). Végül mutassuk meg, hogy az első két eset nem lehetséges.

7.4.7

(a) Igaz: (a1).

(b) \((u, \overline{v}) = (u, b)\) vagy \((u, \overline{v}) = (1 + i)(u, b)\).

7.4.8 Mutassuk meg, hogy \(\beta\) akkor és csak akkor barátja \(\alpha\)-nak, ha \(\beta = \overline{\alpha}\) és \((\alpha, \overline{\alpha}) = 1\). Így \(\alpha\)-nak (0 vagy) 4 barátja van, és könnyen adódik az (a)-beli feltétel is.

7.4.9 \(3^2(2 + i)(-2 - i)(1 + i)^3(4 - 4i)\). — Útmutatás: Érdemes először a 90-et kiemelni és a T 7.4.15 Tétel szerint Gauss-prímek szorzatára bontani. A fennmaradó rész \(3 + 20i = \pi_1 \cdots \pi_r\) felbontásának a meghatározásához térjünk át a normákra: \(850 = \prod \pi_i\). A 850 kanonikus alakjából kapjuk, hogy \(\pi_1 = 4\), és a \(\pi_i\) Gauss-prímek normái 2, 5, 5 és 17. Innen \(\pi_1 = 1 + i\), \(\pi_2 = \pi_3 = 2 + i\) vagy \(2 - i\), aszerint hogy \((3 + 20i)/(2 + i)\) Gauss-egész-e vagy sem (\(\pi_3 = \overline{\pi_2}\) nem lehet, miért?) stb.

7.4.10 Igaz: (b), (c), (e).

7.4.11 Bizonyítsunk \(N(\varepsilon)\) szerinti teljes indukcióval. A kulcslépés: Ha az \(\alpha\) két különböző felbontása Gauss-prímek szorzatára

\[\alpha = \pi_1 \cdots \pi_r = \varepsilon_1 \cdots \varepsilon_s, \quad \text{ahol} \quad \pi_i \neq \varepsilon_j,\]

akkor létezik olyan \(\varepsilon\) egység, hogy \(N(\pi_1) \leq N(\varepsilon_1)\) esetén az

\[\alpha_1 = \varepsilon \alpha = \pi_1 \varepsilon_2 \cdots \varepsilon_s\]

Gauss-egészre \(N(\alpha_1) < N(\alpha)\), és \(\alpha_1\)-nek is két különböző felbontása van Gauss-prímek szorzatára.

13.7.5.

7.5.1 \[
\left[ \begin{array}{c}
\varepsilon(\nu)
\end{array} \right]_k,
\]

ahol \(\nu(\nu)\) a T 7.5.1 Tételben megadott megoldásszám (ha az egyenlet nem oldható meg, akkor \(\nu(\nu) = 0\)). — Útmutatás: Az \(\varepsilon\) és \(\nu\) felszereléséből, illetve az előjelek változtatásával
kapott megoldások nem adnak „lényegesen különböző” megoldást. Ez általában 8 lehetőség, kivéve azokat a megoldásokat, amikor \( x \) és \( y \) valamelyike 0, vagy \( x^2 = y^2 \) (ezek csak az \( n = k^2 \), illetve \( n = 2k^2 \) esetekben fordulhatnak elő).

7.5.2 Válasz: 7. — Útmutatás: A \( 8k + 6 \) alakú számok nem írhatók fel két négyzetszám összegeként vagy különbségeként, tehát \( r \leq 7 \). Azt kell még igazolni, hogy végzetlen sok esetben teljesül, hogy két egymást követő \( 8k + 6 \) alakú szám között minden hét szám előáll a kívánt módon.

7.5.4 A T 7.5.1 Tétel szerint az \( a^2 + b^2 \) kanonikus alakjában szereplő 7 és 11 prímek kívüli páros, azaz legalább 2 kell hogy legyen. — Másik lehetőség: a 7 és a 11 Gauss-primek, tehát

\[
7 | a^2 + b^2 = (a + bi)(a - bi) \implies 7 | a + bi \text{ vagy } 7 | a - bi \implies \frac{a + bi}{7} \text{ vagy } \frac{a - bi}{7} \text{ Gauss-egész} \implies 7 | a \text{ és } b,
\]
e és ugyanez érvényes a 11-re is.

7.5.5 Akkor és csak akkor van megoldás, ha az \( n \)-kanonikus alakjában minden \( 4k - 1 \) alakú prim kitevője páros és a 2 kivetője nem 1. Ekkor a megoldásszám ugyanaz, mint a T 7.5.1 Tételében, ha \( n \) osztható 4-gyel, és az ottani értéke fele, ha \( n \) páratlan.

7.5.6 Akkor és csak akkor van megoldás, ha \( n \) nem osztható 4-gyel és nincs \( 4k - 1 \) alakú primosztója. Ebben az esetben a megoldásszám \( 2^{r - 2} \), ahol \( r \) az \( n \) páratlan (\( 4k + 1 \) alakú) primosztóinak a száma.

7.5.7
(a) Annak megfelelően, hogy \( k \) az átfogó, illetve az egyik befogó hossza, az \( x^2 + y^2 = k^2 \), illetve \( x^2 - y^2 = k^2 \) diofantikus egyenletek „lényegesen különböző”, pozitív egész \( a, b \) megoldásainak a számát kell meghatározni. A T 7.5.1 Tétel (és a 7.5.1 feladat [240]) alapján az első egyenletnél ez a megoldásszám

\[
\frac{(2\beta_1 - 1) \ldots (2\beta_r - 1) - 1}{2},
\]
ahol \( \beta_1, \ldots, \beta_r \), a \( k \)-kanonikus alakjában szereplő \( 4t + 1 \) alakú prímek kitevői. A második egyenletnél pedig a T 7.3.1 Tétel (és a 7.3.1 feladat [226]) felhasználásával kapjuk, hogy a keresett megoldásszám

\[
\frac{1}{2}(d(k^2) - 1) \text{ há k páratlan};
\]
\[
\frac{1}{2}(d(k^2) - 1) \text{ há k páros}.
\]
(b) A 7.5.6 feladat [241] alapján az átfogó akkor és csak akkor lehet \( k \) hosszúságú, ha a \( k > 1 \) szám minden primosztója \( 4t + 1 \) alakú, és ekkor a háromszögek száma \( 2\omega(k - 1) \). Hasonló gondolatmenettel adódik, hogy \( k \) akkor és csak akkor lehet egy befogó hossza, ha \( k > 1 \) páratlan vagy pedig \( 4 \mid k \), és mindkét esetben \( 2\omega(k - 1) \) ilyen háromszög létezik.

A fenti meggondolások helyett a primitív pitagorasi számhármasokat karakterizáló T 7.2.1 Tétel alkalmazása is célhoz vezet.

7.5.8 Először tegyük fel, hogy egy \( 4k - 1 \) alakú \( \ell \) prim az \( n \)-kanonikus alakjában a \( 2n - 1 \) páratlan kitevővel szerepel. Ekkor az egyenletnek nincs megoldása, tehát azt kell igazolni, hogy \( n \) (pozitív) páratlan osztóinak a fele \( 4k + 1 \), a másik fele pedig \( 4k - 1 \) alakú. Az \( n \) tetszőleges páratlan osztója
EREDMÉNYEK ÉS ÚTMUTATÁSOK

felírható \(tg^n\) alakban, ahol \((i, 2q) = 1\) és \(0 \leq n \leq 2q - 1\). Ekkor (bármely \(0 \leq j \leq n - 1\) esetén) a \(tg^{2j}\) és \(tg^{2j+1}\) osztók közül az egyik \(4k + 1\), a másik pedig \(4k - 1\) alakú.

Most vizsgáljuk azt az esetet, amikor az \(n\) kanonikus alakjában minden \(4k - 1\) alakú \(q\nu\) prim kitevője páros, jelöljük \(q\nu\) kitevőjét \(2\nu\nu\)-vel. Ekkor a T 7.5.1 Tétel alapján azt kell megmutatni, hogy

\[
d'(u) - d''(u) = \prod_{i=1}^{r} (\delta_i + 1),
\]

ahol a \(\delta_i\) értékek az \(n\) kanonikus alakjában szereplő \(4k + 1\) alakú prímek kitevői. Végezzük el az előző párositást a \(q\xi\) szerint, ekkor csak azok a (páros párátlan) osztók maradnak ki, amelyekben a \(q\xi\) kitevője \(2u\). Ezekre az osztókra ismételjük meg az eljárást, most a \(q\xi\) szerint stb. Így végül azok a (páros) párátlan osztók maradnak meg, amelyekben mindig \(q\nu\) kitevője \(2\nu\nu\). Ezeknek az osztóknak a száma egyrészt nyilván az (1) jobb oldalán szereplő \(\nu\) kitevője, másrészt ezek az osztók valamennyien \(4k + 1\) alakúak, tehát a számuk éppen \(d'(u) - d''(u)\). — A feladat állítását egy lépésben is bebizonyíthatjuk, ha a \(D = d'(u) - d''(u)\) különbséget az alábbi módon írjuk fel:

\[
D = \sum_{\substack{0 \leq \beta_i, \gamma_i \leq \nu, \\ \beta_i \leq \gamma_i, \beta_i \nu}} (-1)^{\beta_i + \ldots + \gamma_i} \prod_{i=1}^{r} (\delta_i + 1) \prod_{i=1}^{\kappa} (1 - 1 + \ldots + (-1)^{\gamma_i}).
\]

7.5.9 Válasz: \(\pi\). — Útmutatás: Vegyük észre, hogy \(1 + \sum_{i=1}^{n} x(i)\) éppen az origó körüli \(\sqrt{n}\) sugarú kör belsőjébe vagy határára eső rácspontok száma. Mutassuk meg, hogy ezeknek a rácspontoknak a száma aszimptotikusan egyenlő a kör területével (ha \(n \to \infty\)).

7.5.10 Az összes megoldás: \(x = \pm 2, y = 2\) és \(x = \pm 11, y = 5\). — Útmutatás: Az egyenlet bal oldalát a Gauss-egészek körében bontsuk szorzattá, és vizsgáljuk meg a kéttényezők legnagyobb közös osztójának lehetséges értékeit. Ebből kiderül, hogy mindkét tényező egy-egy Gauss-egész köbe. Végül végezzük el a köbrel emelést, és hasonlítuk össze a képleteket.

7.5.11 \(a = c + bi\) akkor és csak akkor nem írható fel ilyen alakban, ha \(b\) páratlan, vagy \(a \equiv b \equiv 2 \pmod{4}\). — Útmutatás: Alkalmazzuk a T 7.3.1 Tétel bizonyításának gondolatmenetét.

7.5.12 A kanonikus alakban szereplő Gauss-prímek helyettesíthetők bármelyik egységszerűsükkel (és ezt a „külön egység” módosításával kompenzáltjuk).

7.5.13 Igaz: (a), (c).

7.5.14 Válasz: \(5/6\). — Útmutatás: Jelölje \(F'(N)\) az \(1, 2, \ldots, N\) egészek között azoknak a számát, amelyek nem írhatók fel három négyzetszám összegeként. Mutassuk meg, hogy

\[
F'(N) = \left\lfloor \frac{N + 1}{8} \right\rfloor - \left\lfloor \frac{N + 1}{8} - \frac{4}{8} \cdot 4 \right\rfloor + \left\lfloor \frac{N + 4^2}{8} \cdot 4^2 \right\rfloor + \ldots,
\]

és innen

\[
\lim_{N \to \infty} \frac{F'(N)}{N} = \frac{1}{8} \sum_{k=0}^{\infty} \frac{1}{8^k}.
\]

7.5.15 Válasz: 10. — Útmutatás: A három-négyzetszám-tétel segítségével igazoljuk, hogy 10 páratlan négyzetszám minden esetben elég, és a két-négyzetszám-tétel alapján mutassuk meg, hogy végíten sok \(8k + 2\) alakú számhoz 10-nél kevesebb páratlan négyzetszám nem elég.
7.5.16 Ha \( n = 4^k(8m + 7) \), akkor \( n - (2^k)^2 \) előáll három négyzetszám összegeként.

7.5.17 Egy \( n \) pozitív egész akkor és csak akkor \( nem \) áll elő így, ha \( n = 4^k(16m + 14) \) alakú. — Útmutatás: Mutassuk meg, hogy \( n \) akkor és csak akkor áll elő a kívánt alakban, ha \( 2n \) felírható három négyzetszám összegeként.

7.5.18 Megoldható. — Útmutatás: Azt kell megmutatni, hogy a megadott szám felírható négy olyan négyzetszám összegeként, amelyek közül legalább az egyik osztható 3-mal.

7.5.19 Chevalley tételéből (illetve a 3.6.2 feladatból [94]) következik, hogy az \( X^2 + Y^2 + Z^2 \equiv 0 \pmod{p} \) kongruenciának létezik nemtrivialis \( X, Y, Z \) megoldása. Ha például \( Z \neq 0 \pmod{p} \), akkor a kongruenciát \( p > 2 \) esetén \( Z^{p-3} \)-mal megszorozva kapjuk, hogy

\[
1 + a^2 + b^2 \equiv 0 \pmod{p}, \quad \text{ahol} \quad c = XZ^{(p-3)/2}, \quad d = YZ^{(p-3)/2}.
\]

7.5.20 A L 7.5.5 Lemma helyett az \( \omega^2 - 1 \equiv 0 \pmod{p} \) kongruencia megoldhatóságáról, a L 7.5.4 Lemma helyett pedig az

\[
(a_1^2 + a_2^2)(b_1^2 + b_2^2) = (a_1b_1 + a_2b_2)^2 + (a_1b_2 - a_2b_1)^2.
\]

7.5.21 (a) Képezzük azokat a \( u \) - \( v \) vektorokat, ahol \( s \) és \( \hat{s} \) megfelelő komponenseire

\[
0 \leq s_i < u_i, \quad 0 \leq t_i < v_i, \quad i = 1, 2, \ldots, k
\]
teljesül. A skatulyaelv alapján ezen \( u \) vektorok között lesz kettő, amelyik kongruens modulo \( P \), és ekkor az ezekhez tartozó \( s \) , illetve \( \hat{s} \) vektorok különbsége megfelel \( \omega \) -nek, illetve \( \omega \) -nek.

(b) Az (a) részt alkalmazzuk a

\[
k = 2, \quad u_1 = u_2 = v_1 = v_2 = \lfloor \sqrt{p} \rfloor, \quad C = \begin{pmatrix} \hat{a} & d \\ -d & \hat{c} \end{pmatrix}
\]
etetre, ahol \( 1 + c^2 - d^2 \equiv 0 \pmod{p} \). Innen azt kapjuk, hogy

\[
0 < x_1^2 + x_2^2 + z_1^2 + z_2^2 < 4p, \quad p | x_1^2 + x_2^2 + z_1^2 + z_2^2.
\]

(c) A 2\( p \) esetben ugyanúgy járhatunk el, mint amikor a T 7.5.3 Tétel bizonyítása során \( m \) páratlanságát igazoltuk.

Ha \( 3p \equiv a_1^2 + a_2^2 + a_3^2 + a_4^2 \) , akkor legyen \( b_1 \) az \( a_i \) legkisebb abszolút értékű maradéka modulo 3, és alkalmazzuk a L 7.5.4Lemma (10) azonosságát. A 2\( p \) -nek az így adódó felírásában mind a négy négyzetszám osztható 3-mal, tehát 9-cel való osztás után azt kapjuk, hogy a \( P \) is „szép”. (Ebben a lépésben tulajdonképpen a T 7.5.3 Tétel bizonyítását ismételtük meg az \( m = \hat{3} \) speciális esetre.)

### 13.7.6.

7.6.1 Ha \( n \) előáll \( s \) darab 600 -adik hatvány összegeként, akkor \( n \) ugyanennyi 200 -adik hatvány összege is, hiszen
7.6.2 A T 7.6.5 Tétel bizonyításához hasonlóan alkalmaz moduluskok szerinti kongruenciák adják a megoldás kulcsát.

(a1) Bizonyítsuk be \( j \) szerinti teljes indukcióval, hogy a \( 31 \cdot 16^j \) alakú számok nem állíthatók elő 16-nál kevesebb negyedik hatvány összegéből.

(a2) A \( 64t + 32 \) alakú számok nem írhatók fel 31 nyolcadik hatványból.

(a3) A 7.6.1 feladathoz [246] hasonlóan következik, hogy \( G'(24) \geq G'(8) \).

(a4) A \( 625t + 125 \) alakú számokhoz nem elég 124 század hatvány.

(a5) Vizsgáljuk a \( 625t + 312 \) alakú számokat.

(b) Az (a1)–(a3) részt a \( k = 2r \) és \( k = 3 \cdot 2r \) esetekre általánosíthatjuk, ahol \( r \geq 2 \). Mutassuk meg, hogy \( a^k \) csak 0 vagy 1 maradékot adhat modulo \( 2^{r+2} \), ennek igazolásához használjuk fel, hogy erre a modulusra nem létezik primitív gyök.

Az (a4) rész a \( p = \rho | p^a | \) esetre általánosítható, ahol \( p > 2 \) prim és \( \alpha \geq 2 \). A bizonyításban (a T 7.6.5 Tételén látt módon) az Euler–Fermat-tételt érdemes alkalmazni.

Az (a5) a \( k = \frac{1}{2} p | p^b | \) esetre általánosítható, ahol \( p > 2 \) prim és \( \alpha \geq 2 \). Lássuk be és használjuk fel, hogy bármely \( \alpha \)-ra

\[
\varphi(p^a) / 2 = 0 \lor (\gamma \pmod {\varphi(p^a)}).
\]

Ily módon a fenti esetekben a következő első becsléseket nyerhetjük \( G(k) \)-ra (\( p > 2 \) prim, \( \alpha \geq 2 \) és \( r \geq 2 \)):

\[
G(3 \cdot 2^r) > G(2^r) \geq 2^{r+2}; \quad G(p^\alpha - p^{\alpha-1}) > p^\alpha; \quad G\left(\frac{p^\alpha - p^{\alpha-1}}{2}\right) \geq \frac{p^\alpha - 1}{2}.
\]

Megjegyezzük, hogy a T 7.6.4 Tétel mellett mindössze ezek az első becslések ismertek \( G(k) \)-ra.

7.6.3 Legyen \( R \) eléggé nagy szám, és képezzük az

\[
x_1^b + \cdots + x_k^b, \quad x_i \in \mathbb{Z}, \quad 0 \leq x_i \leq R, \quad i = 1, 2, \ldots, k + 1
\]

összegeket. Mutassuk meg, hogy sokkal több összeg van, mint ahány különböző értéket felvehetnek. Ebből következik, hogy kell lennie olyan \( u \) -nek, amely sokféleképpen előáll ilyen összeg alakban.

7.6.4

(a) A bal oldalon a műveletek elvégzése és összevonások után csak \( a_i^1 \) és \( a_i^2 \) típusú tagok maradnak, és ezek mindegyike 6, illetve 12 együtthatóval szerepel. Ugyanezt kapjuk, ha a jobb oldalon elvégezzük a négyzetre emelést.

(b) Legyen \( u = 6q + r \), ahol \( 0 \leq r \leq 5 \). A T 7.5.3 Tétel alapján \( q = x_1^4 + x_2^4 + x_3^4 + x_4^4 \). Írjuk fel mind a négy \( x_i \)-t ismét négy négyzetszám összegeként. Ezután az (a)-beli azonosságot alkalmazva azt kapjuk, hogy \( 6q \) előáll 48 negyedik hatványból, a maradék \( r \) pedig legfeljebb 5 darab \( 1^{	ext{st}} \) tag összege.
7.6.5 A $8^6 + 6$ alakú számok nem állnak elő $x^2 \pm y^2$ alakban, tehát két négyzetszám nem elegendő.
Az állítás másik részének igazolásához rendezzük át az $u^2 + v^2 - z^2 = n$ diofantikus egyenletet $x^2 - y^2 = x^2 - n$ alakba, ezután válasszuk meg $x$ értékét tetszőlegesen, csak arra ügyelve, hogy $x^2 - n$ ne legyen $4k + 2$ alakú (bármely $u$ esetén vagy az összes páros vagy az összes páratlan szám biztosan megfelel $x$-nek, esetleg mind a párrosak, mind a páratlanok jöik). Végül használjuk fel a T 7.3.1 Tételt (és azt, hogy ha egy szám elődől két négyzetszám különbségeként, akkor a negatívja is). A másik diofantikus egyenlet esetén hasonlóan járhatunk el.

**13.7.7.**

7.7.1

(a) Ha $m = qk$, akkor

\[ x^m + y^m = z^m \rightarrow (x^q)^k + (y^q)^k = (z^q)^k. \]

(b) Az (a) részből következik, mivel bármely $k > 2$ esetén $k$-nak létezik páratlan prímosztója vagy $4 \mid k$.

7.7.2

(a) Nincs megoldás, ez a Fermat-sejtés $k = 4$ esetéből következik.

(b) Végtelen sok megoldás van. Keressünk $x = 2^\alpha$, $y = 2^\beta$, $z = 2^\gamma$ alakú megoldásokat, ekkor a

\[ 2^{2\alpha} + 2^{2\beta} = 2^{2\gamma} \]

eyenlethez jutunk. Az $\alpha = 4\nu$, $\beta = 3\nu$ választás mellett a $12\nu + 1 = 5\gamma$ feltételnek kell teljesülnie.

**Megjegyzés:** A fenti gondolatmenetek az alábbi $x^k + y^m = z^n$ típusú diofantikus egyenletekre általánosíthatók:

(i) Ha $(k, m, n) \geq 3$, akkor nincs pozitív egész megoldás.

(ii) Ha $(k, m, n) = 1$, akkor végtelen sok pozitív egész megoldás van.

7.7.3 Az összes megoldás: $k = 2$, $x = y = z - 1$.

7.7.4

(a) Nincs megoldás: visszavezethető a Fermat-sejtés $k = 4$ esetére.

(b) Az összes megoldás: $x = uv\xi$, $y = uv\eta$, $z = uv\zeta$, ahol $u$, $v$, $\omega$ (primitív) pitagoraszi számhármas (vagy az „áfogó”) és $\omega$ tetszőleges pozitív egész. — Útmutatás: Azt, hogy ezek valóban megoldások, behelyettesítéssel ellenőrizhetjük. Megfordítva, tegyük fel, hogy $x$, $y$, $z$ megoldás.

Most is elég az $(x, y, z) = 1$ esetett foglalkozni. Legyen $(x, y) = u$, $(x, z) = v$ és $(y, z) = u$. Lássuk be, hogy $u$, $v$ és $w$ páronként relatív prímek, és így $x = uv\xi$, $y = uv\eta$ és $z = uv\zeta$, ahol $x_1 = \xi$, $y_1$ és $z_1$ páronként relatív prímek. Ezeket az egyenletebe beírva, mutassuk meg, hogy $x_1 = y_1 = 1$, továbbá $u^2 + v^2 = w^2$.

(c) Az összes megoldás: $x = a^2d$, $y = b^2d$, $z = (a + b)^2d$, ahol $a$, $b$, $d$ pozitív egészek és $(a, b) = 1$ is feltehető (ez utóbbi a megadott paraméteres előállítás egyértelműségéhez kell). —
Útmutatás: Ez a feladat is visszavezethető az \((x, y, z) = 1\) eset vizsgálatára, ekkor a két negyed négyzetére emelés után kapott

\[
x y = \left(\frac{z - x - y}{2}\right)^2
\]

eyenletben \((x, y) = 1\), és így \(x\) és \(y\) (relatív prim) négyzetszámok.

(d) Az összes megoldás: \(x = a^2d^2\), \(y = b^2d^2\), \(z = (a + b)^2d^2\), ahol \(a\), \(b\), \(d\) pozitív egészek és \((a, b) = 1\). — Útmutatás: Az első köbre emelésnél

\[
x + y + 3 \sqrt{\frac{x}{y}} \sqrt{y} \left(\sqrt{\frac{x}{y}} + \sqrt{\frac{y}{x}}\right) = z
\]
adódik, itt \(\sqrt{\frac{x}{y}} + \sqrt{\frac{y}{x}}\) helyére írjuk be \(\sqrt{\frac{z}{x}} - t\), majd átrendezés után ismét emeljünk köbre. A kapott

\[
x y z = \left(\frac{z - x - y}{3}\right)^3
\]
eyenlet bal oldalán a három tényező páronként relatív prim, tehát külön-külön köbszám.

7.7.5 Használjuk fel a primitív pitagorasi számhármasok karakterizációját.

(a) Az \(x^4 + y^4 - z^4\) egyenlet vizsgálatánál az \(x^2 = \sqrt{mn}\) vagy \(x^2 = \sqrt{n^2 - m^2}\) feltételnek, az \(x^2 + y^2 - z^4\) esetben pedig \(z^2 = m^2 + n^2\) -nek kell teljesülnie. Az \(m\) és \(n\) értékeket végelen sokféleképpen meg lehet választani úgy, hogy \(\sqrt{mn}\), \(\sqrt{n^2 - m^2}\), illetve \(m^2 + n^2\) négyzetszámok legyenek (és emellett \(m > n > 0\), \((m, n) = 1\) és \(m \neq 0 (m \mod 2)\) is fennálljon).

(b) Alkalmazzunk végelen leszállást.

7.7.6 Az összes megoldás: \(x = \pm 1\), \(y = \pm 1\). — Útmutatás: Az egyenlet átírható

\[x^4 - (y^2 - 1)^2 = y^4\]
alakba.

7.7.7 Csak a hetes számrendszert ilyen. — Útmutatás: Sorozatos szorzattá bontások és a primitív pitagorasi számhármasok karakterizációjának felhasználásával az egyenletet visszavezethetjük a 7.3.13 [227]g és 7.7.6 feladatokra [256].

7.7.8 Hasonlóan járhatunk el, mint a 7.4.3 feladatnál [234]. — Válasz: A 0, valamint azok az Euler-egészek, amelyeknek mint komplex számoknak a szöge \(\pi/6\)-nak egész számú többszöröse. Ugyanis más alakban megadva a

\[c, \quad c\omega, \quad c(1 + 2\omega), \quad c(1 + \omega), \quad c(1 - \omega), \quad c(2 + \omega)\]

Euler-egészek, ahol \(c\) tetszőleges egész szám.

7.7.9 Legyen \(\alpha = a + b\omega\), \(\beta = c + d\omega\), ekkor a feladatban szereplő azonosság éppen az

\[
|\alpha|^2 \cdot |\beta|^2 = |\alpha\beta|^2
\]
eyenlőség kifejtett alakja. (Az azonosságot természetesen beszorzással és a két oldalon keletkező tagok összehasonlításával is ellenőrizhetjük, azonban ez a megoldás egyrészt „csúnya”, másrészt nem dertül ki belőle a feladat háttére.)
7.7.10

(a) A két egyenlet kapcsolatát az Euler-egészek normájának felhasználásával lehet a legegyszerűbben megmutatni.

(b) Az egyenletek akkor és csak akkor oldhatók meg, ha az \( n \) \( \mathbb{Z} \)-beli kanonikus alakjában minden \( 3t - 1 \) alakú primszám páros hatványon fordul elő.

A megoldásszámnál a csak a sorrendben vagy előjelben különböző megoldásokat is különbözőknek tekinthetjük. Tegyük fel, hogy az egyenletek megoldhatók, és legyen

\[
L = \prod_{\mu=1}^{r} (\beta_{\mu} + 1),
\]

ahol \( \beta_{1}, \ldots, \beta_{r} \), az \( n \) \( \mathbb{Z} \)-beli kanonikus alakjában a \( 3t + 1 \) alakú primszámok kitevői (ha \( n \) -nek nincs ilyen alakú primosztója, akkor \( L = 1 \)).

Ekkor az \( x^2 - x\eta + \eta^2 - \nu \) egyenlet megoldásszáma \( 6L \) , az \( x^2 + 3\eta^2 - \nu \) egyenleté pedig \( 6L \), ha \( 4 \mid n \), és \( 2L \), ha \( n \) páratlan. [Az \( n \) nem lehet \( 4e + 2 \) alakú, mert a 2 (mint \( 3l - 1 \) alakú primszám) az \( n \) kanonikus alakjában szükségképpen páros kitevővel szerepel.]

Az \( x^2 - x\eta + \eta^2 - \nu \) -re vonatkozó állítást a két-négyzetszám-tétel (7.5.1 Tétel) bizonyításához hasonlóan igazolhatjuk.

Az másik egyenlet megoldásszámat visszavezethetjük az előző eredményre. Ehhez létesítsünk kölcsönösen egyértelmű megfeleltetést (például az (a) rész bizonyításának a mintájára) az \( x^2 + 3\eta^2 - \nu \) diofantikus egyenlet megoldásai és az \( x^2 - x\eta + \eta^2 - \nu \) egyenlet olyan megoldásai között, ahol \( x \) páros. Ennek alapján a \( 4 \mid n \) esetben azt kell belátni, hogy az \( x^2 - x\eta + \eta^2 - \nu \) egyenletnek csak olyan megoldási vannak, ahol \( x \) páros. Végül, páratlan \( n \) esetén az állítás abból következik, hogy egy \( n \) normájú Euler-egész hat egységszerese közül pontosan két esetben lesz a szóban forgó \( x \) érték páros.

7.7.11 Az összes megoldás: \( x = \pm 10 \), \( y = 7 \). — Útmutatás: Kövessük a 7.5.11 feladat [241] megoldásának gondolatmenetét. Első lépésként az egyenletet bal oldalát bontsuk szorzat szerűen az Euler-egész körében, ekkor a két tényező a legnagyobb közös osztójakban szereplő Euler-primektől és esetleges egységtényezőktől eltérően külön-külön is kőbszámmal.

7.7.12

(a) Jelölje \( \tilde{k}_{\mu} \) egy modulo \( \mu \) teljes maradékgrendszer elemszámát. Legyen \( \mathcal{R} \) az Euler-egészek rombuszra és. A \( \mu \)-vel osztható Euler-egészek egy olyan \( \mathcal{R}^{\mu} \) rombuszra észtoknak, amely \( \mathcal{R} \)-ből \( \mu \)-vel való szorzással keletkezik. Így \( \mathcal{R}^{\mu} \)-ben az alaprombusz oldalait alkotó „vektorok” \( \mu \) és \( \omega \mu \). Az \( \mathcal{R}^{\mu} \) rács bármely ilyen alaprombuszába eső Euler-egészek egy teljes maradékgrendszert alkotnak modulo \( \mu \). Ebből következik, hogy \( \tilde{k}_{\mu} \) „körülbelül” az \( \mathcal{R}^{\mu} \) , illetve \( \mathcal{R} \) rácsokat generáló alaprombuszok területeinek az aránya, azaz \( |\mu| = N(\mu) \). A „körülbelül”-től úgy lehet megszabadulni, hogy tekintjük a két rácsnak egy \( \mathcal{H} \) nagy sugarú körbe vagy nagy oldalú négyzetbe stb. eső rács pontjainak a számát. Legyen \( \mathcal{H} \) területe \( T \), az \( \mathcal{R} \), illetve \( \mathcal{R}^{\mu} \) rács \( \mathcal{H} \)-beli rács pontjainak a száma \( t \), illetve \( \tilde{t}_{\mu} \), az alaprombuszok területé pedig \( \mu \), illetve \( \tilde{t}_{\mu} \). Mivel \( \mathcal{R}^{\mu} \) bármely alaprombuszába \( \tilde{k}_{\mu} \) Euler-egész esik, ezért \( T \rightarrow \infty \) mellett

\[
\tilde{k}_{\mu} \sim \frac{t}{\tilde{t}_{\mu}}.
\]
Másrészt

\[ n \sim \frac{T}{t}, \quad n_p \sim \frac{T}{t_p} = \frac{T}{t N(j)}, \]

te hát

\[ \frac{n}{n_p} \sim \frac{\frac{T}{t}}{\frac{T}{t_p}} = \frac{t}{t_p} = N(p). \]  \tag{4}

A (3) és (4) alapján a \( k_p \) és \( N(p) \) konstansok aszimptotikusan egyenlők, és így szükségképpen egyenlők is.

(b) Az (a) rész szerint az elemek darabszáma megfelelő, így csak azt kell igazolni, hogy az elemek páronként inkongruensek modulo \( p^2 \). Ehhez használjuk fel, hogy

\[ \mu \mid \gamma \rightarrow p = N(p) \mid \gamma^2 \rightarrow p \mid j. \]

(c) Alkalmazzuk az Euler–Fermat-tétel (2.4.1 Tétel) bizonyításánál láttott gondolatmenetet.

7.7.13 Nincs megoldás. — Útmutatás: Az egyenletet \( uvw \)-vel beszorozva \( u^2 + v^2 - w^2 = u^2v \) adódik.

Az \( u^2 + v^2 - w^2 \) jelölést bevezetve azt kapjuk, hogy \( uv(c + d) = (uv)^3 \). A szokásos módon elérhető, hogy a bal oldal tényezői páronként relativ primek legyenek, és így \( c \), \( d \) és \( c + d \) (nemnulla) köbszámok, ami ellentmond a Fermat-sejtés.

7.7.14 A pitagoraszi számhármasok képlete szerint a háromszög területe

\[ d^2 mn(m + n)(m - n), \]

ahol \( m > n > 0 \), \( (m, n) = 1 \) és \( m \neq n \) (u.odd 2).

(a) A terület pontosan akkor négyzetszám, ha \( mn(m + n)(m - n) \) négyzetszám. A feltételekből következik, hogy a négy tényező (pozitív és) páronként relatív prim, és így külön-külön is négyzetszámok. Ez ellentmond a L 7.7.3 Lemmának.

(b) A feltétel szerint \( d = 1 \), és így az előző gondolatmenethez hasonlóan kapjuk, hogy \( m \), \( n \) és \( m + n \) köbszámok, ami ellentmond a T 7.7.10 Tételnek.

(c) Végtelen sok ilyen háromszög létezik, sőt minden pitagoraszi háromszögghöz található hozzá hasonló ilyen háromszög: adott \( m \), \( n \) esetén \( d \) értékét válasszuk \( mn(m + n)(m - n) \) -nek. — Ugyanez a paraméteres jellemzés nélkül is elmondható: Ha egy háromszög területe \( T \), akkor az oldalakat \( T \)-szorosra nagyítva az új háromszög területe \( T^3 \) lesz.

(d) Ha \( k \) páros, akkor (a)-ból következik, hogy a terület nem lehet \( k \)-adik hatvány. Ha \( k \) páratlan, akkor (b)-hez, illetve (c)-hez hasonlóan kapjuk, hogy relatív prim oldalak esetén a terület nem lehet \( k \)-adik hatvány, azonban minden pitagoraszi háromszögghöz található olyan hozzá hasonló háromszög, amelynek a területe \( k \)-adik hatvány.

13.7.8.

7.8.1 Ha \( m = 0 \), akkor \( x = \pm 1 \) és \( y \) tetszőleges, ha \( m = -1 \), akkor \( x = 1 \), \( y = 0 \), illetve \( x = 0 \), \( y = 1 \), ha pedig \( m \leq 2 \) vagy \( m = k^2 > 0 \), akkor \( x = \pm 1 \), \( y = 0 \). — Útmutatás: Az \( m = k^2 \) esetben az \((x - ky)/(x + ky) = 1\) szorzattá bontásból kapjuk, hogy mindkét tényező 1, illetve \(-1 \).
7.8.2 A \( 10y^2 + 1 = x^2 \) Pell-egyenletről van szó, tehát végelen sok ilyen négyzetszám létezik.

7.8.3 Ha az \( x^2 - my^2 = r \) egyenlet egy megoldását az \( x^2 - my^2 = 1 \) Pell-egyenlet egy megoldásával (a T 7.8.2 Tétel bizonyításában láttot módon) összeszorozzuk, akkor ismét az \( x^2 - my^2 = r \) egyenlet egy megoldáshoz jutunk.

7.8.4 Végtelen sok megoldás: (a1), (a2), (b1). Nincs megoldás: (b2) (ez utóbbi az \( x^2 - 3y^2 = -1 \) egyenlet modulo 3 vagy modulo 4 vizsgálatából következik).

7.8.5 Végtelen sok. — Útmutatás: Az \( y(n - 1) = 2y^2 \) egyenletet 4-gyel szorzozva a \( x^2 - 8y^2 = 1 \) Pell-egyenlethez jutunk (a \( z = 2n - 1 \) feltétel nem jelent megszorítást, mert a \( x^2 - 8y^2 = 1 \) egyenletnek eleve csak olyan megoldásai lehetnek, ahol \( z \) páratlan). Másik lehetőség: \( u \) és \( u - 1 \) közül az egyik négyzetszám, a másik egy négyzetszám kétszereze, és az így adódó \( u^2 - 2v^2 = \pm 1 \) egyenletek mindegyikének végelen sok megoldása van.

7.8.6 Végtelen sok. — Útmutatás: Az \( x^2 - (x + 1)^2 = x^2 \) egyenletet 2-vel szorzozva a \( (2x + 1)^2 - 2x^2 = -1 \) egyenlethez jutunk. Másik lehetőség: a primitív pitagoraszi számhármasok paraméteres előállításának felhasználása is az \( u^2 - 2v^2 = \pm 1 \) egyenletekhez vezet.

7.8.7 Nincs megoldás: (a), (b), (d), (e). Végtelen sok megoldás van: (c), (f). — Útmutatás: A megoldhatatlanságot egy alkalmas modulus szerinti kongruenciával lehet kimutatni. A 8 mind a négy esetben megfelel ilyen modulusnak, emellett még (a felsorolás sorrendjében) a 3, 7, 9, illetve 3 választás is célhoz vezet. A (c) esetben \( x = 4 \), \( y = 1 \) megoldás, így a 7.8.3 feladat szerint végelen sok megoldás létezik. Az (f) eset 3-mal való szorzás után ekvivalens a \( z^2 - 3y^2 = 3 \) diofantikus egyenlettel. Ennek \( z = 3 \), \( y = 1 \) megoldása, tehát végelen sok megoldás van. Világos, hogy minden megoldásban \( 3 \mid z \), tehát \( x = z/3 \) is egész szám lesz.

7.8.8 Az egyenlet akkor és csak akkor oldható meg, ha \( p \equiv 1 \mod 4 \) vagy \( p = 2 \). — Útmutatás: A szükségeség az egyenlet modulo 4 vizsgálatából azonnal adódik. Az elégségességhez tekintsük az \( x^2 - 2y^2 = 1 \) egyenletnek azt az \( x > 0 \), \( y > 0 \) megoldását, ahol \( x \) minimális. Mutassuk meg, hogy \( x \) csak páratlan lehet, és írjuk át az egyenletet

\[
\frac{x + 1}{2} \cdot \frac{x - 1}{2} = p \left( \frac{y}{2} \right)^2
\]

alakba. Az (5) bal oldalán a tényezők egyike négyzetszám, a másik pedig egy négyzetszám \( P \)-szerese. Innen \( u^2 - pv^2 = \pm 1 \) adódik, az \( x \) minimalitása miatt azonban a + előjél nem lehetséges.

7.8.9 Az előjelekre vonatkozó állítás nyilvánvaló. A kongruenciákra vonatkozó rész igazolásához vegyünk egy olyan nemtriviális megoldást, amelyben \( (x, y, z) = 1 \). Mutassuk meg, hogy \( (z, a) = (y, a) = 1 \). Az egyenletet \( bz(\sqrt{a(c)} - 1) \)-gyel beszorozva és modulo \( a \)-ra tekintve ekkor a

\[
\left( byz^{c(a)} - 1 \right)^2 \equiv -b \mod a
\]

ekongruenciát kapjuk. A másik két kongruencia ugyanúgy adódik.

7.8.10 Végtelen sok. — Útmutatás: Nyilván szükséges, hogy \( 28k^2 + 1 \) négyzetszám legyen, ez végtelen sokszor teljesül. Mutassuk meg, hogy minden ilyen esetben \( 2 + 2\sqrt{28k^2 + 1} \) is négyzetszám lesz. Ehhez az \( r^2 - 1 = 28k^2 \) egyenlőséget összük el 4-gyel és a bal oldalt bontsuk szorzattá, ekkor a keletkező tényezők olyan szomszédos egészek, amelyek egyike négyzetszám, a másik pedig egy
négyszám 7-szerese. Végül lássuk be, hogy szükségképpen az \((r + 1)/2\) tényező négyzeteszám, és így a feladatban megadott \(2r + 2\) is négyzeteszám.

7.8.11 Ha \(\omega = u^2\), akkor az egyenlet átírható \((u^2 - 1)(u^2 - 1) = 2y^2\) alakba. Lássuk be, hogy ekkor \(u^2 - 1\) négyzeteszám, ami \(u \neq \pm 1\) esetén lehetetlen. ( Ez az egyenlet szerepelt a 7.7.7 feladat [256] megoldásában is.) — Az \(y = u^2\) eset megegyezik a 7.3.13g feladattal [227].

13.7.9.

7.9.1 Ha az \(n + 1\) partíciójában szerepel 1-es, akkor egy 1-est hagyunk el, egyébként pedig a legkisebb tagot csökkentésük 1-gyel. Így nyilván \(u\) minden partícióját legfeljebb kétszer kapjuk meg. A második módon csak olyan partíciókat kaphatunk, amelyekben legfeljebb egy darab 1-es fordul elő, tehát \(n > 1\) -re nem kapjuk meg \(n\) minden partícióját. Ezért egyenlőség csak \(\tau_1 = 1\) -re teljesül.

7.9.2 (a) \(\infty\) , (b) \(- \infty\) .

7.9.3 A T 7.9.5 Tétel alapján ezek a \((3k^2 + \hat{k})/2\) alakú számok.

7.9.4 \(\gamma_{n}^{\omega} = 1\) . — Útmutatás: Tekintsük az \(n\) egy \(\omega = \omega_1 + \omega_2 + \cdots + \omega_r\) előállítását (ahol \(r\) és \(x_1, \ldots, x_r\) pozitív egészek), és mérjük fel a \([0, \tau]\) intervallumban az origóból kiindulva egymás után rendre az \(x_1, \ldots, x_r\) hosszúságú szakaszokat. Ez azt jelenti, hogy az intervallumon az \(1, 2, \ldots, n - 1\) pontok közül néhányat kijelöltünk osztópontnak (esetleg az összeset, esetleg egyet sem). Az \(n\) előállításai és az osztópont-halmazok között kölcsönösen egyértelmű megfeleltetés áll fenn. Ezért a keresett előállításszám megegyezik egy \(n - 1\) elemű halmaz összes részhalmazainak a számával.

7.9.5 Az \(n\) egy \(r\) -tagú előállításában minden összeadandóból vonjunk ki 1-et, ekkor az \(n - r\) egy legfeljebb \(r\) tagból álló előállítását kapjuk (a tagok száma akkor lesz \(r\) -nél kevesebb, ha az eredeti előállításban szerepelt 1-es). Mutassuk meg, hogy így kölcsönösen egyértelmű megfeleltetés jött létre a kétféle partíció között.

7.9.6 \(\sum_{n \in \mathbb{N}} \tau_n^{\omega} (1 - \omega_n)\).

7.9.7 A feladat állításait mind alkalmas bijekció megadásával, mind pedig a generátorfüggvények segítségével igazolhatjuk.

(a) Bijekció: Tekintsük \(n\)-nek egy \(\omega = \omega_1 + \cdots + \omega_r\) előállítását, ahol az \(\omega_i\) számok mind különbözők. Mindegyik \(\omega_i\) egyértelműen felírható \(2^{r_i}\) alakban, ahol \(a = \geq 0\) és \(\hat{t}\) páratlan. Az azonos \(\hat{t}\) értékeket kiemelve egy \(\alpha - \hat{\pi} \geq 1 + 3u_2 - 5u_3 - \cdots\) egyenlőséghez jutunk, ahol minden \(\pi_j\) nemnegatív egész. Ezt tekinthetjük az \(n\) olyan partíciójának, amelyben \(u_1\) darab 1-es, \(u_2\) darab 3-as stb szerepel.

Illusztrációs példa: Induljunk ki a \(2\beta = 10 + 6 + 4 + 3\) partícióiból. Ekkor

\[
23 = 2^1 \cdot 5 + 2^1 \cdot 3 + 2^2 \cdot 1 + 2^6 \cdot 3 - 2^1 \cdot 5 + (2^1 + 2^3) \cdot 3 + 2^2 \cdot 1 = 1 \cdot 4 + 3 \cdot 3 + 3 \cdot 2 \cdot 5
\]

szerint a \(2\beta = 5 + 5 + 3 + 3 + 1 + 1 + 1 + 1\) partícióhoz jutunk.

Mutassuk meg, hogy ily módon egy bijekciót adtunk meg az \(n\) kétféle partíció között.

Generátorfüggvény: A megfelelő generátorfüggvények

\[
V(z) = \prod_{i=1}^{\infty} (1 + x^i) \quad \text{és} \quad W(z) = \prod_{j=1}^{\infty} \frac{1}{1 - j^2z^j - 1}.
\]

517
Ha $V(x)$-et átírjuk az

\[(1 + x^i) = \frac{1 - x^{2i}}{1 - x^i}\]

azonosság felhasználásával, akkor az egyszerűsítések után éppen $W(x)$-et kapjuk. A precíz igazoláshoz vagy formális hatványseroikkal és formális végleten szorzatokkal kell dolgozni, vagy pedig gondosan meg kell vizsgálni a végleten szorzatokban a határátmenetnél fellépő problémákat.

(b) A bijekcióhoz a tagokat most $k^* t$ alakban kell felirni, ahol $k \nmid t$.

A generátorfüggvények:

$V_t(x) = \prod_{i=1}^{\infty} (1 + x^i + \cdots + (x^i)^{k-1}) \quad \text{és} \quad W_h(x) = \prod_{i=1}^{\infty} \frac{1}{1 - x^t}$.

7.9.8 Első megoldás: A 7.9.6 feladat [268] szerint

\[\frac{x^n}{(1-x)(1-x^2)\cdots(1-x^n)}\]

sorfejtésében $x^n$ együttátható az $n$ olyan particióinak a száma, ahol a legnagyobb tag $r$, így ezeket az együttáthatókat $r$ szerint összegezve valóban $p(n)$ adódik.

 Második megoldás: $x^n$ együttáthatóját csak a jobb oldali összeg első $n$ tagja befolyásolja, ami közös nevezőre hozva

\[-1 + \frac{1}{(1-x)(1-x^2)\cdots(1-x^n)}\].

A T 7.9.2 Tétel alapján itt $x^n$ együttáthatója megegyezik az $\omega$ olyan tagoknak a száma, ahol a legnagyobb $r$-re, így ezeket az együttáthatókat $r$ szerint összegezve valóban $\nu(n)$ adódik.

7.9.9 Az $U(x) = \prod_{i=1}^{\infty} (1 - x^i)$ egyenlőség logaritmusának vegyük a deriváltját:

\[\frac{U'(x)}{U(x)} = \sum_{i=1}^{\infty} \frac{-ix^{i-1}}{1 - x^i} \quad \text{(6)}\]

(A ténylezettségi logaritmalás és a tagonkénti deriválás $|x| < 1/2$-re jogos.) Szorozzuk be (6)-ot $-x U'(x)$-szel, és használjuk fel, hogy

\[\sum_{i=1}^{\infty} \frac{ix^i}{1 - x^i} = \sum_{i=1}^{\infty} x^i + x^{2i} + \cdots = \sum_{j=1}^{\infty} \sigma(j)x^j\]

Ekkor

\[-x U'(x) = U'(x) \sum_{j=1}^{\infty} \sigma(j)x^j \quad \text{(7)}\]

adódik. Végül írjuk be (7)-be az
képletek, és szorozzuk össze a (7) jobb oldalán álló két hatványsort.

## 13.8 Diofantikus approximáció

### 13.8.1

#### 8.1.1

(a) Közös nevezőre hozva a számláló $as - br \neq 0$, ezért $|as - br| \geq 1$.

(b) Az $|as - br| = 1$ egyenlőség végzetlen sokszor teljesül, mert az $as - br = \pm 1$ diofantikus egyenleteknek végzetlen sok megoldása van.

#### 8.1.2

Mivel $\delta = \rho / s \neq 0$, ezért elég nagy $k$ esetén $|\delta| > 1/(ks)^2$.

#### 8.1.3

(a) Bármely $s > 1$-re legfeljebb egy darab $s$ nevezőjű tört lehet megfelelő.

(b) Az (a) részből következik.

#### 8.1.4

(a) Bármely $k$-ra vagy egy $2^k$, vagy pedig egy $2^k + 1$ nevezőjű tört megfelel.

(b) $\alpha = 1/3$.

(c) Bármely $k$-ra van ilyen $3^k$ nevezőjű tört.

(d) $\alpha = 1/2$.

(e) A $\sqrt{\gamma}$-t jól approximáló $r/s$ törtek négyzetei megfelelnek.

(f) $\alpha = (1 + \sqrt{5})^2/1$.

#### 8.1.5

Használjuk fel, hogy az $\alpha$-t jól közelítő törtekre $r^2 \sim \gamma/s^2$.

#### 8.1.6

A T 8.1.6 Tételhez hasonlóan bizonyíthatunk. A „gyöktelenítéshez” a feladatban szereplő külsőséget $\sqrt{2} + \gamma / s$-sel érdemes beszorozni.

#### 8.1.7

Ha $r/s$ jól közelítő $\alpha$-t, akkor

(a) $\alpha(r/s) + b$ jól közelít $a\alpha + b$-t;

(b) $\gamma^2 / s^2$ jól közelít $\alpha^2$-et.

#### 8.1.8

(a) 0 és 1. — (b) és (c) A teljes $(-1, 1)$ intervallum.

#### 8.1.9
(a) Az \( i \) -edik elem köré rajzoljunk egy \( \epsilon_i/2^i \) hosszúságú intervallumot.

(b) Számosság: Kölcsönösen egyértelmű megfeleltetés létesíthető az ilyen „harmados” törtek és a \([0, 1]\)-beli összes valós szám kettes alapú számrendszer szerinti „kettédes” törtként való felirása között (a 2-es jegy helyett 1-est kell írni). — Nullmértékűség: A Cantor-halmazt úgy kapjuk, hogy a \([0, 1]\) intervallumból elhagyjuk a középső harmadát, majd mindkét megmaradt intervallumnak a középső harmadát, majd a négy megmaradt intervallumnak a középső harmadát stb. Az első \( n \) lépés után a megmaradt intervallumok összhossza

\[
1 - \frac{1}{3} - \frac{2}{9} - \cdots - \frac{2^{n-1}}{3^n} - 1 - \frac{1}{3} - \frac{1 - \left(\frac{2}{3}\right)^n}{1 - \frac{2}{3}} \to 0, \quad \text{ha} \ n \to \infty.
\]

8.1.10

(a) Azonnal következik a definícióból.

(b) A \( L \) darab halmaz mindegyikét fedjük le \( \epsilon_k/2^k \) összhosszúságú intervallumosorozattal.

(c) Az \( i \) -edik halmazt fedjük le \( \epsilon_i/2^i \) összhosszúságú intervallumosorozattal (\( i = 1, 2, \ldots \)).

(d) Bármely halmaz előáll az egy pontból álló részhalmazainak egyesítéseként, és ezek a részhalmazok nyilván nullmértékűek. Ez az egyesítés például a Cantor-halmaz esetén is nullmértékű, a \([0, 1]\) intervallum esetén viszont nem az.

13.8.2.

8.2.1

(a) A T 8.2.1 Tétel mindkét bizonyítása átvihető a térbeli esetre is, a második bizonyításnál ehhez természetesen a L 8.2.2 Lemma térbeli változatára van szükség.

(b) Az \( u \) -dimenziós esetben azt kell felténni, hogy \( H \) térfogata legalább \( 2^u \Delta \). (Ekkor \( \Delta \) az alapparalelepipedon \( u \) oldalának koordinátavektoraitól képzett determináns abszolút értékét jelenti.)

8.2.2 A T 8.2.1 Tételre adott mindkét bizonyítás gondolatmenete alkalmazás az állítás igazolására, a második bizonyításnál ehhez a L 8.2.2 Lemma alábbi általánosítására van szükség (ezt az ottani jelölések segítségével fogalmazzuk meg): Ha a \( K \) halmazok közül bármely \( \tau + 1 \) darab metszete az üres halmaz, akkor \( \tau \leq \tau \Delta \). Bármelyik bizonyítás gondolatmenetéből \( \tau \) darab olyan nemtriviális rácspont adódik, amelyek közül semelyik kettő sem egymás tükörképe az \( O \) középpontra, a további \( \tau \) darabot pedig ennek az \( \tau \) rácspontnak az \( O \) -ra vonatkozó tükörképei biztosítják.

8.2.3 Kövessük a T 8.2.4 Tétel gondolatmenetét. Ha \( \tilde{p} = 3k + 1 \) alakú primszám, akkor alkalmas \( c \) -vel \( c^2 \equiv -3 \pmod{p} \). Ekkor a T 8.2.4 Tétel bizonyításában szereplő (6) rács pontjaira \( \varphi \mid x^2 + 3y^2 \). A Minkowski-tételt a megfelelő ellipszisre alkalmazva egy olyan nemtriviális rácspondot kapunk, amelyre \( x^2 + 3y^2 < 3p \). Mivel \( x^2 + 3y^2 = 2p \) a modulo 3 feltétel miatt nem teljesülhet, így szükségképpen \( x^2 + 3y^2 = p \).

8.2.4 A T 8.2.1 Tétel jelöléseit szerint most \( L \) a szokásos négyzettrácse, tehát \( \Delta = 1 \), \( H \) pedig az

\[
a_{11}x_1 + a_{12}x_2 = \pm b_1, \quad a_{21}x_1 + a_{22}x_2 = \pm b_2
\]

eyenesek által határolt paralelogramma, ennek területe \( \det(b_2/|D|) \). A feladat állítása ezért Minkowski tételeből következik.
8.2.5 A térbeli Minkowski-tétel (lásd a 8.2.1a feladatot [281]) felhasználásával a T 8.2.3 Tétel bizonyításához hasonló gondolatmenetet lehet alkalmazni. Elhelyez tekintsük az

\[ x = s_1 \alpha_1 - r_1, \quad y = s_2 \alpha_2 - r_2, \quad z = s \]

ráscot, írt az alapparalelepipedon térfogata \( \Delta = 1 \). Az approximációs feltételt átírhatjuk a \( z^2 \leq e^2 \)

\[ |z^2| < \varepsilon^2 \]

alakba, ahol \( e = 2/3 \). Ezen nem konvex (és nem korlátos) térbeli halmaz helyett a számtani és mértani közép közötti egyenlőtlenséget is felhasználva vegyük alkalmas értékekre az

\[ \frac{1}{a^2} |z| + 2a|\varepsilon| \leq \sqrt{12}, \quad \frac{1}{e^2} |z| + 2\varepsilon| \leq \sqrt{12} \]

oktaédereket.

13.8.3.

8.3.1 (a) 4, 1, 4, 2.

(b) 1, 1, 2, 1, 2, 1, 2, ...

(c) 2, 4, 4, 4, ...

(d) 1, 1, 1, 1, ...

8.3.2 (a) 43/30. (b) \( (1 + \sqrt{3})/2 \).

8.3.3 Használjuk fel a T 8.3.3 Tételben megadott \( \frac{r_a}{s_n} \) törtek jó közelítését, és azt, hogy (11) alapján \( \left( s_{n-1}, s_n \right) = 1 \).

8.3.4 A 8.3.1d feladat [287] szerint \( (1 + \sqrt{3})/\beta \) minden lánctörjegye 1-es, és így a T 8.3.3 Tételben szereplő \( \frac{r_a}{s_n} \) törtekre a (8a)-(8b) rekurzió szerint \( r_a = r_{a+2} \) és \( s_n = s_{n+1} \).

8.3.5 Használjuk fel a L 8.3.4 Lemmában szereplő (8a), (8b) és (10) képleteket.

8.3.6 Az eredeti számot \( \alpha \)-val, a „tisztán” periodikus részből nyert számot \( \beta \)-val jelölve az

\[ \alpha = L(c_0, c_1, \ldots, c_{M-k}, \beta) \quad \text{és} \quad \beta = L(c_{M-k+1}, \ldots, c_M, \beta) \]

véges lánctörteket kapjuk. Ezekből a feladat állítása az emeltes törtek lebontása és további átrendezések után adódik.

13.8.4.

8.4.1 Sűrűek: (b), (d), (f), (g).

8.4.2 Rajzoljunk minden egyes \( 0 < r < 1 \) racionális szám körül megszámlálható sok olyan zárt intervallumot, amelyek benne vannak \( \left( 0, 1 \right) \)-ben és a hosszuk 0-hoz tart, majd az összes így kapott intervallumot rendezzük egyetlen \( J_1, J_2, \ldots \) intervallumsorozatba. Egy \( \mu \) számsorozat törtrészének mindenütt sűrűségéhez azt kell igazolni, hogy mindegyik \( J_k \) intervallumban található legalább egy \( \left\{ u_i \right\} \).

Ezek után az \( \alpha \)-t egymásba skatulyázott zárt intervallumok közös pontjaként fogjuk megkapni. A kiindulási intervallum legyen (mondjuk) \( \mathcal{H}_0 = [2, 3] \). Ha a \( \mathcal{H}_{k-1} \) intervallum már adott, akkor
$H_{e}$-a $H_{k-1}$ következő részintervallumának defináljuk: választunk egy olyan $n_{e}$ kítevőt, amelyre a $H_{k-1}$-beli $z$ elemek $n_{e}$-adik hatványai kitöltenek egy két egész szám közötti teljes $T$ intervallumot, és $H_{e}$-ba azokat az $z$-eket tesszük, amelyekre
\[ x \in H_{k-1}, \quad x^{n_{e}} \in T \quad \text{és} \quad \{x^{n_{e}}\} \in H_{k}. \]
Az így gyártott $H_{e}$ intervallumok közös pontja megfelel $\alpha$-nak.

8.4.3 Ha egy $P_{a}$ pont „nagyon közel” van a $k$-dimenziós egységkocka egy $Q = (v_{1}, \ldots, v_{k})$ pontjához, akkor minden $1 \leq j \leq k$-ra $\{m_{r_{j}}\} - v_{j}$ „kicsi” abszolút értéki, és így ezek tetszőleges lineáris kombinációjának az abszolút értéke is kicsi. Az $1, \alpha_{1}, \ldots, \alpha_{k}$ lineáris összefüggősége esetén ily módon a $v_{j}$-k alkalmas lineáris kombinációja egy olyan feltétel nyerhető, amely nem teljesülhet tetszőleges $Q$-ra.

8.4.4
(a) Képezzük az új sorozat elemeit úgy, hogy mindig a régi sorozat legelső olyan, még fel nem használt tagját vesszük, amelynek törtrészé rende az alábbi intervallumokba esik:
\[ \left[ 0, \frac{1}{2} \right), \left[ \frac{1}{2}, 1 \right) ; \left[ 0, \frac{1}{3} \right), \left[ \frac{1}{3}, \frac{2}{3} \right) ; \left[ \frac{2}{3}, 1 \right), \left[ 0, \frac{1}{4} \right), \ldots \]
(b) Például minden második tagnak olyan elemet vegyünk, amelynek nagyon kicsi a törtrész.

8.4.5 Igaz: (b), (c).

8.4.6
(a) Legyen $k$ tetszőleges egész szám. Ha $10^{k} \leq m < 10^{k+1}$, akkor
\[ \{\log m\} > \frac{1}{2} \iff m > 10^{k+1}. \]
Ez azt jelenti, hogy az $\left(1/2, 1\right)$ intervallumba a törtrészeknek jóval több, mint a fele esik, ha $n = 10^{k+1}$ (és jóval kevesebb, mint a fele, ha $n = \left|10^{k+1}\right|$.)
(b) Az $1/(2\pi)$ arány irracionalis, ezért az (ívmértékbén mért) $n$ szögek a T 8.4.5 Tétel szerint egyenletes eloszlásuk az egységkörön. Ennek alapján a $\{\sin n\}$ értékek egyenletes eloszlása azt jelenti, hogy azok az $\pi$ valós számok, amelyekre $\{\sin n\} = \{0, 1\}$ intervallum egy előre megadott $\delta$ hosszúságú $I$ részintervallumába esik, az egységkör kerületének a $\delta$ -szeresét foglalják el. Könnyen látható azonban, hogy ez például az $I = \left[1/2, \sqrt{3}/2\right]$ intervallumra nem teljesül.

8.4.7 Azt kell igazolni, hogy $54321 \cdot 10^{0} < t^{n} < 54322 \cdot 10^{0}$ teljesül alkalmas $n$ és $\nu$ természetes számokra. Térjünk át tízes alapú logaritmusra, és $\alpha = \log b$-re alkalmazzuk a T 8.4.1 Tételt.

13.9 Algebrai és transzcendens számok

13.9.1.
(a) Egy jó polinom $x^{20} - 7$.

(b) Emeljük négyzetre az $\alpha - 3 - \sqrt{2}$ egyenlőséget.

(c) Az $\alpha - \sqrt{3} = \sqrt{2}$ egyenlőséget négyzetre emelve, majd az eredményt átrendezés után ismét négyzetre emelve egy megfelelő egész együtthatós polinomot olvashatunk le.

(d) Az $\alpha - \sqrt{2} = \sqrt{4}$ egyenlőséget emeljük köbre, majd az eredményt átrendezés után emeljük négyzetre.

(e) Az $\alpha = \sqrt{2} + \sqrt{4}$ egyenlőséget emeljük köbre, ezután a jobb oldalon keletkező „köbgyökös” rész átalakítható:

$$3\sqrt{2}\sqrt[4]{\sqrt{2} + \sqrt{4}} = 3 \cdot 2\alpha.$$ 

(f) Az előzőkhöz hasonló módon, többszöri négyzetre emeléssel „kiküszöbölhetjük” a gyökjeleket.

9.1.2 Tegyük fel, hogy $\alpha$ gyöke az $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ racionális együtthatós polinomnak, ahol $a_n \neq 0$. Ekkor a megadott számok rendre gyökei az alábbi, szintén az előírt tulajdonságú polinomoknak:

(a) $f(-\omega) = a_0 - a_1 \omega - a_2 \omega^2 + \cdots + (-1)^n \omega^n$;

(b) $f(x)$ (egy valós együtthatós polinomnak $\alpha$-val együtt $\bar{\alpha}$ is gyöke);

(c) $f(1/x) = a_n + a_{n-1} x + \cdots + a_0 x^n$ ($\alpha \neq 0$ miatt feltehető, hogy $a_0 \neq 0$);

(d) $f(x-r) = a_0 + a_1 (x-r) + \cdots + a_n (x-r)^n$;

(e) $f(x/r) = a_0 + a_1 (x/r) + \cdots + a_n (x/r)^n$ (nyilván feltehető, hogy $r \neq 0$);

(f) $f(x^k) = a_0 + a_1 x^k + \cdots + a_n x^{nk}$.

9.1.3 Ha $\zeta(2) = \pi^2 / 6$ algebrai lenne, akkor az előző feladat (e) és (f) része szerint $\pi$ is algebrai lenne.

9.1.4 Tegyük fel indirekt, hogy $f(\alpha) = a_0 + a_1 \alpha + \cdots + a_n \alpha^n$ algebrai, azaz léteznek olyan nem csupa nulla $b_0, b_1, \ldots, b_n$ racionális számok, amelyekre

$$b_0 + b_1 (a_0 + a_1 \alpha + \cdots + a_n \alpha^n) + \cdots + b_n (a_0 + a_1 \alpha + \cdots + a_n \alpha^n)^n = 0.$$ 

A műveleteket elvégezve kapjuk, hogy $\alpha$ gyöke egy racionális együtthatós, nemnulla polinomnak, ami ellentmondás.

9.1.5 Ha van ilyen $h$, akkor $h$ minden gyöke, így speciálisan $\theta$ minden gyöke is algebrai. Megfordítva, ha $\theta$ (multiplicitással számolt) gyökei az $a_1, \ldots, a_r$ algebrai számok, és $\alpha_j$ gyöke egy $J$ egész együtthatós, nemnulla polinomnak ($J = 1, \ldots, r$), akkor $h = \tilde{f}_1 \cdots \tilde{f}_r$ polinom megfelel a feltételeknek.

9.1.6 Az állítás azonnal következik az algebrai szám és a lineáris összefüggés definíciójából.

9.1.7 Az $\alpha$ komplex szám gyöke az alábbi komplex, illetve valós együtthatós polinomnak: (a) $x - \alpha$; (b) $(x - \alpha)(x - \overline{\alpha})$.
13.9.2.

9.2.1

(a)–(e) A fokszám megegyezik \(\deg \alpha\) -val, kivéve ha (e)-ben \(r = 0\). Ennek igazolásához válasszuk a 9.1.2 feladat [294] útmutatásában szereplő \(\tilde{f}\) polinomot \(\tilde{m}_\alpha\) -nak, és lássuk be, hogy ekkor az útmutatásban az \(\tilde{f}\) segítségével megadott \(f(-\pi)\) stb. polinomok is irreducibilisek \(\mathbb{Q}\) felett.

\[(f) \deg \sqrt[r]{r} \leq k \deg \alpha.\]

9.2.2 Először keressünk egy olyan \(f\) racionális együtthatós (nemnulla) polinomot, amelynek az adott \(\alpha\) szám gyöke, majd vizsgáljuk meg, hogy \(\tilde{f}\) irreducibilis-e \(\mathbb{Q}\) felett. Ha \(f\) irreducibilis, akkor \(f - \tilde{m}_x\), és így \(\deg \alpha = \deg \tilde{f}\). Ha \(f\) reducibilis, akkor bontsuk irreducibilisek sorozatára, és keressük meg, melyik tényezőnek győze az \(\alpha\). — Az irreducibilitást gyakran ellenőrizhetjük a Schönemann–Eisenstein-kritérium segítségével, illetve másod- vagy harmadfokú polinom esetén elég azt megvizsgálni, hogy a polinomnak létezik-e racionális gyöke.

(a) 7.

(b) 3. — Fejezzük ki \(1/2 = \cos 60^\circ\) -ot \(\cos 20^\circ\) segítségével.

(c) 3. — Lásd a 9.1.1e feladatnál [294] szereplő útmutatást.

(d) 2. — A „nagy” négyzetgyökök alatt „teljes négyzet” szerepel.

(e) 4.

(f) 4. — A számhoz adjunk hozzá 1-et, és az így kapott négytagú összegre alkalmazzuk a mértani sorozat összegképletét.

9.2.3 Ha \(\alpha = r + \sqrt[r]{r}\), akkor \(\alpha\) gyöke az \((x - r)^2 - s\) másodfokú, a \(\mathbb{Q}\) felett irreducibilis polinomnak. A megfordításhoz használjuk fel a másodfokú egyenlet megoldóképletét.

9.2.4

(a) Használjuk fel, hogy ha \(\alpha\) algebrai és \(r\) racionális, akkor \(\deg (\alpha + r) = \deg \alpha\) (lásd a 9.2.1d feladatot [297]).

(b) Ha az \(\alpha\) komplex szám nem valós, akkor az \(s(\alpha - a)\) számok mindenütt sűrűek a komplex számsíkon, ahol \(r\) és \(s\) végigfutnak a racionális számokon.

9.2.5

(a) Bármely \(i\) -re \(\deg \alpha_i \leq \deg \tilde{f}\).

(b) Egyenlőség pontosan akkor teljesül, ha \(\tilde{f}\) irreducibilis \(\mathbb{Q}\) felett.

(c) Írjuk fel \(\tilde{f}\) -et (a \(\mathbb{Q}\) felett) irreducibilis polinomok szorzataként: \(\tilde{f} = f_1 \cdots f_k\), ahol \(\tilde{f}\) reducibilitása miatt \(k \geq 2\). Legyen \(\deg \tilde{f}_j = n_j\). Ekkor \(\alpha_1 + \cdots + \alpha_k = \tau\) és

\[\sum_{i=1}^{n} \deg \alpha_i = \sum_{j=1}^{k} n_j. \quad (1)\]

Lássuk be, hogy az (1) jobb oldalán szereplő összeg akkor maximális, ha \(k = 2\), és \(\tau_1\) és \(\tau_2\) közül az egyik 1, a másik \(\tau - 1\).
9.2.6 $m_0 = x^3 + 5x^2 + 10x - 10$. — Útmutatas: A feltételekből $f = g m_0$, ahol $\deg g = 1$.
Ebből következik, hogy $f$-nek van racionális gyöke. Határozzuk meg ezt a gyököt, ezután osszuk le $f$-et a megfelelő gyöktényezővel (ez utóbbit a leggyorsabban a Horner-eltendezéssel végezhetjük el).

9.2.7 Használjuk fel, hogy $[m_0, \beta] \mid f$, továbbá ha $m_{\alpha} \not\equiv m_{\beta}$, akkor a minimálpolinomok irreducibilitása miatt $(m_{\alpha}, m_{\beta}) = 1$.

9.2.8 Ha $f$ irreducibilis lenne, akkor a feltételekből $f = m_0 \mid g$ következnne.

13.9.3.

9.3.1

(a) Legyen $\alpha$ algebrai és $\beta$ transzcendens. Ha $\alpha + \beta$ algebrai lenne, akkor $\beta = (\alpha + \beta) - \alpha$ is algebrai lenne, ami ellentmondás.

(b) Például $\pi + (1 - \pi)$ algebrai, $\pi + (1 + \pi)$ transzcendens.

(c) Az összeghez képest annyi a változás, hogy egy algebrai és egy transzcendens szám szorzata lehet algebrai is, mégpedig abban a kivételes esetben, amikor az egyik tényleg $0$.

9.3.2

(a) $\alpha$ és $\beta$ algebrai.

(b) $\alpha$ és $\beta$ transzcendens.

(c) $\alpha$ és $\beta$ közül legalább az egyik transzcendens (mutassunk példát a többféle lehetőség mindegyikére).

(d) $\alpha$ és $\beta$ algebrai, vagy $\alpha = 0$ és $\beta$ transzcendens.

(e) $\alpha$ és $\beta$ transzcendens.

(f) $\alpha$ és $\beta$ transzcendens, vagy pedig közülük az egyik $0$ és a másik transzcendens.

(g) $\alpha$ és $\beta$ közül legalább az egyik transzcendens.

(h) $\alpha$ és $\beta$ algebrai. — Útmutatas: az $\alpha + \beta = c$, $\alpha \beta = d$ „egyenletrendszert” oldjuk meg, ekkor a másodfokú egyenlet megoldóképletéből (vagy a T 9.3.6 Tétel alapján) kapjuk, hogy $\alpha$ és $\beta$ is algebrai.

A racionális-irracionális esetben csak (d)-nél és (h)-nál van változás; ekkor az alábbi megoldásokat kapjuk, ahol $r > 0$ és $s$ racionális számok:

(d) $\alpha = 0$ és $\beta \neq 0$ tetszőleges, vagy $\alpha = \sqrt{r}$ és $\beta = s \sqrt{r} (\neq 0)$;

(h) $\alpha = s + \sqrt{r}$ és $\beta = s - \sqrt{r}$.

9.3.3 Algebrai: (b).

9.3.4 Használjuk fel (a)-nál a 9.3.2a feladatot [301], (b)-nél pedig a T 9.3.3 Tételt.

9.3.5 Algebrai: (a), (b).
9.3.7 Lássuk be, hogy \( \lfloor n \rfloor \) irracionális, majd használjuk fel a T 9.3.5 Tételt.

9.3.8 Tegyük fel, hogy valamely \( \tilde{k} \neq m \) pozitív egészekre \( \alpha^{k} + \beta^{k} = c \) és \( \alpha^{m} + \beta^{m} = d \), ahol \( c \) és \( d \) algebrai számok, amelyek közül legalább az egyik nem nulla. Innen

\[
(c - \beta^{k}) \alpha = (d - \beta^{m}) \tilde{k},
\]

és így \( \beta \) gyöke egy algebrai együthatós nemnulla polinomnak, azaz a T 9.3.6 Tétel alapján maga is algebrai. Ugyanígy kapjuk, hogy \( \alpha \) is algebrai, és ekkor valóban minden \( n \) -re \( \alpha^{n} + \beta^{n} \) is algebrai.

9.3.9 Alkalmazzuk meg, hogy végtelen sok olyan pozitív egész létezik, amely az \( \alpha \) -nak nem racionális hatványa. Ezek a T 9.3.5 Tétel szerint az \( \alpha \) -nak szükségképpen transzcendens kifejtőjű hatványa.

Transzcendens: Az \( \alpha \) -nak kontinuum sok transzcendens kifejtőjű hatványa van, és ezek közül csak megszámlálható sok lehet algebrai szám.

13.9.4.

9.4.1 (b) A T 9.4.2 Tételben megadott szám Liouville-szám, és így az (a) részből következik, hogy végtelen sok Liouville-szám van. — Kontinuum: A T 9.4.2 Tétel bizonyításához hasonlóan adódik, hogy a \( 10^{-k!} \) sorozat tetszőleges végtelen részsorozatából képzett végtelen sor is Liouville-szám.

9.4.2 (a) Legyen \( f = f_{1} \cdots f_{k} \) az \( \tilde{f} \) felbontása \( \mathbb{Q} \) felett irreducibilis polinomok szorzata. Ekkor a szóban forgó (12) diofantikus egyenlet a

\[
g_{j}(y, z) = y^{e_{j}^{*}} \tilde{f}_{j}(\tilde{z}_{j}) = b_{j}, \quad j = 1, 2, \ldots, k
\]

eyenletrendszerre vezethető vissza, ahol \( \prod_{j=1}^{k} b_{j} = b \). Így \( b \neq 0 \) esetén csak véges sok ilyen egyenletrendszer kapunk, és ezek mindegyikének a (sőt már akármelyik egyenletnek is) \( a(z \ eredeti) \) T 9.4.4 Tétel szerint csak véges sok megoldása lehet. Ha \( \tilde{b} = 0 \), akkor legalább az egyik \( \tilde{b}_{j} = 0 \), tehát ilyen esetben csak véges sok egyenletet kell nézni, és ezek mindegyikének csak véges sok megoldása lehet.

(b) A T 9.4.4 Tétel bizonyításában csak ezeket a tulajdonságokat használtuk fel.

9.4.3 Kövessük a T 9.4.4 Tétel bizonyításának a gondolatmenetét. Ha \( z_{i}/y_{i} \) -nek nincs korlátos részsorozata, akkor cseréljük meg \( z_{i} \) és \( y_{i} \) szerepét, azaz \( f(z_{i}/y_{i}) \) helyett tekintsük \( f(y_{i}/z_{i}) \) -t. A T 9.4.3 Tétel (ii) állítását elég (például) a \( i^{k} = 0, 0, 9 \) speciális esetben alkalmazni.

9.4.4 Használjuk fel, hogy ha az \( \tilde{f} \) polinomnak \( \alpha \) többszörös gyöke, akkor \( \alpha \) gyöke az \( \tilde{f} \) deriváltjának is.

13.9.5.

9.5.1 Alkalmazzunk a T 9.5.1 Tétel bizonyításához hasonló gondolatmenetet.

9.5.2 (a) Őrjük fel \( \sin \) -re, illetve \( \cos \) -re a \( \sin \alpha \), illetve \( \cos x \) hatványsorából adódó végtelen sort, és alkalmazzuk a T 9.5.1 Tétel gondolatmenetét.
(b) Bizonyítsunk indirekt a T 9.5.2 Tétel bizonyításának a mintájára: az ottani \( \int \) integrálban \( \sin(\pi x) \) helyére tegyük \( \sin(\tau x) \)-et, és \( \alpha \) legyen most az \( 1/\tau \), \( \cos \tau \) és \( \sin \tau \) racionális számok közös nevezője.

(c) Fejezzük ki \( \sin(2\tau x) \)-et és \( \cos(2\tau x) \)-et \( \tau \) segítségével. Innen látszik, hogy ha \( \tau \) racionális, akkor \( \sin(2\tau) \) és \( \cos(2\tau) \) mindkettő racionálisak, ami ellentmond a (b) résznek.

9.5.3 Használjuk fel, hogy a T 9.5.2 Tétel bizonyításában minden második parciális integrálásnál \( \sin x = \sin 0 = 0 \) miatt a „kiintegrált rész” 0. Ebből adódik, hogy két parciális integrálást együtt használva egy lépésnek tekintve, tulajdonképpen mindig csak összesen egy új „kiintegrált tag” keletkezik, amelynek „nevezője” mindig \( \pi^2 \)-szereze az előzőnek. Így a \( \pi^2 = a/b \) indirekt feltevéseből kiindulva a

\[
\pi a^{n+1} \int_0^1 \sin(\pi x) f(x) \, dx
\]

integrál vizsgálatával a T 9.5.2 Tétel gondolatmenetét követve ellentmondásra fogunk jutni.

13.9.6.

9.6.1 Az \( \alpha \) minimálpolinomja ugyanaz, mint az \( \alpha \) minimálpolinomja, a másik három szám pedig rendre előállítható \( \alpha \) -ból és \( \alpha \) -ból a következő műveletek segítségével: összeadás, kivonás és \( z \) -vel való szorzás, szorzás és négyzetgyökvonás.

9.6.2 Csak (c) algebrai egész. — Útmutatás (d)-hez: Tegyük fel indirekt, hogy \( \cos 1^\circ \) algebrai egész, és mutassuk meg, hogy ekkor \( \sin 1^\circ \) is az, sőt az összegzési képletek alapján bármely \( k \) egészre \( \cos k^\circ \) és \( \sin k^\circ \) is algebrai egész. Ez azonban például \( k = 30 \) -ra nem igaz.

9.6.3 Igaz: (a), (c), (e), (f), (h).

9.6.4 Létezik, például \( \varphi = y = 1 \), \( z = \sqrt{2} \) megfelel.

9.6.5 Igaz: (a), (c), (d).

9.6.6 Mivel \( \alpha \) algebrai szám, ezért alkalmas \( a_i \) egész számokra

\[
a_0 + a_1 \alpha + \cdots + a_n \alpha^n = 0, \quad n \in \mathbb{N}, \quad a_i \neq 0.
\]

Ezt \( a_i^{n-1} \)-gyel szorzva és átalakítva kapjuk, hogy \( a_n \alpha \) algebrai egész, azaz \( \alpha \) előáll egy algebrai egész és az \( a_n \) egész szám hányadosaként. Ha ezt \( \alpha \) helyett \( 1/\alpha \) -ra alkalmazzuk, akkor az adódik, hogy \( \alpha \) felirható egy egész számnak és egy algebrai egésznek a hányadosaként (ha \( \alpha = 0 \), akkor pedig ez triviálisan igaz).

9.6.7 Az \( \alpha \) (normált, egész együthátó) minimálpolinomjában a konstans tag \( \perp 1 \).

9.6.8

(a) Megfelel például \( \beta_n = (\sqrt{2} - 1)^n \).

(b) Legyen \( \beta_n = \sqrt{2}^n \).

(c) Legyen az \( \alpha \) algebrai egész minimálpolinomja \( a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n \) (ahol minden \( a_i \) egész), ekkor \( \alpha/a \) minimálpolinomja \( a_0 + a_1 b x + \cdots + a_{n-1} b^{n-1} x^{n-1} + b^n x^n \). Ezt normálva a konstans tag csak úgy lesz egész, ha \( b^a \mid a_0 \), tehát csak véges sok ilyen \( b \) egész létezik (hiszen \( \alpha \neq 0 \) miatt \( a_0 \neq 0 \)).
9.6.9 Mindkét kérdésre igenlő a válasz, megfelel például $\cos \varphi + i \sin \varphi$, ahol (a) $\cos \varphi = 1/3$; (b) $\cos \varphi = \sqrt{2} - 1$.

9.6.10

(a) A T 8.4.1 Tétel alapján példa alakú számok, ahol $a$ és $b$ egész szám, mindenütt sűrűek a számegyenesen.

(b) A másodfokú egyenlet megoldóképletéből adódik, hogy bármely nem valós másodfokú algebrai egész valós része csak 2 nevezőjű tört lehet, ezért a másodfokú algebrai egészek nem lesznek mindenütt sűrűek a számsíkon. A negyedfokúak viszont igen: az $(a - b\sqrt{2}) + i(e + d\sqrt{2})$ alakú számok, ahol $a$, $b$, $c$ és $d$ egész szám, „általában” negyedfokú algebrai egészek, és mindenütt sűrűek a síkon.

9.6.11

(a) Mivel racionális $\tau$ esetén $a = \cos r^\circ + i \sin r^\circ$ egységgyök, és így algebrai egész, ezért $2 \Re a = 2 \cos r^\circ$ is algebrai egész. Ha $2 \cos r^\circ$ emellett még racionális is, akkor csak egész szám lehet. Így $\cos r^\circ$ értéke $0$, $\pm 1/2$ vagy $\pm 1$. — A feladatot megoldhatjuk az algebrai egészek felhasználása nélkül is. Ha $\tau$ racionális, akkor van olyan $n$ pozitív egész, amelyre $n\tau$ a 360-nak egész számú többszöröse, azaz $\cos(n\tau^\circ) = 1$. A

$$\cos(n\alpha) = 2 \cos((n - 1)\alpha) \cos \alpha - \cos((n - 2)\alpha)$$

összefüggés alapján igazoljuk teljes indukcióval, hogy $2 \cos(n\alpha)$ a $2 \cos \alpha$-nak egy egész egyúthatós, normált polinomja. Ebből következik, hogy ha $\cos(n\tau^\circ) = 1$, akkor $2 \cos r^\circ$ gyöke egy egész egyúthatós, normált polinomnak. Egy ilyen polinom racionális gyökei csak egészek lehetnek, tehát $2 \cos r^\circ$ egész szám.

(b) Az $\tau$ és $\sin \tau^\circ$ értékek közül legalább az egyik irrationális, kivéve ha $\tau$ olyan egész szám, amely a 30-nak páratlan többszöröse vagy pedig osztható 180-nal.

Tegyük fel, hogy $\tau^\circ$ értelmezve van, azaz $\tau^\circ$ nem páratlan többszöröse 90-nek. Ekkor az $\tau$ és $\tan \tau^\circ$ értékek közül legalább az egyik irrationális, kivéve ha $\tau$ olyan egész szám, amely a 45-nek páratlan többszöröse vagy pedig osztható 180-nal.

A szinuszra vonatkozó állítás azonnal adódik az (a) részből és a $\sin \tau^\circ - \cos(90 - \tau^\circ)$ összefüggésből, a tangensre vonatkozó állítás pedig ezután a 9.5.2(c) feladathoz [313] adott útmutatás szerint következik.

13.10 Algebrai számtestek

13.10.1.

10.1.1 Az $L \subset T \subset M$ bővítésláncban a fokszámérték szerint valamelyik lánccsal elsőfokú.

10.1.2 (a) $2$.

(b) $\infty$.

(c) $\infty$.

10.1.3
(a) Az egyik irány nyilvánvaló, a másik pedig következik a T 9.3.6 Tételből.

(b) (b1) 1.
(b2) 2.
(b3) 2.
(b4) 3.

10.1.4
(a) Igaz: (a1).

(b) \[ m_m,\beta | m_{\beta,\lambda} \text{ és } deg_m,\beta \leq deg_{\lambda,\beta} \, . \]

13.10.2.

10.2.1 A T 10.2.2 Tétel alapján a \( \mathbb{Q}(\alpha) = \mathbb{Q}(\beta) \) egyenlőséghez elég azt igazolni, hogy \( \alpha \in \mathbb{Q}(\beta) \) és \( \beta \in \mathbb{Q}(\alpha) \).

10.2.2
(a) Ez leegyszerűbben a T 10.2.2 Tételből következik.

(b) \( \mathbb{Q}(\alpha) \) altér a \( \mathbb{Q} \) feletti \( \mathbb{Q}(\beta) \) véges dimenziós vektortéren, és egy véges dimenziós \( \mathbb{V} \) vektortér egy \( \mathcal{U} \) alterére \( \mathcal{U} = \mathcal{V} \) pontosan akkor teljesül, ha \( \dim \mathcal{U} = \dim \mathcal{V} \).

(c) A \( \eta \) és \( \alpha \) számok pontosan a megadott feltétel esetén fejezhetők ki különbözően egymással a D 10.2.1 Definícióban megadott módon.

10.2.3 Igaz: (b), (d). (Ezek igazolásánál ne felejtkezzünk el arról, hogy \( \eta \) transzcendens szám is lehet.)

10.2.4 (a) \( 12 + 2\sqrt{2} + 9\sqrt{4} \).

(b) \( \frac{1}{2} \sqrt{4} \).

(c) \( \frac{\eta}{2} - \frac{\sqrt{3}}{2} \sqrt{5} + \frac{\sqrt{\eta}}{2} \sqrt{4} \).

10.2.5 (a) 4.

(b) 10.

(c) 7.

(d) 4.

Útmutatás: Az alábbi két észrevételt érdemes felhasználni: (i) Ha \( \alpha \) eleme egy véges bővítésnek, akkor \( \deg \alpha \) osztója a bővítés fokának.

(ii) Ha \( \alpha \) algebrai és egy \( \kappa \) -adfokú szám eleme \( \mathbb{Q}(\alpha) \) -nak, akkor \( \kappa \mid \deg \alpha \).

10.2.6 (a) \( \emptyset \).

(b) \( \mathbb{Q}(\sqrt{2}) \).

(c) \( \mathbb{Q}(\sqrt{5}) \).
Útmutatás (b)-hez: Használjuk fel, hogy \( \mathbb{Q}(\sqrt{3}) \) része a metszetnek, továbbá a metszet (\( \mathbb{Q} \) feletti) foka osztója mindkét bővítés fokának. — Másik lehetőség: A metszet egy tetszőleges elemét írjuk fel a T 10.2.3 Tételek megfelelően egyrészt mint \( \mathbb{Q}(\sqrt{7}) \)-beli, másrészt mint \( \mathbb{Q}(\sqrt{3}) \)-beli elemet. Mindkét előállítást tekintjük most mint ugyanannak a \( \mathbb{Q}(\sqrt{7}) \)-beli elemnek a T 10.2.3 Tétel szerinti felirását, ekkor ennek az előállításnak az egyértelműségéből adódik a jelzett eredmény.

10.2.7 (a) \( \mathbb{Q} \).

(b) \( \mathbb{Q}(\sqrt{3}) \).

(c) \( \mathbb{Q}(\sqrt{2}) \).

10.2.8 Induljunk ki a \( |\nu| = 1 \)-ből adódó

\[
\text{Res} \nu = \frac{\nu + \overline{\nu}}{2} = \frac{1}{2}(\nu + \frac{1}{\nu})
\]

összefüggésből. (A bizonyítás során ne feledkezzünk el arról, hogy \( \nu \) transzcendens szám is lehet.)

10.2.9 A bővítések és a fokszámok vizsgálatából vezessük le, hogy \( \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{\nu}) \). (Használjuk fel a T 10.2.5 és T 10.2.3 Tételeket, valamint a 10.2.2 feladatot [325].)

10.2.10 Válasz: \( k \), illetve \( k/2 \) (ez utóbbi természetesen csak páros \( k \) esetén fordulhat elő). — Útmutatás: Alkalmazzuk a fokszámítét a \( \mathbb{Q} \subseteq \mathbb{Q}(\sqrt{\nu}) \subseteq \mathbb{Q}(\nu) \) bővítésának. (Páros \( k \) esetén mutassunk példát mindkét lehetőség megvalósulására.)

10.2.11 Válasz: \( \pm 1 \). — Útmutatás: A 10.2.8 feladathoz [326] hasonló gondolatmenetet alkalmazva tekintjük a \( \mathbb{Q} \subseteq \mathbb{Q}(\text{Res} \nu) \subseteq \mathbb{Q}(\nu) \) bővítéslánccra. — Másik lehetőség: Mutassuk meg, hogy \( \nu \)-nak és \( 1/\nu \)-nak ugyanaz a minimálpolinomja, és ennek felhasználásával lássuk be, hogy az \( 1 \) vagy a \( -1 \) gyöke ennek a minimálpolinomnak.

10.2.12 Az (a) rész a 10.2.6 (vagy a 9.3.1), a (b) rész pedig a 10.2.7 (vagy a T 9.3.6) Tételre adott bizonyításból következik.

10.2.13

(a) \( A \) \( \subseteq \) irány nyilvánvaló, a \( \Rightarrow \) irány pedig abból adódik, hogy \( \nu \) transzcendenciája miatt \( (g_1 h_2 - g_2 h_1)(\nu) = 0 \) csak a \( g_1 h_2 - g_2 h_1 = 0 \) esetben lehetséges.

(b) Az (a) rész alapján a

\[
\begin{align*}
g(x) & \rightarrow g(\nu) \\
h(x) & \rightarrow h(\nu)
\end{align*}
\]

megfeleltetés bijekció a \( \mathbb{Q} \) feletti algebrai törtek és \( \mathbb{Q}(\nu) \) között, a művelettartás pedig nyilvánvaló.

13.10.3.

10.3.1

(a) A T 10.3.5 Tétel bizonyításának \( E(\sqrt{2}) \) részéhez hasonlóan igazoljuk, hogy \( E(\sqrt{3}) \)-ban a norma abszolút értéke szerint elvégzhető a maradékos osztás.
EREDMÉNYEK ÉS ÚTMUTATÁSOK

(b1) Mindkét felbontásban felbonthatatlanok szerepelnek, ezek azonban csak egységtényezőkben különböznek:

\[ 5 + 3\sqrt{3} = (2 + \sqrt{3})(1 + \sqrt{3}) \quad \text{és} \quad - 4 + 3\sqrt{3} = (2 - \sqrt{3})(1 - 2\sqrt{3}). \]

(b2) Mindkét felbontásban szerepel olyan tényező, amely nem felbonthatatlan.

(c) Alkalmazzuk a T 10.3.8 Tételt. — Az összes prímet (egységszerestől eltekintve) a pozitív prímszámok felbontásából nyerjük:

(c1) \[ 3 = (\sqrt{3})^2, \quad 2 = \varepsilon(1 + \sqrt{3})^2, \] ahol \( \varepsilon = 2 - \sqrt{3} \) egység.

(c2) Ha \( \mathcal{P} \equiv \pm 5 \pmod{12} \), akkor \( \mathcal{P} \) prím.

(c3) Ha \( \mathcal{P} \equiv \pm 1 \pmod{12} \), akkor \( \mathcal{P} \) két prim szorza, amelyek nem egymás egységszeresei.

(d) Megoldhatóság esetén a megoldásszám végleten, lásd a 7.8.3 feladatot [261]. Az egyenlet akkor és csak akkor oldható meg, ha \( \mathfrak{a} \) kanonikus alakjában minden \( 12k \pm 5 \) alakú prímszám kitevője páros, továbbá a 2, a 3 és a \( 12k - 1 \) alakú prímszámok kitevőjének az összege is páros. — Útmutatás: Használjuk fel (c) rész eredményét, és kövessük a két-négyzetszám-tétel bizonyításának gondolatmenetét. Vegyük figyelembe, hogy minden egység normája + 1. A 2, a 3 és a \( 12k - 1 \) alakú prímszámok kitevőjét azért kell vizsgálni, mert az ezeknek a prímszámoknak a felbontásából származó \( \mathcal{F}(\sqrt{3}) \)-beli prímek normája negatív, így ha a szóban forgó kitevőösszeg páratlan, akkor \( \mathfrak{a} \) áll elő \( \omega^2 - 3y^2 \) alakban.

10.3.2

(a) A Gauss-egészekhez hasonlóan igazolható, hogy a norma szerint elvégezhető a maradékos osztás.

(b) A T 10.3.8 Tételből következik, hogy az összes prímet (egységszerestől eltekintve) a pozitív prímszámok felbontásából nyerjük, a következőképpen:

(b1) \[ 2 = - (\sqrt{2})^2. \]

(b2) Ha \( \mathcal{P} \equiv 5 \pmod{8} \) vagy \( 7 \pmod{8} \), akkor \( \mathcal{P} \) prím.

(b3) Ha \( \mathcal{P} \equiv 1 \pmod{8} \) vagy \( 3 \pmod{8} \), akkor \( \mathcal{P} \) két prim szorza, amelyek nem egymás egységszeresei.

(c) Válassz: \( x = \pm 5, \quad y = 3 \). — Útmutatás: Az \( [x + \sqrt{-2}][x - \sqrt{-2}] = y^4 \) bal oldalán a két tényező közös primosztója csak \( \sqrt{-2} \) lehet, ebből azonban következik, hogy \( x \) páros, ami az eredeti egyenlet modulo 4 vizsgálatával ellentmondásra vezet. A két tényező így relatív prim, és mivel az egységek csak a \( \pm 1 \), amelyek maguk is köbszámok, ezért mindkét tényező teljes köb. Az eredmény ezután az \( x = \sqrt{-2} = \frac{(a + b\sqrt{-2})^3}{3} \) egyenlőségben a \( \sqrt{-2} \) együtthatójának összehasonlításából adódik.

10.3.3 Tekintsük például az alábbi felbontásokat:

(a) \[ (1 + \sqrt{15})(1 - \sqrt{15}) = (-2) \cdot 7. \]

(b) \[ (1 + \sqrt{-26})(1 - \sqrt{-26}) = (-5) \cdot 5. \]

(c) \[ (2 + \sqrt{-6})(2 - \sqrt{-6}) = 2 \cdot 5. \]

(d) \[ (2 + \sqrt{-10})(2 - \sqrt{-10}) = 2 \cdot 7. \]
10.3.4 Kövessük a Gauss-, illetve Euler-egészeknél látott gondolatmenetet (T 7.4.8 Tétel). Ha \( t \not\equiv 1 \pmod{4} \), akkor \( E(\sqrt{t}) \) elemei egy téglatestprácos alkotnak a komplex számsíkon, ahol az „alapépaprálap” vízszintes oldala 1, függőleges oldala pedig \( \sqrt{t} \) hosszúságú. A maradékos osztáshoz arra van szükség, hogy a rácsponkok köré rajzolt egységkörök belseje tartalmazza \( Q(\sqrt{t}) \) minden elemét. Ez biztosan teljesül, ha a körök lefedik az egész síkokat, azaz \( \sqrt{t} \leq \sqrt{3} \), vagyis \( t = -1 \) vagy \( -2 \), továbbá biztosan nem teljesül, ha az \( \sqrt{t} > \sqrt{3} \), vagyis \( t < -3 \) (mivel \( -3 \equiv 1 \pmod{4} \), ezért \( t = 3 \) most nem jöhet szóba). Hasonlóan okoskodhatunk a \( t \equiv 1 \pmod{4} \) esetben is, ekkor egy olyan paralelogrammarácsról van szó, ahol az alapparalelogramma vízszintes oldala 1 hosszúságú, a magassága \( \frac{1}{2} \sqrt{t} \), és a vízszintes oldalhoz tartozó magasság talpontja az oldal felezőpontjában van.

10.3.5 Használjuk fel a T 10.3.8/(vii) Tételt.

10.3.6 Lássuk be, hogy bármely \( 0 \leq n \leq k - 2 \) esetén \( n^2 + n + k = N(\alpha_n) \), ahol \( \alpha_n \) felbonthatatlan \( E(\sqrt{-4k + 1}) \)-ben. Ebből vezessük le, hogy ha valamely \( n \)-re \( N(\alpha_n) \) nem lenne primszám, akkor \( N(\alpha_n) \) kétfélelekképpen bomlana felbonthatatlanok szorzatára.

10.3.7 A felbonthatatlanság azonnal adódik a norma tulajdonságai ből. — Az állítás másik részéhez először lássuk be, hogy a feltétel alapján minden \( \beta \in E(\sqrt{t}) \)-hez létezik olyan \( b \) egész szám, amelyre \( \alpha | \beta - b \). Ekkor \( \alpha \) prim volta a következőben igazolható:

\[
\alpha \mid \beta - b \implies \alpha \mid b \implies p = N(\alpha) \mid \beta^2 - \beta \implies p \mid b \text{ vagy } p \mid c \implies \alpha \mid \beta \text{ vagy } \alpha \mid \gamma.
\]

10.3.8 Mivel \( \beta^2 / \alpha^2 \) algebrai egész, ezért a négyzetgyöke, \( \beta / \alpha \) is az. Emellett \( \beta / \alpha \in Q(\sqrt{t}) \), tehát \( \beta / \alpha \in E(\sqrt{t}) \) is teljesül.

10.3.9

(a) \( 5 = -\sqrt{5} \).

(b) A T 10.3.6 Tétel bizonyításában láttuk, hogy a 2 felbonthatatlan, továbbá

\[
2 \mid \beta - (1 + \sqrt{5})(1 - \sqrt{5}) = \epsilon \alpha, \quad 2 \not\mid 1 \pm \sqrt{5},
\]

teht a 2 nem prim.

(c) Használjuk fel a T 10.3.7 Tételt, és azt, hogy \( \left( \frac{-5}{p} \right) = -1 \) pontosan a megadott alakú \( P \) primszámokra teljesül.

(d) Az, hogy ezek nem prímek, az előzőkből következik, a felbonthatatlanság pedig azért igaz, mert egy ilyen \( P \) (sőt általában egy 10-es \( \pm 3 \) alakú szám) nem lehet egy \( E(\sqrt{-5}) \)-beli elem normája.

(e) Azt kell igazolni, hogy ezek a \( P \) prímek előállnak normaként, azaz (egész \( a \), \( b \)-vel) \( P = a^2 + 5b^2 \) alakban, hiszen ekkor \( P = \frac{a + b\sqrt{5}}{a - b\sqrt{5}} \). Az \( x^2 = -5 \pmod{p} \) kongruencia megoldhatóságát felhasználva a T 8.2.4 Tétel bizonyításának a mintájára vagy a 7.5.21a feladatban [242] szereplő Thue-lemma segítségével mutassuk meg, hogy a \( P \)-nek egy kis többszöröse előáll \( a^2 + 5b^2 \) alakban, majd ebből vezessük le, hogy akkor maga a \( P \) is felírható így.
13.10.4.

10.4.1

(a) $\pm \sqrt{2} \pm \sqrt{3}$.

(b) $\sqrt{3}(\pm 1 \pm i)$.

(c) $\cos 20^\circ$, $\cos 140^\circ$, $\cos 260^\circ$.

(d) $\cos k^2 + i \sin k^\circ$, ahol $1 < k < 360^\circ$, $k$ egész és $(k, 360) = 1$.

10.4.2

(a) A $\eta$ minimálpolinomjára a gyökök és együtthatók közötti összefüggést alkalmazva kapjuk, hogy $\eta'(1) + \eta'(2)$ racionális, és így $\eta(2) \in \mathbb{Q}(\eta'(1))$.

(b) Létezik olyan $\eta_j$, amely valós szám, tehát $\mathbb{Q}(\eta_j(\eta)) \subseteq \mathbb{R}$, és így $\mathbb{Q}(\eta_j) \neq \mathbb{Q}(\eta)$.

(c) A $\mathbb{Q} \subseteq \mathbb{Q}(\eta_j(\eta)) \cap \mathbb{Q}(\eta_k(\eta)) \subseteq \mathbb{Q}(\eta_j(\eta))$ bővítésláncban a két láncszem fokának a szorzata 3, így az állításhoz csak azt kell igazolni, hogy bármelyik két $\mathbb{Q}(\eta_j(\eta))$ különböző. Lássuk be, hogy ha a három $\mathbb{Q}(\eta_j(\eta))$ közül valamelyik kettő megegyezik, akkor a harmadik is ugyanez kell hogy legyen. Ez azonban ellentmond a feladat (b) részének.

10.4.3 (Az R.K. rövidítés a relatív konjugáltakat jelöli.)

(a) R.K.: $1 \pm \sqrt{2}$, $1 \pm i \sqrt{2}$, $N(\alpha) = -1$.

(b) R.K.: $1 \pm \sqrt{2}$ kétszeres multiplicitással. $N(\beta) = 1$.

(c) R.K.: $(1 + \sqrt{2})(1 + \sqrt{2})$, $(1 + i \sqrt{2})(1 - \sqrt{2})$, $N(\gamma) = -1$.

10.4.4 Kövessük a T 10.3.4 Tétel bizonyításának a gondolatmenetét. (Figyeljünk arra, hogy az $\varepsilon$ relatív konjugáltjai általában nem elemei $\mathbb{Q}(x)$-nak, viszont a szorzatuknak az $\varepsilon$-nal vett hányadosa már igen.)

10.4.5

(a) Például $(3 + 4i)/5$ megfelel.

(b) Legyen a másodfokú bővítés $\mathbb{Q}(\sqrt{2})$ alakú, ahol $t$ négyzetmentes egész és $t \neq 1$, és legyen $p > 2$ egy olyan prim, amelyre $(t, p) = 1$. Ekkor az $x^2 - t \equiv 0 \ (\text{mod } p)$, és így az $x^2 - t \equiv 0 \ (\text{mod } p^2)$ kongruencia is megoldható, azaz létezik olyan $c$ egész szám, amelyre $(c + \sqrt{2})/p$ nem algebrai egész, de a normája egész szám.

13.10.5.

10.5.1 (a) $-4$.

(b) $-3$.

(c) $-10\bar{5}$. 
EREDMÉNYEK ÉS ÚTMUTATÁSOK

(d) \( 2^{n-1}q^{n}(-1)^{(n-1)(n-2)/2} \).

Útmutatás (d)-hez: A keresett diszkrimináns egy Vandermonde-determináns négyzete, ezt a determináns önmagával való (sor-oszlop) szorzásával érdemes kiszámítani.

10.5.2
(a) Ekkor

\[
\begin{pmatrix}
\beta_1 \\
\beta_2 \\
\vdots \\
\beta_n
\end{pmatrix} = C \begin{pmatrix}
\alpha_1 \\
\alpha_2 \\
\vdots \\
\alpha_n
\end{pmatrix},
\]

ahol \( C \) egész elemű mátrix, és így a T 10.5.3/(iii) Tétel szerint

\[
\Delta(\beta_1, \ldots, \beta_n) = \Delta(\alpha_1, \ldots, \alpha_n)(de\pm C)^2.
\]

(b) Az (a) rész szerint a két diszkrimináns egymásnak kölcsönösen pozitív egész számszorosa.

10.5.3 A másodfokú bővítések \( \mathbb{Q}(\sqrt{t}) \) alakúak, ahol \( t \) négyzetmentes egész szám és \( t \neq 1 \).

A keresett diszkrimináns \( 4t \), ha \( t \neq 1 \mod 4 \), és \( t \), ha \( t = 1 \mod 4 \) .

10.5.4 A 10.5.2 feladatnál [348] látott gondolatmenetet érdemes alkalmazni.

10.5.5
(a) A keresett feltétel: \( a, b, c, d \in \mathbb{Z} \) és

\[
\begin{vmatrix}
a & b \\
c & d
\end{vmatrix} = \pm 1.
\]

(b) Legyen \( \omega = \cos(2\pi/3) + i \sin(2\pi/3) \). Ekkor az \( a + b\omega \) és \( c + d\omega \) Euler-racionálisok pontosan akkor alkotnak egész bázist, ha \( a, b, c, d \) -re teljesül az (a) résznél megadott feltétel.

10.5.6 Azokban a \( \mathbb{Q}(\sqrt{t}) \) bővítésekben, ahol ( \( t \) négyzetmentes egész szám, \( t \neq 1 \) és) \( t \equiv 1 \mod 4 \).

10.5.7 Közvetlenül következik a diszkrimináns definíciójából. — Másik lehetőség: Alkalmazzuk a 10.5.3/(iii) Tételt az \( \alpha^{t} = \alpha^{t-1} \) szereposztással, és használjuk ki, hogy \( \Delta(1, \hat{1}, \ldots, \hat{n}^{t-1}) \) egy olyan Vandermonde-determináns négyzete, amelynek a generátorai valós számok.

10.5.8
(a) Például \( \mathbb{Q}(\sqrt{t}) \)-ben \( 1/2 \) és \( 2 \) megfelel.

(b) Használjuk fel, hogy ha az \( \tau_1, \ldots, \tau_n \) racionális számok szorzata 1, akkor

\[
\Delta(\tau_1, \alpha_1, \ldots, \tau_n, \alpha_n) = \Delta(\alpha_1, \ldots, \alpha_n).
\]

13.11 Ideálok

13.11.1.

11.1.1 (a) \( (2) \). (b) \( (1 + i) \). (c) Nem ideál.
(d) \(\langle 1 + \i \rangle\).

(e) Nem ideál.

(f) \(\langle 7 \rangle\).

11.1.2 (a) \(\langle 2x - 1 \rangle\). (b) \(\langle x^2 - 2, x^2 - 3 \rangle\).

(c) Nem ideál.

(d) \(\langle x - 3, 2 \rangle\).

(e) Nem ideál.

11.1.3 Legyen \( R \) test és \( I \neq \emptyset \) ideál \( R \) -ben. Azt kell igazolni, hogy ekkor \( I = \bar{R} \). Ha \( a \neq \emptyset \) eleme \( I \) -nek és b tetszőleges eleme \( \bar{R} \) -nek, akkor az osztás elvégezhetősége miatt van olyan \( c \in \bar{R} \), amelyre \( a \omega = b \), azaz \( b \in I \), vagyis \( I = \bar{R} \). — A megfordításnál vegyünk \( R \) -ben egy \( a \neq \emptyset \) elemet. Ekkor a feltétel szerint \( (a) = \bar{R} \), tehát bármely \( b \in \bar{R} \) -re \( b \in (a) \). Ez azt jelenti, hogy alkalmas \( c \) -vel \( a \omega = b \) teljesül, vagyis elvégezhető \( R \) -ben az osztás, és így \( R \) valóban test.

11.1.4 Legyen \( I = \langle \xi_1^{2^{\frac{1}{k_1}}} \cdots \xi_n^{2^{\frac{1}{k_n}}} \rangle \), ahol \( \xi_1, \ldots, \xi_n \in E \). Ekkor \( I \) minden eleme \( \xi_2^{2^{\frac{1}{m}}} \) alakú, ahol \( \xi \in E \) és \( m = [k_1, \ldots, k_n] \). Mivel (például) \( 3^{2^{(n-1)}} \) nem lehet ilyen alakú, ezért \( I \neq \bar{K} \), vagyis \( \bar{K} \) nem generálható véges sok elemmel.

11.1.5 Mutassuk meg, hogy az egyik ideál generátorai kifejezhetők a másik generátorainak a segítségével, és viszont.

11.1.6

(a) a1: 4,

a2: 9,

a3: 5.

Test: a2, a3.

(b) Ha \( a \neq \emptyset \), akkor \( G/(\alpha) \) elemszáma \( N(\alpha) \), és \( G/(\alpha) \) akkor és csak akkor test, ha \( \alpha \) Gauss-prím. — Útmutatás: A „modulo \( \alpha \) maradékosztályok” számának meghatározásához lásd a 7.7.12 feladathoz [257] adott útmutatást. A másik állítás ahhoz hasonlóan bizonyítható, ahogyan azt igazoltuk, hogy \( Z/(m) \) akkor és csak akkor test, ha \( \exists \) prim (T 2.8.4 Tétel, természetesen azt is végig kell gondolni, hogy az ehhez felhasznált valamennyi korábbi tétel megfelelője is átvihető a Gauss-egységekre).

11.1.7

(a) Alkalmazzunk ahhoz hasonló gondolatmenetet, mint amikor (a T 11.1.3 Tétel utáni Példák között) azt igazoltuk, hogy \( Z[x] \) -ben \( \langle 2, x \rangle \) nem föideál.

(b) b1: 2, test.

b2: 6, nem test.

b3: 121, test.

11.1.8
(a) Test: a2.

(b) $T[x]/(f)$ test $\iff$ f irreducibilis T felett.

(c) A faktorgyűrűnek 4 eleme van (a maradékosztályok az $a_0 + a_1 x$ maradékokkal reprezentálhatók, ahol $a_0 = 0$ vagy 1), és egyszerűen ellenőrizhető, hogy a három darab $\neq 0$ elemnek létezik inverze.

Másik lehetőség: A faktorgyűrű izomorf $\mathbb{Z}_2[x]/(x^2 + x + 1)$-gyel, ahol $\mathbb{Z}_2$ a modulo 2 maradékosztályok teste. Ekkor $\mathcal{S}$ a feladat (b) része alapján test.

11.1.9

(a) Kövessük a T 11.1.6 Tétel utáni Példánál a speciális esetben látott gondolatmenetet. A bizonyítás lényege: $\mathbb{Q}[x]$ -nek az $(m_\alpha x)$ főideál szerinti egy-egy maradékosztályát egyértelműen jellemzi az adott osztályba eső polinomoknak az $m_\alpha$ polinommal való osztási maradéka, és az ezekkel a maradékokkal való számolásnál az egyetlen „szabály” az, hogy az $m_\alpha$ többszörösei „nem számítanak”. Ez pontosan megfelel a $\mathbb{Q}[x]$ -beli elemek szokásos felírásának és az ottani (kizárólag az $(m_\alpha x) = 0$ összefüggést felhasználó) számolásnak. — Másik lehetőség: A $\mathbb{Q}[x]$ -ből $\mathbb{Q}(\vartheta)$ -ba az $f \mapsto f(\vartheta)$ leképezés gyűrűhomomorfizmus, amelynek a képe $\mathbb{Q}(\vartheta)$, a magja pedig az $m_\alpha$ által generált főideál. Így az állítás következik a gyűrűk homomorfizmustételéből.

(b) Az (a) rész általánosítását szem előtt tartva legyen $M = \mathcal{I}[x]/(f)$. Az $f$ irreducibilitását felhasználva igazolható, hogy $M$ test, továbbá a konstans+$\langle f \rangle$ maradékosztályok halmaza megfelel $\mathcal{I}^*$ -nak, az $x + \langle f \rangle$ maradékosztály pedig $\vartheta$ -nak.

11.1.10

(a) Az állítást elég főideálokra igazolni, ugyanis ha $\alpha \in \mathcal{I}$, akkor $(\alpha) \subseteq \mathcal{I}$ miatt az $\mathcal{I}$ szerinti maradékosztályok száma legfeljebb annyi, mint az $(\alpha)$ szerinti maradékosztályok száma. Legyen tehát $\alpha \neq 0$, és mutassuk meg, hogy „modulo $\alpha$ ” csak véges sok maradék létezik. Legyen $\omega_1, \ldots, \omega_n$ egész bázis $E(\vartheta)$ -ban. Ekkor bármely $\xi \in E(\vartheta)$ felírható $\xi = k_1 \omega_1 + \cdots + k_n \omega_n$ alakban, ahol $k_i \in \mathbb{Z}$, $i = 1, \ldots, n$. Mivel $\alpha \mid N(\vartheta)$, ezért minden modulo $\alpha$ maradékosztálynak van olyan $\zeta$ reprezentánsa, ahol $0 \leq k_i < N(\vartheta)$, $i = 1, \ldots, n$.

(b) Ekkor az $R/A_1$ faktorgyűrűk elemszáma szigorúan monoton csökken. Ez azonban lehetetlen, hiszen $A_2 \neq 0$ miatt $R/A_2$-nek csak véges sok eleme van.

(c) Ha egy $\mathcal{I} \neq \varnothing$ ideál nem lenne végesen generált, akkor létezne benne ideáloknak egy szigorúan növő

$$\{a_1\} \subset \{a_1, a_2\} \subset \{a_1, a_2, a_3\} \subset \ldots$$

láncra.

13.11.2.

11.2.1 (a) (5), (b) (60).

11.2.2 (a) 4, (b) 16.

11.2.3 Fogalmazzuk át a feladatot oszthatóságra a T 11.2.1 Tétel felhasználásával.
11.2.4

(a) A 2 és az $1 + \sqrt{-5}$ egyaránt közös osztók, nincs azonban olyan közös osztó, amely ezeknek többszöröse lenne.

(b) $(2), (1 + \sqrt{-5}), (1)$.

(c) Például $\alpha = 2$, $\beta = 1 + \sqrt{-5}$.

**13.11.3.**

11.3.1

(a) A normált minimálpolinomjuk egész együtthatós és a konstans tag 1 vagy $-1$ (lásd a 9.6.7 feladatot [316]).

(b) $\alpha = \sqrt{\alpha} \sqrt{\alpha}$.

11.3.2

(a) Ha $a \neq 0$ és $b$ tetszőleges, valamint ha $a = b = 0$.

(b) Minden $a \neq 0$ egység, és így eleve nem léteznek felbonthatatlanok, illetve primek.

(c) Alaptétel: az állítás „ábers”, hiszen a 0-tól és egységektől különböző elemekre vonatkozik, ilyenek azonban testben nincsenek. — Főideálgyűrű: testben csak a triviális (0) és (1) ideálok léteznek (lásd a 11.1.3 feladatot [354]), és ezek valóban főideálok. — Euklideszi gyűrű: mivel elvégezhető az osztás, ezért mindig elérhető, hogy a maradék 0 legyen (és így „tetszőleges” függvény megfelel $\bar{f}$-nek).

11.3.3

(a) Ez a 2.

(b) Az eljárással most egy egységet kapunk, és annak nincs felbonthatatlan osztója.

(c) Az 1.5.5c feladat [21] útmutatásához hasonlóan konstruálhatunk megfelelő $\bar{f}$-et.

(d) $(0), (1), (2), (2^2), (2^3), \ldots$

11.3.4 A D 11.1.1 Definíció követelményeinek a teljesülését kell ellenőrizni.

11.3.5 Útmutatás a szükségességhoz: Ha $\bar{R}[\bar{a}]$ főideálgyűrű, akkor tetszőleges $a$ konstans polinommal $(a, \bar{z})$ is főideál.

11.3.6 Mutassuk meg, hogy ha $c \neq 0$ olyan elem, amelyre $\bar{f}(c)$ minimális, akkor $c$ egység. Ekkor $c \mid e$ is teljesül, azaz alkalmas $e$ -vel $\bar{e} = c$. A nullosztómentesség felhasználásával igazoljuk, hogy $c$ egységelem.

11.3.7 Igaz: (a).

11.3.8 A legkisebb abszolút értékű maradék szerinti maradékos osztás kielégíti a feltételt, azaz ha ($b \neq 0$ és) $a = bq + r$, ahol $|r| \leq \frac{|b|}{2}$, akkor $\bar{f}(r) < f(\bar{b})$.

11.3.9
(a) Először mutassuk meg, hogy $P$ minden ideálja végesen generált, majd lássuk be, hogy $(a, b) = (d)$, ahol $d = \gcd(a, b)$.

(b) Következik az (a) részből a 11.1.10a feladat [355] alapján.

11.3.10 Az „akkor” részre vonatkozóan lásd a 10.3.4 feladatot [338] és az ahhoz tartozó útmutatást.

Megfordítva, ha valamely $t < -3$-ra $E(\sqrt[3]{t})$ euklideszi gyűrű, akkor tekintsünk egy olyan $\beta \neq 0$, $\pm 1$ elemet, amelyre $f(\beta)$ minimális. Mutassuk meg, hogy $N(\beta) \leq 3$. Ebből már következik, hogy $(t < -3$ esetén) csak $t = -7$ és $t = -11$ lehetséges.

13.11.4.

11.4.1

(a) A D 11.4.3 Definíció előtti P1 vagy P2 példákban szereplő $A$ és $B$ ideálok esetén $H$ nem ideál. (P1 esetén például $2 \cdot 3 + [x + 3][x - 2] = x^2 + x$, P2 esetén pedig $3 \cdot 3 - |1 + \sqrt{-5}|1 - \sqrt{-5} = 3$ nem áll elő $ab$ alakban.)

(b) Ha $A = \{\alpha\}$, akkor

$$\sum_{i=1}^{\kappa} a_i b_i = \sum_{i=1}^{\kappa} [r_i \alpha] b_i = \alpha \sum_{i=1}^{n} r_i b_i = \alpha b.$$

11.4.2

(a), (b) A bizonyítás ugyanúgy történik, mint az egész számoknál.

(c) A T 11.4.2 Tétel (iv) állításából következik.

(d) Használjuk fel (c)-t.

(e) A szükségességhez legyen $A = \{1\}$, és használjuk fel (c)-t.

11.4.3

(a) Ha $\alpha = \beta \gamma$, akkor a T 11.4.2 Tételben a (iii) állítás bizonyításából kapjuk, hogy $(\alpha) = (\beta)(\gamma)$.

Megfordítva, ha $(\beta)C = (\alpha)$, akkor a 11.4.1b feladathoz [371] adott útmutatás szerint $(\beta)C$ minden eleme, így speciálisan $\alpha$ osztható $\beta$-val.

(b) Az (a) részből adódó $\gamma = \alpha / \beta$ elem megfelel a feltételeknek.

11.4.4

(a) Azt kell igazolni, hogy $D$ ideál, $D$ tartalmazza $A$ -t és $B$ -t, valamint ha $C$ tetszőleges olyan ideál, amelynek része $A$ és $B$, akkor $D \subseteq C$.

(b) Ellentett: $A \subseteq A + B \equiv (0) \implies A = (0)$.

(c) Az $A(B, C)$ ideál elemei $\sum_{i=1}^{\kappa} c_i b_i + c_i$ alakúak, így a zárójelek felbontása után kapjuk, hogy ezek $(A\{B, C\})$-nek is elemei. A másik irányú tartalmazáshoz vegyük észre, hogy $(AB, AC)$ elemeit

$$\sum_{i=1}^{\kappa} a_i b_i + \sum_{j=1}^{\lambda} n_j c_j = \sum_{i=1}^{\kappa} a_i b_i + 0 + \sum_{j=1}^{\lambda} n_j [0 + c_j]$$
alakba írva \( \mathcal{A}(B, C) \)-beli elemeket kapunk.

11.4.5 A legkisebb közös többszörös olyan közös többszöröse \( A \)-nak és \( B \)-nek, amely minden közös többszöröse\( n \) osztója. Ezt (5) alapján a tartalmazásra átfogalmazva \( \mathcal{M} \) a legbővebb olyan ideál, amely része \( A \)-nak és \( B \)-nek, azaz \( \mathcal{M} = A \cap B \).

11.4.6 Például \( \mathbb{Z}[x] \)-ben \( A = (x) \), \( B = (2, x) \) megfelel.

11.4.7 A \( \langle 12 \rangle \Rightarrow \langle 11 \rangle \) irányt bizonyítsuk indirekt, a megfordításhoz pedig alkalmazzuk (11)-et az \( A = \langle a \rangle \), \( B = \langle b \rangle \) szereposztással.

11.4.8 (a) a1: Csak a két triviális osztója létezik.

a2: Az egyetlen nemtriviális osztó az a1-beli ideál.

a3: Két nemtriviális osztója van: \( \langle 2, 1 + \sqrt{-5} \rangle \)-s és \( \langle 3, 1 + \sqrt{-5} \rangle \).

(b) b1: \( \langle 2, 1 + \sqrt{-5} \rangle \);

h2: (1).

(c) Felbonthatatlan ideál: c1, c3.

11.4.9 Igaz: (b), (c), (d).

11.4.10

(a) \( A = (2, x) \), \( B = (4, x^2) \), \( C = (4, 2x, x^2) \).

(b) A f11.4.1b feladat [371] alapján \( \langle a \rangle B = \{\alpha b \mid b \in B\} \), \( \langle a \rangle C = \{\alpha c \mid c \in C\} \), és \( a \neq 0 \), valamint \( R \)-nullosztómentessége miatt \( \alpha b = \alpha c \Rightarrow b = c \).

11.4.11

(a) Ellenőrizzük az ideál definíciójában foglaltak teljesülését.

(b) Lássuk be, hogy \( I \)- maximális ideál, azaz rendelkezik a (9) tulajdonsággal. Ebből könnyen adódik, hogy a megadott hármon kívül \( I \)-nek nincs több felbontása. Végül, az \( I : I = I \) egyenlőség igazolásához használjuk fel, hogy \( x^a = x^{a/2}x^{a/2} \).

11.4.12

(a) Ha \( P = AB \), akkor egyrészt \( P \subseteq A \) és \( P \subseteq B \), másrészt a (12)-vel ekvivalens (11) tulajdonság miatt \( A \subseteq P \) vagy \( B \subseteq P \). Innen kapjuk, hogy \( P = A \) vagy \( P = B \).

(b) Ilyen például \( \mathbb{Z}[x] \)-ben a \( \langle 4, x \rangle \) ideál.

(c) Tegyük fel indirekt, hogy \( M \) maximális ideál és mégis van olyan \( a \notin M \), \( b \notin M \), amelyre \( ab \in M \). Jelölje \( \langle a, M \rangle \), illetve \( \langle b, M \rangle \) az \( a -t \) és az \( M \)-et, illetve a \( b -t \) és az \( M \)-et tartalmazó legszükebb ideált. Az \( M \) maximalitása folytán \( \langle a, M \rangle = \langle b, M \rangle = R \). Ekkor \( R = R \subseteq \langle c, \langle a, M \rangle \rangle = \langle c, \langle a, M \rangle \rangle = M \), ami ellentmondás.
(d) Ilyen például $\mathbb{Z}[x]$-ben az $(x)$ ideál.

(e) A maximális ideálról vonatkozó állításhoz mutassuk meg, hogy általában bijekció létesíthető az $\mathcal{I}$-nek az $\mathcal{I}$-t tartalmazó ideáljai és az $\mathcal{I}/\mathcal{I}$ faktorgyűrű ideáljai között, majd használjuk fel a 11.1.3 feladatot [354]. A primideálra vonatkozó állítás azonnal adódik a (12) feltételnek az $\mathcal{I}/\mathcal{I}$ faktorgyűrűre történő átfogalmazásából.

### 13.11.5.

11.5.1 Mindkét feltétel ekvivalens $\mathcal{A} \mid \langle \alpha \rangle$ fennállásával.

11.5.2

(a) A $N(\alpha)/\alpha$ hányados egyrészt algebrai egész, másrészt eleme $\mathbb{Q}(\sqrt{d})$-nak.

(b) Az (a) rész (vagy a T 11.5.5 Tétel) szerint $\mathcal{A}$-ban található nemnulla egész szám, így ekkor ennek az egész számú többszörösei is elemei $\mathcal{A}$-nak. Az állítás másik részéhez lássuk be, hogy az összes $\mathcal{A}$-beli egész számot a legkisebb ilyen pozitív egész (egész számú) többszöröseként kapjuk.

11.5.3 Következik a T 11.5.8 Tételből.

11.5.4

(a) A 11.5.2 feladat [382] alapján bármely $\mathcal{P}$ primideálban van $c > 1$ egész szám, Bontsuk fel $c$-t prímszámok szorzatára. Mivel $\mathcal{P}$ primideál, ezért ezen prímszámok valamelyike szükségképpen eleme $\mathcal{P}$-nek. Ha $\mathcal{P}$ tartalmazna két különböző pozitív prímszámot, akkor az ezek alkalmas egész számként képzett kombinációjaként előálló 1-et is tartalmazná, ami lehetetlen.

(b) Következik az (a) részből.

(c) Igen.

(d) Nem, ez következik a 11.5.3 feladatból [382].

11.5.5 Használjuk fel az ideálak legnagyobb közös osztójáról és legkisebb közös többszöröséről tanultakat.

11.5.6 Írjuk fel többféleképpen az $(\alpha)^2$ és $(\beta)^2$ ideálak legnagyobb közös osztóját.

11.5.7

(a) 

$$(21) = (3,4 + \sqrt{-5})(3, 4 - \sqrt{-5})(7, 4 + \sqrt{-5})(7, 4 - \sqrt{-5})$$

[Természetesen ezek a prímidéálok más generátorokkal is megadhatók, például $(3, 4 + \sqrt{-5}) = (3, 1 + \sqrt{-5}) = (3, 1 - 2\sqrt{-5}) = (2 - \sqrt{-5}, 1 + \sqrt{-5})$ stb.]

(b) $\mathcal{P} = 2$ és 3.

(c) $\mathcal{P} = 2, 5$, valamint a $20k + 1, 20k + 3, 20k + 7$ és $20k + 9$ alakú primek.

11.5.8 Mindkét tulajdonság azzal ekvivalens, hogy $E(\sqrt{d})$ minden ideálja fölideál (lásd a 11.3.9b feladatot [365], a T 11.4.2/(iii) Tételt és a T 11.5.8 Tételt).

### 13.11.6.

11.6.1 $(2, \sqrt{-6})(3 + \sqrt{-6}) = (3, \sqrt{-6})(2 - \sqrt{-6})$. 

540
11.6.2 Mindkét feltétel ekvivalens azzal, hogy $E(4^2)$ föideálgyűrű (vö. a 11.3.9b feladattal [365]).

11.6.3 Használjuk fel, hogy alkalmas $u$ és $v$ pozitív egészekel $kuv = 1 + hv$.

11.6.4

(a) Nincs megoldás.

(b) $x = y = 1$.

(c) $x = \pm 95\,y = 99$.

(d) $x = \pm 36$, $y = 11$. — Ne felejtse el, hogy $33 \equiv 1 \pmod{4}$ miatt $a + b\sqrt{-35} \in E(\sqrt{-35})$ esetén $a$ és $b$ nem feltételenül egész számok.

### 13.12 Kombinatorikus számmelmélet

#### 13.12.1

12.1.1

(a) $[\sqrt{n}/2] + 1$, azaz $h + 1$, ha $n = 2h$ vagy $2h + 1$. — Útmutatás: Megfelelő számhalmazt alkotnak az $[\sqrt{n}/2, n]$ intervallum összes egészéi. Annak igazolásához, hogy ennél több szám már nem adható meg, vegyük észre, hogy ha $u + v = ak$, ahol $0 < u < v$, akkor $u$ és $v$ közül legfeljebb az egyik szerepelhet az $a_i$-k között.

(b) Álljon rögzített $r$ mellett az $A_r$ sorozat az $a_1 + a_2 + \cdots + a_r + c$ számokból, ahol $s = r + 1, r + 2, \ldots$ (így $A_n$ az eredeti sorozat), és jelölje $A_r(n)$ az $A_r$ sorozat $n$-nél nem nagyobb elemeinek a számát. A feltétel szerint az $A_r$ sorozatok páronként diszjunktak, ezért

$$u \geq \sum_{i=0}^t A_r(u) \geq (t + 1)A_r(r)$$

bármi $u$-re és $t$-re. Másrész

$$A_r(n) = A \left( u - \sum_{i=1}^t a_i \right) - t \geq A(u) - \sum_{i=1}^t a_i - t.$$ 

A két egyenlőségből

$$A(n) \leq \frac{\gamma}{t + 1} + \sum_{i=1}^t a_i + t,$$

amit $u$-nél leosztra, $u \to \infty$ esetén a jobb oldal $\frac{j}{t + 1}$-hez tart, és mivel $t$ tetszőleges volt, ezért valóban $A(n)/\gamma \to 0$.

12.1.2 Ilyen tulajdonságú és a kívánt „sűrűségű” halmazt alkotnak a $3$-mal nem osztható számok. Annak igazolásához, hogy nagyobb sűrűség már nem lehetséges, vegyük észre, hogy bármely $[r, 4r]$ intervallumban legfeljebb $2r + 1$ darab $a_i$ lehet, mert a $2r$-nél nem nagyobb $a_j$-kre az $a_j + a_{j-1}$
-ek, kivéve esetleg az utolsót, a \(2r + 1, 4r\) részbe esnek, és a feltétel szerint különbözők az itt levő \(e_i\) -től. Ezután bontsuk fel az \([1, n]\) intervallumot ilyen típusú részintervallumokra.

12.1.3 A konstrukcióhoz vegyük először \(k/2\) számot, és legyen \(t\) ezek összege. Ha most az első két tagot elhagyjuk, és egy olyan új tagot hozzávezsünk, ami éppen az elhagyott tagok összegével egyenlő, akkor az összeg nem változott. Ezután ugyanazt az eljárást ismételjük, ameddig csak lehet. Annak igazolásához, hogy ennél nagyobb előállításszám nem létezik, használjuk fel, hogy \(t\) minden előállításában más az utolsó tag, valamint más a tagszám.

12.1.4 A feltétel szerint bármely \(1 \leq j \leq \nu\) egész legfeljebb egy \(a_i\) -vel lehet osztható, ezért \(\sum_{i=1}^{k} t_i / a_i \leq \nu\), és így \(\sum_{i=1}^{k} 1 / a_i < n + k\). 

12.1.5 \(\frac{1}{a_i a_{i+1}} = \frac{a_{i+1} - a_i}{a_i a_{i+1}} = \frac{1}{a_i} - \frac{1}{a_{i+1}}\). 

12.1.6 

(a) Az alsó becsléshez használjuk fel, hogy a \(3j + 1\) alakú egészek kielégítik a feltételt. A felső becsléshez vegyük észre, hogy ha \(t^2\) a legnagyobb négyzetszám \(n\) -ig és \(u + v = t^2\), akkor \(u\) és \(v\) közül legfeljebb az egyik szerepelhet az \(e_i\)-k között.

(b) Keressünk \(11\) olyan maradékot modulo 32, amelyek közül semmilyen kettőnek az összege nem lehet az \(\nu\)-beli maradékok számával osztható.

12.1.7 Megfelelnek azok a számok, amelyek ötös számrendszerbeli alakjában a (hátulról nézve) páratlanadik helyeken 0 vagy 2 áll (a többi jegy tetszőleges). Ekkor \(k\) értéke kb. \(n^2\), ahol \(c = (1 - \log_2 3)/2 = 0.71\ldots\)

12.1.8 A prímek egy ilyen tulajdonságú halmazt alkotnak, tehát \(s(n) \geq \pi(n)\). Az \(s(n) < \pi(n) + 2n^{2/3}\) becslés igazolásához legyen \(C\) az \(1\) és \(n^{2/3}\) közötti egész számok halmaza, továbbá \(D\) a \(C\)-nek az \(n\) -ig terjedő prímszámokkal való egyesítése. Először lássuk be, hogy minden szám felírható \(u = ax\) alakban, ahol \(a \in C, d \in D\) (a felírás általános nem egyértelmű). Ezután az \(a_i\) számoknak rögzítsük egy ilyen \(a_l = c_i d_l\) alakú előállítását, majd készítsünk el egy \(\lvert C\rvert + \lvert D\rvert \leq \pi(n) + 2n^{2/3}\) csúcspáros gráfot, amelynél a csúcsok egyik csoportja a \(C\) halmaz, a másik pedig a \(D\), és az \(a_l\) számok a \(c_i\) és \(d_i\) csúcsot összekötő \(\ell\) élel felel meg. Ha az élek száma legalább annyi, mint a csúcsok száma, akkor a gráfban van kör. A párosság miatt ennek a körnek a csúcsok közül valóan van, és a konstrukció alapján a minden második élnek megfelelő \(G_i\) -k szorozata megegyezik a kör többi élének megfelelő \(d_j\) -k szorozatával (hiszen mindkét szorzat a kör összes csúcsaihoz szereplő számok szorzata).

12.1.9 \(\pi(n)\). — Útmutatás: A prímek nyilván rendelkeznek ezzel a tulajdonsággal, tehát a maximum legalább \(\pi(n)\). Indirekt tegyük fel, hogy \(\pi(n) + 1\) ilyen tulajdonságú \(a_i\) is megadható lenne. Ekkor minden \(\omega_i\) -hez lenne olyan prim, amelynek a kitevője \(\omega_i\) kanonikus alakjában nagyobb lenne, mint az összes többi \(d_j\) kanonikus alakjában együttvéve. A skatulyaelv szerint lenne olyan prim, amely két \(\alpha_i\) -nél is ezt a szerepet játssza, és ez könnyen láthatóan ellentmondás.

12.1.10 \(2n^{1/3}\). — Útmutatás: A 6-hoz nem relatív prim (azaz a 2 és a 3 közül legalább az egyikkel osztható) \(2n^{1/3}\) darab szám megfelel a feltételnek. Ha viszont több, mint \(2n^{1/3}\) elemet veszünk, akkor a skatulyaelv szerint lesz olyan \(s\), hogy a \(6^s + 1, \ldots, 6^s + 6\) számok között legalább öt darab \(e_i\) fordul elő; lássuk be, hogy ezek között biztosan található három olyan, amelyek páronként relatív prímek. — Megjegyzés: A feladatot három helyett \(t\) -ra a következőképpen általánosíthatjuk: Mennyi
k maximuma, ha bármely τ darab aₙ között található kettő olyan, amelyek nem relativ primek. Ilyen halmozat alakottnak például azok a számok, amelyek az első τ − 1 prim közül legalább az egyikkel oszthatók. (Miért?) Erdős azt sejtette, hogy (minden, az τ-tól függően elég nagy n esetén) ez adja a maximumot. Ezt a sokáig megoldatlan sejtést Ahlswede és Khachatrian igazoltak 1994-ben.

12.1.11 Az aₙ,-k inkojával végigosztva elérhető, hogy az aₙ,-k relatív primek legyenek. Ha van közük k -val osztható, pl. k | aᵢ és k | aⱼ, akkor (12.9) prim volta miatt k | (aᵢ, aⱼ), tehát (aᵢ, aⱼ) > k. Ha egyik aᵢ sem osztható k -val, akkor van közöttük kettő, amelyek kongruensek mod k. Ha aᵢ és aⱼ ilyenek, akkor (aᵢ, aⱼ) = (aᵢ, aⱼ) (mod k), és így a két hányados közül a nagyobbik nagyobb, mint k.

12.1.12 Legyen az u = 2ⁱ esetre a₁, a₂, ..., aₖ egy megfelelő konstrukció. Ekkor 2ⁱ₊₁ ≤ n < 2ⁱ₊₁+1 esetén jó lesz az a₁, a₂, ..., 2ⁱ⁻¹, a₅, a₆, ..., aₖ számhalmaz.

12.1.13 A Csebisev-egyenlőtlenségben az optimális választás ε = √3, ekkor (9)-ben és (10)-ben 8/3 helyett 3√3/2 adódi. További javítási lehetőség, hogy (10)-ből elég nagy u -re a (6)-nál erősebb k ≤ (1 + ε)log₂ n következik, ahol ε > 0 tetszéses kicsi lehet, és így (7) jobb oldalán az 1 ősszeadandó „lényegében” elhagyható. Mindezek alapján a (2) becsülésbe a képlet végén álló 2 helyett a log₂(3√3/2) = 1.377 esetén akár n²/3-nél nagyobb konstans írható (elég nagy u -et feltételezve).

13.12.2.

12.2.1 A mohó algoritmus mellett mindig maga a legelső olyan elemet választjuk, amelyik nem rontja el a Sidon–tulajdonságot. Tegyük fel, hogy a₁ < a₂ < ... < aₖ < n már megyan. Egy d elem akkor rossz, ha valamennyi i, j, k ≤ e-re d − vᵢ = aⱼ + aₖ, azaz d = vᵢ + aⱼ + aₖ. Esetet nem kell külön számításba venni, mert a d -vel csak ilyen probléma lenne, akkor d < aₖ miatt korábban az aₖ-helyett a d -et kellett volna a sorozatba választanunk. Ezzel legfeljebb s² (sőt tulajdonképpen kevesebb mint s²/2) elemet zártunk ki, azaz n < n₁/3 esetén még találunk u₁ -nél kisebb további jó elemet.

12.2.2 A Sidon-tulajdonság igazolásához tegyük fel, hogy vᵢ + aⱼ = vⱼ + aᵢ, azaz

2p(i + j + l) + (vᵢ mod p) + (vⱼ mod p) − (k mod p) − (l mod p) = 0.

Itt a második tag osztható 2p -vel, de abszolút értéke 2p -nél kisebb, tehát csak 0 lehet. Emiatt az első tag is 0. Vagyis i = k = l = j és s² = k² = r² (mod p). Innen egyszerű számolással adódik, hogy vagy i = k és j = l vagy pedig i = l és j = k.

12.2.3 A p² elemű testtel és a benne levő P elemű résztesttel hasonlóan (csak egyszerűbben) kell okoskodni, mint a T 12.2.2 Tétel bizonyításában tettük.

12.2.4 Vegyük egy q primitív gyököt modulo P , és legyen aᵢ az x ≡ i (mod p − 1) , x = gᵢ (mod p) szimultán kongruenciarendszer megoldása modulo p(P − 1) , i = 1, 2, ..., p − 1 .

12.2.5 A T 12.2.1 Tétel szerint vegyük 1 l és n₁ között egy kb. √n₁ elemszámú S₁ Sidon-sorozatot. Legyen n₁ sokkal nagyobb n₁ -nél. Az [n₁, n₁ + n₁] intervallumban ne vegyük elemeket, viszont n₁ + n₁ és n₂ között helyezzünk el egy kb. √n₁ elemszámú Sidon-halmazt, és abból hagyjuk el azokat az elemárokot, amelyeknek a különbsége < n₁, a maradékot jelölje S₂ . (Megfelelne
céljainknak az is, ha minden elempáróból csak az egyik elemet hagynánk el.) A Sidon-tulajdonság miatt az elhagytott elemek száma \(< 2n_1\). Így \(n_1 + 2n_2\)-ig összesen körülbelül \(\sqrt{n_2} + \sqrt{n_1} - 2n_1 \approx \sqrt{n_2}\) elemünk van. Lássuk be, hogy \(S_1 \cup S_2\) Sidon-tulajdonságú. Ezután válasszunk egy, az \(n_1 + 2n_2\)-nél jóval nagyobb \(n_3\)-at, \(n_1 + 2n_2 + n_3\) és \(n_1 + 2n_2 + 2n_3\) között helyezzünk el egy kb. \(\sqrt{n_3}\) elemszámú Sidon-halmazt, abból töröljük azokat az elemeket, amelyeknek a különbsége \(< n_1 + 2n_2\) stb. Az eljárást folytatva a feladat feltételeit teljesítő végételen Sidon-sorozatot kapunk.

12.2.6

(a) Általánosítsuk a 12.2.3 feladat [404] módszerét a \(p^h\) elemű testre.

(b) Az elemekből képezhető \(h\)-tagú összegek egyrészt mind különbözők, másrészt valamennyien 1 és \(\alpha h\) közé esnek.

12.2.7 Nyilván elég belátni, hogy minden pozitív egész egyértelműen előáll \(u_i - u_j\) alakban, ahol \(i > j\). A sorozatnak mindig két-két új elemét definiáljuk úgy, hogy ezek egyrészt olyan nagyok legyenek, hogy a korábbi elemekkel alkotott különbségeik ne egyezhessenek meg semelyik két korábbi elem különbségével, másrészt az ő különbségük legyen az a legkisebb pozitív egész, amely még nem állt elő két korábbi elem különbségéktől.

12.2.8 Álljon \(A\), illetve \(B\) azokból a számokból, amelyek kettes számrendszerbeli alakjában (hátulról nézve) minden páros, illetve minden páratlan helyen 0 számjegy áll.

13.12.3.

12.3.1

(a) Legyen \(A = \{a_1 < a_2 < \cdots < a_k\}\), ekkor \(a_1 + a_1 < a_1 + a_2 < a_2 + a_2 < a_2 + a_3 < \cdots < a_k + a_k\) éppen \(2^k - 1\) különböző összeg. Ha \(|A + A| = 2^k - 1\), akkor minden \(a_i + a_j\), speciálisan \(a_i + a_{i+2}\) is a fenti összegek valamelyike, és nagyságrendi megfontolások miatt csak \(a_{i+1} + a_{i+1}\)-gyel egyezhet meg, vagyis \(a_{i+1} = \frac{(a_i + a_{i+2})}{2}\).

(b) Ha \(A = \{a_1 < a_2 < \cdots < a_k\}\), \(B = \{b_1 < b_2 < \cdots < b_k\}\) és \(k > r\), akkor \(a_1, a_1 + b_1 < a_1 + b_2 < a_2 + b_2 < a_2 + b_3 < \cdots < a_r + b_r < a_{r+1} + b_r < \cdots < a_k + b_r\) a kívánt számú különböző összeg. Egyenlőség esetén minden további \(a_i + b_j\) a fenti összegek valamelyike. Az \(\omega_2 + \hat{b}_1\), \(a_1 + \hat{a}_1\), \(a_4 + \hat{b}_2\) stb. összegeket nagyságrendi megfontolásokkal rendre „beazonosíthatjuk”, és innen egyszerűen adódik, hogy \(A\) első \(r\) és \(D\) azonos differenciájú számtani sorozatot alkot. A kiindulási \(k + r - 1\) tagú összegsorozat alkalmas módosításával ugyanez \(A\) bármely \(r\) szomszédos elemére hasonlóan igazolhatjuk.

(c) Bizonyítsuk \(t\) szerinti teljes indukcióval.

12.3.2 Hagyjuk el \(D\)-ből a 0-n kívül az \(m\)-hez nem relatív prim elemeket, és ezután kövessük a T 12.3.1 Tétel első bizonyítását. A becslés élességének igazolásához legyen például \(m = p^2\),

\(A = \{0, p, 2p, \ldots , (p - 1)p\}\), 
\(B = \{0, p, 2p, \ldots , 1, p + 1, 2p + 1, \ldots , (p - 1)p + 1\}\).

12.3.3

(a) Kövessük a T 12.3.1 Tétel első bizonyítását. A megadott feltételt ott kell felhasználni, amikor \(b \neq 9\) esetén \(A + b = A\) lehetetlenségét mutatjuk meg.
(b) Például az \( A = \{0, 1, \ldots, k - 1\} \) és \( B = \{0, 1, \ldots, r - 1\} \) halmazokra (ahol \( k + r \leq m + 1 \)) egyenlőség teljesül.

(c) Ugyanaz a bizonyítás elmondható az általános esetben is.

12.3.4 A T 12.3.1 Tétel második bizonyításához hasonlóan okoskodhatunk: legyen \( A = B \), \( C = A + A \) és

\[
f_1(x, y) = (x + y)^{k_1} (x - y)^{k_2} \prod_{c \in C} (x + y - c),
\]

ahol \( 2m + |C| = 2k - 4 \).

12.3.5

(a) A T 12.3.1 Tétel második bizonyításában látottakhoz hasonlóan „redukáljuk” azokat az \( x^i y^j \) tagokat, amelyekben \( i \geq k \) vagy \( j \geq r \), majd használjuk a L 12.3.2 Lemmát.

(b) Legyen \( |A_i| = k_i, i = 1, \ldots, n \), továbbá \( F(x_1, \ldots, x_n) \) olyan \( \mathcal{T} \) feletti \( n \) -változós polinom, amelynek a foka \( \sum_{i=1}^{n} k_i - 1 \), és amelyben a \( \prod_{i=1}^{n} x_i^{k_i - 1} \) tag egyúthatója nem nulla. Ekkor van olyan \( a_i \in A_i, i = 1, \ldots, n \), amelyre \( F(a_1, \ldots, a_n) \neq 0 \).

12.3.6 Ha \( C = D = \mathbb{Z}_p \), akkor a \( c \neq d \) párosítás jó, hiszen \( \mathbb{Z}_p \) -ben \( 2u = 2v \) -ből \( p \) páratlanára miatt \( u = v \) következik. Ha \( |C| = |D| = n < p \), akkor alkalmazzuk a 12.3.5b feladatot [414] \( A_1 = \cdots = A_n = D \) és

\[
F(x_1, \ldots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j)(x_i + c_i - x_j - c_j)
\]
szerrepostással.

12.3.7 Legyen \( p \) prim, \( A_1 \subseteq \mathbb{Z}_p \), \( i = 1, \ldots, n \). Ekkor

\[
|A_1 + \cdots + A_n| \geq \min(p, |A_1| + \cdots + |A_n| + 1 - n).
\]

Ezt a T 12.3.1 Tételből \( n \) szerinti teljes indukcióval igazolhatjuk.

12.3.8

(a) Azt kell igazolni, hogy \( 2n - 1 \) egész számából mindig kiválasztható \( n \) olyan, amelyek összege osztható \( n \) -vel. A 3.6.6 feladatban [94] látott módon elég ezt arra az esetre bizonyítani, amikor az \( n \) egy \( P \) prímszám. Feltehető, hogy a számainkra \( 0 \leq a_1 \leq a_2 \leq \cdots \leq a_{2p-1} \leq p - 1 \) teljesül.

Ha van \( P \) darab egyforma \( a_i \), akkor ezek összege osztható \( P \) -vel. Egyébként — átírve \( \mathbb{Z}_p \) -re — legyen \( A_i = \{a_i, a_i + 1, \ldots, a_i + p - 1\} \), \( i = 1, \ldots, n \), ekkor \( |A_i| = 2 \). A 12.3.7 feladat [414] alapján \( |A_1 + \cdots + A_{p-1}| = p \), tehát \( \mathbb{Z}_p \) minden eleme, így \( a_{2p-1} \) is előáll \( a^{(1)} + \cdots + a^{(p-1)} \) alakban, ahol \( a^{(1)} \subseteq A_1 \), azaz \( a^{(1)} + \cdots + a^{(p-1)} + a_{2p-1} \) osztható \( P \) -vel.

(b) A \( P \) és \( Q \) rácsponkok \( F \) felezőpontja akkor és csak akkor rács pont, ha \( P \) és \( Q \) első, illetve második kordinátái is azonos paritásúak. A skatulyaelv alapján 5 rácsponk között biztosan lesz két ilyen tulajdonságú.
(c) Tekintsünk olyan rácspontokat, amelyek koordinátáit modulo $n$ redukálva $\langle 0, 0 \rangle, \langle 0, 1 \rangle, \langle 1, 0 \rangle$, illetve $\langle 1, 1 \rangle$ adódik, és vegyük mindegyik fajtából $n - 1$ darabot. Ekkor ezen $4n - 4$ rácspont közül nem választható ki $n$ olyan, amelyek első és második koordinátáinak az átlaga is egész szám lenne.

(d) (i) Az alsó becsles a (c)-beli konstrukció általánosításával igazolható. A felső becsles következik abból, hogy ennyi rácspont között a skatulyaevel alapján biztosan található $n$ olyan, amelyek bármelyik koordinátáját tekintve, ezek azonos maradékot adnak modulo $n$. — (ii) Ahhoz hasonlóan érdemes eljáíni, mint amikor a 3.6.6 feladatban [94] azt mutattuk meg, hogy ha az ottani állítás két száma érvényes, akkor igaz ezek szorzatára is.

12.3.9 Legyen $|A| = k$, $c$ kvadratikus nemmaradék mod $P$ és tekintsük az $a_i - c a_j$ összegeket, ezek száma $k^2$. Ha $k^2 > P$, akkor az összegek között biztosan van két egyenlő, amit átrendezve $a_i - a_j = c(a_i - a_j)$ adódik. Itt $a_i - a_j$ és $a_i - a_j$ közül (pontosan) az egyik kvadratikus maradék mod $P$.

12.3.10 Általánosítsuk a T 12.3.3 Tétel kimondása előtti megondolásokat.

13.12.4.

12.4.1 Az utolsó három egyenlőség nyilvánvaló, az elsőnél $R(3, 2) \leq 6$ -ot már igazoltuk, így csak azt kell belátni, hogy egy 5 szögpontú teljes gráf élei kiszínezhetők két színnel úgy, hogy ne keletkezzék egyszínű háromszög. Erre megfelel, ha egy ötszög oldalait pirosra, az átlóit pedig kékre festjük.

12.4.2 A T 12.4.1 Tétel bizonyításának I. részében az $R(3, t) \leq t(R(3, t - 1) - 1) + 2 \text{ (*)}$ egyenlőtlenséget igazoltuk. Innen $R(3, 4) \leq 11$ és (a) azonnal adódik teljes indukcióval. Az élesebb (b) becslesnél az indukcióhoz használjuk (*)-ot és az $e$ sorfejtéséből kapott

$$\left| s^{e!} \right| = s^{\left( 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{e!} \right)} + 1$$

alakot.

12.4.3

(a) Következik az előző feladat (b) része alapján $S(t) < R(3, t)$ -ből (lásd a T 12.4.2 Tétel bizonyítását).

(b) Vegyük az $1, 2, \ldots, t = S(t)$ számoknak egy „rossz” színezését $t$ színnel (azaz, amikor az $x = y = z$ egyenletnek nincs egyszinű megoldása), majd használjuk a $t + 1$-edik szint az $\eta + 1, \ldots, 2n + 1$ számok mindegyikénél, végül színezzük ki a $2n, 2, \ldots, 3n + 1$ számokat ugyanúgy, mint az első $\eta$ -et (azaz $2n + 1 + \eta$ színe legyen ugyanaz, mint az $\eta$ színe). Mutassuk meg, hogy ez az $1, 2, \ldots, 3n + 1$ számoknak egy rossz színezése $l + 1$ színnel.

(c) Bizonyítsuk teljes indukcióval (b) alapján.

(d) A (b)-beli konstrukciót általánosítsuk. Legyen $\nu$ az $1, \ldots, n = S(t)$ egy rossz színezése $t$ színnel és $\rho$ az $1, \ldots, r = S(\nu)$ egy rossz színezése $\nu$ másik színnel. Ekkor az alábbi konstrukció az $1 \leq \nu \leq 2nr + n + r$ számok egy rossz színezése lesz $t + \nu$ színnel: írjuk fel $m$-et $\nu = \nu(j) = \nu(2\nu + 1) + j$ alakban, ahol $1 \leq j \leq 2\nu + 1$, és legyen $m$ színe $\nu(j)$, ha $1 \leq j \leq n$, és az $m$ színe $\nu(2\nu + 1)$, ha $n + 1 \leq j \leq 2\nu + 1$. 
illetve $\varrho(d)$, ha $n + 1 \leq j \leq 2n + 1$ (azaz a $2n + 1$ hosszúságú intervallumok első felében mindig ismételjük meg az $1, 2, \ldots, n$ -nél az $\nu$ szerinti színezését, az intervallumok második fele pedig legyen egysínű, ahol a szint az intervallum $1, 2, \ldots, r$ sorszámának a $d$ szerinti színezése adja).

12.4.4 $5n - 1$.

12.4.5 Alkalmazzuk a T 12.4.2 Tétel bizonyításának gondolatmenetét $R(3, t)$ helyett $R(4, t)$ -vel.

12.4.6 Ha $B^t + C^t \equiv D^t \pmod{p}$, ahol $BCD \neq 0 \pmod{p}$, és $CF \equiv 1 \pmod{p}$, akkor $(BF)^t + 1 \equiv (DF)^t \pmod{p}$.

12.4.7

(a) Használjunk váltakozva egyre hosszabb piros, illetve kék intervallumokat.

(b) Az összes számtani sorozatot sorozatba rendezzük, és rendre mindegyikbe beteszünk egy kék elemet, arra vigyázzva, hogy a következő kék szám mindig legalább a duplája legyen az előzőnek. — „Konkrétabb” konstrukció: az $u^1 + \nu$ alakú számok legyenek a kék, ekkor minden $a + m\nu$, $m = 1, 2, \ldots$ számtani sorozatban lesz kék elem, mert pl. $a = a + \nu$ -re $(a + \nu)! + a + \nu \equiv a \pmod{\nu}$, tehát nincs végahlen piros számtani sorozat, és a gyors növekedés miatt 3-tagú kék sincs.

12.4.8 Legyen $n^m = \omega(k, t) + 1$, ekkor a T 12.4.4A Tétel alapján kapunk egy $m$ -nél kisebb $k$ -tagú egysínű számtani sorozatot (a továbbiakban $k$ -ESZ). Tekintsük most az $m, 2m, \ldots, (m - 1)m$ számat, és alkalmazzuk újra a T 12.4.4A tételt (mintha az $m$ „gyújtatot” lennének így színezve), ekkor az $m$ többszöröseiiből kapunk egy újabb $k$ -ESZ-t, amik kisebb $m^2$ -nél, stb. Az így nyert végahlen sok $k$ -ESZ közül végahlen soknak azonos a színe, mert csak véges sok szín lehetséges.

12.4.9 Alkalmazzuk a Van der Waerden-tételt a kettőhatványok kitevőire.

12.4.10 PPKKPPKK mutatja, hogy 8 szám még kevés. Azt, hogy 9 már elég, (minél kevesebb) esetszétválasztással lehet igazolni; érdemes a (szín- és szám)szimmetriákat felhasználni: az 1, 5, 9 közül az 5 piros, az 1 kék és a 9 vagy kék, vagy piros, majd a 3 és a 7 színet nézzük stb.

12.4.11

(a) Az $1, 2, \ldots, r$ számokat $2^n$ -féléképpen színezhetjük ki két színnel. Számoljuk meg egyet azokat a színezéseket, amelyeknél előfordul $k$ -tagú egysínű számtani sorozat $(k$ -ESZ). A $k$ -ESZek száma (pl. a kezdőtag és a differencia szerint összeszámolva) legfeljebb $n^2/2(k - 1)$, egy $k$ -ESZ színe kétféle lehet, a többi szám színezése pedig $2^{n-k}$ -féle. Ennélfogva összesen legfeljebb $n^22^{n-k}/(k - 1)$ színezésnél fordulhat elő $k$ -ESZ (persze így számos rossz színezést többszörösen is megzámoltunk). Ezért, ha $n^22^{n-k}/(k - 1) < 2^n$, azaz $n < k^{2/k-1}$, akkor biztosan van olyan színezés, amelyben nem fordul elő $k$ -ESZ.

(b) Tekintsük a $2^p$ elemű $T$ véges testet, legyen $\Delta$ a multiplikatív csoport generátoreleme és $W$ egy $p - 1$ -dimenziós al térben (mint $\mathbb{Z}_2$ feletti vektortérben). A színezés: $k$ akkor piros, ha $\Delta^k \in W$. Az $1, 2, \ldots, 2^p(p - 1)$ számokat így módon kiszínezve nem fordul elő $p + 1$ -tagú egysínű számtani sorozat.

12.4.12 Írjuk fel a számokat $d$ alapú számrendszerben, ahol $d$ értékét később alkalmasan megválasztjuk. Tekintsük most azokat a számokat $n$ -ig, amelyek felirásában minden számjegy $< d/2$ és a számjegyek négyzet- összege egy adott $q$ érték. Mutassuk meg, hogy egy ilyen számhalmazban
nem fordul elő háromtagú számtani sorozat, továbbá $q$ és $d$ alkalmassal megválasztásával elérhető, hogy a halmaz elemzésére a feladat állításának megfelelően nagy legyen.

13.12.5.

12.5.1 Az $1, 2, \ldots, M = [m_1, \ldots, m_k]$ számok közül az $a_i \mod m_i$ maradékosztály $M/m_i$ elemeit tartalmaz, és mivel minden szám benne van legalább az egyik maradékosztályban, ezért $\sum_{i=1}^{k} M/m_i \geq M$.

12.5.2 Az új maradékosztálynak részhalmaza a régi.

12.5.3 Legyen $m_i$ tetszőleges és $I$ a többi $m_j$ legkisebb közös többszöröse. A feltétel szerint van olyan $c$, amely nincs benne a $I \neq I$ -hez tartozó maradékosztályok egyikében sem. Ekkor $c + L$ is ilyen tulajdonságú. Ez azt jelenti, hogy mindkét számot az $a_i \mod m_i$ maradékosztálynak kell tartalmaznia, azaz $c + L$,$n_i$ $| L$.

12.5.4 Használjuk fel az előző három feladatot.

12.5.5 Válasszuk például modulusnak a 120 osztóit (az 1 és a 2 kivételével).

12.5.6

(a) Járjunk el hasonlóan, mint a 12.5.1 feladatnál [423].
(b) Ez a T 12.5.1 Tétel bármelyik bizonyításából leolvasható.
(c) Legyen $m_i = 2^i$, ha $1 \leq i \leq k - 1$.

12.5.7 Ilyenek például a 3-mal osztható páros számok, a $3^3 \div 3$ alakúak kivételével. Ha az $a = 0$ kitevőt is megengedjük, akkor az $1 + p$ alakúakat is le kell számítani, ahol $p$ (egy $6^k - 1$ alakú) primszám, de még így is végtelen sok nem előálló marad, a primek „ritkasága” miatt. Az általános esetben hasonlóan kell eljárni a 3 helyett az $b$-val, illetve $b/2$-vel. (Ez mutatja, hogy $b = 2$ volt az egyetlen nehéz eset, lásd a T 12.5.2 Tételt.)


12.6.1 A pontos megfogalmazás: Tekintsük a nemnegatív egészek egy tetszőleges felbontását az $I$ és $J$ végében részhalmazok diszjunkt egyesítésére, és írjuk fel az $nt$ számot $c$ alapú számrendszerben: $n = \sum_{i=0}^{t} \gamma_i c^i$ , $0 \leq \gamma_i < c$ . Legyen $A = \{ \gamma_i | \gamma_i = 0$ minden $i \in I \}$ és $B = \{ \gamma_j | \gamma_j = 0$ minden $j \in J \}$ . A komplementumságot az biztosítja, hogy minden szám felírható $c$ alapú számrendszerben. Minden ilyen konstrukciónál $\lim_{n \to \infty} A(n)B(n)/n = 1$ (de könnyen láthatóan $\lim_{n \to \infty} A(n)B(n)/n > 1$).

12.6.2 Nem, ez a T 12.5.2 Tételből következik.

12.6.3 (a) Szükséges és elégséges. — (b) Elégséges, de nem szükséges, lásd pl. a 12.4.7b feladat [419] piros halmazát. — (c) Szükséges, de nem elégséges. — (d) Se nem szükséges, se nem elégséges.

12.6.4 A T 12.6.1 Tétel bizonyításához hasonlóan érdemes eljárnani. Mivel $a_{i,j} \equiv t \mod 2^i3^j$ , ha $i, j \leq t$ , ezért az $a_{i,j}$ számtani sorozat, $\log_2 k + 1 \leq s \leq \leq \log_2 k + d_k$ , teljes maradékdérendszerben alkotnak mod $d_k$, ha $d_k = 2^i3^j$ és $d_k < k - 5\log_2 k$ . Az elemzésbecslésekhez később felhasználnandó $d_k \sim k$ és $d_k \leq d_{k+1}$ további feltételek azért biztosíthatók, mert a nagyság szerint rendezett $2^i3^j$
EREDMÉNYEK ÉS ÚTMUTATÁSOK

alakú számok sorozatában a szomszédos elempárok hányadosa 1-hez tart, ugyanis a $\log_2(2^{2/3})$ értékek törtrésze a T 8.4.1 Tétel szerint mindenütt sűrű $[0, 1]$ -ben.

Ha most $a_k \leq u < a_{k+1}$, akkor $u = a_k + rd_k$, ahol $6^k(1 - 1/k) < rd_k < 6^k + 1$, tehát az ilyen $rd_k$ -kat választva $B$-nek, az $A$ komplementumát kapjuk. Az elemzésben az $A(n) = k$ és $B(n)$ nél azoknak az $rd_k$-nek a számát kell viszonylag pontosan becülni, amelyekre $k \geq j \geq n = \lfloor k - 2\log_6 k \rfloor$, majd ezek kezeléséhez használjuk a $d_0$ „közös nevezőt”, a $j < v$ -hez tartozó tagok száma pedig legfeljebb $6^v$ .

12.6.5 Mivel ekkor $A(n) = \pi(n) \sim n/\log n$, ezért

$$S(n) \sim 10\sum_{i=2}^{n} \frac{\log^2 n}{n} \sim 10 \int_{2}^{\infty} \frac{\log^2 x}{x} \, dx \sim \frac{10(\log n)^3}{3}.$$ 

12.6.6 Használjuk a T 12.6.4 Tételt. Mivel $(\log A(i))/A(i) \to 0$, ezért bármely $\varepsilon > 0$-hoz van olyan $i_0$, hogy $i \geq i_0$-ra $(\log A(i))/A(i) < \varepsilon/20$. Ekkor

$$B(n) \sim 10\sum_{i=2}^{n} \frac{\log A(i)}{A(i)} \sim C \sim 10\sum_{i=i_0}^{n} \frac{\log A(i)}{A(i)} < C + \frac{10\varepsilon}{20} < \varepsilon n.$$
14. fejezet - MEGOLDÁSOK

1. Számelméleti alapfogalmak

- **1.1.18 [4]** Mivel bármely \( n \) -re csak véges sok „játék” lehetséges, és mindegyik játék az egyik játékos győzelmével végződik, ezért valamelyik játékosnak biztosan van nyerő stratégiája.

Megmutatjuk, hogy ez mindig az első játékos. Indirekt tegyük fel, hogy valamilyen \( n \) -re a második játékosnak, Tündének lenne nyerő stratégiája. Ez azt is jelenti, hogy ha Csongor \( d_1 = 1 \)-gyel kezd, akkor Tünde tud olyan \( d_2 = r \)-et mondani, majd tovább úgy játszani, hogy nyerjen. Ekkor viszont Csongor \( d_1 = r \)-rel kezdve nyrne, hiszen pontosan ugyanúgy kell játszania, mint Tündének az előbb (az előző játékhöz képest legfeljebb a még fel nem használt 1-es szám okozhatna eltérést, azonban az 1 most sem választható későbbi lépésben, hiszen már \( d_1 = r \)-nek osztója). Ellentmondásra jutottunk, tehát bármely \( u > 1 \)-re a kezdő játékosnak van nyerő stratégiája. — Végyük észre, hogy a bizonyítás csak a nyerési lehetőség tényleg adja a kezdő részére, a konkrét stratégia megtervezésére semmilyen információt sem nyújt. Bonyolult szerkezetű \( n \)-ek esetén nem ismeretes, hogyan kell Csongornak optimálisan játszania (és ebben az esetek őriási számára tekintettel egy számítógép sem tud rajta segíteni).

- **1.1.22 [4] (f)** Mivel az \( 1 + \sqrt{2} \) egység, továbbá egy egység negatívja és minden (egész kitevőjű) hatványa is egység, ezért a megadott számok valóban egységek. A megfordításhoz indirekt tegyük fel, hogy ezeken kívül is létezik egy \( \varepsilon \) egység. Ezt szükség esetén \( -1 \)-gyel beszorozva egy \( \delta > \varepsilon \) egységet kapunk. Ekkor létezik olyan \( k \) egész, amelyre \( (1 + \sqrt{2})^k < \delta < (1 + \sqrt{2})^{k+1} \).

Az egyenlőtlenséget az \( (1 + \sqrt{2})^{-k} \) egységgel beszorozva egy olyan \( u + \sqrt{2} \) egységhez jutunk, amelyre \( 1 < u + \sqrt{2} < 1 + \sqrt{2} \). Itt \( u \) és \( v \) előjele nyilván nem lehet azonos (és egyikük sem lehet nulla). A továbbiakban felhasználjuk, hogy \( |u^2 - 2v^2| = 1 \). Ha \( u^2 - 2v^2 = -1 \), akkor \( \delta = \sqrt{2} - u = 1/(\sqrt{2} - u) \) miatt \( \theta < 1 \). Ugyanakkor \( \nu > 0 \), \( \mu < \theta \) esetén \( \rho > 1 \), illetve \( \nu < 0, \mu > 0 \) esetén \( \theta < 0 \) adódik, ami ellentmondás. Ugyanúgy jutunk ellentmondásra az \( u^2 - 2v^2 = 1 \) esetben is.

- **1.1.23 [5] (a)** Ha \( e \) egységelem, akkor \( e \) nyilván egység is. Megfordítva, legyen \( e \) egység. Ekkor \( e \big| e \), azaz \( e \) van olyan \( q \), amelyre \( e = q \cdot e \). Megmutatjuk, hogy \( q \) egységelem. Tetszőleges \( c \)-re \( ce = cge \), azaz \( e(c - qe) = 0 \). Egy nulloszámmentesesség miatt \( c = qe \), azaz \( q \) valóban egységelem.

- **1.3.11 [14]** Mivel \( (a, b) \big| |a| \), ezért \( e(a, b) \big| |a| \), ugyanúgy \( e(a, b) \big| |b| \). Ez azt jelenti, hogy \( e(a, b) \) közös osztója \( a \) -nak és \( b \) -nek, ennélfogva \( e(a, b) \) osztója \( a \) és \( b \) kitüntetett közös osztójának, \( (a, b) \) -nek is. Ennek alapján alakítsunk \( q \) egésszet \( e(a, b)q = (e(a, b), q) \). Azt kell még megmutatnunk, hogy \( q \) egység.

Mivel \( e(a, b)q = (c(a, b), q) \big| |ac| \), ezért \( q(a, b) \big| |a| \), ugyanúgy \( q(a, b) \big| |b| \). Ez azt jelenti, hogy \( q(a, b) \) közös osztója \( a \) -nak és \( b \) -nek, ennélfogva osztója a kitüntetett közös osztójuknak is, azaz \( q(a, b) \big| (a, b) \). Innen \( q = 1 \), tehát \( q \) valóban egység.

- **1.3.13 [15]** Mivel \( \nu \big| |n| \), ezért \( u^{(n, k)} - 1 \big| |a| \), ugyanúgy \( u^{(n, k)} - 1 \big| |a| \). Ez azt jelenti, hogy \( u^{(n, k)} - 1 \) közös osztója \( a \) -nak és \( b \) -nek és \( e \) -nek.
Most a kitüntetett tulajdonságot igazoljuk, vagyis azt, hogy $a^n - 1$ és $a^k - 1$ bármely $d$ közös osztója osztja $a^{(n,k)} - 1$-et is. Az $(n,k) = mn + kn$ előállításban $u$ és $v$ nyilván ellentétes előjelűek, ezért feltehető, hogy $(n,k) = nr - ks$, ahol $r$, $s$ pozitív egészek. Ekkor

$$d \mid a^n - 1 \mid a^{ar} - 1 \quad \text{és} \quad d \mid a^k - 1 \mid a^{ks} - 1,$$

innen

$$d \mid (a^{ar} - 1) - (a^{kn} - 1) = a^{ar} - a^{ks} - a^{ks}(a^{ar} - kn - 1) = a^{ks}(a^{(n,k)} - 1).$$

Itt $d$ az utolsó szorzat első tényezőjéhez, $a^{ks}$ -hez relativ prim, hiszen $d \mid a^{ka} - 1$. Ezért $d$ szükségképpen osztja a második tényezőt, $a^{(n,k)} - 1$-et.

• 1.4.5 [17] Arra fogunk támaszkodni, hogy a $k$ páratlansága miatt bármely $c$ esetén $a^k = (t + 1 - t)c^k$ osztható $c + (t + 1 - t) = t + 1$-gyel.

Legyen először $t$ páros. Ekkor az

$$\left(k^k + t^k\right) + \left(2^k + (t - 1)^k\right) + \cdots + \left(\left(t/2\right)^k + (1 + (t/2))^k\right)$$
csoropositásból az előzőek alapján látszik, hogy a szóban forgó összeg osztható $t + 1$-gyel. Ezért csak úgy lehet prim, ha értéke éppen $t + 1$-et ér. Azonban

$$1^k + 2^k + 3^k + \cdots + t^k \geq 1 + 2 + \cdots + t - t(t + 1)/2 \geq t + 1,$$

és egyenlőség csak akkor teljesül, ha $t = 2$ és $k = 1$, és ekkor $1^k + 2^k = 3$ valóban prim.

Ha $t$ páratlan, akkor a helyzet csak annyiban változik, hogy az összegnek van középső tagja, $\left(t + 1/2\right)^k$, tehát az előző gondolatmenet alapján az összeg osztható $(t + 1)/2$-vel. Ugyanakkor az összeg nagyobb, mint $(t + 1)/2$, vagyis sohasem lehet prim.

A feladat egyetlen megoldása tehát $t = 2$, $k = 1$.

Hasonló gondolatmenettel érhetünk célhoz úgy is, hogy $t + 1$ helyett a $t$-vel való oszthatóságot vizsgáljuk.

• 1.5.8 [21] Legyen $P$ felbonthatatlan és tegyük fel, hogy $P \mid ab$. Azt kell igazolnunk, hogy ekkor $P \mid a$ és $P \mid b$ közül legalább az egyik fennáll.

Ha $a = 0$, akkor $P \mid a$. Ha $a$ egység, akkor $P \mid b$.

Ha $a$ és $b$ nullától és egységtől különbözők, akkor bontsuk fel őket felbonthatatlanok szorzatára:

$$a = u_1 \cdots u_k, \quad b = v_1 \cdots v_l.$$

Innen kapjuk, hogy $ab = u_1 \cdots u_k v_1 \cdots v_l$.

A $P \mid ab$ feltételből $ab = ps$ alkalmas $s$ egésszel. Bontsuk fel $s$-et felbonthatatlanok szorzatára: $s = w_1 \cdots w_n$, ekkor $ab = pw_1 \cdots w_n$. 

551
A számelmélet alaptétele szerint az $cb$ -re kapott két felbontás lényegében ugyanaz, tehát a $P$ meg kell hogy egyezzen valamelyik $u$, vagy $v$-tal alkalmaz egységszeresével. Ennek megfelelően $p | c$ vagy $p | b$ teljesül.

- **1.5.10** [22] A 2 és a 3 megfelel, például $2 = 1^3 + 1^3$, illetve $3^2 = 2^5 + 1^3$.

Megfordítva, tegyük fel, hogy $\omega^3 + \gamma^3 = \beta^2$. Az egyenletet $\omega^3 + \gamma^3$-nal leosztva egy hasonló típusú egyenlet keletkezik, ahol (az új) $\omega$ és $\gamma$ már relatív prímek (és az új $\omega$ esetleg kisebb, mint az eredeti volt).

Szorzattá bontás után $(x + y)(x^2 - xy + y^2) = \beta^2$ adódik, ahonnan a számelmélet alaptétele (és a pozitivitás feltetelek) szerint azt kapjuk, hogy

\[ x + y = \beta, \quad x^2 - xy + y^2 = p^2, \quad \beta > 0, \quad \gamma \geq 0, \quad \beta + \gamma = \omega. \quad (1) \]

Az $(x + y)^2 - (x^2 - xy + y^2) = 3xy$ azonosságba (1)-et beirva nyerjük, hogy

\[ \beta^{2\tau} - \gamma^{2\tau} = 3xy. \quad (2) \]

Ha $\gamma = 0$, akkor

\[ 1 = x^2 - xy + y^2 = (x - y)^2 + xy \geq xy \geq 1 \cdot 1 = 1 \]

alapján $x = y = 1$ és $p = 2$.

Ha $\gamma > 0$, akkor (2) szerint $p | 3xy$. Ha itt $p | x$, akkor $p | x + y = \beta^{2\tau}$ miatt $p | y$ is teljesül, ami ellentmond annak, hogy $x$ és $y$ relatív prímek. Ugyanígy $p | y$ is ellentmondásra vezet. Ezért csak $p | 3$, azaz $p = 3$ lehetséges.

- **1.6.3** [27] (a) Indirekt tegyük fel, hogy valamilyen $x, z > 0$ és $k \geq 2$ egészekre $x(x + 1) = z^k$. Mivel $(x, x + 1) = 1$, ezért az 1.6.2a feladat [27] szerint léteznek olyan $u$ és $v$ pozitív egészek, amelyekkel $x = u^k$ és $x + 1 = v^k$. Innen $\omega^k - u^k = 1$. Ez azonban lehetetlen, hiszen

\[ \omega^k - u^k \geq (k + 1)^h - u^k \geq kn^{k-1} > 1. \]

- **(b)** Az előző gondolatmenetet kell egy kicsit módosítani. A három tényező általában nem lesz páronként relatív prim, azonban a középső szám relatív prim a másik kettőhöz, és így $(x - 1)z(x + 1) = z^k$, $(x, x^2 - 1) = 1$ alapján $x = u^k, x^2 - 1 = v^k$. Ekkor $(u^2)^k - v^k = 1$, ami lehetetlen.

- **(c)** Először megmutatjuk, hogy négy egymást követő pozitív egész szorzata nem lehet négyzeteszmán, azaz ($z \geq 2$ -re)

\[ (x - 1)x(x + 1)(x + 2) = z^2 \quad (1) \]

nem teljesülhet. Legyen $x(x + 1) = 2y$, ekkor $(x - 1)(x + 2) = 2y - 2$ és így (1) átírható $y(y - 1) = (z/2)^2$ alakba. Az (a) részben láttuk, hogy két szomszédos pozitív egész szorzata nem lehet négyzeteszmán, és ezért (1) sem állhat fenn.

A továbbiakban legyen $k \geq 3$, és tegyük fel indirekt, hogy négy egymást követő pozitív egész szorzata $k$-adik hatvány. A négy tényező között található olyan, amelyik a másik háromhoz relatív
megoldások: a két középső szám közül a parátlan biztosan megfelel. Ekkor a (b)-ben láttott gondolatmenet szerint mind ez a tényező, mind pedig a másik három tényező szorzata \( k \)-adik hatvány. Ez azt jelenti, hogy

\[
(u^k - 1)(u^k + 1)(u^k + 2) = u^k
\]

vagy

\[
(u^k - 1)(n^k + 1)(n^k - 2) = n^k.
\]

Megmutatjuk azonban, hogy \( k \geq 3 \) -ra (2) és (3) bal oldala két szomszédos egész szám \( k \)-adik hatványa közé esik, vagyis nem lehet \( k \)-adik hatvány.

Vizsgáljuk először (2) bal oldalát, ez \( u^{5k} + 2u^{2k} - n^k - 2 \). Belátjuk, hogy

\[
(u^3)^k < u^{5k} + 2u^{2k} - n^k - 2 < (u^3 + 1)^k.
\]

Itt az első egyenlőtlenség nyilvánvaló, a második pedig az alábbi módon következik (\( k \geq 3 \)):

\[
(u^3)^k + n^k > u^{3k} + 2u^{2k} > u^{5k} + 2u^{2k} - n^k - 2.
\]

Tekintsük most (3) bal oldalát, ez \( u^{5k} - 2u^{2k} - n^k - 2 \). Azt igazoljuk, hogy

\[
(u^3)^k > u^{5k} - 2u^{2k} - n^k + 2 > (n^3 - 1)^k.
\]

Az első egyenlőtlenség most is nyilvánvaló. A második egyenlőtlenség \( k = 3 \) esetén

\[
(u^5 - 1)(u^3 - 3) > 0 \]

-val ekvivalens, ami igaz. Ha \( k \geq 4 \), akkor a második egyenlőtlenséget írjuk át

\[
(u^3)^k - (u^5 - 1)^k > 2u^{2k} + u^k - 2
\]

alakba. Ennek fennállását a következőképpen láthatjuk be:

\[
(u^5 - 1)^k - (u^3 - 3)^k > u^{3(k-1)} + u^{3(k-2)} + \cdots + (u^3 - 1)^{k-1} > 0
\]

\[
> u^{5k-5} + u^{3k-6} + n^4 - 2 > 2u^{2k} + n^k - 2.
\]

1.6.4 [28] Tegyük fel, hogy \( p^2 - 1 = n^2p \). Mivel \( p = 2 \) nem megfelelő, ezért \( P - 1 \) páros, és az egyenlet átírható

\[
(2(p-1)/2 - 1)(2(p-1)/2 + 1) = n^2p
\]

alakba.

A bal oldalon a két tényező relatív prim, ezért a következő két eset lehetséges:

\[
2(p-1)/2 - 1 = n^2, \quad 2(p-1)/2 + 1 = p^2, \quad (i)
\]

illetve

\[
2(p-1)/2 - 1 = pn^2, \quad 2(p-1)/2 + 1 = p, \quad (ii)
\]

Az (i) esetben az első egyenlőség bal oldala \( P > 3 \) -ra 4-gyel osztható 3-at ad maradékul, és így nem lehet négyzetszám. Vagyis csak \( P = 3 \) lehetséges, ami valóban ki is elégti a feladat feltételeit.
A (ii) esetben a második egyenlőség átírható \(2^{\left(\mu-1\right)/2} - \left(\nu - 1\right)/1\) alakba. Ez csak úgy lehet, ha \(\nu - 1\) és \(\nu + 1\) mindkettő kettőhatványok. Mivel a különbségük kettő, ezért csak a 2 és 4, azaz \(\nu = 3\) jöhet szóba. Az innen adódó \(p = 7\) valóban ki is elégti a feladat feltételeit.

A feladat összes megoldása tehát \(p = 3\) és \(p = 7\).

1.6.10 [28] Első megoldás: Ha \(n = 1\), akkor \(A(1) - B(1) = d(1) - 1\), tehát ekkor egyenlőség teljesül. Legyen \(n > 1\), és legyen az \(n\) kanonikus alakja \(n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}\), ahol \(\alpha_i > 0\).

A négyzetmentes osztókat az jellemzi, hogy bennük minden \(p_i\) kitevője 0 vagy 1, tehát \(A(n) = 2^r\).

A négyzetszámosztókban minden \(p_i\) kitevője páros, tehát \(B(n) = \left(1 + \left[\alpha_1/2\right]\right) \cdots \left(1 + \left[\alpha_r/2\right]\right)\).

Az (a) rész állítása azonnal adódik a \(2\left(1 + \left[\alpha_i/2\right]\right) \geq \alpha_i - 1\) egyenlőtlenségből (páros \(\alpha_i\) esetén itt \(\geq\), páratlan \(\alpha_i\) esetén \(=\)), hiszen \(\sum = 1, 2, \ldots, r\) -re a bal oldalakat összeszorozva \(A(n)B(n)\), a jobb oldalakat összeszorozva \(d(n)\) adódik. Így az is látszik, hogy egyenlőség pontosos akkor teljesül, ha minden \(\sum\) -re \(2\left(1 + \left[\alpha_i/2\right]\right) = \alpha_i + 1\), azaz ha minden \(\alpha_i\) páratlan.

 Második megoldás: Egy számot a maximális négyzetszám osztóját leválasztva a számelmélet alaptétele alapján kapjuk, hogy minden pozitív egész egyértelműen írható fel egy négyzetszám és egy négyzetmentes szám szorzataként. Így \(n\) minden osztója is egyértelműen írható fel \(n\) egy négyzetszám osztójának és egy négyzetmentes osztójának a szorzataként, tehát \(d(n) \leq A(n)B(n)\).

Egyenlőség akkor áll fenn, ha az ilyen szorzatként adódó számok valamennyien osztói az \(n\) -nek. Ha \(n\) -ben valamelyik \(p_i\) ömsevének \(p\) osztója, akkor \(p\) a \(2^\alpha\) szorzat már nem lesz osztója \(n\) -nek. Hasonlóan látható, hogy ha viszont \(n\) -ben minden \(p_i\) kitevője páratlan, akkor minden \(p_i\) osztója \(n\) -nak osztója. Vagyis egyenlőség pontosos akkor teljesül, ha \(n\) kanonikus alakjában minden \(p_i\) kitevője páratlan.

1.6.28 [30] A megfelelő rozmárlétszámok éppen a kettőhatványok. Ha a fejet \(-1\) -nak, az írást \(+1\) -nek vesszük, akkor a feladatot a következőképpen fogalmazhatjuk át. Legyen \(x_1, x_2, \ldots, x_n\) mindegyike \(1\) vagy \(-1\), és képezzük az \(x_1 x_2, x_2 x_3, \ldots, x_n x_1\) számtartományokat, majd ugyanaz az eljárást ismételjessük. A feladat azt kérdezi, hogy milyen \(n\) esetén jutunk el garantáltan a csupa \(1\)-ből álló sorozathoz.

Lássuk be először, hogy páratlan \(n > 1\) -re a játék nem feltétlenül ér véget. A számtartományok mindkettő szorzata \(n\) egyértelműen \(n\) számot szorozzák, tehát a második lépéstől kezdve biztosan \(+1\).

Emiatt a \(-1\) -ek száma minden lépésben páros kell legyen. Ha eredetileg nem a csupa \(-1\)-ből és nem a csupa \(+1\) -ből indultunk ki, akkor a játék véget ér előtt minden számnak \(-1\) -nek kell lennie, ami páratlan sok \(-1\) lenne, tehát nem valósulhat meg. (Innen az is látszik, hogy páratlan \(n\) -re a játék csakis akkor ér véget, ha a csupa \(+1\) vagy a csupa \(-1\) sorozat volt a kezdő helyzet.)

Legyen most \(n = r^t\), ahol \(t > 1\) páratlan. Ha a kiinduló helyzet periodikus \(t\) szerint (és nem minden elem azonos), akkor a páratlan esetre látottak biztosítják, hogy a játék nem ér véget.

Végül megmutatjuk, hogy \(n = 2^k\) esetén a játék biztosan véget ér. Néhány lépést felírva megsejthető, majd \(r\) szerinti teljes indukcióval vagy a Pascal-háromszög alapján bizonyítható, hogy az \(r\) -edik lépésben a sorozatunk első tagja

\[
d_1 \left(\frac{\alpha_1}{2}\right) \cdots \left(\frac{\alpha_r}{2}\right)
\]

ahol \(x_1, x_2, \ldots, x_{t-1}\) -re az \(x_1 = x_2 = x_3 = \cdots = x_{2^{t-1} - 1}\) és \(x_2 = x_3 = \cdots\) stb. módon értelmezünk (mindez nemcsak kettőhatványokra, hanem bármely \(n\) -re érvényes). Ezt most \(r = n = 2^k\) -ra
alkalmazva kapjuk, hogy (1)-ben minden kitevő párós, hiszen \(x_1 \cdot \ldots \cdot x_2\), a többi \(x_i\) -nél pedig \(\left(\frac{x_i}{x_i-1}\right)\), ami párós (lásd az 1.6.27 feladat [30] (e2) részét). Így a szorzat négyzetszám, vagyis \(+1\). Hasonlóan kapjuk, hogy az \(n\) -edik lépésben kapott többi szám is \(+1\), tehát a játék (legkésőbb ekkorra biztosan) végét ért.

- **1.6.29 [30] Első megoldás:** Legyen \(1 < k < n\). Ekkor \(n! + k > k\) miatt választhatunk olyan \(P\) prímszámot, hogy \(n! + k\) a \(P\) -nek magasabb hatványával osztható, mint \(k\). Legyen például \(p^t \mid k\), \(p^t + 1 \mid n! + k\) és \(p^t + 1 \mid n!\) (ahol \(\alpha \geq 0\) egész). Állítjuk, hogy \(P\) nem osztja az \(n! + t\) (\(t = 1, 2, \ldots, n, t \neq k\) számoknak.

Ha \(P > n\), akkor ez nyilvánvaló, hiszen ekkor \(n\) darab egymás utáni szám közül \(P\) legfeljebb egynek lehet osztója. Tegyük fel tehát, hogy \(P \leq n\). Ha még \(p \mid n! + t\) is fennállna (ahol \(1 \leq t \leq n\) és \(t \neq k\)), akkor \(p \mid n!\) miatt \(p \mid t\), és így \(kt \mid n!\) miatt \(p^t + 1 \mid n!\) következne, ami ellentmond annak, hogy \(p^t + 1 \mid n! + k\) és \(p^t + 1 \mid k\)

- **Második megoldás:** Először megmutatjuk, hogy mindegyik \(n! + k\) számnak (\(1 \leq k \leq n\)) van \(n/2\) -nél nagyobb prímosztója. Sőt, belátjuk, hogy az \(n! + k - k(n! / k + 1)\) alakban a második tényező egy tetszőleges \(P\) prímosztójára \(P > n/2\). Tegyük fel indirekt, hogy \(P \leq n/2\). Az \(n! / k\) szám az 1-től \(n\) -ig terjedő számok közül a \(k\) kivételével a többi \(n - 1\) -nek a szorza. Mivel \(P \leq n/2\) miatt \(n!\) tényezői között \(P\) és \(2p\) is szerepel, így \(n! / k -\)ban ezek közül legalább az egyik megmarad (\(k = 2p\) esetén a \(P\), \(k = p\) esetén a \(2p\), más \(k\) -ra pedig mindkettő), tehát \(n! / k\) osztó \(P\)-vel. Elnézést \(n! / k + 1\) nem lehet osztó \(P\)-vel, ami ellentmondás.

Most belátjuk, hogy az \(n! + k\) számok egy-egy \(n/2\) -nél nagyobb tetszőleges prímosztója megfelel a feladat feltételeinek. Ehhez elég azt igazolni, hogy egy \(n/2\) -nél nagyobb \(q\) prímszám legfeljebb egy darab \(n! + j\) -nek lehet osztója (\(1 \leq j \leq \tau\)). Ha \(q > n\), akkor ez abból következik, hogy \(n\) szomszédos szám közül legfeljebb egy osztóható \(Q\)-val. Ha \(n/2 < q < n\), akkor \(Q\) szerepel \(n!\)-ban, tehát ha \(Q\) osztója \(n! + j\) -nek, akkor osztója \((n! + j) - n! = j\) -nek is. Mivel \(2q > n \geq j > 0\), ezért ez csak úgy lehetséges, ha \(Q = j\), tehát a \(j\) most is egyértelműen meghatározott.

- **1.6.30 [30] A keresett maximum értéke 9.**

Először megmutatjuk, hogy a 9 elérhető. Legyenek \(P_1, P_2, \ldots, P_{10}\) különböző prímszámok, és jelölje \(P\) ezek szorzatát. Ekkor az alábbi 5000 szám megfelel a feltételeknek:

\[
a_i = P_i / p_i, i = 1, 2, \ldots, 10; b_j = p_j, j = 1, 2, \ldots, 8 \quad \text{és} \quad b_0 = p_9 \cdot p_{10} \cdot \ldots \cdot p_{5001}
\]

Itt a \(b_1, b_2, \ldots, b_8\) számok páronként relatív prímeik. Belátjuk továbbá, hogy bármely tíz számnak a legkisebb közös többszöröse éppen \(P\). Egyrészét \(P\) mindegyik \(a_i\) -vel és \(b_j\) -vel osztható, így \(P\) -nél nagyobb érték nem jöhet szóba, másrészt \(k\) (vagy több) \(a_i\) -nek, illetve az összes \(b_j\) -nek a legkisebb közös többszöröse \(P\), és bármely tíz szám között vagy megtalálható az összes \(b_j\), vagy pedig szerepel legalább két \(a_i\).

Most bebizonyítkujjuk, hogy tíz páronként relatív prim szám már nem fordulhat elő. Tegyük fel indirekt, hogy a \(c_1, c_2, \ldots, c_{10}\) számok közül bármely tíznek a legkisebb közös többszöröse \(C\) és \(c_{10}\) páronként relatív prímeik. Ekkor \(c_1, c_2, \ldots, c_{10}\) legkisebb közös többszöröse \(C = c_1 \cdot c_2 \cdot \ldots \cdot c_{10}\). Tekintsük most \(c_{11}\) -et. A feltétel szerint \(c_2, c_3, \ldots, c_{10}, c_{11}\) legkisebb közös többszöröse is \(C\). Ez azt jelenti, hogy \(c_{11}\) -nek csak olyan prímosztói lehetnek, amelyek \(c_1, \ldots, c_{10}\) valamelyikében már előfordultak, továbbá \(c_{11}\) a \(C\)
primitényezőit pontosan ugyanazon a hatványon kell hogy tartalmazza, mint amelyiken azok a \(c_1\)-ben szerepeltek (hiszen ezekkel a primékekkel — a páronként relatív prímseg miatt — a \(c_2\) és ..., \(c_{10}\) számok egyike sem osztható). Ismételjük meg ugyanazt a gondolatmenetet arra a tíz számra, amikor a \(c_{11}\)-hez a \(c_1, c_2, ..., c_{10}\) számok közül rendre mindig másik kilevél veszünk hozzá, és így képezzük a legkisebb közös többszörözőt. Innen kapjuk, hogy csak \(c_{11} = C\) lehetséges. Ugyanez adódik \(c_{12}\)-re is, ami ellentmondás, hiszen a számainknak különbözőknek kell lenniük.

### 1.6.34 [31] 1. Először belátjuk, hogy az \(S(i)\) értékek között \((i \geq 2\) esetén) csak (pozitív) összetett számok szerepelnek. \(\bar{S}(i) \neq 1\), mert \(S(i) \geq i \geq 2\). Továbbá \(S(i)\) nem lehet prim, mert egy olyan, különböző pozitív egészkeből képezett sorzat, amelynek a legnagyobbn ténylege prim, nem lehet négyzetszám, hiszen a sorzat ennek a primnek csak az első hatványával osztható.

II. Most megmutatjuk, hogy \(i < j\) esetén \(\bar{S}(i) \neq \bar{S}(j)\). Indirekt tegyük fel, hogy \(\bar{S}(i) = \bar{S}(j) = n\). Ekkor vannak olyan \(i = \hat{i} \cdot b_1 \cdot b_2 \cdot ... \cdot b_k\) szorzat és \(j = \hat{j} \cdot c_1 \cdot c_2 \cdot ... \cdot c_k\) szorzat is négyzetszám. Szorozzuk ezeket össze, majd hagyjuk el a kétser előforduló tényezők mindkét példányát (azaz a \(\hat{i} \cdot b_1 \cdot b_2 \cdot ... \cdot b_k \cdot c_1 \cdot c_2 \cdot ... \cdot c_k\) szorzatot leszajtoljuk azon számok sorzatának a négyzetével, amelyek mind a \(b\) és \(c\)-k között szerepelnek).

Az így kapott sorzat tényezői között \(i < j\) miatt biztosan megtalálható az \(i\), ugyanakkor hiányzik az \(j\). Nyilván ez a sorzat is négyzetszám, amelynek a legkisebb tényezője \(i\), legnagyobb tényezője viszont \(n\) -nél kisebb. Ez azonban ellentmond \(\bar{S}(i)\) definíciójának.

III. Végül azt igazoljuk, hogy minden \(n\) összetett szám fellép az \(\bar{S}(i)\) értékek között. Tekintsük ehhez az összes olyan \(v_1 < v_2 < ... < v_k\) számhalmazt, amelyre \(u_k = n\) és az \(u_1 \cdot u_2 \cdot ... \cdot u_k\) szorzat négyzetszám. Ilyen számhalmaz biztosan létezik: ha \(n\) négyzetszám, akkor a \(k = 1\), \(u_1 = n\) választás megfelel egyébként pedig vegyük hozzá \(n\) -hez azokat a priméket, amelyek \(n\) primitényezős felbontásában páratlan hatványon szerepelnek.

Tekintsük most \(u_1\) lehető legnagyobb értékét, legyen ez \(v_1\). Bebizonyítjuk, hogy \(\bar{S}(v_1) = n\).

Indirekt tegyük fel, vannak olyan \(v_1 < v_2 < ... < v_q\) egészak, amelyekre \(v_1 = m\), \(v_1 \cdot v_2 \cdot ... \cdot v_q\) négyzetszám és \(v_q < n\). Ekkor a II. pontban látott gondolatmenethez hasonlóan képezzük az \(u\) szorzatát és \(u\) -k szorzatára, majd ebből elhagyjuk a kétser előforduló tényezők mindkét példányát. Az így kapott szorzat tényezői között megmarad az \(v_1\) , de hiányzik az \(v_q\). Vagyis ez a szorzat egy olyan négyzetszám, amelynek a legnagyobb tényezője \(v_1\) , de a legkisebb tényezője nagyobb \(v_q\) -nél. Ez viszont ellentmond \(\bar{S}(v_1)\) választásának.

### 1.6.35 [31] (a) Nem létezik.

- **Először bizonyítás**: Indirekt tegyük fel, hogy az \(a + kd, k = 0, 1, 2, ...\) számtani sorozat megfelelne. Legyen \(p\) olyan prim, amely nem osztója \(d\) -nek. Ekkor könnyen láthatóan az \(a + kd\) számok \(k = 1, 2, ... p^2\) -re csoportosító maradékat adnak \(p\) -tel oszva. Ez azt jelenti, hogy ezek a számok minden lehetséges maradéket kiadnak \(p^2\) -tel oszva, így speciálisan a \(p\) maradékoit is. Egy teljes hatvány azonban nem lehet \(m/p^2 + p\) alakú, hiszen egy ilyen szám \(p\) -nek pontosan az első hatványával osztható.

- ** Második bizonyítás**: Egy \(d\) differenciájú számtani sorozatnak \(N\) -ig kb. \(N/d\) eleme van, azonban \(N\) -ig csak ennel jóval kevesebb teljes hatvány található: legfeljebb \(N^{1/2} + N^{1/3} + N^{1/4} + ... \leq N^{1/2} \cdot \log \sqrt{N} \cdot N^{1/5} < 2\sqrt{N}\), ha \(N\) nagy. Ez azt jelenti, hogy ha \(N\) -et megfelelően nagyra választjuk, akkor „nincs élég sok” teljes hatvány ahhoz, hogy a számtani sorozat minden tagja az legyen.

556
MEGOLDÁSOK

- **Harmadik bizonyítás:** Felhasználjuk a számtani sorozatok prímszámaira vonatkozó Dirichlet-tételt, amely szerint \( (A, D) = 1 \) esetén az \( A + kD \) számtani sorozat végtelen sok prímszámot tartalmaz (T 5.3.1 Tétel). Ezerint \( a + kd \) -ből \( m = (a, d) \) -t kiemelve \( a + kd = m(A + kD) \) végtelen sokszor lesz \( mp \) alakú, amely elég nagy \( p \) prim esetén nem lehet teljes hatvány.

- **Negyedik bizonyítás:** Ha a számtani sorozat első tagja (amelyről feltehetjük, hogy 1-nél nagyobb) \( a = b' \), ahol \( r > 1 \) a lehetséges hatványnkitevő, akkor némi számolás után adódik, hogy az \( a + (a^r b^{-1})d \) tag nem lehet teljes hatvány.

- **(b)** Létezik. Teljes indukcióval bizonyítunk: Tegyük fel, hogy \( a^h, \ldots, a^n \) egy \( d \) differenciájú számtani sorozat, és legyen ennek \( u + 1 \) -edik tagja \( s = a^h + d \). Ekkor minden tagot \( a^i(k_1 \ldots k_r) \) -nel beszorzva egy teljes hatványokból álló \( u + 1 \) tagú számtani sorozatot nyerünk.

2. Kongruenciák

- **2.2.4 [40] (f)** Akkor és csak akkor létezik modulo \( m \) teljes maradékkrendszer csupaegyként, ha \( m = 3^h \) alakú.

  Tegyük fel először, hogy \( m \)-nek van egy \( \overline{p} \neq 3 \) primosztója, és mégis lennének olyan csupaegyek, amelyek minden lehetséges maradéket kiadnának modulo \( m \). Ekkor nyilván modulo \( \overline{p} \) is létrejönne minden lehetséges maradék, vagyis létezne modulo \( \overline{p} \) is teljes maradékkrendszer csupaegyként.

  Ennek a modulo \( \overline{p} \) teljes maradékkrendszerei az elemeit szorozzuk meg 9-vel, és az eredményhez adjunk hozzá 1-et. Mivel \( \overline{9p} = 1 \), ezért így ismét egy teljes maradékkrendszert kapunk modulo \( \overline{p} \), amelynek az elemei tizennégyválasztások a be sem azonban adhatnak ki minden maradéko \( \overline{p} \) -vel osztva: ha \( \overline{p} = 2 \) vagy 5, akkor csak a nulla maradék jön létre, más \( \overline{p} \) esetén pedig a nulla maradék biztosan nem jön létre.

  Ez az ellentmondás mutatja, hogy ha \( m \) nem háromhatvány, akkor ilyen csupaegyek nem léteznek.

  Legyen most \( m = 3^h \). Belátjuk, hogy ekkor az első \( m \) darab csupaegy mind különböző maradékot ad \( m \)-mel osztva (és így a megfelelő darabszám miatt teljes maradékkrendszert alkot modulo \( m \)).

  Tegyük fel indirekt, hogy valamely \( 1 \leq i < j \leq m \) -re a \( j \) -edik és az \( i \) -edik csupaegy különbsége osztható lenne \( 3^h \) -val. Ekkor \( (3^h, 10) = 1 \) miatt ennek a különbségnek a \( 1)j^h -edresze, ami éppen a \( j - i \) -edik csupaegy, is osztható lenne \( 3^h \) -val. Másrészt viszont \( r \) szerinti teljes indukcióval igazolható, hogy \( 3^r -rel legelőször \( 3^r \) -edik csupaegy osztható (lásd az 1.3.12b feladatot [14]). Ebből \( 3^h = m \leq j - i < m \) következik, ami ellentmondás.

  Így \( m = 3^h \) valóban megfelel a feladat feltételeinek.

- **(g)** Akkor és csak akkor létezik modulo \( m \) teljes maradékkrendszer teljes hatványokból, ha \( m \) négyszám, azaz csupa különböző prímszám szorzata (vagy \( m = 1 \)).

  Ha \( m \) nem négyszám, tehát valamely \( P \) primre \( m \) osztható \( P^2 \) -tel, akkor például a \( P \) maradék nem jöhet létre: ennek a maradékosztálynak minden eleme \( P \) -nek pontosan az első hatványával osztható, és így nem lehet teljes hatvány.

  Az állítás másik felének igazolásához először megmutatjuk, hogy bármely \( P \) primhez és bármely \( c \) -hez van olyan \( s > 0 \), hogy \( c^{s+1} - c \) osztható \( P \) -vel. Ha \( c \) osztható \( P \) -vel, akkor ez tetszőleges \( s \)
-re nyilvánvaló. Minden más esetben is \(c\) hatványai csak véges sokféle maradékat adhatnak \(P\)-vel osztva, ezért van olyan \(r < t\), hogy \(P\) osztója \(c^r - c^t = c^{t-r} - 1\) -nek és így \(\langle z, c \rangle = 1\) miatt \(c^{t-r} - 1\) -nek is.

Legyen most \(m = p_1 \cdots p_r\), \(p_k \neq p_j\). Belátjuk, hogy tetszőleges \(c\) -hez van olyan \(T > 0\), hogy \(c^{T+1} - T\) - azonos maradédat adnak \(m\) -mel osztva, azaz \(c^{T+1} - T\) osztható \(m\) -mel. Tekintsük a \(c\) -hez és a \(p_k\) -hez tartozó előző bekezdésbeli \(S\) kivévek, ezek szorzata megfelel \(T\) -nek.

Végül tekintsünk egy \(c_1 \cdots c_n\) teljes maradékrendszer moduló \(m\), ahol \(c_i > 1\). Az előbbiek szerint minden \(c_i\) -hez létezik olyan \(k_i > 1\), amelyre \(c_i = c_i^{k_i} \pmod{m}\). Ekkor a \(c_i^{k_i}\) teljes hatványok teljes maradékrendszer alkotnak moduló \(m\).

2.2.8 [40] (a) Pontosan akkor tudnak összegyűlni, ha \(m\) páratlan vagy osztható 4-gyel.

Ha \(m\) páratlan, akkor a legnagyobb fán levő módos maradjon ott, a két szomszédja egy lépésben odaugrik, a két másodszomszédja két lépésben odaugrik stb.

Ha \(m\) osztható 4-gyel, akkor a fenti lépések után csak a legnagyobb fával szemközti fán marad egy módos, amely páros sok ugrással eljut a legnagyobb fára, miközben egy másik módos ide-oda ugrál a legnagyobb fára és valamelyik szomszédja között.

Végül, ha \(m\) páros, de 4-gyel nem osztható, akkor a módosok nem tudnak összegyűlni. Tekintsük ugyanis, hány ugrással juthat el egy-egy módos valamely kijelölt fára. Ezeknek az ugrásszámoknak az összege mindenféle páratlan, tehát a feladat feltételei szerint nem valósítható meg.

(b) Pontosan a páratlan \(m\) -ekre lesz módosgyűlés.

Az (a)-beli gondolatmenetek továbbra is érvényesek, ha \(m\) nem osztható 4-gyel.

A 4-gyel osztható (illetve tetszőleges páros) \(m\) -ekre számozzuk meg a fákat sorban 1 -től \(m\) -ig. Minden helyzetben adjuk össze azoknak a fáknak a sorszámait, amely fákon főkös ül, mégpedig minden sorszámtan annyiszor, ahány módos található az adott fán. Ennek az összegnek az \(m\) -mel vett maradékát nem változik az ugrálás során. A kiindulási helyzetben ez a maradék \(1 + 2 + \cdots + m - T(m - 1)/2 = -T \cdot m/2\) maradéka, amit \(m/2\) (itt hivatkozhatunk volna a 2.2.7a feladat [40] eredményére is). Ha minden módos ugyanazon a fán tanyázik, akkor a maradék nyilván 0, tehát ez az állapot nem jöhet létre.

2.2.12 [41] (a) Ha \(\langle a, m \rangle = 1\), akkor az \(ar_i\) számonk redukált maradékrendszer alkothatnak, tehát páronként inkongruens moduló \(m\).

Belátjuk, hogy \(m = 4k + 2\) esetén \(\langle a, m \rangle = 2\) mellet is fennáll a páronkénti inkongruencia. Tegyük fel, hogy \(ar_i = ar_j \pmod{m}\). A T 2.1.3 Tétel egyszerűsítési szabálya szerint ekkor

\[
r_i = r_j \pmod{m/2}.
\]

Továbbá \(\langle r_i, m \rangle = \langle r_j, m \rangle = 1\) miatt \(r_i\) és \(r_j\) páratlanok, tehát

\[
r_i = r_j \pmod{2}.
\]

Mivel \(\langle m/2, 2\rangle = 1\), ezért az (1) és (2) kongruenciakból \(r_i \equiv r_j \pmod{m}\), vagyis \(i = j\) következik.

Most azt mutatjuk meg, hogy a fentiektől eltekintve az \(ar_i\) számonk nem lesznek páronként inkongruens moduló \(m\).
A vizsgálatot két esetre bontjuk: (A) Az \( m \)-nek és az \( a \)-nak létezik egy közös \( p > 2 \) prímosztója; 
(B) \( 2 \mid a \) és \( 4 \mid m \).

Az (A) esetben

\[
a \cdot \left( \frac{m}{p} + 1 \right) \equiv a \cdot 1 \equiv a \cdot \left( \frac{2m}{p} + 1 \right) \pmod{m}.
\]

Ha itt \( \left( \frac{m}{p} \right) + 1, m \right) = 1 \), akkor alkalmas \( i \neq j \) -re

\[
\tau_i \equiv 1 \neq \frac{r_i}{p} + 1 \equiv r_j \pmod{m}, \quad \text{de} \quad a \tau_i \equiv a \tau_j \pmod{m}.
\]

Ha \( \left( \frac{2m}{p} + 1, m \right) = 1 \), akkor is ugyanígy kapjuk, hogy az \( a \tau_i \) számok nem lesznek páronként inkongruensek modulo \( m \).

Így az (A) eset lezárásához elég azt igazolni, hogy \( \frac{m}{p} + 1 \) és \( \frac{2m}{p} + 1 \) közül legalább az egyik relatív prim az \( m \)-hez.

Legyen \( \left( \frac{m}{p} + 1, m \right) = \delta \). Ekkor \( d \mid (m/p + 1) - m = p \), azaz csak \( d = p \) vagy \( d = 1 \) lehetséges. Ugyanígy adódik, hogy \( \left( \frac{2m}{p} + 1, m \right) = p \) vagy \( 1 \).

Mindkét legnagyobb közös osztó azonban nem lehet \( P \), ugyanis

\[
2(m/p + 1) - (2m/p + 1) = 1
\]

miatt \( m/p + 1 \) és \( 2m/p + 1 \) relatív prímek.

Végül, a (B) esetben \( \left( \frac{m}{2} + 1, 2 \right) = 1 \) miatt (3)-ból a fentiekhez hasonlóan kapjuk, hogy az \( a \tau_i \) számok nem lesznek páronként inkongruensek modulo \( m \). Most még egy bizonyítást mutatunk a feladat állításának arra a részére, hogy az \( a \tau_i \) számok csak a megadott esetekben lehetnek páronként inkongruensek modulo \( m \). Ehhez az Euler-féle \( \varphi \)-függvényt fogjuk felhasználni.

Legyen \( P \) az \( m \) tetszőleges prímosztója. Az \( \tau_i \) számok száma \( \varphi(m) \), és ezek (legfeljebb) \( \varphi(m/p) \)-féle maradékosztályba eshetnek modulo \( m/p \). Ha tehát \( \varphi(m) > \varphi(m/p) \), akkor biztosan van olyan \( r_i \) és \( r_j \) ( \( i \neq j \)), amelyek azonos maradékot adnak \( m/p \)-vel osztva, és így ha \( P \mid \varphi \), akkor \( m \mid a \tau r_i - a \tau r_j \). Vagyis, ha az \( a \tau r_i \) számok mind különböző maradékokat adnak \( m \)-mel osztva, akkor az \( a \)-nak az \( m \)-mel csak olyan \( P \) közös prímosztója lehet, amelyre \( \varphi(m) = \varphi(m/p) \).

A \( \varphi \)-függvény képletéből (lásd a T 2.3.1 Tételt) könnyen adódik, hogy

\[
\varphi(m) = p \varphi(m/p), \quad \text{ha} \quad p \mid m, \quad \text{és} \quad \varphi(m) = (p - 1) \varphi(m/p), \quad \text{ha} \quad (p, m/p) = 1.
\]

Így a \( \varphi(m) = \varphi(m/p) \) egyenlőség pontosan akkor teljesül, ha \( p = 2 \) és \( \left( \frac{m}{2} \right) = 1 \). Ez azt jelenti, hogy ha az \( a \tau r_i \) számok páronként inkongruensek, és \( a \) és \( m \) relatív prímek, akkor csak az az eset lehetséges, hogy \( m \) páros és nem osztható 4-gyel, továbbá \( \left( \frac{m}{2} \right) = 2 \).

(b) Mivel az \( r_i + 1 \) elemek száma \( \varphi(m) \), és nyilván páronként inkongruensek modulo \( m \), ezért akkor és csak akkor alkotnak redukált maradékosztályt, ha valamennyien relatív prímek \( m \)-hez.

Legyen az \( m \) összes különböző prímosztója \( \mathfrak{P} = P_1, \ldots, P_s \). Először azt látjuk be, hogy ha \( \mathfrak{P} = P_1, \ldots, P_s \mid b \), akkor \( (r_i + b, m) = 1 \).
Ez valóban igaz, hiszen bármely 

\[ p_j \mid \overline{b}, p_j \mid \overline{a}, \implies p_j \mid \overline{a} + \overline{b} \]

vagyis \( a_i + b - \)nek és \( a_i - \)nek nincs közös prímosztója.

Most megmutatjuk, hogy más \( b \) értékek nem felelnek meg, azaz található hozzájuk olyan \( \overline{a} \), amelyre \( (\overline{a} + \overline{b}, m) \neq 1 \).

Tegyük fel, hogy a \( p_j \) primek közül pontosan a \( p_1, \ldots, p_k \) osztója a \( b - \)nek. Itt a feltétel szerint \( k < s \). Ha a \( b \) egyik \( p_j - \)vel sem osztható, akkor ezt tekinthetjük a \( k = 0 \) esetnek.

Legyen \( v = p_{k+1} \cdots p_k - b \). Ekkor \( (v, m) = 1 \), ugyanis \( v \) nem osztható egyik \( p_j - \)vel sem, hiszen bármelyik \( j - \)re a \( p_{k+1} \cdots p_k - b \) különbségnek pontosan az egyik tagja osztható \( p_j - \)vel.

Ez azt jelenti, hogy van olyan \( \overline{a} \), amelyre \( \overline{a} \equiv v \pmod{m} \). Ugyanakkor \( \overline{a} + \overline{b} \equiv v + b - p_{k+1} \cdots p_k - b \pmod{m} \), tehát \( \overline{a} + \overline{b} \) nem relatív prim az \( m - \)hez.

- 2.2.13 [41] Akkor és csak akkor léteznek ilyen maradékrendszerek, ha \( (k, m) = 1 \).

Elégőségesség: Tegyük fel, hogy \( (k, m) = 1 \), és legyen

\[ a_i = 1 + ki, \quad i = 1, 2, \ldots, m, \quad \text{illetve} \quad b_j = 1 + mj, \quad j = 1, 2, \ldots, k. \]

A T 2.2.4 Tétel alapján ezek valóban teljes maradékrendszerek modulo \( m \), illetve modulo \( k \).

Megmutatjuk, hogy az \( a_i \cdot b_j \) szorzatok teljes maradékrendszert alkotnak modulo \( mk \). Mivel a számuk \( m \cdot k \), tehát csak a páronkénti inkongruenciát kell belátni.

Tegyük fel, hogy

\[ (1 - k\overline{i})(1 - m\overline{j}) \equiv (1 - k\overline{v})(1 - m\overline{s}) \pmod{mk}. \]

A beszorzások elvégzése után mindkét oldalból 1-et kivonva és az \( m \cdot k \)-val osztható tagokat elhagyva a

\[ k\overline{i} - m\overline{j} = k\overline{v} + m\overline{s} \pmod{mk} \]

kongruenciához jutunk.

Tekintsük (1)-et most csak modulo \( m \), ekkor \( k\overline{i} \equiv k\overline{v} \pmod{m} \) adódik. Mivel \( (k, m) = 1 \), ezért ezt \( k \) -val végigosztva \( \overline{i} \equiv \overline{v} \pmod{m} \), azaz \( i = v \) következik. Ugyanígy kapjuk, hogy \( j = s \).

Szükségesség: Tegyük fel, hogy \( (m, k) \neq 1 \). Azt kell igazolnunk, hogy az \( a_1, \ldots, a_m \) modulo \( m \), illetve \( b_1, \ldots, b_k \) modulo \( k \) teljes maradékrendszerekből képzett \( a_i \cdot b_j \) szorzatok nem alkothatnak teljes maradékrendszert modulo \( mk \).

Legyen \( p \) az \( m \) és a \( k \) egy közös prímosztója. Ekkor az \( a_i \), illetve \( b_j \) elemek között \( m \cdot p \), illetve \( k \cdot p \) darab \( p \) -vel osztható található.

Az \( a_i \cdot b_j \) szorzat pontosan akkor osztható \( p \) -vel, ha egy tetszőleges \( a_i \) -t egy \( p \) -vel osztható \( b_j \) -vel szorzunk meg, vagy fordítva, de így kétszer számoltuk azokat a szorzatokat, ahol mindkét tényező osztható volt \( p \) -vel. Ebből következik, hogy az \( a_i \cdot b_j \) szorzatok közül
MEGOLDÁSOK

\[
\tau_n : \frac{k}{p} + \frac{k}{q} - \frac{m}{p} \cdot \frac{k}{p} - \frac{m}{q} = \frac{2nk}{p} - \frac{nk}{p^2} \tag{2}
\]

a \mathcal{P} -vel oszthatók száma. Ugyanakkor egy modulo \(nk\) teljes maradékrendszerben a \(\mathcal{P}\)-vel oszthatók száma \(nk/p\), ami (\(\mathcal{P} > 1\) miatt) nem egyenlő (2)-vel, tehát az \(a_1 \cdot b_1\) szorzatok nem alkothatnak teljes maradékrendszer modulo \(nk\).

- **2.2.14 [41]** (a) **Szükségesség:** Ha \((a, b) = \mathcal{d} > 1\), akkor T-ben csak \(\mathcal{d}\)-vel osztható számok szerepelnek, tehát például a redukált maradékosztályok egyáltalán nincsenek reprezentálva.

**Elégségesség:** \(\mathcal{T}\) elemszáma \(ab\), így csak a páronkénti inkongruenciát kell igazolni. Ha

\[i_1 \cdot b + j_1 \cdot a \equiv i_2 \cdot b + j_2 \cdot a \pmod{ab},\]

akkor ez a kongruencia modulo \(a\) is teljesül: \[i_1 \cdot b \equiv i_2 \cdot b \pmod{a}\]. Itt \((a, b) = 1\) miatt egyszerűsíthetünk \(b\)-vel, ekkor \(i_1 \equiv i_2 \pmod{a}\), vagyis \(i_1 = i_2\) adódik. Hasonlóan kapjuk, hogy \(j_1 = j_2\).

- **(b)** A szükségesség, valamint az elégségességnél a páronkénti inkongruencia igazolása ugyanúgy történik, mint az (a) részben. Az elégségességnél azt kell még belátni, hogy \((a, b) = 1\) esetén \(\mathcal{R}\) minden eleme valamelyik redukált maradékosztályba tartozik, és valamennyi redukált maradékosztálynak valóban szerepel reprezentánsa \(\mathcal{R}\)-ben. Más szóval:

(A) \(\mathcal{R}\) elemei relatív primek \(ab\)-hez; és

(B) ha \((a', ab) = 1\), akkor van R-nek olyan \(\nu\) eleme, amelyre \(a' \equiv \nu \pmod{ab}\).

(A) igazolásához tekintsük \(ab\) egy tetszőleges \(\mathcal{P}\) prímosztóját, és mutassuk meg, hogy \(\mathcal{P}\) nem osztója \(\tau_1 \cdot b + aj\) -nak.

Mivel \(\mathcal{P}\) prim és \((a, b) = 1\), ezért az alábbi két eset lehetséges:

\[\alpha \mid \nu \pmod{\mathcal{P}}, \quad (\beta) \mid \nu \pmod{\mathcal{P}}\]

Az \((\alpha)\) esetben \(\mathcal{P} \mid b\ p \mid \tau_1\), és ezért \(\mathcal{P}\) prim volta miatt \(\mathcal{P} \mid \tau_1\cdot b\), ugyanakkor \(\mathcal{P} \mid s\cdot e\), tehát valóban \(\mathcal{P} \mid \tau_1\cdot b + sj\cdot e\). Hasonlóan intézhető el a \((\beta)\) eset is.

Végül (B) igazolásához legyen \((a', ab) = 1\), és írjuk fel az \(\nu\) számot

\[u = rb + sa\]

alakban. Ez megtehető, hiszen \((a, b) = 1\) miatt az \(u = bx + ay\) diofantikus egyenlet megoldható.

Az (1) előállításban \((r : a) = 1\), hiszen különben \((r, a)\) nemtriviális közös osztója lenne \(u\) -nak és \(ab\) -nek. Ezért van olyan \(i\), amelyre \(r = \tau_1 \pmod{a}\). Hasonlóan kapjuk, hogy van olyan \(\tilde{r}\), amelyre \(s = sj \pmod{b}\).

Megmutatjuk, hogy \(\mathcal{R}\) -nek az így adódó \(\nu = r_1 \cdot b + sj\cdot e\) eleme kongruens \(u\) -val modulo \(ab\). A

\[\nu - u = (r_1 \cdot b + sj\cdot e) - (rb + sa) = (r_1 - r) \cdot b + (s - s) \cdot e\]
előállítás végén szereplő összeg első tagjában \( r - r \) osztható \( a \)-val, a második tagban pedig \( s_j - s \) osztható \( b \)-vel, tehát \( r - r \) valóban osztható \( a/b \)-vel.

- (c) Egyrészt a \((b)\)-beli \( R \) halmaz elemszámá \( \varphi(a)\varphi(b) \), másrészt \((a, b) = 1 \) esetén \( R \) redukált maradéktrendszer modulo \( ab \), tehát elemszámá \( \varphi(a/b) \).

- 2.3.18 [45] Az \( n \leq 3 \) egészek nyilván megfelelők.

Megmutatjuk, hogy \( n > 3 \)-ra \( \varphi(n!) = k! \) nem teljesülhet. Ez \( n = 4 \)-re nyilvánvaló, a továbbiakban legyen \( n \geq 5 \).

Jelöljük \( A(j^i) \)-vel a 2 kitevőjét a \( j! \) kanonikus alakjában.

Mivel a feltétel szerint \( k < n \), ezért

\[ A(k) \leq A(n). \]  

Másrészt \( \varphi(n!) \)-ban biztosan szerepelne a \( 2^{\lambda(n)} - 1 \), \( 3 - 1 \) és \( 5 - 1 \) tényezők, ezért

\[ A(\varphi(n!)) \geq (A(n) - 1) + 1 + 2 > A(n). \]

Az (1) és (2) egyenlőtlenségekből \( A(\varphi(n!)) > A(k) \) adódik, így a \( \varphi(n!) = k! \) egyenlőség valóban nem teljesülhet.

- 2.3.19 [46] Akkor és csak akkor létezik olyan számtani sorozat, amely redukált maradéktrendszer modulo \( m \), ha \( m \) kettőhatvány, prim vagy egy primszám kétszerese.

**Elégségesség:** Ha \( m = 2^k \), akkor \( 1, 3, \ldots, 2^k - 1 \), ha \( m = p \), akkor \( 1, 2, \ldots, p - 1 \), ha pedig \( m = 2p \) (ahol \( p > 2 \)), akkor \( p + 2, p + 4, \ldots, 2p - 1, 2p + 1, \ldots, 3p - 2 \) megfelel.

**Szükségesség:** Indirekt, tegyük fel, hogy \( m \) nem a fenti alakú, és mégis találtuk egy olyan

\[ a, a + d, \ldots, a + (\varphi(m) - 1)d \]  

számtani sorozatot, amely redukált maradéktrendszer modulo \( m \).

Legyen \( n \) az \( m \) egy páratlan prímösszöja.

Ha \( p \parallel \varphi(d) \), akkor az (1) számtani sorozat, vagyis a redukált maradéktrendszer minden eleme \( a \)-val kongruens modulo \( p \). Ez azonban az \( \{1\}_m \) és a \( \{-1\}_m \) redukált maradékosztályokat reprezentáló elemeire egyszerre nem teljesülhet, ugyanis \( 1 \neq -1 \pmod{m/d} \).

Ha \( \varphi(d) = 1 \), akkor az \( a, a + d, \ldots, a + (\varphi(m) - 1)d \) elemek teljes maradéktrendszerzert alkotnak modulo \( p \). Így ezek között lesz \( p \)-vel osztható is, ami nem relatív prim az \( m \)-hez. Ez azt jelenti, hogy ez az elem nem szerepelhet (1)-ben. Ez csak úgy lehetséges, ha \( p - 1 \geq \varphi(m) \), azaz

\[ p \geq \varphi(m). \]

Írjuk fel \( m \)-et \( m = bp \) alakban, ahol a feltételek szerint \( i \geq 2 \). Ekkor \( \varphi(i) \geq 2 \) és a 2.3.10a feladat [45] felhasználásával kapjuk, hogy

\[ \varphi(m!) = \varphi(bp) \geq \varphi(i)\varphi(p) \geq 2(p - 1) > p. \]
ami ellentmond (2)-nek.

- **2.5.7 [54]**

**Első megoldás:** Ha \( (a,n) = d \), akkor a \( b = d, 2d, \ldots, (m/d) \) darab értékre \( f(b) = d \), a többi \( 1 \leq b \leq m \)-re pedig nincs megoldás, tehát \( f(b) = 0 \). Ezért a keresett összeg \( \sum_{b=1}^{m} f(b) = (\tau/n)d = m \).

- **Második megoldás:** Az \( \omega = 1, 2, \ldots, m \) számok mindegyike pontosan egy darab \( b \) esetén lesz az \( ax = b \) (mod \( m \)) kongruencia megoldása, ennélfogva \( \sum_{b=1}^{m} f(b) = m \). Ez a meggondolás nemcsak lineáris kongruenciákról, hanem tetszőleges magasabb fokú \( h \) polinomot véve a \( h(x) = b \) (mod \( m \)) kongruenciánál is ugyanily érvényes.

- **2.6.9 [61]** Az útmutatásnak megfelelően az \( x \equiv 39^{38^{17}} \) (mod \( 14401 \)) kongruenciáról van szó, és \( 14401 = 2^3 \cdot 3^3 \cdot 5 \) alapján ebben a \( 2^3 \), \( 3^3 \) és \( 5 \) modulusokra adódó kongruenciarendszert vizsgáljuk.

**Mivel** \( 39 \equiv -1 \) (mod \( 5 \)) és \( 38^{17} \) páros, így \( x \equiv 1 \) (mod \( 5 \)).

Mivel \( 3 \equiv 0 \) (mod \( 9 \)), ezért \( x \equiv 0 \) (mod \( 9 \)).

Végül, \( 39 = 7 \) (mod \( 32 \)) és \( 7^4 = 49^2 = 17^2 = 1 \) (mod \( 32 \)), továbbá \( 4 \equiv 38^{17} \), ennélfogva \( x \equiv 1 \) (mod \( 32 \)).

Ennek megfelelően az

\[ x \equiv 1 \text{ (mod } 5), \quad x \equiv 0 \text{ (mod } 9), \quad x \equiv 1 \text{ (mod } 32) \]

szimultán kongruenciarendszerre megoldani.

Az első és utolsó kongruenciából \( x \equiv 1 \) (mod \( 5 \cdot 32 = 160 \)), azaz \( x = 160z + 1 \). Ezt a középső kongruenciába visszahelyettesítve \( 160z + 1 = 0 \) (mod \( 9 \)), ahonnan \( z \equiv 5 \) (mod \( 9 \)), vagyis \( z = 9t + 5 \). Innen

\[ x = 160(9t + 5) + 1 = 1440t + 801, \quad \text{tehát} \quad x \equiv 801 \text{ (mod } 1440). \]

A keresett pontos idő tehát 13 óra 21 perc.

- **2.8.5 [68] (c)** Az útmutatásban jelzett négy állítást bizonyítjuk.

(i) A műveletek „jósága”, az azonosságok teljesülése, a nullelem és az ellentett létezése az (a) pontban láttottak mintájára igazolvántható.

(ii) Legyen \( m = t^k \), ahol a feltételek szerint \( t > 1 \) és \( (t, k) = 1 \). A szóban forgó maradékosztályok \( (r^k)_m \), ahol \( 0 \leq r \leq t - 1 \). (Ha más \( r \)-eket veszünk, akkor is ugyanezeket a maradékosztályokat kapjuk, csak más reprezentánsokkal.)

Az \( (sk)_m \) maradékosztály pontosan akkor lesz egységelem, ha

\[ (sk)_m (rk)_m = (rk)_m, \quad \text{azaz} \quad srk^2 \equiv rk \text{ (mod } tk), \quad r = 0, 1, \ldots, t - 1. \quad (1) \]

Ha az (1)-beli kongruencia \( \tau = t \)-re teljesül, vagyis

\[ sk^2 \equiv k \text{ (mod } tk), \quad (2) \]

563
akkor (2)-t $r$ -rel beszorozva kapjuk, hogy (1) minden $r$ -re fennáll. Ez azt jelenti, hogy (2) is ekvivalens azzal, hogy az $(sk)_m$ maradékosztály egységelem.

A (2) kongruenciát $k$ -val elosztva a vele ekvivalens $sk \equiv 1 \pmod{t}$ kongruenciát kapjuk. Az egységelem létezéséhez tehát azt kell belátnunk, hogy az $xk \equiv 1 \pmod{t}$ lineáris kongruencia megoldható. Ez pedig $(t, k) = 1$ miatt valóban igaz.

(iii) A feltétel szerint $(t, k) = 1$ és $t$ prim. (i) és (ii) alapján már csak azt kell igazolni, hogy minden $1 \leq r \leq t - 1$ esetén az $(rk)_m$ maradékosztálynak létezik inverze. Legyen $(sk)_m$ az egységelem, és keressük $(rk)_m$ inverzét $(uk)_m$ alakban:

$$(rk)_m(uk)_m = (sk)_m, \quad \text{azaz} \quad ruk^2 \equiv sk \pmod{tk}, \quad (3)$$

A (3)-beli kongruenciát $k$ -val elosztva a vele ekvivalens $ukr \equiv s \pmod{t}$ kongruenciához jutunk. Így azt kell belátnunk, hogy az $xkr \equiv s \pmod{t}$ lineáris kongruencia megoldható. Mivel $(t, k) = 1$ és $t$ prim volta miatt $(t, r) = 1$, ezért $(tkr) = 1$ is teljesül, tehát a kongruencia valóban megoldható.

Megjegyzés: A fenti gondolatmenet finomításával az is belátható, hogy ha $(t, k) = 1$, de $t$ összetett, akkor nem kapunk testet. Sőt, ennél általánosabban az is igaz, hogy hárny tűgyű „teljesen ugyanolyan”, mint a modulo $t$ maradékosztályok gyűrűje (pontos megfogalmazásban ez azt jelenti, hogy a két gyűrű izomorf, azaz létezik közöttük egy kölcsönösen egyértelmű, művelettartó leképezés).

(iv) Használjuk a korábbi jelöléseket. Az $(rk)_m \neq [0]_m$ maradékosztály pontosan akkor nullosztó, ha van olyan $(vk)_m \neq [0]_m$, amelyre

$$(rk)_m(vk)_m = [0]_m, \quad \text{azaz} \quad ruk^2 \equiv 0 \pmod{tk}. \quad (4)$$

A (4)-beli kongruenciát $k$ -val elosztva a vele ekvivalens $ukr \equiv 0 \pmod{t}$ kongruenciát kapjuk. Így azt kell belátnunk, hogy az $zkr \equiv 0 \pmod{t}$ lineáris kongruenciának van $u \neq 0 \pmod{t}$ megoldása is. Mivel a megoldásszám $(t, kr) > 1$, ez valóban teljesül.

3. Magasabb fokú kongruenciák

- **3.2.6 [75]** Tegyük fel, hogy $o_p(a) = o_p(-a) = k$. Ekkor

$$1 \equiv a^k \equiv (-a)^k \equiv (-1)^k a^k \equiv (-1)^k \pmod{p}, \quad (1)$$

tehát $k$ páros, $k = 2l$. Innen adódik, hogy $p \mid a^{2l} - 1 = (a^l - 1)(a^l + 1)$, amiből $p$ prim tulajdonsága és $l < o_p(a)$ miatt $p \mid a^l + 1$, azaz $a^l \equiv -1 \pmod{p}$ következik. Ugyanígy kapjuk, hogy $(-a)^l \equiv -1 \pmod{p}$. Innen az (1)-hez hasonló gondolatmenettel azt nyerjük, hogy $t$ is páros, azaz valóban $4 \mid o_p(a)$.

A megfordításhoz legyen $o_p(a) = 4s$. Ekkor $(-a)^{4s} = a^{4s} \equiv 1 \pmod{p}$ miatt $r = o_p(-a) \mid 4s$. Tegyük fel indirekt, hogy $r < 4s$. Ha $r$ páros, akkor $1 \equiv (-a)^r = a^r \pmod{p}$ ellentmond
$o_2(a) = 4s$-nek. Ha $r$ páratlan, akkor $r \mid s$ és $1 \equiv (-a)^{2r} \equiv a^{2r} \pmod{p}$ miatt ugyanígy ellentmondásra jutunk.

Megjegyezzük, hogy a megfordítás összetett modulus esetén is igaz (a bizonyításban sem használtuk ki, hogy a modulus prím), a másik irány azonban nem igaz, például $o_{21}(\bar{s}) = o_{21}(\bar{s}) = 2$.

- **3.2.9 [76]** A feltételből $(u, p) = 1$, tehát $o_p(u)$ létezik. A kis Fermat-tétel szerint $1 \equiv a^{2p-2} = a^{2p-10} a^8 \equiv -a^8 \pmod{p}$, tehát $a^8 \equiv -1 \pmod{p}$. Ezt négyzetre emelve kapjuk, hogy $a^{16} = 1 \pmod{p}$. A T 3.2.2 Tétel (i) állítását (és a $p > 2$ miatt fennálló $1 \neq -1 \pmod{p}$ inkongruenciát) felhasználva azt nyerjük, hogy $o_p(u) \mid 16$, de $o_p(u) \neq 8$, tehát $o_p(u) = 16$.

- **3.3.10 [83]** Ha $a = b^r \pmod{p}$ és $b = a^s \pmod{p}$, akkor a 3.2.4a feladat [75] alapján $o_p(u)$ és $o_p(b)$ közösösen osztják egymást, tehát egyenlök.

A megfordításhoz vegyünk egy $\varphi$ primitív gyököt, legyen $a \equiv g^\varphi \pmod{p}$, illetve $b \equiv g^s \pmod{p}$. A 3.2.4c feladat [75] alapján ekkor $o_p(u) = (p-1)/(p-1, u)$, illetve $o_p(b) = (p-1)/(p-1, v)$. A rendek egyenlősége miatt innen $(p-1, u) = (p-1, v)$ következik.

Az $a$ és $b$ szerepe szimmetrikus, így elég olyan $r$ létezését igazolnunk, amelyre $a \equiv b^r \pmod{p}$.

Ez a kongruencia átíróható $g^k \equiv g^s \pmod{p}$ alakba, amely az $a \equiv g^s \pmod{p}$ lineáris kongruenciával ekvivalens (ahol $r$ az ismertetlen). Ez a lineáris kongruencia a $(p-1, v) = (p-1, u)$ feltétel teljesülése miatt valóban megoldható.

Az $r$ létezését az alábbi módon is beláthatjuk: Legyen $\omega_1(b) = k$. Ekkor egyreszt a 3.3.9 feladat [83] (vagy a T 3.3 Tétel második bizonyítása) szerint az összes $k$-adrendű elem száma $\varphi(k)$, másrészt a 3.2.4b feladat [75] alapján a $k, b^k, \ldots, b^k$ elemek között is $\varphi(k)$ darab $k$-adrendű elem található, tehát ezek adják az összes $k$-adrendű elemet.

Megjegyzés: Hasonlóan igazolható a következő általánosabb eredmény is: $o_p(u) \mid o_p(b)$ akkor és csak akkor teljesül, ha van olyan $r$ pozitív egész, amelyre $a \equiv b^r \pmod{p}$.

- **3.4.9 [86]** Először tegyük fel, hogy $\text{ind}_4 u = \text{ind}_4 b$. A 3.2.4c feladat [75] alapján ekkor

$$o_p(a) = \frac{p-1}{\text{ind}_4 a, p-1} = \frac{p-1}{\text{ind}_4 b, p-1} = o_p(b).$$

Most tegyük fel megfordítva, hogy $o_p(a) = o_p(b)$, és legyen $\theta$ egy tetszőleges primitív gyök mod $p$, $\text{ind}_4 a = r$, $\text{ind}_4 b = s$. Ismét a 3.2.4c feladat [75] alapján kapjuk, hogy ekkor $(r, p-1) = (s, p-1)$.

Az $\text{ind}_4 b = r$ feltételt teljesítő $h$ primitív gyököt $h = g^\varphi \pmod{p}$ alakban keressük, ahol $(k, p-1) = 1$ a T 3.3.4 Tétel (i) állítása szerint. Ekkor a feltétel átírható a

$$g^s = h^r = (g^\varphi)^r = g^{kr} \pmod{p}$$

alakba, ami

$$s \equiv kr \pmod{p-1}$$

(1)
MEGOLDÁSOK

fennállásával ekvivalens. Az (1) összefüggés a \( k \) -ra nézve egy lineáris kongruencia, amely \( (2) \) számokat \( d \)-vel. Ekkor (1)-et \( d \) -vel egyszerűsítsünk a vele ekvivalens

\[
\frac{s}{d} = k \cdot \frac{r}{d} \left( \text{v. o. d. } \frac{p-1}{d} \right)
\]

kongruenciához jutunk. A (2) bal oldala relatív prim a modulushoz, hiszen \( \left( \frac{s}{d}, \frac{(p-1)}{d} \right) = 1 \).

Ezért a jobb oldal is relatív prim a modulushoz, tehát \( \left( \frac{k}{d}, \frac{(p-1)}{d} \right) = 1 \) is teljesül.

Ha \( p-1 \) minden prímosztója szerepel már \( \frac{(p-1)}{d} \)-ben is, akkor innen \( \left( \frac{k}{d}, \frac{(p-1)}{d} \right) = 1 \) következik, tehát készen vagyunk. Ellenkező esetben legyen \( Q \) a \( p-1 \) azon prímosztóinak szorzata, amelyek relatív primek \( \frac{(p-1)}{d} \)-hez és \( k \) a (2) kongruencia egy tetszőleges megoldása. Ekkor az

\[
\omega \equiv k \cdot \left( \text{v. o. d. } \frac{p-1}{d} \right), \quad x \equiv 1 \text{ (v. o. d. } Q) \]

szimultán kongruenciarendszer megoldásaként kapott \( k \): minden feltételnek eleget tesz: továbbra is kielégíti az (1) kongruenciát és emellett relatív prim \( p-1 \)-hez.

\[ \text{3.5.12 [90]} \]

Első bizonyítás: Ha az \( a \) szám 100-adik hatványmaradék, azaz \( \frac{a^{100}}{p} \) és van olyan \( u \), amelyre \( a \equiv \omega^{100} \text{ (v. o. d. } p) \), akkor \( a \equiv \left( \frac{u^{20}}{20} + \frac{\omega^{20}}{20} \right) \text{ (v. o. d. } p) \), tehát \( a \) egyben 20-adik és 50-edik hatványmaradék is.

A megfordításhoz tegyük fel, hogy az \( a \) szám 20-adik és 50-edik hatványmaradék is, vagyis \( \frac{a^{20}}{20} \) és van olyan \( u \) és \( v \), amelyre \( u^{20} = v^{20} = a \text{ (v. o. d. } p) \). Ekkor \( a^{100} = a^{2} \left( \text{v. o. d. } p \right) \) és \( a^{100} = a^{2} \left( \text{v. o. d. } p \right) \). Ezeket az \( a \cdot (a^{2})^{2} - a^{5} \) egyenlőségebé beírva \( a^{100} = \omega^{100} \text{ (v. o. d. } p) \) adódik. Mindkét oldalt \( \left( \frac{x^{2} - 3}{100} \right)^{100} -zal szorzozva a kis Fermat-tétel miatt kapjuk, hogy \( a \equiv \left( \frac{x^{100} - 3a^{100}}{100} \right) \text{ (v. o. d. } p) \), tehát az \( a \) valóban 100-adik hatványmaradék az.

Második bizonyítás: A T 3.5.3 Tétel „indexes” kritériuma szerint az alábbi ekvivalenciát kell igazolni:

\[
(100, p-1) \mid \text{ind } a \iff \begin{cases} (20, p-1) \mid \text{ind } a \\ (50, p-1) \mid \text{ind } a \end{cases}
\]

Itt \( (20, p-1) \mid (100, p-1) \), illetve \( (50, p-1) \mid (100, p-1) \) miatt az egyik irány nyilvánvaló.

A megfordításhoz azt kell megmutatnunk, hogy ha \( (20, p-1) \mid \text{ind } a \) és \( (50, p-1) \mid \text{ind } a \), akkor \( (100, p-1) \mid \text{ind } a \) is teljesül. Ha \( 25 \mid p-1 \), illetve \( 4 \mid p-1 \), akkor \( (100, p-1) \equiv (20, p-1) \), illetve \( (100, p-1) \equiv (50, p-1) \), tehát készen vagyunk. Ha \( 25 \mid p-1 \) és \( 4 \mid p-1 \), akkor \( (50, p-1) \equiv 50 \mid \text{ind } a \) és \( (20, p-1) \equiv 20 \mid \text{ind } a \), tehát \( (50, 20) \equiv 100 \equiv (100, p-1) \mid \text{ind } a \).

Hasonló módon nyerhetünk egy harmadik bizonyítást a T 3.5.3 Tétel „hatványos” kritériuma alapján, ezt nem részletezzük.

Az útmutatásoknál már megfogalmaztuk a feladat általánosítását: \( a \) akkor és csak akkor lesz egyszerre \( k \) -adik és \( n \) -edik hatványmaradék, ha \( \left[ \frac{k}{n} \right] \) -edik hatványmaradék.
Mindhárom bizonyítás átvihető az általános esetre is. Ekkor a „nehezebb iránynál” az első bizonyításban az \[ a \cdot (a^2)^2 = a^5 \] alapjál szolgáló \( 1 - 1 \cdot 5 - 2 \cdot 2 \) egyenlőség helyére az előállítás lép, a második (és harmadik) bizonyításnál pedig a \( |(k, p - 1) \cdot (n, p - 1) = (k, n)| \) összefüggést lehet felhasználni (lásd az 1.6.19b feladatot).

- **3.7.3 [98] (b)** Bebizonyítjuk, hogy páratlan \( a \) és \( k \geq 3 \) esetén az

\[
x^2 \equiv a \pmod{2^k}
\]

kongruencia akkor és csak akkor oldható meg, ha

\[ a \equiv 1 \pmod{8}, \]

és megoldhatóság esetén a megoldásszám 4.

Mivel páratlan \( c \) -re \( c^2 \equiv 1 \pmod{8} \), ezért (2) az (1) kongruencia megoldhatóságának szükséges feltétele.

Most azt igazoljuk, hogy megoldhatóság esetén a megoldásszám 4. Tegyük fel, hogy egy rögzített (páratlan) \( a \) -ra \( x \equiv c \pmod{2^k} \) megoldása (1)-nek. Ebben az esetben a \( d \) akkor és csak akkor megoldás, ha

\[ 2^k \mid d^2 - c^2 = (d - c)(d + c). \]

Mivel \( c \) és \( d \) páratlan, ezért mindkét tényező páros szám. Megmutatjuk azonban, hogy \( c + d \) és \( c - d \) nem lehet egyszerre 4-gyel osztható. Ellenkező esetben ugyanis

\[ 4 \mid (d - c) + (d + c) = 2d \]

elsőnél, ami ellentmond \( d \) páratlanságának.

Ebből az következik, hogy (3) pontosan akkor érvényes, ha a \( d - c \) és \( d + c \) közül (pontosan) az egyik osztható \( 2^{k-1} \)-gyel. Innen \( d \equiv \pm c \pmod{2^{k-1}} \), azaz (1) re valóban négy (páronként inkongruens) megoldást kapunk mod \( 2^k \):

\[ x \equiv c, \quad x \equiv c + 2^{k-1}, \quad x \equiv -c, \quad x \equiv -c + 2^{k-1}. \]

Végül belátjuk, hogy (1) megoldhatóságához a (2) feltétel nemcsak szükséges, hanem egyben eléges is.

Nyilván elég a mod \( 2^k \) páronként inkongruens \( 1 \leq a < 2^k \) értékekre szorítkozni. Ekkor egy mod \( 2^k \) reduált maradékrendszer minden eleme pontosan egy ilyen \( a \) esetén lesz az (1) kongruenciának megoldása. Ez azt jelenti, hogy a kongruencia \( \varphi(2^k)/4 = 2^{k-1} \) darab \( a \) -ra lesz megoldható. Mivel a (2) feltételt éppen ennyi \( a \) teljesíti, ezért az (1) kongruenciának ezek mindegyikére megoldhatónak kell lennie.

### 4. Legendre- és Jacobi-szimbólum

- **4.1.13 [103] (a)** (Valamennyi kongruencia a 13 modulusra vonatkozik.) Először elérjük, hogy a másodfokú tag együtthatója 1 legyen. Ehhez a kongruenciát megszorozzuk \(-4\) -gyel (mivel \( (4, 13) = 1 \), ezért ez ekvivalens lépés): \(-12x^2 - 20x - 20 \equiv 0 \), azaz \( x^2 + 6x + 6 \equiv 0 \). Most alakítsunk teljes négyzetét:

\[ (x + 3)^2 \equiv 3 \equiv 16 \iff x + 3 \equiv \pm 1 \iff x \equiv 1 \text{ és } 6. \]
A $-4$-gyel való szorzás helyett oszthatunk is 3-mal, ha előtte a többi tag együthatóját 3-mal oszthatókra cseréljük: $3x^2 + 5x + 5 \equiv 3x^2 + 18x + 18 \equiv 0$, és így $x^2 + 6x + 6 \equiv 0$.

Egy újabb lehetőség, hogy az eredeti kongruenciát beszorozzuk 4 · 3 -mal, és ezután alakítunk teljes négyzetté:

$$36x^2 + 60x - 60 = (6x + 5)^2 + 35 \equiv 0 \iff (6x + 5)^2 \equiv 1 \iff 6x + 5 \equiv \pm 2.$$  

Ezután a $6x \equiv -3$ és $6x \equiv -7$ lineáris kongruenciákat kell megoldani.

- **4.2.8 [109]** Az útmutatásban szereplő $f = (x^2 + 1)(x^2 - 17)(x^2 + 17)$ polinommak nyilván nincs racionális gyöke.

Az $f(x) \equiv 0 \pmod m$ kongruencia megoldhatóságához a kínai maradéktétel szerint eléggé igazolni, hogy az $f(x) \equiv 0 \pmod p^k$ kongruencia megoldható minden $p^k$ primhatványra.

Az $x^2 \equiv 17 \pmod {2^k}$ kongruencia megoldható, mert $17 \equiv 1 \pmod 8$, lást a 3.7.3b feladat [98] megoldását.

Ha $p > 2$ és $p \neq 17$, akkor

$$\left( \frac{-1}{p} \right) \left( \frac{17}{p} \right) = \left( \frac{-17}{p} \right) \left( \frac{17}{p} \right) = 1$$

miatt az $f$-et alkotó három tényező közül legalább az egyiknek létezik megoldása mod $p$. Innen $p$ páratlanasága miatt a 3.7.2 feladat [98] (vagy a T 3.7.1 Tétel) alapján adódik, hogy mod $2^k$ is létezik megoldás.

Végül $p = 17$ esetén az $x^2 \equiv -1 \pmod {17}$ kongruencia megoldható, mert $17 = 1 \pmod 4$, és így mod $17^k$ is van megoldás.

- **4.3.7 [112] (b)** Megmutatjuk, hogy éppen a négyzetszámok a keresett $a$ értékek.

A négyzetszámok valóban megfelelők, ugyanis ha $a = s^2$, akkor

$$\left( \frac{a}{m} \right) \left( \frac{s^2}{m} \right) = \left( \frac{s}{m} \right)^2 = 1.$$  

A megfordításhoz tegyük fel, hogy $a$ nem négyzetszám. Legyen először $a > 0$. Ekkor van olyan prim, amely páratlan hatványon szerepel az $a$ kanonikus alakjában.

Ha a 2 ilyen prim, azaz $a = 2^t \cdot l$, ahol $l$ és $t$ páratlan, akkor legyen $m$ az $x \equiv 5 \pmod 8$, $x \equiv 1 \pmod t$ szimultán kongruenciarendszer egy (pozitív) megoldása. Ekkor ($t > 1$-re)

$$\left( \frac{a}{m} \right) = \left( \frac{2}{m} \right)^t \left( \frac{l}{m} \right) = \left( -1 \right)^t \left( \frac{m}{l} \right) = \left( -1 \right)^{l+1} = -1.$$  

Ha egy $p > 2$ prim kitevője páratlan, azaz $a = 2^p \cdot q$, ahol $q \geq 0$, $j$ páratlan és $(q, 2^p) = 1$, akkor legyen $m$ az $x \equiv 1 \pmod 8$, $x \equiv 1 \pmod v$, $x \equiv c \pmod p$ szimultán kongruenciarendszer egy (pozitív) megoldása, ahol $c$ egy kvadratikus nemmaradék mod $p$. Ekkor

568
Legyen végül $a < 0$. Ha $|d|$ nem négyzetszám, akkor járjunk el a fentiek szerint. Ha $a = -s^2$, akkor bármely $4k + 3$ alakú $m$ megfelel (amely páratlan, 1-nél nagyobb és relatív prim $a$-hoz):

$\left( \frac{-s^2}{m} \right) = \left( \frac{-1}{m} \right) \left( \frac{s}{m} \right) = -1.$

5. Prímszámok

- **5.1.5 [116]** Indirekt tegyük fel, hogy $P < n$ a legkisebb olyan prim, amelyre $(p, d) = 1$. Ekkor a primekből álló számtani sorozat első $P$ tagja, $a, a + d, \ldots, a + (P - 1)d$ teljes maradékszer modulo $P$, és így van közöttük $P$-vel osztható, ami a feltétel szerint csak maga a $P$ lehet, azaz $p = a + jd$. Ha itt $j > 0$, akkor $P$ minimalitása miatt az $a$ prim osztója $d$-nel, tehát $a$ osztója minden tagnak, ami ellentmond ezek prim voltának. Ezért csak $p = c$ lehetséges, ekkor viszont a számtani sorozat $p + 1$-edik tagja, $a + pd = s(1 + d)$ nem prim.

- **5.2.5 [125]** Gauss tétel szerint azt kell megvizsgálnunk, mely $2^k - 1$ alakú számkirakók lehetőek fel különböző Fermat-primek szorzataként.

Először megmutatjuk, hogy $k$ szükségképpen kettőprím. Indirekt tegyük fel, hogy $k$-nak létezik egy $q$ páratlan prímosztója. Ekkor $2^q - 1 \mid 2^k - 1$ teljesül. Továbbá az T 5.2.3 Tétel szerint $2^q - 1$ minden prímosztója $2^{q}q + 1$ alakú, ami $q$ páratlanlásága miatt nem lehet Fermat-prím. Ez viszont ellentmond annak, hogy $2^k - 1$ minden prímosztója Fermat-prím.

Legyen tehát $k = 2^n + 1$. Ekkor az 5.2.3 feladat [124] alapján $2^k - 1 = 2F_0F_1 \ldots F_n$. Ha $0 \leq n \leq 4$, akkor kapjuk, hogy $2^k - 1$ valóban csupa különböző Fermat-primek szorzata, tehát ez az őt $k$ érték megfelel. Ha azonban $n \geq 5$, akkor $2^k - 1$ osztható $F_5$-tel, és így 641-gyel is, ami nem Fermat-prím.

Összefoglalva, szabályos $2^k - 1$-szög akkor és csak akkor szerkeszthető, ha $k = 2, 4, 8, 16$ vagy $32$.

- **5.2.7 [125]** Tegyük fel először, hogy $2p - 1 \mid M_p$, és legyen $q$ a $2p - 1$ tetszőleges prímosztója. Ekkor $q \mid M_p$ is teljesül, ezért az T 5.2.3 Tétel szerint $q = 2^p k + 1$ alakú. Mivel $q \mid 2p + 1$, így csak $q = 2p + 1$ lehetséges, vagyis $2p + 1$ prim. Azt kell még igazolni, hogy $p \equiv 3 \pmod{4}$. Nyilván $p \neq 2$. Ha $p \equiv 1 \pmod{4}$, akkor $q = 2p + 1 \equiv 3 \pmod{8}$ és így $(q^2) = -1$ következne. Ez azonban ellentmond annak, hogy a $2p + 1 \mid M_p$ feltétel átírható a $2^{(q - 1)/2} \equiv 1 \pmod{q}$ alakba.

A megfordításhoz legyen $q = 2p + 1$ prim és $p \equiv 1 \pmod{4}$. Ekkor $q = 7 \pmod{8}$, ezért $(q^2) = 1$, azaz $(2^{(q - 1)/2}) \equiv 1 \pmod{q}$, ami éppen a bizonyítani kívánt $2p + 1 \mid M_p$ oszthatóságot jelenti.

- **5.2.9 [125]** A számpár páros elemek csak kettőprím lehetséges.

Vizsgáljuk először azt az esetet, amikor $n + 1 = 2^a$ és $n = q^b$ (ahol $q$ páratlan prim, $a, b \geq 1$). Ekkor $2^a = q^b + 1$.
MEGOLDÁSOK

Ha \( \beta = 1 \), akkor \( \mathcal{Q} \) Mersenne-prím.

Ha \( \beta \) páros, akkor a jobb oldal 2 maradékot ad 4-gyel osztva, ami lehetetlen.

Ha \( \beta > 1 \) páratlan, akkor a jobb oldal \( (q^\beta - 1)(q^\beta - 2 + \cdots + 1) \) alakba írható. Mivel itt a második tényező egy 1-nél nagyobb páratlan szám, ez nem lehet kettőhatvány, tehát ellentmondásra jutottunk.

Tegyük most fel, hogy \( r = q^\beta \), és \( n + 1 = q^\beta \). Ekkor \( 2^n = q^\beta - 1 \).

Ha \( \beta \) páros, akkor \( \mathcal{Q} \) Fermat-prím.

Ha \( \beta > 1 \) páratlan, akkor a jobb oldal \( (q^{3/2} - 1)(q^{3/2} + 1) \) alakba írható. Itt mindkét tényező maga is kettőhatvány, a különbségük kettő, tehát csak a \( 2 \cdot 4 \) szorzatról lehet szó. Ekkor \( 2^n = 8, q^\beta = 9 \).

Végül, ha \( \beta > 1 \) páratlan, akkor a jobb oldal \( (q^{3/2} - 1)(q^{3/2} + 1) \) alakba írható. Mivel itt a második tényező egy 1-nél nagyobb páratlan szám, ez nem lehet kettőhatvány, tehát ellentmondásra jutottunk.

Az összes megfelelő számpár tehát a következő: \( (8,9), (M_{\nu}, M_{\nu} + 1) \), ahol \( M_{\nu} \) Mersenne-prím; \( (2^{3^\nu}, F_n) \), ahol \( F_n \) Fermat-prím.

5.5.9 [140](a) Ha \( n = k^3 \), akkor \( (k - 1)^3 = n + 3n^{2\nu} - 3n^{\nu^3} - 1 > n + n^{2\nu} \). Az T 5.5.4 Tétel (A) része szerint minden elég nagy \( n \) -re \( n \) és \( n + n^{2\nu} \) között található prímszám, tehát a \( (k^3, (k + 1)^3) \) intervallum is tartalmaz prímszámot.

(b) Az útmutatásban vázolt gondolatmenetet fogjuk követni. Előállítunk egy \( \mathcal{U} \) prímszámsorozatot, amelyhez található lesz olyan \( \alpha \), hogy

\[ q_n = \left[ \alpha^{3^n} \right] \]

teljesüljön. Legyen

\[ \varepsilon_n = \sqrt[3]{q_n} \quad \varepsilon \quad \hat{d}_n = \sqrt[n]{q_n + 1} \]

Ezzel a jelöléssel (1) éppen azt jelenti, hogy

\[ \varepsilon_n \leq \alpha < \hat{d}_n \]

A \( \mathcal{U} \) prímekeit úgy fogjuk megválasztani, hogy \( [\varepsilon_n, \hat{d}_n] \) egy egymásra skatulyázott zárt intervallumsorozatot alkosson, azaz minden \( n \) -re

\[ \sqrt[n]{q_n} < x^{n+1} \sqrt[n+1]{q_{n+1}} < x^{n-1} \sqrt[n-1]{q_{n-1} + 1} < x^{n} \sqrt[n]{q_n} + 1 \]

teljesüljön. A (3) egyenlőtlenséget \( 3^{n+1} \)-edik hatványra emelve a

\[ q_n^\frac{3}{n} \leq q_{n+1} \leq (q_n + 1)^3 - 1 \]

feltételhez jutunk.

Ennek megfelelően legyen \( \mathcal{U} \) egy nagy prímszám, \( \mathcal{Q} \) egy olyan prim, amely \( q_1^{\frac{3}{n}} \) és \( (q_1 - 1)^3 \) közé esik, és általában, ha \( \mathcal{U} \) -et már kiválasztottuk, akkor \( \mathcal{Q} + 1 \) legyen egy olyan prim, amely eleget tesz
Ily módon tehát egy egymásba skatulyázott \([k_n, d_n]\) zárt intervallumsorozatot kaptunk. Ennek van közös pontja, jelöljük ezt \(\alpha\)-val. Megmutatjuk, hogy \(\alpha\) megfelel a feladat állításának.

Az \(\alpha\) konstrukciója szerint minden \(n\)-re \(c_n \leq \alpha \leq d_n\), és nekünk a hajszálynival élessebb (2) egyenlőtlenségre van szükségünk. Az jelenthetne problémát, ha valamely \(n\)-re \(\alpha = d_n\) teljesülne. Mivel azonban a \(d_j\) számok (3) és (4) miatt szigorúan monoton csökkennek, ezért \(\alpha \leq d_{n+1} < d_n\), tehát \(\alpha = d_n\) nem fordulhat elő.

\(\bullet\) (c) A (b) rész bizonyításában lattuk, hogy csak \(\alpha\) létezését tudjuk garantálni, \(\alpha\) konkrét értékét nem tudjuk megadni. Sőt, a helyzet tulajdonképpen ennél is sokkal furcsább: "előbb „gyártanunk” kellett, utána "képletből" visszakapjuk ugyanazokat a prímeket, amelyeket az \(\alpha\) elkészítéséhez fel kellett használnunk.

\(\bullet\) 5.6.1 [148] Jelölje az (a), (b), … részekben szereplő számsorozatokat rendre \(A = \{a_1, a_2, \ldots\}\), \(B = \{b_1, b_2, \ldots\}\) stb., és ezekben az \(n\)-nél nem nagyobb elemek számát \(A(n)\), \(B(n)\) stb.

\(\bullet\) (a) Nyilván \(a_n = L/n\), tehát

\[
\sum_{n=1}^{\infty} \frac{1}{a_n} = L \sum_{n=1}^{\infty} \frac{1}{n} = \infty \quad \text{és} \quad A(n) = \frac{n}{L} \sim \frac{n}{L},
\]

\(\bullet\) (b) Mivel pozitív tagú sorról van szó, a tagokat tetszőlegesen átrendezhetjük. Csoportosítsuk a teljes hatványokat azerint, hogy melyik számnak a hatványai (így bizonyos hatványokat többször is megiszámolunk, pl. \(64 = 4^3 = 8^2\)). Ekkor

\[
\sum_{n=1}^{\infty} \frac{1}{b_n} < \sum_{j=2}^{\infty} \frac{1}{j^2} - \sum_{j=2}^{\infty} \frac{1}{j^2(1 - \frac{1}{j})} - \sum_{j=2}^{\infty} \frac{1}{j(j - 1)} = 1.
\]

Rátérve \(B(n)\) vizsgálatára, megmutatjuk, hogy itt lényegében csak a négyzetszámok számítanak, a magasabb hatványok száma ehhez képest elhanyagolható.

Rögzített \(k > 1\) kitevőre az 1-nél nagyobb és \(n\)-nél kisebb vagy egyenlő \(k\)-adik hatványok száma \(\lfloor \sqrt[n]{k} \rfloor - 1\). Igy bizonyos számokat (például a 64-et) több \(k\)-nál is figyelembe vettünk, továbbá csak olyan \(k\) értékek jöhetnek szóba, amelyekre \(k^k \leq n\), azaz \(k \leq \lfloor \log_2 n \rfloor\). Ennek megfelelően

\[
\lfloor \sqrt[n]{n} \rfloor - 1 \leq B(n) \leq \sqrt[n]{n} + \sum_{k=3}^{\lfloor \log_2 n \rfloor} \sqrt[n]{n} \leq \sqrt[n]{n} + (\log_2 n) \sqrt[n]{n}.
\]

Innen \(\sqrt[n]{n}\)-nel való osztással kapjuk, hogy \(B(n) \sim \sqrt[n]{n}\).

\(\bullet\) (c) A négyzetmentes számok között megtalálhatók a prímek is, és már ez utóbbiak reciprocösszege is divergencs.

\(\bullet\) (d) Az T 5.6.1 Tétel harmadik bizonyításának mintájára adódik, hogy

\[
\sum_{d_j \leq \alpha} \frac{1}{d_j} \leq \prod_{\nu \leq L} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^{\nu}}\right).
\]
MEGOLDÁSOK

ahol

\[ p^{n_k} \leq n < p^{n_k+1}, \quad \text{azaz} \quad \nu_k = \lfloor \log n, p \rfloor. \]

A mértani sorozatokat összegezve és felülről becsüelve azt kapjuk, hogy

\[ \sum_{d_j \leq \sqrt{n}} \frac{1}{d_j} \leq \prod_{\nu \leq L} \frac{1}{1 - \frac{1}{\nu}}. \]

Mivel itt a jobb oldal független az \( \nu \)-től, ezért a sor konvergens.

Áttérve \( D(n) \) becslésére, legyenek \( p_1, \ldots, p_k \) az \( L \)-nél kisebb prímek. Ekkor a \( D \) sorozat tagjainak kanonikus alakja

\[ d = p_1^{n_1} \cdots p_k^{n_k}. \]

Ha \( d \leq n \), akkor (1)-ben nyilván minden \( i \)-re

\[ p_i^{n_i} \leq n, \quad \text{azaz} \quad 0 \leq \alpha_i \leq \frac{\log n}{\log p_i}. \]

Ebből következik, hogy

\[ D(n) < \prod_{i=1}^{k} \left(1 - \frac{\log n}{\log p_i}\right) < c \left(\log n\right)^k, \]

ahol \( c \) alkalmas konstans.

A \( D(n) \) alsó becsléséhez vegyük észre, hogy ha (1)-ben minden \( i \)-re

\[ p_i^{n_i} \leq \sqrt[2]{n}, \quad \text{azaz} \quad 0 \leq \alpha_i \leq \frac{\log n}{k \log p_i}, \]

akkor \( d \leq \sqrt{n} \). Innen az előzőkhoz hasonlóan adódik, hogy alkalmas \( c' \) konstansra

\[ D(n) > c' \left(\log n\right)^k. \]

Az aszimptotika igazolásához az (1) logaritmisált alakjával dolgozunk:

\[ \log d = \alpha_1 \log p_1 + \cdots + \alpha_k \log p_k. \]

Ekkor \( D(n) \) azoknak az \( \left(\alpha_1, \ldots, \alpha_k\right) \) szám \( k \)-asoknak a száma, ahol

\[ \alpha_1 \log p_1 + \cdots + \alpha_k \log p_k \leq \log n \quad \text{és minden} \quad \alpha_i \text{ nemnegatív egész.} \]

A bizonyítást először \( L = 6 \)-ra részletezzük, utána pedig jelezní fogjuk, hogyan vihető át ez a gondolatmenet tetszőleges \( L \)-re.

Ha \( L = 6 \), akkor \( k = 3 \); a 2, 3 és 5 prímekről van szó. Ekkor (2) szerint \( D(n) \) az

\[ \alpha_1 \log 2 + \alpha_2 \log 3 + \alpha_3 \log 5 \leq \log n \]

egyenlőtlenség nemnegatív egész \( \left(\alpha_1, \alpha_2, \alpha_3\right) \) megoldásainak a száma.
Az $x_1 \log 2 + x_2 \log 3 + x_3 \log 5 = \log n$ egyenlőséget úgy is felfoghatjuk, mint a térben egy síknak az egyenletét. Ekkor az

$$x_1 \log 2 + x_2 \log 3 + x_3 \log 5 \leq \log n, \quad x_i \geq 0$$

eyenlőtlensérgrendszer annak a $G_n$ háromoldalú gúlának az $(x_1, x_2, x_3)$ pontjai elégítenek ki, amelyet a fenti sík és a koordinátatengelyek pozitív félegyenesei határolnak.

Az egész koordináttájú $(x_1, x_2, x_3)$ pontok éppen a szokásos (egységnyi oldalú, az origót is tartalmazó) kockarácspontjaí a térben. Ezerint (3) nemnegatív egész megoldásainak a száma éppen a $G_n$ gúlába eső rácspontok száma.

Szemléletesen világos (és könnyen igazolható, vő. a 7.5.9 feladattal [241]), hogy nagy $n$ esetén a $G_n$ gúlába eső rácspontok száma „körülbelül” a $G_n$ gúla térfogata. Preciz fogalmazásban ez azt jelenti, hogy $n \to \infty$ mellett a rácspontok száma és a gúla térfogata aszimptotikusan egyenlő.

A $G_n$ gúla $V(G_n)$ térfogata az origóból kiinduló három páronként merőleges él sorzatának az egyhatoda. Mindezek alapján

$$D(n) \sim V(G_n) = \frac{(\log n)^{5}}{6 \cdot \log 2 \cdot \log 3 \cdot \log 5}.$$  

Tetszőleges $L$ esetén is hasonlóan kell eljárni: (2) szerint ekkor a $k$ -dimenziós térben keressük a megfelelő „gúla” (ún. szimplex) rácspontjainak a számát, ami aszimptotikusan egyenlő a gúla térfogatával. Ebben az esetben

$$D(n) \sim V(G_n) = \frac{(\log n)^{k}}{k! \prod_{p \leq L} (1 - \frac{1}{p})}.$$  

$\bullet$ (e) Ezek között a számok között megtalálhatók az $L$ -nél nagyobb prímszámok is, és már ez utóbbiak reciprokoköszegje is divergensi.

Az $E(n)$ becsülésehez vegyük észre, hogy itt éppen azokról a számokról van szó, amelyek az $L$ -nél nem nagyobb primek mindegyikéhez relatív primek. Legyen $M = \prod_{p \leq L} p^t$. Ekkor az előbbiek szerint bármely $M$ egynégyzet növekedésével a $E$ sorozatnak pontosan $p(M)$ eleme található. Ennek megfelelően

$$\lim_{n \to \infty} E(n) = tM < (t + 1), \quad \text{akkor} \quad t\varphi(M) \leq E(n) \leq (t + 1)\varphi(M).$$

Az $E(n)$ -re és az $n$ -re vonatkozó egyenlőtlenségekből kapjuk, hogy

$$\frac{t\varphi(M)}{(t + 1)M} \leq \frac{E(n)}{n} \leq \frac{(t + 1)\varphi(M)}{tM}.$$  

Mivel $t = \lceil n/M \rceil$, ezért ha $n \to \infty$, akkor $t$ is a végképletben, $t/(t + 1) \leq (t + 1)/t$ pedig $1$-hez tart. Ez azt jelenti, hogy

$$\lim_{n \to \infty} \frac{E(n)}{n} = \frac{\varphi(M)}{M} = \prod_{p \leq L} \left(1 - \frac{1}{p}\right), \quad \text{ezáltal} \quad E(n) \sim n \prod_{p \leq L} \left(1 - \frac{1}{p}\right).$$

$\bullet$ (f) A négyzeteljtes számok reciprokaiból képzett $\sum_{j=1}^{\infty} 1/j^2$ sor konvergenciáját kétféleképpen is bebizonyíthuk. (Egy harmadik bizonyítás az 5.6.7 feladat [149] alapján adható.)
**MEGOLDÁSOK**

*Első bizonyítás:* Az T 5.6.1 Tétel harmadik bizonyításához hasonlóan adódik, hogy

\[
\sum_{j_1 \leq \nu} \frac{1}{j_j} \leq \prod_{p \leq \sqrt{n}} \left( 1 + \frac{1}{p^2} + \frac{1}{p^4} + \cdots + \frac{1}{p^{\nu_p}} \right),
\]

ahol

\[
p^{\nu_p} \leq n < p^{\nu_p+1}, \quad \nu_p = \lfloor \log_p n \rfloor.
\]

Itt az egyes tényezőkben az 1 után mértani sorozatok állnak, ezeket összegezve és felülről becsülve azt kapjuk, hogy

\[
\sum_{j_1 \leq \nu} \frac{1}{j_j} \leq \prod_{p \leq \sqrt{n}} \left( 1 + \frac{1}{p^2(1-p)} \right) = \prod_{p \leq \sqrt{n}} \left( 1 - \frac{1}{p^2} \right).
\]

Ha \(p_k\) a \(k\)-adik prim, akkor \(k > 1\) esetén \(p_k(\sqrt{p_k} - 1) > p_k^2 - 1\). Ennek alapján a (4) jobb oldalán a \(p = p_1 = 2\)-nek megfelelő

\[
1 + \frac{1}{2 - 1} = \frac{3}{2}
\]

tényezőt változtatlanul hagyva és \(k > 1\) esetén a \(p = p_k\) -nak megfelelő tényezőre az

\[
1 - \frac{1}{p_k(\sqrt{p_k} - 1)} < 1 + \frac{1}{p_k^2 - 1}
\]

becslést alkalmazva a (4) jobb oldalára a következő felső becslést nyerjük:

\[
\prod_{p \leq \sqrt{n}} \left( 1 + \frac{1}{p(p - 1)} \right) < \frac{3}{2} \prod_{p \leq \sqrt{n}} \left( 1 + \frac{1}{p^2} \right) < 2 \sum_{j=1}^{\infty} \frac{1}{j^2}.
\]

*Második bizonyítás:* Először megmutatjuk, hogy minden négyzeteljtes szám felírható egy négyzetszám és egy köbszám szorzataként. Legyen az \(f\) négyzeteljtes szám kanonikus alakja

\[f = q^{\alpha_1} \cdot \ldots \cdot q^{\alpha_r} \cdot b, \quad \mu_i \geq 2, \quad i = 1, 2, \ldots, r.
\]

A \(\mu_i\) ketvek felírhatók \(\mu_i = 2\alpha_i + 3\beta_i\) alakban, ahol \(\alpha_i, \beta_i \geq 0\) (például \(\beta_k\) aszerint legyen 0 vagy 1, hogy \(\mu_i\) páros, illetve páratlan). Ekkor

\[
f = a^2 \cdot b^3, \quad \text{ahol} \quad a = \prod_{i=1}^{r} q_i^{\alpha_i}, \quad b = \prod_{i=1}^{r} q_i^{3\beta_i}.
\]

(5)-ből következik, hogy a négyzeteljtes számok reciprokosszegé e kisebb, mint a négyzetszámok reciprokosszegének és a köbszámok reciprokosszegének a sorzata, ami igazolja a konvergenciát.

Az \(F(n)\) becsléséhez (5)-öt fogjuk felhasználni. Láttuk, hogy az is elérhető, hogy minden \(q_i = 0\) vagy 1, vagyis a \(b\) négyzetmentes. Az is azonnal adódik, hogy ilyen feltételek mellett az \(f = a^2 b^3\) előállítás már egyértelmű, vagyis minden négyzeteljtes szám egyértelműen írható fel egy négyzetszámnak és egy négyzetmentes szám k öb nének a szorzataként. Nyilvánvaló továbbá, hogy az 1 kivételével az ilyen \(a^2 b^3\) szorzatok valóban négyzeteljtesek.
Mindenek alapján \( F(n) \) -et úgy kapjuk meg, hogy az \( n \) -nél nem nagyobb ilyen \( a^2 b^3 \) szorzatok számából 1-et levonunk. Egy ilyen szorzatban \( b \) négyzetmentes és \( b \leq \sqrt[3]{n} \), valamint rögzített \( b \) mellett \( 1 \leq a \leq \sqrt[6]{n/b^3} \). Ennek megfelelően

\[
F(n) = -1 + \sum'_{l \leq \sqrt[6]{n}} \left\lfloor \frac{n}{b^l} \right\rfloor,
\]

ahol \( \sum' \)-vel azt jelöljük, hogy csak a négyzetmentes \( b \) értékekre kell az összegzést végezni.

A (6) jobb oldalát az egészrészek felbontása után

\[
\sqrt{n_2} \sum'_{l < \sqrt[6]{n}} \frac{1}{b^l} + l'(n)
\]

alakba írhatjuk, ahol az \( U(n) \) hibatag a másik részhez képest elhanyagolható, ugyanis

\[
|U(n)| \leq 1 + \sum'_{l < \sqrt[6]{n}} 1 \leq 1 + \sqrt{n}.
\]

Ebből következik, hogy

\[
F(n) \sim c\sqrt{n}, \quad \text{ahol} \quad c = \sum_{l=1}^{\infty} \frac{1}{b^{\sqrt[6]{n}/2}}.
\]

\section*{5.6.6 [149] Az \( (1 - 1/x^s)^{-1} \) tényezőket írjuk fel végzetlen mértani sorként, és használjuk fel, hogy két pozitív tagú konvergens sor (vagy általában két abszolút konvergens sor) „ugyanúgy szorozható össze, mint azt a véges sok tagból álló összegek szorzásánál megszoktuk”. Ebből következik, hogy

\[
\prod_{l \leq n} \frac{1}{1 - \frac{1}{3^l}} = \prod_{l \leq n} \left(1 + \frac{1}{3^l} + \frac{1}{3^{2l}} + \ldots\right) = \sum_{j \in \mathbb{W}_n} \frac{1}{j^s},
\]

ahol \( \mathbb{W}_n \) azoknak a számoknak a halmaza, amelyek minden prímosztója kisebb vagy egyenlő, mint \( n \). Nyilván

\[
\sum_{j-1}^{n} \frac{1}{j^s} \leq \sum_{j \in \mathbb{W}_n} \frac{1}{j^s} < \sum_{j-1}^{\infty} \frac{1}{j^s}.
\]

Mivel (7) bal oldala \( n \to \infty \) esetén a jobb oldalhoz tart, ezért

\[
\lim_{n \to \infty} \prod_{l \leq n} \frac{1}{1 - \frac{1}{3^l}} = \lim_{n \to \infty} \sum_{j \in \mathbb{W}_n} \frac{1}{j^s} = \sum_{j=1}^{\infty} \frac{1}{j^s} = \zeta(s).
\]

\section*{5.7.4 [160] A feltétel szerint az \( n \) összetett száma

\[
2^n - 1 \equiv 1 \pmod{n}
\]

teljesül. Azt kell belátnunk, hogy \( 2^n - 1 \) is összetett, ez azonnal következik \( n \) összetettségéből (lásd az 1.4.4a feladatot), továbbá hogy

\[
2^{2^n - 2} \equiv 1 \pmod{2^n - 1}
\]

575
is fennáll.

Mivel nyilván $2^n \equiv 1 \pmod{2^n - 1}$, ezért (2)-höz elég megmutatni, hogy $n \mid 2^n - 2$. Ez azonban azonnal következik (1)-ből.

- **5.7.17 [161]** Legyen az $n \geq 1$ páratlan szám kanonikus alakja

$$n = q_1^{e_1} \cdots q_k^{e_k}, \quad \text{és} \quad n - 1 = 2^r \sigma, \quad \text{ahol} \quad \sigma \text{ páratlan.}$$

Azt kell igazolnunk, hogy ha egy $a$ -ra

$$a^r, a^{2r}, a^{4r}, \ldots, a^{2^{r-1}r} = a^{\frac{2^r - 1}{2}}, a^{2^{r-1}r} = a^{\frac{2^r - 1}{2}}$$

jó sorozat, azaz ezek modulo $n$ vett legkisebb abszolút értékű maradékai között előfordul $-1$ vagy pedig $a^r$ maradéka 1, akkor

$$a^{\frac{2^r - 1}{2}} \equiv \left( \frac{a}{n} \right) \pmod{2^r} \quad \text{(**) \text{tartalom}}$$

is fennáll.

Ha $a^r \equiv 1 \pmod{n}$, akkor egyrészt ezt a kongruenciát $2^{k-1}$ hatványnak emelve kapjuk, hogy $a^{r(2^{k-1} - 1)/2} \equiv 1 \pmod{2^r}$, másrészről

$$1 = \left( \frac{1}{n} \right)^r = \left( \frac{a^r}{n} \right)^r = \left( \frac{a}{n} \right)^r,$$

ahonnan $\sigma$ páratlansága miatt $\left( \frac{a}{n} \right) - 1$ következik. Így (**) ekkor valóban teljesül.

Tegyük most fel, hogy

$$a^{2^r} = -1 \pmod{n}, \quad \text{ahol} \quad 0 \leq j \leq k - 2. \quad \text{(3)}$$

Ekkor ($\sigma < k - 1$ miatt) $a^{r(2^{k-1} - 1)/2} \equiv 1 \pmod{n}$. Azt kell igazolni, hogy $\left( \frac{a}{n} \right) - 1$ is teljesül.

A (3) kongruenciát mod $q_i$ tekinve, majd négyzetre emelve kapjuk, hogy

$$a^{2^r} = -1 \pmod{q_i} \quad \text{és} \quad a^{2^{r+1}r} = 1 \pmod{q_i}.$$ 

Ez azt jelenti, hogy

$$a_{2^r} (a) \mid 2^r \quad \text{és} \quad a_{2^r} (a) \mid 2^{r+1} r_i,$$

vagyis

$$a_{2^r} (a) = 2^{r+1} r_i, \quad \text{ahol} \quad r_i \mid r. \quad \text{(4)}$$

Mivel $q_i$ prim, ezért (4)-ből

$$a^{2^r} = -1 \pmod{q_i} \quad \text{(5)}$$

következik, továbbá $a_{2^r} (a) \mid q_i - 1$ alapján azt is kapjuk, hogy alkalmas $i_1$ -vel.
Az (5) és (6) összefüggések felhasználásával

\[
\frac{a^k}{(q^k)} = a^{(q-1)k/q} = a^{2^r-1} = \left( a^{2^r} \right)^{\frac{a^k}{q^k}} = \left( (-1)^{h_i} \right) (\text{mod } q_i) \tag{7}
\]

adódik. A (7) alapján

\[
\left( \frac{2^{a^k}}{q^i} \right) = \prod_{i=1}^{h_i} \left( \frac{2^{a^k}}{q^i} \right)^{a^k} = \left( (-1) \cdot \sum_{i=1}^{h_i} a_i h_i \right),
\]

vagyis \( \left( \frac{2^{a^k}}{q^i} \right) = 1 \)-hez azt kell megmutatni, hogy \( \sum_{i=1}^{h_i} \alpha_i r_i h_i \) páros. Mivel minden \( r_i \) páratlan, ez azzal ekvivalens, hogy \( \sum_{i=1}^{h_i} \alpha_i r_i h_i \) páros.

A (6) felhasználásával

\[
u = \prod_{i=1}^{k} q_i^{a^k} = \prod_{i=1}^{k} \left( 1 + 2^{j+1} r_i h_i \right)^{a^k}, \tag{8}
\]

A (8) jobb oldalán a beszorzást elvégezve a legtöbb tag osztható lesz \( 2^{j+2} \)-vel:

\[
u = 1 + 2^{j+1} \sum_{i=1}^{k} \alpha_i r_i h_i + 2^{j+2} C', \tag{9}
\]

Mivel \( u = 1 - 2^{k-r} \), azaz \( u = 1 + 2^{k-r} \), ezért (9)-ből

\[
q^{k-r} = 2^{j+1} \sum_{i=1}^{k} \alpha_i r_i h_i + 2^{j+2} C',
\]

majd \( 2^{j+1} \)-gyel történő egyszerűsítés után

\[
q^{k-r-1} = 2^{j+2} C' = \sum_{i=1}^{k} \alpha_i r_i h_i \tag{10}
\]

következik. A (10) bal oldalán \( j < k - 1 \) miatt páros, tehát a jobb oldalon álló \( \sum_{i=1}^{k} \alpha_i r_i h_i \) összeg is valóban páros.

Végül az

\[
a^{2^{j-1} r_i} = a^{2^{j-1} r_i} \equiv -1 \text{ (mod } q_i)\]

esetben is ugyanily járhatunk el. Ekkor \( \frac{a^{k}}{q_i} = -1 \)-et kell igazolnunk, ami \( \sum_{i=1}^{k} \alpha_i r_i h_i \) páratlanságával ekvivalens. Ekkor \( j = k - 1 \)-nek megfelelően (10) bal oldalán \( r = 2C' \) áll, ami \( r \) páratlansága miatt valóban páratlan.

6. Számelméleti függvények

- **6.1.7 [170](a) Az** \( f(a^k) = (e_i, r_i)[v, i] \) egyenlőség és a teljes additivitás miatt az \( f(a^k) \) függvényértéket kétféleképpen kiszámíthatjuk éppen a kivánt.
megoldások

\[ f(a) + f(b) = f((a, b)) + f([a, b]) \]  \hspace{1cm} (1)

eyenlőséget kapjuk.

\( \bullet \) **(b)** Legyen \( a \) és \( b \) kanonikus alakja

\[ a = p_{1}^{\alpha_{1}} 1^{\beta_{1}} \ldots 1^{\beta_{v}} \quad \text{és} \quad b = p_{1}^{\beta_{1}} 1^{\beta_{2}} \ldots 1^{\beta_{v}}, \quad \text{ahol} \quad \alpha_{i} \geq 0, \beta_{j} \geq 0. \]

Ekkor

\( (a, b) = \prod_{i=1}^{v} p_{i}^{\min(\alpha_{i}, \beta_{i})} \prod_{i=1}^{v} p_{i}^{\max(\alpha_{i}, \beta_{i})} \)

és

\[ [a, b] = \prod_{i=1}^{v} p_{i}^{\max(\alpha_{i}, \beta_{i})} \prod_{i=1}^{v} p_{i}^{\max(\alpha_{i}, \beta_{i})}. \]

Innen a T 6.1.7 Tétel alapján kapjuk, hogy

\[ f(a) + f(b) = \sum_{i=1}^{v} f(p_{i}^{\alpha_{i}}) + f(p_{i}^{\beta_{i}}) \]  \hspace{1cm} (2)

és

\[ f((a, b)) + f([a, b]) = \sum_{i=1}^{v} f(p_{i}^{\min(\alpha_{i}, \beta_{i})}) + f(p_{i}^{\max(\alpha_{i}, \beta_{i})}). \]  \hspace{1cm} (3)

(Mindennel \( f(1) = 0 \) miatt akkor is érvényes, ha a kitermők között a 0 is előfordul.)

Mivel tetszőleges két valós szám egyike a két szám minimuma, másika pedig a két szám maximuma, ezért az \( \alpha_{i}, \beta_{i} \) és \( \min(\alpha_{i}, \beta_{i}) \), \( \max(\alpha_{i}, \beta_{i}) \) értékek bármely \( i \) esetén megegyeznek. Ennélégvőg (2)-ből és (3)-ból azonnal következik (1).

\( \bullet \) **(c)** Megmutatjuk, hogy a feltételt az \( f = g + c \) alakú függvények elégtik ki, ahol \( g \) additív, \( c \) pedig konstans.

Mivel az additív függvényekről már láttuk, hogy megfelelnek, ezért azonnal adódik, hogy a fenti alakú függvények is jók.

Megfordítva, tegyük fel, hogy az \( f \) függvényre (1) bármely \( a, b \) esetén teljesül, és próbáljuk előállítani \( f \)-et a keresett \( f = g \) \( + c \) alakban, ahol \( g \) additív és \( c \) konstans.

A \( g(1) = 0 \) feltételből kapjuk, hogy \( c \) értéke csak \( f(1) \) lehet. Ennélégvőg azt kell igazolnunk, hogy a \( g(a) = f(a) - f(1) \) függvény additív. Ez azt jelenti, hogy bármely \( (a, b) = 1 \) esetén

\[ f(ab) - f(1) = (f(a) - f(1)) + (f(b) - f(1)), \]

azaz

\[ f(1) - f(a) - f(b) = f(ab). \]  \hspace{1cm} (4)

Mivel \( (a, b) = 1 \) miatt \( [a, b] = ab \), ezért (4) bal oldalán \( f(1) \), illetve \( f(ab) \) helyére \( f((a, b)) \), illetve \( f([a, b]) \) írható. Ennélégvőg (4) azonnal következik (1)-ből.

\( \bullet \) **(d)** Az előzőkhöz hasonlóan igazolhatjuk, hogy az
egyenlőség minden \( a; b \) esetén teljesül a teljesen multiplikatív, sőt a multiplikatív függvényekre, valamint ezek konstansszorosaira, továbbá, hogy \( f(1) \neq 0 \) esetén ez utóbbiak adják az összes lehetséges \( f \) -et.

Vizsgáljuk most az \( f(1) = 0 \) esetet. Ha \( f = 0 \), akkor (5) nyilván teljesül. Tegyük fel, hogy \( f \neq 0 \) kielégíti (5)-öt, és legyen \( K \) a legkisebb pozitív egész, amelyre \( f(K) \neq 0 \).

Ha \( K \mid n \), akkor

\[
f(K)f(n) = f([K, n])f([K, n]),
\]

Mivel a feltétel szerint \( (K, n) < K \), ezért \( f([K, n]) = 0 \), továbbá \( f(K) \neq 0 \), és így (6) alapján \( f(n) = 0 \).

Legyen most \( h(n) = f(Kn) \). Ekkor \( h \) is kielégíti (5)-öt bármely \( a; b \) esetén:

\[
h(a)h(b) = f(Ka)f(Kb) = f([Ka, Kb])f([Ka, Kb]) =
\]

\[
= f([K(a, b)])f([Ka, Kb]) = h([a, b])h([a, b]).
\]

Továbbá \( h(1) = f(K) \neq 0 \), ezért \( h \) egy multiplikatív függvény konstansszorosa.

Összefoglalva, azt kaptuk, hogy

\[
f(n) = \begin{cases} 0, & \text{ha } K \nmid n; \\ c\varrho\left(\frac{n}{K}\right), & \text{ha } K \mid n. \end{cases}
\]

ahol \( \varrho(n) \) multiplikatív, \( c \) konstans és \( K \) rögzített pozitív egész. Megfordítva, könnyen adódik, hogy a (7)-beli \( f \) függvényekre (5) valóban teljesül minden \( a; b \) esetén. A (7) tartalmazza az \( f(1) \neq 0 \), illetve \( f = 0 \) eseteket is, amikor \( K = 1 \), illetve \( c = 0 \) (vagy \( g = 0 \)). Ezzel beláttuk, hogy a (7) képlet adja az összes keresett függvényt.

- **6.1.9 [170](d)** A feladat megoldásában az olyan additív függvények játszanak szerepet, amelyek egy vagy két prim hatványtól eltekintve minden primhatvány helyen 0 értéket vesznek fel.

Legyen \( P \) tetszõleges primszám. Nevezzünk házi használatra egy \( h \) additív függvényt \( P \) -talpúnak, ha \( h \) a \( P \) hatványain tetszõleges értéket vehet fel, a többi primhatvány helyen viszont csak 0-t. Egy általános \( n \) helyen felvett függvényértéket innen a következőképpen kapunk meg: az \( t; r \) felírható \( n = tr^a \) alakban, ahol \( (t, r) = 1 \) , ekkor \( h(ta) = h(tr^a) \). (Ez az \( a = 0 \) esetben is helyes, hiszen az additivitás miatt \( h(1) = 0 \) ) Az ilyen függvényeket úgy is jellemezhetjük, hogy minden \( (e, p) = 1 \) esetén \( h(e) = 0 \).

Hasonlóképpen definiáljuk a \( (P, q) \) -talpú függvényeket, ahol \( P \) és \( q \) különbözõ primek: ekkor a \( h \) additív függvény a \( P \) és \( q \) hatvainyain tetszõleges értéket vehet fel, a többi primhatvány helyen viszont csak 0-t. Egy általános \( n \) helyen felvett függvényértéket innen a következőképpen kapunk meg: az \( n \) felírható \( n = tq^a r^b \) alakban, ahol \( (t, q) = 1 \) , ekkor \( h(n) = h(tq^a) + h(r^b) \). Az ilyen függvényeket úgy is jellemezhetjük, hogy minden \( (e, q) = 1 \) esetén \( h(e) = 0 \).

Rátérve a feladat megoldására, ha \( f = 0 \) vagy \( g = 0 \), akkor nyilván minden teljesül.
Most megmutatjuk, hogy ha $\mathcal{f}$ és $\mathcal{g}$ is $\mathcal{P}$-talpú (uygananzzal a $\mathcal{P}$ primmel), akkor $\mathcal{f}\mathcal{g}$ is additív.

Azt kell igazolni, hogy bármely $(a, b) = 1$ esetén fennáll

$$\mathcal{(f\mathcal{g})}(ab) = (\mathcal{f}\mathcal{g})(a) + (\mathcal{f}\mathcal{g})(b).$$

(5)

Ha $a$ és $b$ egyike sem osztható $\mathcal{P}$-vel, akkor a (8) mindkét oldala 0.

Ha $a = b\mathcal{P}^\alpha$, ahol $\alpha > 0$, $(\mathcal{f}, \mathcal{g}) = 1$, akkor $(a, b) = 1$ miatt $\mathcal{P}^\alpha b$, és így

$$\mathcal{(f\mathcal{g})}(b) = 0, \quad (\mathcal{f}\mathcal{g})(\mathcal{e}) = (\mathcal{f}\mathcal{g})(\mathcal{e}\mathcal{P}^\alpha) = \mathcal{f}(\mathcal{P}^\alpha)\mathcal{g}(\mathcal{P}^\alpha),$$

tehát (8) ekkor is teljesül.

További megoldásokat kapunk, ha $\mathcal{f}$ és $\mathcal{g}$ is $(\mathcal{P}, \mathcal{Q})$-talpú (uygananzzal a $\mathcal{P}$, $\mathcal{Q}$ primekkel), és létezik olyan $c$, hogy

$$\mathcal{g}(\mathcal{P}^\alpha) = c\mathcal{f}(\mathcal{P}^\alpha), \quad \mathcal{g}(\mathcal{Q}^\beta) = -c\mathcal{f}(\mathcal{Q}^\beta), \quad \alpha, \beta = 1, 2, 3, \ldots$$

(9)

Ekkor (8) igazolása az előzőek mintájára történhet, ha $a$ és $b$ közül legalább az egyik se $\mathcal{P}$-val, se $\mathcal{Q}$-val nem osztható.

A fennmaradó esetben $a = b\mathcal{P}^\alpha$ és $b = a\mathcal{Q}^\beta$ (vagy fordítva), ahol $(\mathcal{P}, \mathcal{Q}) = 1$. Ekkor (9)-et is felhasználva kapjuk, hogy

$$\mathcal{(f\mathcal{g})}(\mathcal{a}) = \mathcal{f}(\mathcal{P}^\alpha)\mathcal{g}(\mathcal{Q}^\beta) = c(\mathcal{f}(\mathcal{P}^\alpha))^2,$$

$$\mathcal{(f\mathcal{g})}(\mathcal{b}) = \mathcal{f}(\mathcal{Q}^\beta)\mathcal{g}(\mathcal{P}^\alpha) = -c(\mathcal{f}(\mathcal{Q}^\beta))^2,$$

$$\mathcal{(f\mathcal{g})}(ab) = (\mathcal{f}(\mathcal{P}^\alpha) + \mathcal{f}(\mathcal{Q}^\beta))(\mathcal{g}(\mathcal{P}^\alpha) + \mathcal{g}(\mathcal{Q}^\beta)) =$$

$$ = (\mathcal{f}(\mathcal{P}^\alpha) + \mathcal{f}(\mathcal{Q}^\beta))(c\mathcal{f}(\mathcal{P}^\alpha) - c\mathcal{f}(\mathcal{Q}^\beta)), $$

ahonnan (8) leolvasható.

Összefoglalva, eddig a következő megoldásokat találtuk:

I. $\mathcal{f} = 0$ vagy $\mathcal{g} = 0$.

II. $\mathcal{f}$ és $\mathcal{g}$ tetszőleges $\mathcal{P}$-talpú függvény.

III. $\mathcal{f}$ és $\mathcal{g}$ olyan $(\mathcal{P}, \mathcal{Q})$-talpú függvények, amelyek kielégítik (9)-et.

Most azt igazoljuk, hogy a fentiekben az összes megoldást megadunk, vagyis ha $\mathcal{f}$ és $\mathcal{g}$ additív, akkor az $\mathcal{f}\mathcal{g}$ függvénypár ezen három típus valamelyikébe tartozik.

Tegyük fel, hogy $\mathcal{f}, \mathcal{g}$ és $\mathcal{f}\mathcal{g}$ is additív.. Ekkor bármely $(a, b) = 1$ esetén fennáll

$$\mathcal{f}(\mathcal{a})\mathcal{g}(\mathcal{a}) + \mathcal{f}(\mathcal{b})\mathcal{g}(\mathcal{b}) = \mathcal{f}(ab)\mathcal{g}(ab) = (\mathcal{f}(\mathcal{a}) + \mathcal{f}(\mathcal{b}))(\mathcal{g}(\mathcal{a}) + \mathcal{g}(\mathcal{b})), $$

azaz

$$\mathcal{f}(\mathcal{a})\mathcal{g}(\mathcal{b}) + \mathcal{f}(\mathcal{b})\mathcal{g}(\mathcal{a}) = 0. $$

(10)

Feltehetjük, hogy $\mathcal{f} \neq 0$ és $\mathcal{g} \neq 0$. Az $\mathcal{f}$ és $\mathcal{g}$ függvények primhatvány helyeken felvett értékeit fogjuk vizsgálni. Két esetet különböztetünk meg:
(A) Van olyan \( p^\alpha \) primhatvány, amelyre \( f(p^\alpha) \neq 0 \) és \( g(p^\alpha) = 0 \).

(B) Bármely \( w \) primhatványra \( f(w) = 0 \iff g(w) = 0 \).

Az (A) esetben alkalmazzuk (10)-et az \( r \) és \( \gamma \) értékekre, ahol \( r \) a \( P \) -tól különböző prim. Ekkor \( g(r^\gamma) = 0 \) adódik. Ez azt jelenti, hogy a \( g \) függvény \( P \)-talpú. Mivel \( g \neq 0 \), ezért van olyan \( \kappa \), amelyre \( g(p^\kappa) \neq 0 \). Ekkor (10)-et az \( a = p^\kappa \) és \( b = r^\gamma \) értékekre alkalmazva kapjuk, hogy \( f(r^\gamma) = 0 \). Eszerint az \( f \) is \( P \)-talpú, vagyis egy II. típusú \( f, g \) páról van szó.

Térjünk át a (B) esetre, és legyen a \( p^\alpha \) olyan primhatvány, amelyre \( f(p^\alpha) = 0 \) és \( g(p^\alpha) \neq 0 \). Ha az \( f \) függvény \( P \)-talpú, akkor a (B) feltétel szerint a \( g \) is az, tehát ismét a II. típusú \( f, g \) párhoz jutottunk.

Így feltehetjük, hogy van egy \( q^\beta \) primhatvány is, ahol \( q \) a \( P \) -tól különböző prim és \( f(q^\beta) \neq 0 \), \( g(q^\beta) \neq 0 \).

Először megmutatjuk, hogy \( f \) és \( g \) is \( \{p, q\} \)-talpú, vagyis tetszőleges, a \( P \) -tól és \( Q \) -tól különböző \( r \) prim esetén minden \( \gamma \)-ra \( f(r^\gamma) = g(r^\gamma) = 0 \) teljesül.

Tegyük fel indirekt, hogy van olyan \( r^\gamma \), amelyre \( f(r^\gamma) \neq 0 \).

Ha \( f(a)f(b) \neq 0 \), akkor (10) átírható a

\[
g(a) = f(a) = \frac{g(b)}{f(b)} \tag{11}
\]

alakba. Alkalmazzuk (11)-et rendre a \( p^\alpha \), \( q^\beta \) és \( r^\gamma \) számokból képzett párokra:

\[
g(p^\alpha) = f(p^\alpha) \frac{g(q^\beta)}{f(q^\beta)} = \frac{g(r^\gamma)}{f(r^\gamma)} = \frac{g(q^\beta)}{f(q^\beta)}f(r^\gamma)
\]

ami ellentmond \( g(t^\alpha) \neq 0 \)-nak.

Végül (9) igazolásához alkalmazzuk (11)-et először \( a = t^\mu \), \( b = q^\beta \) szereposztással, és legyen a két oldal közös értéke \( c \). Ezután az \( a \) változatlanul tartása mellett legyen \( b = q^\nu \), ahol \( \nu \) végigfut az összes olyan kitevőn, amelyre \( f(q^\nu) \neq 0 \), majd hasonló módon, rögzített \( b = q^\beta \) mellett legyen \( a = p^\mu \) az összes olyan \( P \) -vel, amelyre \( f(p^\mu) \neq 0 \). Ekkor (11)-ből éppen a (9) összfüggések adódnak.

Ezzel megmutattuk, hogy az \( f, g \) függvénypár III. típusú.

\[
6.1.13 \text{ [171](a)] Tegyük fel, hogy az } f \text{ additív függvény } k \text{ különböző értéket vesz fel. Ezek között } f(1) = 0 \text{ miatt szerepel a } 0 \text{ is.}
\]

Először azt igazoljuk, hogy bármely \( k \) darab, páronként relatív prim \( a_1, a_2, \ldots, a_k \) szám közül kiválasztható néhány (esetleg csak egy, esetleg az összes), amelyek szorzatán az \( f \) értéke 0.

Tekintsük az

\[
f(a_1), f(a_1a_2), \ldots, f(a_1a_2 \cdots a_k)
\]
függvényértékeket. Ha ezek mind különbözők, akkor szerepel közöttük a 0 is, tehát készen vagyunk. Ha pedig van közük két egyenlő, azaz valamilyen \(1 \leq i < j \leq k\) -ra \(f(u_i u_j \ldots u_j) = f(u_1 u_2 \ldots u_i)\), akkor

\[
0 = f(u_1 u_2 \ldots u_j) - f(u_1 u_2 \ldots u_i) = \ldots = f(u_1) + f(u_2) + \ldots + f(u_j) - (f(u_1) + f(u_2) + \ldots + f(u_i)) = \ldots = \sum_{i=1}^{j} f(u_i) - f(u_{i+1} \ldots u_j).
\]

Legyen most \(b\) tetszőleges. A \(b\)-nél nagyobb prímek sorozatát osszuk be \(k\)-hosszúságú blokkokba. Ekkor az előzőek szerint bármely \(\tau\) -re az \(\tau\)-edik blokk néhány alkalmas primének a \(G\) sorozatát véve \(f(u_\tau) = 0\). Ilyen \((b, u_\tau) = 1\) miatt \(f(b u_\tau) = f(b) + f(u_\tau) = f(b)\), tehát az \(f(b)\) értéket a függvény végén sok helyen felveszi.

6.1.15 [171] Nyilván \(\varphi_2(1) = 1\). Egy \(\tau = \tau^\alpha\) primhatványra \((\tau, \varphi^\alpha) \neq 1 \iff \tau | j\), ezért az \(i = \tau p\), illetve \(i = \tau p - 1\) alakú számok esetén lesz \((i, \varphi^\alpha) \neq 1\), illetve \((i + 1, \varphi^\alpha) \neq 1\). Ennek megfelelően \(\varphi_2(p^\alpha)\) meghatározásához az \(1, 2, \ldots; \tau^\alpha\) számok számából le kell vonni a

\[p - 1, p, 2p - 1, 2p, \ldots, p^\alpha - 1 = p^\alpha - 1 - p - 1, p^\alpha = p^\alpha - 1\]

számok számát, vagyis

\[\varphi_2(p^\alpha) = p^\alpha - 2p^\alpha - 1. \quad (12)\]

Most belátjuk, hogy \(\varphi_2(n)\) multiplikatív. Legyen \((a, b) = 1\) és

\[1 \leq u_1 < u_2 < \ldots < u_r \leq a, \quad \text{illetve} \quad 1 \leq v_1 < v_2 < \ldots < v_s \leq b\]

az összes olyan szám \((1 \leq a\), illetve \(1 \leq b\) között), amelyre

\[(u_1, a) = (u_1 + 1, a), \quad \text{illetve} \quad (v_j, b) = (v_j + 1, b) = 1.\]

Ekkor tehát \(\tau = \varphi_2(a)\) és \(a = \varphi_2(b)\).

Tekintsük az

\[x = u_i \mod a, \quad x = v_j \mod b\]

szimultán kongruenciarendszert. Mivel \((a, b) = 1\), ezért ennek a rendszernek bármely \(i = 1, \ldots, \varphi_2(a)\), \(j = 1, \ldots, \varphi_2(b)\) esetén pontosan egy megoldása van modulo \(ab\). Jelöljük \(w_{ij}\) -vel az \(1 \leq u_i j \leq ab\) feltételt is kielégítő (egyértelműen meghatározott) megoldást. Ezzel összesen \(\varphi_2(a)\varphi_2(b)\) darab \(w_{ij}\) számot defináltunk.

Megmutatjuk, hogy

\[(w_{ij}, ab) = (w_{ij} + 1, ab) = 1, \quad (14)\]

és ezek adják az összes ilyen tulajdonságú számot \(1 \leq a\) és \(ab\) között. Ebből következik, hogy a \(w_{ij}\) értékek száma \(\varphi_2(ab)\), amit az előzőkkel összevetve éppen a kívánt multiplikativitás adódtik.

A (14)-hez azt kell belátni, hogy \(w_{ij} \neq w_{ij} + 1\) az \(a\)-hoz és \(b\)-hez is relatív prímek. Mivel \(w_{ij} = u_i \mod a\), ezért

582
MEGOLDÁSOK

\[(v_{ij}, a) = (u_t, a) = 1 \quad \text{és} \quad (v_{ij} + 1, a) = (u_t + 1, a) = 1.\]

Hasonlóan adódik, hogy \((v_{ij}, b) = (v_{ij} + 1, b) = 1\) is teljesül.

Most tegyük fel, hogy \(1 \leq c \leq ab\) és \((c, ab) = (c + 1, ab) = 1\). Azt kell igazolni, hogy alkalmas \(i\)-vel és \(j\)-vel \(c = w_{ij}\) . Legyen \(c\) legkisebb pozitív maradéka \(a\)-val, illetve \(b\)-val osztva \(c'\), illetve \(c''\). Ekkor

\[(c', a) = (c, a) = 1 \quad \text{és} \quad (c' + 1, a) = (c + 1, a) = 1.

Ez azt jelenti, hogy alkalmas \(i\)-vel \(c' = u_i\) . Hasonlóan kapjuk, hogy \(c'' = q_j\).

Ebből következik, hogy \(c\) megoldása a (13) szimultán kongruenciarendszernek, tehát \(c = w_{ij}\) . Ezzel \(\varphi_2(n)\) multiplikativitásának a bizonyítását befejeztük.

Végül, legyen az \(n\) kanonikus alakja \(n = \prod_{i=1}^{r} p_i^{\alpha_i}\). Ekkor a multiplikativitás és (12) felhasználásával kapjuk, hogy

\[\varphi_2(n) = \prod_{i=1}^{r} \left( p_i^{\alpha_i} - 2p_i^{\alpha_i - 1} \right) = n_2 \prod_{\alpha \geq 1, \alpha + 1 = \alpha} \left( 1 - \frac{2}{p} \right).

6.2.7 [176]

Elő megoldás: Megmutatjuk, hogy \(\sigma(n) \neq 2p\), ahol \(P\) egy tetszőleges \(6k - 1\) alakú prim.

Tegyük fel indirekt, hogy valamilyen \(n\) pozitív egészre \(\sigma(n) = 2p\). Legyen az \(n\) kanonikus alakja \(n = q_1^{\alpha_1} \cdots q_v^{\alpha_v}\), ekkor

\[2p = \sigma(n) = \prod_{i=1}^{v} \sigma(q_i^{\alpha_i}).\]

Mivel a 2 nem szerepel a \(\sigma\)-függvény értékkészletében, ezért \(v = 1\), azaz \(n = q^a\) (ahol \(q\) prim), és

\[2p = 1 + q + q^2 + \cdots + q^a.\]

Mivel (1) bal oldala páros, ezért \(q > 2\) és \(\alpha\) páratlan, így (1) jobb oldalán kiemelhető \(1 + q\). Nyilván \(1 + q \neq 1, 3, p\), tehát csak \(1 + q = 2p\) lehetséges (és ekkor \(\alpha = 1\)). A feltétel szerint \(2p \equiv 1 \mod 3\), ezért innen \(3 \mid q\) adódik. Ez azt jelenti, hogy \(q = 3\), vagyis \(p = 2\), ami ellentmondás.

Ugyanigy igazolható az is, hogy \(\sigma(n) \neq 2p\), ahol \(P\) egy 3-nál nagyobb \(5k - 2\) alakú prim vagy egy tetszőleges \(7k - 3\) vagy \(11k - 5\) alakú prim stb.

 Második megoldás: Megmutatjuk, hogy \(\sigma(n) \neq 3^s\), ha \(s > 1\).

Most indirekt bizonyítunk. A \(\sigma\)-függvény multiplikativitásából adódik, hogy az \(n\) kanonikus alakjában szereplő bármely \(q^a\) primhatványa \(\sigma(q^a) = 3^t\) (ahol \(1 \leq t \leq s\)), azaz

\[3^t = 1 + q + q^2 + \cdots + q^a.\]
MEGOLDÁSOK

Vizsgáljuk először a $q = 2$ esetet, ekkor (2) átírható a

$$3^t = 2^{t+1} - 1$$  \hspace{1cm} (3)

alakba. Ha $\alpha = 1$, akkor $t = 1$ és megoldást kapunk. Ha $\alpha > 1$, akkor (3) bal oldala 8-cal osztható 3-at vagy 1-et ad maradéknak, a jobb oldal pedig 7-et, ami ellentmondás.

A továbbiakban feltehetjük tehát, hogy $q > 2$ és $t > 1$. A (2) egyenlőséget modulo 2, illetve modulo 3 tekintve azt kapjuk, hogy $\alpha$ páros, továbbá $q \equiv 1 \pmod{3}$ és $\alpha \equiv 2 \pmod{3}$.

Ezért (2) jobb oldalán kiemelhető $1 + q + q^2$, ami így szintén a 3-nak hatványa. Ez azonban lehetetlen, mert $1 + q + q^2$ nem osztható már 9-tel sem (ezt például a $q = 1, 4$ és 7 $(\text{mod } 9)$ esetek behelyettesítésével ellenőrizhetjük).

Ezzel megmutattuk, hogy a 2 az egyetlen primhatvány, és így a 2 az egyetlen olyan $\alpha$ is, amelyre $\sigma(x)$ a 3-nak hatványa. Ez azt jelenti, hogy $s > 1$-re $\sigma(x) = 3^t$ nem lehetséges.

● Harmadik megoldás: Azt mutatjuk meg, hogy a „legtöbb” páratlan szám nem szerepel a $\sigma$ -függvény értékkészletében.

Legyen $N$ tetsőleges („nagy”) egész szám, és vizsgáljuk meg, legfeljebb hány olyan $x$ van, amelyre $\sigma(x)$ egy $2N$ -nél kisebb páratlan szám. Ekkor egyrészt nyilván $x < 2N$, továbbá a 6.2.6a feladat [176] szerint $\omega$ csak négyzetszám vagy egy négyzetszám kétszerese lehet. A $2N$ -nél kisebb négyzetszámok száma $\lfloor \sqrt{2N} - 1 \rfloor$, a $2^2$ alakú számok száma pedig $\lfloor \sqrt{N} - 1 \rfloor$. Ennek megfelelően a szóba jövő $x$ -ek száma kisebb, mint $(\sqrt{2} + 1)\sqrt{N}$. A $2N$ -nél kisebb páratlan számok száma ugyanakkor $N$. Ez azt jelenti, hogy a $2N$ -nél kisebb páratlan számok közül legalább

$$N - (\sqrt{2} + 1)\sqrt{N} \hspace{1cm} (4)$$

nen szerepel a $\sigma$ -függvény értékkészletében. (A (4)-beli függvény „nagyon erősen” tart a végtelenhez, mert a második tag „elhanyagolható” az $N$ -hez képest.)

● Negyedik megoldás: Legyen $N$ tetsőleges egész, és vizsgáljuk meg, legfeljebb hány olyan $x$ van, amelyre $\sigma(x)$ $\leq N$. Ekkor egyrészt nyilván $x \leq N$, másrészt a $2N/3$ -nál nagyobb $s$ páros számok nem jós, mert ezekre $\sigma(s) \geq s + s/2 > N$. A $2N/3$ és $N$ közötti páros számok száma

$$\left\lfloor \frac{N}{2} \right\rfloor - \left\lfloor \frac{N}{3} \right\rfloor > \frac{N}{6} - 2,$$

ezért a szóba jövő $x$ -ek száma legfeljebb $5N/6 + 2$. Ez azt jelenti, hogy az $1, 2, \ldots, N$ számok közül legalább $N/6 - 2$ nem szerepel a $\sigma$ -függvény értékkészletében.

● Ötödik megoldás: A negyedik megoldáshoz hasonló gondolatmenetet alkalmazunk, de most nem azt használjuk ki, hogy bizonyos $x \leq N$ -ek esetén $\sigma(x) > N$, hanem azt, hogy „sok” olyan $x_i \neq x_j$ páron, amelyre $\sigma(x_i) = \sigma(x_j)$. Ilyen párok például a $6t$ és a $11t$, ha $(t, 66) = 1$. Ezek száma $N$ -ig körülbelül

$$\frac{N \cdot \varphi(66)}{66 \cdot 11} = 0.027 \ldots N.$$

Mivel az $x \leq N$ helyek közül legalább ennyi esetben a $\sigma$ -függvény értéke „összeszik”, ezért legalább ennyi szám ki kell hogy maradjon a függvény értékkészletéből.
Megjegyzés: A feladat állítása jelentősen élesíthető: a "legtöbb" egész szám hiányzik a $\sigma$-függvény értékészletéből, vagyis az értékészlet a természetes számoknak egy „ritka” részsortozatát alkotja. Ez pontosan a következőt jelenti. Legyen $\mathcal{U} \leq N$ azoknak az $\mathcal{U} \leq N$ értékeknek a száma, amelyek előfordulnak a $\sigma$-függvény értékészletében. Ekkor $\mathcal{U} \leq N \cdot \mathcal{U} \leq N = 0$. A bizonyításhoz a prímzámoknak a számtani sorozatokban való eloszlásáról szóló eredményeket kell felhasználni, lásd a 6.4.8 [189] és 6.4.9 feladatokat [190].

1. **6.2.8 [177]** Az $n = 1$ érték nyilván megfelel. Megmutatjuk, hogy más megoldás nincs. Ha $n \geq 2$, akkor

$$\frac{\sigma(n!)}{n!} = \prod_{p \leq n} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^{\alpha_p}}\right) < \prod_{p \leq n} \frac{p - 1}{p - 1} \leq \prod_{\frac{n}{2} \leq e \leq n} \frac{\nu}{\nu - 1} = n.$$ 

Innen $n! < \sigma(n!) < n - n! < (n + 1)!$, azaz $\sigma(n!) \neq k!$.

2. **6.2.17 [178](b)** Megmutatjuk, hogy $g(n)$ értéke csak 0 és $\pm 1$ lehet.

Ha $n$ nem négyzetmentes, akkor az összeg minden tagja 0, tehát $g(n) = 0$.

A továbbiakban tegyük fel, hogy $n$ négyzetmentes.

Ha $n$ az összes 100-nál kisebb prímmel osztható, akkor $g(n) = \mu(n) = \pm 1$.

Egyébként legyen $S$ az összes olyan 100-nál kisebb prim szorzata, amelyek nem osztói $n$-nek. Ha $(n, k) \neq 1$ vagy $k$ nem négyzetmentes, akkor $\mu(nk) = 0$, ezért

$$g(n) = \sum_{k \in S} \mu(nk) = \sum_{k \in S} \mu(n) \mu(k) = \mu(n) \sum_{k \in S} \mu(k) = 0$$

az utolsó lépésben a T 6.2.4 Tételt használtuk.

3. **6.3.5 [181](a)** Ha $n = 2^{n-1}$, ahol $2^n - 1$ Mersenne-prím, akkor $\sigma(n) = 2^n - 1$ és $\sigma(\sigma(n)) = 2^{n-1} - 2n$.

A megfordításhoz tegyük fel, hogy $n$ páros és szupertökéletes. Legyen $n = 2^k t$, ahol $k \geq 1$ és $t$ páratlan.

Ekkor $\sigma(n) = (2^{k+1} - 1)\sigma(t)$, ahonnan $k \geq 1$ miatt következik, hogy $(2^{k+1} - 1)\sigma(t)$ és $\sigma(t)$ a $\sigma(n)$-nek két különböző osztója. Így

$$2^{k+1} t = 2n = \sigma(\sigma(n)) \geq (2^{k+1} - 1)\sigma(t) + \sigma(t) = 2^{k+1} \sigma(t).$$

Ez csak úgy lehetséges, ha $\sigma(t) = t$, azaz $t = 1$, továbbá $\sigma(n)$-nek a megadott két számon kívül nincs más pozitív osztója, azaz $\sigma(n) = 2^{k+1} - 1$ prim.

4. **(b)** A 6.2.6a feladat [176] szerint egy páratlan $\nu$ pontosan akkor négyzetszám, ha $\sigma(n)$ páratlan. Így elég belátni, hogy egy páratlan $\nu$ szupertökéletes szám esetén $\sigma(\nu)$ páratlan.

Tegyük fel indirekt, hogy $\nu$ szupertökéletes és $\sigma(n) = 2^{\nu-1}$, ahol $\nu$ páratlan és $\nu \geq 1$. Ekkor

$$2n = \sigma(\sigma(n)) = (2^{\nu+1} - 1)\sigma(n),$$
ahonnan alkalmaz $z$-vel $\sigma(v) = 2z$ és $x = (2^{v+1} - 1)z$ következik. Innen $v \geq 1$ alapján azt kapjuk, hogy

$$\sigma(\eta) \geq (2^{v+1} - 1)z + z = 2^{v+1}z,$$

ugyanakkor

$$\sigma(\eta) = 2^s \eta < 2^s \sigma(\eta) = 2^{v+1}z,$$

ami ellentmondás. ($w < \sigma(w)$ egyenlőtlenség abból adódott, hogy $\sigma(w) = 2z$ miatt $w \neq 1$.)

- (c) Tegyük fel, hogy $p^\gamma$ szupertökéletes, ahol $p$ páratlan prim. Legyen $\sigma(p^\gamma)$ kanonikus alakja $\prod_{j=1}^s q_j^{\beta_j}$, azaz

$$\sigma(p^\gamma) = 1 + p + \cdots + p^\gamma = \prod_{j=1}^s q_j^{\beta_j}.$$  \tag{5}

Ekkor

$$2p^\gamma = \sigma(2p^\gamma) = \prod_{j=1}^s (1 + q_j + \cdots + q_j^{\beta_j}).$$  \tag{6}

A (6) jobb oldalán szereplő tényleg közül pontosan egy páros, legyen ez mondjuk az első tényleg. Ez azt jelenti, hogy

$$1 + q_1 + \cdots + q_1^{\beta_1} = \frac{q_1^{\gamma+1} - 1}{q_1 - 1} = 2p^\gamma,$$  \tag{7a}

továbbá

$$1 + q_j + \cdots + q_j^{\gamma_j} = \frac{q_j^{\gamma_j+1} - 1}{q_j - 1} = p^\gamma, \quad j = 2, \ldots, s, $$  \tag{7b}

ahol a $\gamma_j$ kitevők alkalmaz pozitív egészek. (A bizonyítás lépései az $s = 1$ esetben is helyesek lesznek.)

A (7a) és (7b) egyenlőségekből következik, hogy

$$q_j^{\beta_j+1} \equiv 1 \pmod{p}, \quad j = 1, 2, \ldots, s.$$  \tag{8}

(7a)-ből azt is kapjuk, hogy $\beta_1$ páratlan, és így $1 + q_1 + \cdots + q_1^{\gamma_1}$-ből kiemelhető $1 + a_1$. Ennek alapján $1 + q_1 = 2p^\delta$ alakú, ezért

$$q_1 \equiv -1 \pmod{p}.$$  \tag{9}

(7b) szerint $j \geq 2$ esetén a $\beta_j$ kitevő páros, tehát

$$K = (\beta_2 + 1) \cdots (\beta_s + 1) \páratlan.$$  \tag{10}

Szorozzuk be (5)-öt $\theta_1 \cdots \theta_s$-sel.
\[ \prod_{j=1}^{r} q_j^{q_j+1} - q_1 q_2 \ldots q_s (1 + p + \ldots + p^e). \quad (11) \]

Tekintsük (11)-et modulo \( p \), ekkor (8) és (9) felhasználásával \( 1 \equiv -q_2 \ldots q_s \mod p \), azaz
\[ q_2 \ldots q_s \equiv -1 \mod p \quad (12) \]
adódik. Emeljük (12)-t a \( K \)-adik hatványra. Ekkor (10) alapján
\[ (q_2 \ldots q_s)^K \equiv -1 \mod p. \quad (13) \]
Ugyanakkor \( j \geq 2 \Rightarrow \beta_j + 1 \mid K \) és (8) felhasználásával azt kapjuk, hogy
\[ (q_2 \ldots q_s)^K \equiv 1 \mod p, \]
ami \( \beta > 2 \) miatt ellentmond (13)-nak.

6.4.8 [189(b)] Az útmutatásban vázolt gondolatmenetet követjük.

Legyen \( \varepsilon > 0 \) tetszőleges. Azt kell igazolni, hogy ha \( N \) elég nagy, akkor az \( 1, 2, \ldots, N \) számok közül legfeljebb \( \varepsilon N \) darab szerepel a \( \varphi \)-függvény értékkészletében.

Rögzítésüknél az \( r \) pozitív egész értékét úgy, hogy
\[ 2^r > \frac{2}{\varepsilon} \]
teljesüljön.

A \( \varphi(n) \) értékkészletét osszuk két csoportba: \( H_1 \)-be tartozzanak a \( 2^r \)-rel osztható függvényértékek, \( H_2 \)-be pedig azok, amelyek nem oszthatók \( 2^r \)-rel.

A \( H_1 \) halmaz \( N \)-nél nem nagyobb elemeinek a száma nyilván
\[ \left[ \frac{N}{2^r} \right] < \frac{\varepsilon N}{2}. \]

A feladat állításához így elég megmutatni, hogy elég nagy \( N \) esetén a \( H_2 \) halmaz \( N \)-nél nem nagyobb elemeinek a száma szintén legfeljebb \( \varepsilon N / 2 \).

Ha \( \varphi(n) \geq r + 1 \), akkor \( 2^r \mid \varphi(n) \), tehát minden ilyen \( n \) esetén \( \varphi(n) \in H_1 \).

Így a továbbiakban elég az olyan \( n \) -eket vizsgálni, amelyekre \( \omega(n) \leq r \). Ebben az esetben
\[ \frac{\varphi(n)}{n} = \prod_{p \mid n} (1 - \frac{1}{p}) \quad (14) \]
nyilván akkor a legkisebb, ha az \( n \) kanonikus alakjában éppen az első \( r \) prímszám, \( p_1, \ldots, p_r \) szerepel. Ekkor (14)-et a
\[ \prod_{i=1}^{r} (1 - \frac{1}{p_i}) = c \]

587
jelölés segítségével
\[ \varphi(n) \geq n^c \] (15)
alakba írhatjuk.

A (15) egyenlőtlenségből az következik, hogy ha \( \varphi(n) \leq N \), akkor
\[ n \leq \frac{\varphi(n)}{c} \leq \frac{N}{c} , \]
vagyis \( H_2 \)-nek az \( N \)-nél nem nagyobb elemei csak a
\[ \varphi(1), \varphi(2), \ldots, \varphi(N') \]
függvényértékek közül kerülhetnek ki, ahol \( N' = \lfloor N/c \rfloor \).

A feladat (a) része szerint létezik olyan \( \tau_0 \), hogy ha \( N' > n_0 \), akkor az \( 1, 2, \ldots, N' \) számok között legfeljebb
\[ \frac{c \varepsilon N'}{2} \leq \frac{\varepsilon N}{2} \]
onyan van, amelyre \( \varphi(n) \) nem osztható \( \mathcal{P}' \)-rel, és így nyilván legfeljebb \( c N'/2 \) darab \( H_2 \)-be tartozó \( \varphi(n) \) érték keletkezhet.

- 6.6.12 [199](a) Mivel \( d(n) = (1 + 1)(n) \), ezért a T 6.6.4 Tétel szerint a \( d(n) \) Dirichlet-sora
\[ D(s) = \zeta^2(s) \], és így speciálisan \( s = 2 \)-re
\[ D(2) = \sum_{n=1}^{\infty} \frac{d(n)}{n^2} = \zeta^2(2) = \left( \frac{\pi^2}{6} \right)^2 . \]

- (b) Jelöljük a \( d^2(n) \) függvény Dirichlet-sorát \( T(s) \)-sel. Mivel \( d^2(n) \) multiplikatív, ezért a 6.6.10a feladat [199] szerint
\[ T(s) = \sum_{n=1}^{\infty} \frac{d^2(n)}{n^s} = \prod_{p} \left( \sum_{k=0}^{\infty} \frac{d^2(p^k)}{p^{ks}} \right) \]
(16)

Legyen
\[ H(x) = \sum_{k=0}^{\infty} (k+1)^2 x^k , \] (17)
ekkor (16) és (17) alapján
\[ T(s) = \prod_{p} H\left( \frac{1}{p^s} \right) . \] (18)

Feltesszük, hogy \( s > 1 \), ekkor \( p \geq 2 \) miatt \( H(x) \)-et a \( 0 < x < 1/2 \) tartományban vizsgáljuk. A \( H(x) \) végtelen sorhoz úgy jutunk el, ha a
ők = j - 1 helyettesítés mutatja, hogy (19) bal oldalán éppen \( H(x) \) áll. A jobb oldalon szereplő tört számlálóját és nevezőjét 1 - x -szel bővítve így

\[
H(x) = \frac{1 - x^2}{(1 - x)^4}
\]  

adódik. A (20)-at (18)-ba beírva azt nyerjük, hogy

\[
T(s) = \prod_{\ell} \frac{1 - \frac{1}{\rho^s}}{(1 - \frac{1}{\rho})} = \frac{\zeta(s)}{\zeta(\ell s)}. 
\]

A (21) képletet \( s = \frac{9}{2} \)-re alkalmazva kapjuk, hogy

\[
T(2) = \sum_{n=1}^{\infty} \frac{d^2(n)}{n^2} \frac{\zeta(2)}{\zeta(4)} = \left( \frac{\pi^2}{6} \right) ^4 = \frac{5\pi^4}{72}.
\]  

6.7.4 [211] Az útmutatásban jelzett gondolatmenetet követjük.

Először megmutatjuk, hogy ha \( n \) elég nagy, akkor az \( 1, 2, \ldots, n \) számok között több, mint \( n/2 \) olyan \( i \) van, amelyre \( \sigma(i) \leq 2n \). Legyen \( t \) azoknak az \( i \) értékeknek a száma, amelyekre ez nem teljesül, ekkor azt kell igazolni, hogy \( t < n/2 \). Erre a \( t \) darab „rossz” \( i \) -re a \( \sigma(i) > 2n \), a többi \( i \) -re pedig a triviális \( \sigma(i) > 0 \) becslést alkalmazva azt kapjuk, hogy

\[
\sigma(1) + \sigma(2) + \cdots + \sigma(n) > 2n. 
\]  

Másrészt a T 6.7.3 Tétel szerint elég nagy esetén

\[
\sigma(1) + \sigma(2) + \cdots + \sigma(n) < n^2.
\]

A (22) és (23) egyenlőtlenségekből azonnal adódik, hogy valóban \( t < n/2 \).
Legyen most \( k \) tetszőleges. A 6.4.9 feladat [190] alapján elég nagy \( u \) esetén az \( 1, 2, \ldots, 2^{11} \) számok között legfeljebb
\[
\frac{2^{11}}{4k}
\]
olyan \( j \) érték szerepel, amely benne van a \( \sigma \) -függvény értékkészletében. Mivel az előző bekezdés szerint több, mint \( u/2 \) olyan \( j \) van, amelyre a \( \sigma(j) \) egy ilyen \( j \) függvényérték, ezért a skatulyaelv alapján kell lennie olyan \( j \) -nek, amelyet a \( \sigma \) -függvény legalább
\[
\frac{u}{2} : \frac{2^{11}}{4k} = k
\]
helyen vesz fel.

7. Diofantikus egyenletek

- **7.1.4 [219]** Jelöljük a szóban forgó huszadik századi évszámot \( \lambda \) -mel. Először megmutatjuk, hogy A és B nem születhettek mindkettőn 1899 után.

Indirekt tegyük fel, hogy mégis ez lenne a helyzet. Legyen A születési éve \( \overline{19x0} \), B születési éve pedig \( \overline{19xz} \) (nyilván egyikük sem születhetett 2000-ben). Ekkor a feltétel szerint
\[
M = 1900 + 10u + v + 1 + 9 + u + v = 1910 + 11u + 2v = 1910 + 11x + 2z.
\]
Ezt átrendezve \( 11(u - z) = 2(z - v) \) adódik, amiből kapjuk, hogy \( 11 \mid z - v \). Mivel \( |z - v| \leq 9 \), ezért csak \( z = v \) lehetséges. Ha azonban \( z = v \), akkor \( u = z \) is teljesül, ami ellentmondás, hiszen A és B különböző korúak.

Hasonlóan adódik, hogy A és B nem születhettek mindkettőn 1900 előtt: ha a születési évszámuk \( \overline{18uv} \), illetve \( \overline{18xz} \), akkor
\[
M = 1809 + 10u + v + 1 + 8 + u + v = 1809 + 11u + 2v = 1809 + 11x + 2z
\]
ugyanígy ellentmondásra vezet.

Ez azt jelenti, hogy (mondjuk) A születési évszáma \( \overline{19uv} \), B-é pedig \( \overline{18xz} \). Ekkor
\[
M = 1910 + 11u + 2v = 1809 + 11x + 2z, \quad \text{vagyis} \quad 101 = 11(x - u) + 2(z - v).
\]
Innen egyrészt \( x - u \) párátlan, másrészt \( z - v \leq 9 \) miatt
\[
x - u \geq \frac{101 - 18}{11} > 7,
\]
vagyis csak \( x - u = 9 \) lehetséges. Ebből
\[
x = 9, \quad u = 0 \quad \text{és} \quad z = v + 1 \quad (v = 0, 1, \ldots, 8),
\]
és ezek az értékek (alkalmas \( \lambda \) mellett) ki is elégtik a feladat feltételeit. Így a korkülönbség
\[
\overline{19uv} - \overline{18xz} = \left(1900 + v\right) - \left(1809 + v + 1\right) = 9 \cdot v.
\]
Megmutatjuk, hogy a triviális \( x = y = s = t = 0 \) értékrendszeren kívül nincs más megoldás.

**Első megoldás:** Tegyük fel indirekt, hogy létezik egy nemtriviális racionális megoldás. Ekkor a nevezők legkisebb közös többszöörővel végigsorozva, majd szükség esetén az így adódó egész számok legnagyobb közös osztójával végigosztva olyan egész megoldáshoz jutunk, ahol \( (x, y, s, t) = 1 \).

Vizsgáljuk a számok paritását. A feltétel alapján

\[
t^2 + s^2 + x^2 = t^2 + (s + x)^2 - (y - t)^2 + x^2 \equiv y^2 + t^2 + x^2 \text{ (mod 2)},
\]

tehát \( s \) és \( y \) azonos paritású.

Ekkor az egyenletrendszer modulo 4 nézve azt kapjuk, ugyanilyen paritású \( t, s + x, y + t \) és \( x \) is.

Mind a hat szám nem lehet páratlan, mert ha \( s, y \) páratlan, akkor \( y + t \) páros.

Mind a hat szám páros sem lehet, hiszen \( (x, y, s, t) = 1 \).

Ezzel ellentmondásra jutottunk.

**Második megoldás:** Most is indirekt bizonyítunk. Az előző megoldáshoz hasonlóan feltételezzük, hogy ezek egy szabályos háromszöget alkotnak.

Tekintsük az egész koordinatátú négyzetek négyzetösszegei a \( (0, 0) \), az \( (s, y) \) és az \( (s + x, -t) \) koordinátájú rácspontokat. A feltétel éppen azt jelenti, hogy ezek egy szabályos háromszöget alkotnak.

Rácspontok azonban nem alkothatnak szabályos háromszöget, ugyanis az ötöt befoglaló rácstéglát és a „sarokháromszögek” területe is nyilvánvalóan racionális, ugyanakkor a szabályos háromszög területe az oldala négyzetének \( \sqrt{3}/4 \) -szere, az oldal négyzetegyüttes pedig (Pitagorasz tétele alapján) egész szám.

**7.3.10 [227]** Legyen a 8 szám számtani közepé \( s \). Ekkor \( 2s = t \), ahol \( t \) páratlan egész, továbbá a 8 szám kőbén összege

\[
\left( s - \frac{\tau}{2} \right)^3 + \left( s - \frac{5}{2} \right)^3 + \left( s - \frac{3}{2} \right)^3 + \left( s - \frac{1}{2} \right)^3 + \left( s + \frac{1}{2} \right)^3 + \left( s + \frac{3}{2} \right)^3 + \left( s + \frac{5}{2} \right)^3 + \left( s + \frac{7}{2} \right)^3 = 8s^3 + 126s = t^3 + 63t. \quad (14.1)
\]

Így a \( t^3 + 63t = v^3 \) egyenlet olyan megoldásait keresünk, ahol \( v \) egész és \( t \) páratlan egész. Ha a \( (v, t) \) pár megoldás, akkor a \( (v, -t) \) pár is megoldás, ezért elég a \( t > 0 \) megoldásokat keresnünk.

Nyilván \( v > t \), továbbá \( (t + 3)^3 > t^3 + 63t = v^3 \), tehát \( v < t + 5 \). Ennek alapján (figyelembe véve, hogy \( v \) szükségképpen páros) csak \( v = t + 1 \) és \( v = t + 3 \) lehetséges.

Az elsőből nem kapunk megoldást, a másodikból \( t = 1 \) és \( t = 3 \) adódik. A keresett köbszámok ennek megfelelően \( 64 - 4^3; 216 - 6^3; -64 - (-4)^3 \) és \( -216 - (-6)^3 \).

**7.3.13 [227](g)** Az \( x = \pm 1 \), \( y = 0 \) értéke nyilván kielégíti az egyenletet. Megmutatjuk, hogy más egész megoldás nincs.

Indirekt bizonyítunk. Nyilván feltételezjük, hogy \( x > 1 \).
MEGOLDÁSOK

Az egyenletet \((x + 1)(x - 1) = 2y^4\) alakba írva látszik, hogy \(x\) páratlanásága miatt \(x + 1\) és \(x - 1\) páros, ezért \(y\) is az, \(y = 2\alpha\). Az egyenlet mindkét oldalát 4-gyel osztva

\[
\frac{x + 1}{2} \cdot \frac{x - 1}{2} = 8\alpha^4
\]

adódik. Az (1) bal oldalán két szomszédos pozitív egész szám szorzata áll, ezért a tényezők relatív primnek is. Így egyikük egy negyedik hatvány, a másik pedig egy negyedik hatvány 8-szorosa. Mivel a két szám eltérése 1, tehát

\[
w^4 - 8z^4 = 1 \quad \text{vagy} \quad w^4 - 8z^4 = -1.
\]

Az utóbbi eset nem lehetséges, mert egy négyzetszám nem adhat \(-1\) maradékot 8-cal osztva. Az első esetben átrendezés és szorzattá bontás után a \((w^2 + 1)(w^2 - 1) = 8z^4\), azaz a

\[
\frac{w^2 + 1}{2} (w^2 - 1) = (2z^2)^2
\]

összefüggéshez jutunk.

Megmutatjuk, hogy a (2) bal oldalán álló két (pozitív) tényező relatív prim. Jelölje a legnagyobb közös osztójukat \(d\). Mivel \((w^2 + 1)/2\) páratlan, ezért \(d\) is csak páratlan lehet. Továbbá

\[
d \mid 2w^2 + 1 - (w^2 - 1) = 2,
\]

teht valóban \(d = 1\).

Ez azt jelenti, hogy \((w^2 + 1)/2\) és \(w^2 - 1\) külön-külön is négyzetszámok. Két pozitív négyzetszám különbsége azonban nem lehet 1, tehát \(w^2 - 1\) nem lehet négyzetszám, és így ellentmondásra jutottunk.

- (b) Megmutatjuk, hogy az összes megoldás: \(x = y\), valamint \(x^2 = 4\) és \(x = 4\), \(y = 2\).

Ezek nyilván megoldások. Így azt kell igazolni, hogy \(y > x\) esetén \(x = 2\) és \(y = 4\).

- Első bizonyítás: Legyen \((x, y) = d\), ekkor \(x = \alpha d\), \(y = db\), ahol \((\alpha, b) = 1\). Ezt az egyenletbe visszaírva, majd \(d\)-edik gyököt vonva

\[
(d\alpha)^b = (db)^a, \quad \text{azaz} \quad b > a \text{ miatt} \quad d^b \cdot a^b = y^a
\]

adódik. Innen kapjuk, hogy \(a \mid b^b\), de ez \((\alpha, b) = 1\) miatt csak \(a = 1\) esetén lehetséges. Ekkor (3) a

\[
d^{b-1} = b
\]

eyenletet jelenti. Itt \(b > a = 1\), és így \(d > 1\). Ha \(d > 2\), akkor bármi \(b > 1\)-re \(d^{b-1} > b\), és \(d = 2\) esetén is csak úgy teljesülhet (4), ha \(b = 2\). Innen valóban a kivánt

\[
x = d\alpha = 2 \cdot 1 = 2 \quad \text{és} \quad y = db = 2 \cdot 2 = 4
\]

értékeket kapjuk.

- Második bizonyítás: Ha \(y > x > 1\), akkor az egyenlet ekvivalens az.
egyenlettel. Mivel az \( f(z) = z/\log z \) függvény az \( 1 < z < e \) intervallumban szigorúan monoton fogy, és \( z > e \)-re szigorúan monoton nő, így két különböző egész helyen csak akkor vehet fel azonos értéket, ha a kisebbik hely a 2. Ez azt jelenti, hogy csak \( z = 2 \) lehetséges. Ekkor \( y = 4 \) megfelel, továbbá az \( f \) függvény \( z > e \)-re szigorúan monoton, ezért más \( y \) már nem lehet jó.

- (i) Az \( x = 5 \), \( y = 1 \) értékek nyilván megfelelnek. Megmutatjuk, hogy más megoldás nincs.

Az egyenlet fennállása esetén az

\[ y^5 = 2^x \quad (\text{v. od } 31) \quad (5) \]

kongruenciának is teljesülnie kell. Mivel az eredeti egyenletből nyilvánvaló, hogy \( 31 \not| y \), ezért (5) miatt a \( 2^x \) szükségképpen ötödik hatványmaradék modulo 31. Ekkor a T 3.5.3 Tétel szerint

\[ (2^x)^{30/31} \equiv 2^x \equiv 1 \quad (\text{v. od } 31). \quad (6) \]

A (6)-ból következik, hogy

\[ 5 \mid 2x, \quad \text{ezért} \quad 5 \mid x, \quad \text{azaz} \quad x = 5n. \]

Ezt az eredeti egyenletbe visszaírva azt kapjuk, hogy

\[ (2^x)^5 - y^5 = 31, \quad (7) \]

tehát két (pozitív) ötödik hatvány különböse 31. Azt, hogy (7) egyedül a \( 2^5 - 1^5 \) esetben valósulhat meg, ahhoz hasonlóan igazolhatjuk, ahogy a II. módszer példájának megoldása során az \( a^3 - b^3 = 7 \) egyenletet kezeltük: vagy az használjuk fel, hogy minden más esetben két pozitív ötödik hatvány különböse nagyobb, mint 31, vagy pedig a (7) bal oldalát szorzattá bontva bizonyítjuk.

- 7.5.10 [241] Az egyenlet bal oldalát bontsuk szorzattá: \( (x + 2i)(x - 2i) = y^3 \). Legyen \( \delta = (x + 2i, x - 2i) \), ekkor

\[ 5 \mid (x + 2i) - (x - 2i) = 4i = (-i)(1 + i)^3 \]

Ebből következik, hogy \( \delta = (1 + i)^r \), ahol \( 0 \leq r \leq 4 \).

A konjugálás tulajdonságaiból adódik (lásd a 7.4.2a feladatot [234]), hogy

\[ (1 + i)^4 \mid x + 2i \iff (1 - i)^4 \mid x - 2i. \quad (5) \]

Az \( 1 + i \) és \( 1 - i \) egymás egységszerei, ezért (8)-ból következik, hogy az \( 1 + i \) kitevője \( x + 2i \) és \( x - 2i \) kanonikus alakjában egyaránt \( r \). Az \( (x + 2i)(x - 2i) \) szorzat (a Gauss-egészek körében is) köbszám, tehát a kanonikus alakjában minden Gauss-prím, így az \( 1 + i \) kitevője is osztható 3-mal. Ez azt jelenti, hogy \( 3 \mid 2r \), tehát \( r = 3t \) (azaz \( r = 0 \) vagy 3).

A fentiek alapján

\[
\frac{x + 2i}{(1 + i)^3t} \cdot \frac{x - 2i}{(1 - i)^3t} = \left( \frac{y}{2i} \right)^3 \quad \text{és} \quad \left( \frac{x + 2i}{(1 + i)^3t} \cdot \frac{x - 2i}{(1 - i)^3t} \right)^3 = 1.
\]

593
Innen a számelmélet alaptételéből következik, hogy \( x + 2i \) és \( x - 2i \) is „köbszámok” egységszeresei, és mivel a Gauss-egészek körében minden egység köbszám, így \( x + 2i \) és \( x - 2i \) maguk is köbszámok.

Ekkor
\[
x + 2i = (c - d \bar{c})^3 - c^3 - 3c \bar{d}^2 + (3c^2 \bar{d} - d^3)\bar{y}.
\]
A képzetes részeket összehasonlítva \( \gamma = d(3c^2 - d^2) \) adódik. Innen \( d = \pm 1 \) vagy \( \pm 2 \), és ezeket visszahelyettesítve csak a \( d = 1 \) és \( d = -2 \) esetben kapunk \( c \)-re egész értéket, mindkétszer \( c = \pm 1 \).

Végül (9)-ből \( x = c^3 - 3c d^2 \), ahonnan az \( x = \pm 2 \), \( y = 2 \) és \( z = \pm 11 \), \( y = 5 \) megoldásokat nyerjük.

● 7.5.11 [241] A \( \xi^2 + \psi^2 = \alpha \) egyenletet vizsgáljuk, ahol \( \alpha \) adott Gauss-egész, és \( \xi \) és \( \psi \) az „ismeretlen” Gauss-egészek.

Az egyenlet bal oldalát szorzattá bontva \( (\xi + \psi \bar{\xi})(\xi - \psi \bar{\xi}) = \alpha \) adódik, tehát
\[
\xi + \psi \bar{\xi} = \delta_1, \quad \xi - \psi \bar{\xi} = \delta_2 . \quad \text{ahol} \quad \delta_1 \delta_2 = \alpha ,
\]
Innen
\[
\xi = \frac{\delta_1 + \delta_2}{2} , \quad \psi = \frac{\delta_1 - \delta_2}{2i} ,
\]
Mivel \( \bar{\alpha} \) egység, továbbá \( \delta_1 + \delta_2 = (\delta_1 - \delta_2) + 2i \), ezért \( \xi \) és \( \psi \) pontosan akkor lesznek Gauss-egészek, ha
\[
2 \mid \delta_1 - \delta_2 . \quad (10)
\]
Legyen \( \alpha = a + bi \).

Először azokat az eseteket tekintjük, amikor alkalmas \( \delta_1 \), \( \delta_2 \) osztópárja (10) teljesül (tehát \( \alpha \) felírható \( \xi^2 + \psi^2 \) alakban).

Ha \( a \) páratlan és \( b \) páros, akkor a \( \delta_1 = \alpha, \delta_2 = 1 \) választás kielégiti (10)-et: \( 2 \mid (a - 1) + bi \).

Ha \( a \) páros és \( a \) páratlan, akkor a \( \delta_1 = \alpha/2, \delta_2 = 2 \) választás megfelel, hiszen ekkor \( \delta_1 \) és \( \delta_2 \) külön-külön is oszthatók 2-vel.

Ha \( a \) és \( b \) párosak, és közülük pontosan az egyik osztható 4-gyel, akkor \( \alpha \) kanonikus alakjában az \( 1 + i \) Gauss-prím pontosan a második hatványon szerepel, tehát
\[
\alpha = (1 + i)^2(c + di), \quad \text{ahol} \quad 1 + i \nmid c + di, \quad \text{azaz} \quad c \nmid d \quad (\text{mod} \; 2).
\]

Ekkor a
\[
\delta_1 = \frac{\alpha}{1 + i} = (c + di)(1 + i), \quad \delta_2 = 1 + i
\]
választás megfelelő. Ugyanis
\[
\delta_1 - \delta_2 = (1 + i)(c - 1 + di),
\]

594
MEGOLDÁSOK

továbbá

\[ c - 1 = d' \pmod{2} \implies 1 + i \mid c - 1 + d_i, \]

tehát \( \delta_1 - \delta_2 \) osztható \((-i)(1 + i)^2 = 2\) -vel.

Most megmutatjuk, hogy a többi esetben \( \alpha \) nem áll elő \( \xi^2 + \psi^2 \) alakban.

Ha \( a \equiv b \equiv 2 \pmod{4} \), akkor \( \alpha \) kanonikus alakjában az \( 1 + i \) Gauss-prím pontosan a harmadik hatványon szerepel. Ez azt jelenti, hogy bármely \( \delta_1, \delta_2 \) osztópárnak pontosan az egyik eleme osztható \((-i)(1 + i)^2 = 2\) -vel, tehát (10) nem teljesülhet.

Végül, ha \( b \) páratlan, akkor \( u + bi \neq (w_1 + x_2i)^2 + (y_1 + y_2i)^2 \), ugyanis a jobb oldal képzetes része páros, míg a bal oldalé páratlan.

Összefoglalva, azt láttuk be, hogy \( \alpha - u - bi \) akkor és csak akkor nem írható fel \( \xi^2 + \psi^2 \) alakban, ha \( b \) páratlan, vagy \( a \equiv b \equiv 2 \pmod{4} \).

### 7.5.17 (241)

Azt igazoljuk, hogy \( \eta \) pontosan akkor áll elő a kívánt alakban, ha \( 2\eta \) férőható három négyzeteszám összegeként. Ebből a három-négyzeteszám-tétel alapján következik, hogy azok az \( \eta \) értékek „rosszak”, amelyekre

\[ 2n = 4^{k+2} \left( 8^{m+1} - 7 \right), \quad \text{azaz} \quad n = 4^k \left( 16^{m} + 14 \right). \]

Ha \( \eta \) előáll az előírt alakban, azaz \( n = 2x^2 + y^2 + z^2 \), akkor

\[ 2n = (2x)^2 + (y + z)^2 + (y - z)^2. \]

Megfordítva, ha \( 2\eta = a^2 + b^2 + c^2 \), akkor feltehető, hogy \( a \) páros és \( b \) és \( c \) azonos paritású, és ekkor

\[ n = 2 \left( \frac{a}{2} \right)^2 - \left( \frac{b + c}{2} \right)^2 + \left( \frac{b - c}{2} \right)^2. \]

### 7.7.5 (256)(b)

A végtelen leszállás módszerét alkalmazzuk. Tegyük fel indirekt, hogy az
diofantikus egyenletnek létezik pozitív egész megoldása (megoldáson a továbbiakban mindig csak pozitív egész megoldást fogunk érteni), és tekintsük azt az \( z_0 \), \( y_0 \), \( z_0 \) megoldást, ahol \( 2\eta \) minimális.

Megmutatjuk, hogy létezik egy olyan \( z_1 \), \( y_1 \), \( z_1 \) megoldás, amelyre \( z_1 < z_0 \), és ez ellentmond \( z_0 \) minimalitásának.

Ha \( (x_0, y_0, z_0) = d' > 1 \), akkor

\[ \begin{align*}
\frac{x_0}{d'} & = \frac{y_0}{d'} = \frac{z_0}{d'}
\end{align*} \]

is kielégíti (11)-et, és \( \frac{z_0}{d'} \) ellenmond \( z_0 \) minimalitásának.

Ebből következik, hogy \( x_0 \), \( y_0 \) és \( z_0 \) relatív prímek, és a szokásos módon igazolható, hogy páronként is relatív prímek.

A fentieken alapján \( z_0^2 \), \( y_0^2 \) és \( z_0 \) primitív pitagoraszi számhármasat alkotnak. Ezért

595
ahol
\[ m > n > 0, \quad (m, n) = 1 \quad \text{és} \quad m \neq n \pmod{2}. \]

A (12b) egyenletet modulo 4 vizsgálva kapjuk, hogy az \( m \) és \( n \) közül most \( m \) a páratlan és \( n \) a páros; \( n = 2n_1 \). Ezt (12a)-ba beírva kapjuk, hogy

\[ \left( \frac{x_0}{y_0} \right)^2 = mn_1, \quad \text{ahol} \quad (m, n_1) = 1. \]

Ebből következik, hogy

\[ m = u^2 \quad \text{és} \quad n_1 = v^2, \quad \text{ahol} \quad (u, v) = 1. \quad (13) \]

A (13)-at (12b)-be beírva kapjuk, hogy

\[ y_0^2 = (u^2)^2 - (2v^2)^2, \]

azaz \( y_0, 2v^2 \) és \( u^2 \) primitív pitagoraszi számnáramast alkot. Ebből következik, hogy

\[ 2v^2 = 2\tau s \quad \text{és} \quad u^2 = r^2 + s^2 \quad (14a), \]

\[ (r, s) = 1. \] A (14a)-ból így azt nyerjük, hogy \( r = t^2, \quad s = u^2, \) és ekkor (14b) átírható az

\[ u^2 = t^4 + u^4 \]

alakba. Ez azt jelenti, hogy \( x_1 = t, \quad y_1 = u^2, \quad z_1 = u \) megoldása (11)-nek, továbbá (12c) és (13) alapján

\[ z_0 = m^2 + n^2 > m = u^2 \geq u = z_1, \]

ami ellentmond \( z_0 \) minimalitásának.

7.7.7 [256] Legyen a számrendszer alapszáma \( \varpi \). Ekkor az

\[ x^3 + x^2 + x + 1 = \varpi^2 \quad (15) \]

diofantikus egyenlet olyan megoldásait kinogni, ahol \( \varpi \geq 2 \). Bebizonyítjuk, hogy az egyetlen ilyen megoldás \( \varpi = 7, \quad \varpi = 2 \). (Könnyen látható, hogy \( x \leq 1 \) esetén csak az \( x = 0 \) és \( x = 1 \) értékekből kapunk egész megoldást.)

A (15) bal oldalát szorzattá bontva

\[ (x + 1)(x^2 + 1) = \varpi^2 \quad (16) \]

adódik. Jelöljük a (16) bal oldalán szereplő két tényező legnagyobb közös osztóját \( h \)-val, ekkor

\[ h \mid (x^2 + 1) - (x + 1)(x - 1) = 2. \quad \text{tehát} \quad h = 1 \text{ vagy } 2. \]

596
MEGOLDÁSOK

Ha \( \hat{u} = 1 \), akkor \( x^2 + 1 \) (és \( u + 1 \) is) négyzetszám: \( x^2 + 1 = z^2 \). Ez azonban (\( x \neq 0 \) miatt) lehetetlen.

A \( \hat{u} = 2 \) esetben

\[
x + 1 = 2u^2 \quad \text{és} \quad x^2 + 1 = 2u^2 \quad (u > 1, v > 1).
\]  \( (17) \)

Az első egyenletből \( x = 2u^2 - 1 \), ezt a második egyenletbe beírva kapjuk, hogy

\[
(2u^2 - 1)^2 + 1 = 2v^2.
\]  \( (18) \)

(18)-ból átrendezés és 2-vel való osztás után

\[
(2u^2 - 1)^2 + 1 = 2v^2
\]  \( (19) \)

adódik. A (19) egyenletből \( u > 1, v > 0 \) és \( (2u^2 - 1)^2 + 1 \) alapján következik, hogy

\[
\begin{align*}
u^2, \quad u^2 - 1 & \quad \text{és} \quad v
\end{align*}
\]

primitív pitagorasi számhármas alkotnak. Innen azt nyerjük, hogy (a „szokásos” tulajdonságú alkalmas \( n \) és \( u \) egészkekkel) vagy

\[
u^2 = n^2 - u^2
\]  \( (20a) \)

és

\[
u^2 - 1 = 2mn.
\]  \( (20b) \)

vagy pedig fordított szereposztással

\[
u^2 = 2mn
\]  \( (21a) \)

és

\[
u^2 - 1 = 2n^2 - u^2
\]  \( (21b) \)

teljesül.

Nézzük először a (20a)–(20b) esetet. A (20a) egyenlet és \( (m, n) = 1 \) alapján \( u \), \( v \) és \( m \) primitív pitagorasi számhármas. Mivel a feltételek szerint \( \hat{u} \) páratlan, ezért

\[
u = r^2 - s^2, \quad u = 2rs \quad \text{és} \quad m = r^2 + s^2.
\]

Ebből következik, hogy

\[
\begin{align*}
\tau n - n = (r - s)^2.
\end{align*}
\]  \( (22) \)

A (20a) egyenletből (20b)-t kívonva

\[
\tau n^2 - n^2 - 2mn = 1, \quad \text{azaz} \quad (\tau n - n)^2 - 2n^2 = 1
\]  \( (23) \)

adódik. (22) alapján (23) átírható a következő alakba:

\[
(r - s)^4 - 1 = 2n^2.
\]  \( (24) \)
Bontsuk (24) bal oldalát szorzattá:

\[(r-s)^2 + 1 = 2n^2. \quad (25)\]

A (25) bal oldalán a két tényező különbsége 2, mindkét tényező páros, így a legnagyobb közös osztójuk 2. Mivel egy páratlan szám négyzete 4-gyel osztva 1 maradékot ad, ezért az első tényező (páros, de) 4-gyel már nem osztható. Mindebből következik, hogy

\[(r-s)^2 + 1 = 2r^2 \quad \text{és} \quad (r-s)^2 - 1 = w^2.\]

Ez utóbbi azonban ( \(w \neq 0\) miatt) lehetetlen. Ezzel beláttuk, hogy a (20a)–(20b) eset nem valósulhat meg.

Rátérve a (21a)–(21b) esetre, most \(ut\) páros, és így (21b) modulo 4 vizsgálatából kapjuk, hogy szükségképpen \(ut\) páros és \(n\) páratlan. Mivel \(\mathbf{\langle cm,n \rangle} = 1\), ezért (21a)-ből következik, hogy

\[\mathbf{m} = 2a^2, \quad n = b^2, \quad \text{és így} \quad u^2 = 4a^2b^2. \quad (26)\]

A (26)-ot (21b)-be beírva a

\[4a^2b^2 - 1 = 4a^4 - b^4\]

eyenlethez jutunk, amelyből átrendezés után

\[(2a^2 + b^2)^2 - 1 = 8a^4 \quad (27)\]

adólik. A (27) bal oldalát szorzattá bontva a két tényező páros és különbségük 2, tehát a legnagyobb közös osztójuk 2. Igé az alábbi két lehetőség van:

\[2a^2 + b^2 + 1 = 2a^2 \quad \text{és} \quad 2a^2 + b^2 - 1 = 4d^1, \quad (28)\]

vagy

\[2a^2 + b^2 + 1 = 4d^1 \quad \text{és} \quad 2a^2 + b^2 - 1 = 2c^1. \quad (29)\]

A (28)-beli két egyenletet egymásból kivonva 2-vel való osztás után

\[c^4 - 2d^4 = 1\]

adólik. A 7.3.13g feladat [227] szerint ebből \(d = 0\) következik, ami most nem lehetséges.

(29)-ből hasonló módon a

\[c^4 - 2d^4 = -1\]

eyenletet kapjuk. A 7.7.6 feladat [256] szerint ekkor \(c = \pm 1, \ d = \pm 1\). Ezt (29)-be visszairva kapjuk, hogy \(2a^2 + b^2 = 3\), ahonnan \(a^2 = b^2 = 1\). Igé (26) alapján \(u^2 = 4\), és végül (17) miatt \(x = 7\).

7.7.10 [257](a) Tegyük fel először, hogy az

\[x^2 + 3y^2 = n \quad (30)\]
diofantikus egyenlet megoldható, legyen \(x = a, \ y = b\) egy megoldás. Ekkor
megoldása az
\[ x^2 - 3xy + y^2 = \epsilon \] (31)
diofantikus egyenletnek.

Legyen most \( x = c \), \( y = d \) megoldása (31)-nek. Ha van olyan \( a \), \( b \) egész szám, amelyre
\[ c = a + b \]
\[ d = 2b, \] (32)
akkor az előző gondolatmenet megfordításával kapjuk, hogy \( x = c \), \( y = b \) megoldása (30)-nak.

(32) pontosan akkor teljesül, ha \( d \) páros. Mivel az \( x^2 - 3xy + y^2 \) egyenlet \( x \)-ben és \( y \)-ban szimmetrikus, ezért az is megfelel, ha \( c \) páros. Végül, ha \( c \) és \( d \) is páratlan, akkor
\[ x = c + d \]
\[ y = -d \] is megoldása (31)-nek, és itt \( c - d \) már páros.

Természetesen a fentieket az Euler-egészek felhasználása nélkül, „trükkös” átalakítások formájában is el lehet mondani.

7.7.11 [257] A 7.5.10 feladat [241] megoldásának gondolatmenetét követjük. Az
\[ x^2 + 243 = y^3 \] (33)
eyenlet bal oldalát az Euler-egészek körében szorzattá bonthatjuk:
\[(x + 9i\sqrt{3})(x - 9i\sqrt{3}) = y^3. \] (34)

Legyen
\[ \alpha = x + 9i\sqrt{3} = z + 9 + 18a, \]
ekkor \( \bar{\alpha} = x - 9i\sqrt{3}. \)

Belátjuk, hogy \( \alpha \) és \( \bar{\alpha} \) egy-egy köbszám egységszerese (köbszámokon most Euler-egészek köbét értjük).

Legyen \( \delta = (\alpha, \bar{\alpha}) \), ekkor \( \delta \) osztója az
\[ \alpha - \bar{\alpha} = 18i\sqrt{3} = 2(\sqrt{3})^3 \]
Euler-egésznek.

A (33) egyenlet modulo 8 vizsgálatából adódik, hogy \( \alpha \) szükségképpen páros, tehát \( 2 | \alpha + 9 \), és így \( 2 \nmid \alpha \). Ebből következik, hogy a 2 Euler-prím nem osztója \( \delta \)-nak, vagyis
\[ \delta = \pi^r, \]
ahol \( \pi = \sqrt{3} \)
\[ 0 \leq r \leq 5. \]

Mivel
A fentiektől elvétve az alábbi számpárok a megoldásai:

\((3, 2); \quad (3, 1); \quad (-1, 2); \quad (-1, -3); \quad (-2, 1); \quad (-2, -3)\).

A fentiek alapján

\[
\alpha = x + 9 + 18\omega = \varepsilon(c + d\omega)^3. \tag{35}
\]

Mivel \(\varepsilon = 1\) köbszám, ezért (35)-öt elég az \(\varepsilon = 1, \varepsilon\) és \(\omega^2\) esetekben megvizsgálni.

A \(\varepsilon = 1\) esetben \(\omega^3 = 1\) és \(\omega^2 = -1 - \omega\) figyelembevételével kapjuk, hogy

\[
(c + d\omega)^3 = c^3 + 3c^2d\omega + 3cd^2\omega^2 + d^3\omega = c^3 + d^3 + 3\varepsilon d^2 - (3c^2d - 3\varepsilon d^2)\omega.
\]

Ekkor (35)-ben az „\(\omega\) -mentes rész”, illetve \(\omega\) együthatóit összehasonlítva

\[
x + 9 = c^3 + d^3 - 3\varepsilon d^2 \tag{36a}
\]
\[
18 = 3c^2d - 3\varepsilon d^2 \tag{36b}
\]

adódik. (36b) ekvivalens a \(c^3 - d^3 = 6\) diofantikus egyenlettel, amelynek az alábbi \((c, d)\) számpárok a megoldásai:

\((3, 2); \quad (3, 1); \quad (1, 2); \quad (-1, -3); \quad (-2, 1); \quad (-2, -3)\).

Ezeket (36a)-ba behelyettesítve az \(x = \pm 10\) értékeket kapjuk, és ekkor (33) szerint \(y = 7\).

A \(\varepsilon = \omega\) esetben teljesen hasonlóan (36b) helyett a

\[
18 = c^3 + d^3 - 3\varepsilon d^2 \tag{37}
\]
diofantikus egyenlethez jutunk. Megmutatjuk, hogy ennek nincs megoldása.

Vizsgáljuk (37)-et modulo 3. A kis Fermat-tétel szerint bármely \(a\) -ra \(a^3 \equiv e \pmod{3}\), így

\[
0 \equiv c^3 + d^3 \equiv c + d \pmod{3}.
\]

Ha \(3 \mid c\), akkor \(3 \mid d\), és így (37) jobb oldala osztható 27-tel, a bal oldal viszont nem.

Egyébként \(c = 3r + 1\) és \(d = 3s - 1\), vagy fordítva, és így

\[
c^3 + d^3 = (3r + 1)^3 + (3s - 1)^3 = 27(r^3 + s^3 + r^2 - s^2) + 9(r + s),
\]

tehát a (37) átrendezésével kapott
egyenlet jobb oldala osztható 9-cel, a bal oldal viszont nem.

Ezzel beláttuk, hogy a (37) diofantikus egyenlet nem oldható meg.

Végül az $\varepsilon = \omega^2$ eset (37) helyett a

$$18 = -c^3 - d^5 + 3cd^2$$

diofantikus egyenletre vezet, amelyről az előzővel egyező módon látható be, hogy nincs megoldása.

Összefoglalva, azt kaptuk, hogy az $x^2 + 243 = y^3$ diofantikus egyenlet összes megoldása: $x = \pm 10, y = 7$.

8. Diofantikus approximáció

8.1.8 [276][c] Megmutatjuk, hogy egy $\vartheta$ valós szám akkor és csak akkor írható fel $h(\alpha) = \{\alpha\}^2 - \{\alpha^2\}$ alakban, ha $-1 < \varepsilon < 1$.

A szükségesség azonnal adódik abból, hogy bármely $c$-re $0 \leq \varepsilon < 1$.

Az elégségességhez legyen $0 \leq \hat{\vartheta} < 1$, $k$ pozitív egész és $\alpha = k + \hat{\vartheta}$.

Ekkor

$$\{\alpha\}^2 = n^2 \quad \text{és} \quad \{\alpha^2\} = \{\vartheta^2 + 2k\vartheta\}. \quad (1)$$

Ha

$$0 \leq \vartheta^2 + 2k\vartheta < 1, \quad \text{azaz} \quad 0 \leq \vartheta < -k + \sqrt{k^2 + 1}, \quad (2)$$

akkor (1) alapján

$$h(\alpha) = \{\alpha\}^2 - \{\alpha^2\} = \vartheta^2 - \{\vartheta^2 + 2k\vartheta\} = \vartheta^2 - \{\vartheta^2 + 2k\vartheta\} = -2k\hat{\vartheta}. \quad (3)$$

Figyelembe véve (2)-t

$$0 \geq -2k\hat{\vartheta} > -2k(-k + \sqrt{k^2 + 1}) \quad (4)$$

adódik. Ekkor (3) és (4) alapján a $h(\alpha) = -2k\hat{\vartheta}$ értékek között a

$$\left(-2k(k + \sqrt{k^2 + 1}), 0\right)$$

intervallum minden pontja előfordul. Mivel

$$-2k(k + \sqrt{k^2 + 1}) = \frac{-2k}{k + \sqrt{k^2 + 1}} = \frac{-2}{1 + \sqrt{1 + k^{-2}}} \to -1, \quad \text{ha} \quad k \to \infty,$$

ezért a $h(\varepsilon)$ értékek a teljes $(-1, 0]$ intervallumot kiadják.

Ha az előző gondolatmenetet (2) helyett a

$$2k \leq \hat{\vartheta}^2 + 2k\vartheta < 2k + 1, \quad \text{azaz} \quad -k + \sqrt{k^2 + 2k} \leq \hat{\vartheta} < 1$$

601
feltételt kielégítő $v$ -kra megismételjük, akkor azt kapjuk, hogy a $\tilde{u}(\alpha)$ értékek között a $[0,1]$ intervallum minden eleme is fellép.

- **8.3.5 [287]** A L 8.3.4 Lemma (8a), (8b) és (10) képletei alapján
  \[
  \tau_n s_{n-2} - \tau_{n-2} s_n = (c_n r_{n-1} + \tau_{n-2}) s_{n-2} - \tau_{n-2} (c_{n-1} s_{n-1} + s_{n-2}) =
  
  c_n (r_{n-1} s_{n-2} - \tau_{n-2} s_{n-1}) = (-1)^n c_n.
  \]
  Ezt $\sigma_n s_{n-2}$-vel osztva a feladat állítását kapjuk.

- **8.3.6 [287]** A feltétel szerint
  \[
  \alpha = L(c_0, c_1, \ldots, c_{M-1}, c_{M-k+1}, \ldots, c_M), c_{M-k+1}, \ldots, c_M, c_M, \ldots).
  \]
  Legyen
  \[
  \beta = L(c_{M-k}, \ldots, c_M), c_{M-k+1}, \ldots, c_M, \ldots)
  \]
  Ekkor
  \[
  \alpha = L(c_0, c_1, \ldots, c_{M-k}, \beta) \quad \text{és} \quad \beta = L(c_{M-k+1}, \ldots, c_M, \beta).
  \]
  Ezeket az „emeletes törteket kifejtve”
  \[
  \alpha = \frac{\nu_1 \beta + \nu_2}{\nu_3 \beta + \nu_4}, \quad \text{illetve} \quad \beta = \frac{\nu_5 \beta + \nu_6}{\nu_7 \beta + \nu_8}
  \]
adóik, ahol az $u_k$ -k alkalmas egész számok. Az első egyenlőségből fejezzük ki $\beta$ -t $\alpha$ segítségével, és ezt helyettesítsük be a második egyenlőségbe. Ekkor átrendezés után egy olyan egész együtthatós másodfokú egyenlethez jutunk, amelynek az $\alpha$ gyöke. (Mivel végig a lánctörtről van szó, ezért az $\alpha$ iracionális, és így elsőfokú egész együtthatós egyenletnek nem lehet gyöke.)

- **8.4.1 [290](a)** Mivel $\left(1 + \sqrt{2}\right)^n - \left(1 - \sqrt{2}\right)^n$ egész szám és $\lim_{n \to \infty} \left(1 + \sqrt{2}\right)^n = 0$, ezért páros $n$ -re az $\left\{1 + \sqrt{2}\right\}$ törtrészek (réz) sorozata 1-hez, páratlan $n$ -re pedig 0-hoz tart, és így nem lehet mindenütt sűrű $[0,1]$ -ben.

- **(b)** A sorozat szomszédos elemeinek a különbsége 0-hoz tart:
  $$\sqrt{n} + 1 - \sqrt{n} = \frac{1}{\sqrt{n} + 1 + \sqrt{n}} \to 0, \quad \text{ha} \quad n \to \infty.$$
  Ezért a szomszédsos elemek törtrészének a különbsége is 0-hoz tart, kivéve, amikor a törtrész „visszaugrik” az 1 közeléből a 0 közelébe. Ebből következik, hogy a törtrészek mindenütt sűrűek $[0,1]$ -ben.

- **(c)** Mivel
  $$\left\{\sqrt{n^2 + 1}\right\} = \sqrt{n^2 + 1} - n = \frac{1}{\sqrt{n^2 + 1} + n} \to 0, \quad \text{ha} \quad n \to \infty,$$
  ezért $\left\{\sqrt{n^2 + 1}\right\}$ nem lehet mindenütt sűrű $[0,1]$ -ben.

- **(d)** Mivel
  $$\sqrt{2n^2 + 1} - n\sqrt{2} \to 0, \quad \text{ha} \quad n \to \infty,$$
MEGOLDÁSOK

és \( \left\{ n\sqrt{2} \right\} \) a T 8.4.1 Tétel szerint mindenütt sűrű \([0, 1]\) -ben, ezért \( \left\{ \sqrt{2n^2 + 1} \right\} \) is mindenütt sűrű \([0, 1]\) -ben.

- **(e)** A szinuszfüggvény periodikussága miatt a sorozat csak véges sok (181) különböző értéket vesz fel, ezért a törtrészek sorozata nem lehet mindenütt sűrű \([0, 1]\) -ben.

- **(f)** Mivel \( \pi \) irracionalitása miatt az \( 1/(2\pi) \) arány is irracionalis, ezért az (ivmértékekben mért) \( \tau \) szögek a T 8.4.1 Tétel szerint mindenütt sűrűn helyezkednek el az egységkörön. A szinuszfüggvény folytonossága miatt ezért a súlyú értékek is mindenütt sűrűek a szinuszfüggvény \([-1, 1]\) értékészletében, és így a törtrészek mindenütt sűrűek \([0, 1]\) -ben.

- **(g)** Mivel

\[
\log(u + 1) - \log u - \log \left( 1 + \frac{1}{\tau^2} \right) \to 0, \quad \text{ha} \quad u \to \infty,
\]

ezért a (b) részénél adott indoklás szerint a törtrészek sorozata mindenütt sűrű \([0, 1]\) -ben.

- **8.4.3 [290]** Induljunk ki abból, hogy a \( P_\alpha = \left\{ \left\{ n\alpha_1 \right\}, \left\{ n\alpha_2 \right\}, \ldots, \left\{ n\alpha_k \right\} \right\} \) pontok mindenütt sűrűek, vagyis a \( k \) -dimenziós egységkocka bármely \( \alpha \)-hoz létezik olyan \( n \), hogy

\[ \left| \frac{n\alpha_j - v_j}{\tau_j} \right| < \varepsilon, \quad j = 1, 2, \ldots, k, \]

vagyis alkalmaz \( \tau_j \) egészekre

\[
\left| n\alpha_j - v_j - \tau_j \right| < \varepsilon, \quad j = 1, 2, \ldots, k. \tag{7}
\]

Azt kell igazolnunk, hogy az \( 1, \alpha_1, \ldots, \alpha_k \) számok lineárisan függetlenek. Indirekt bizonyítunk: fel tesszük, hogy léteznek olyan nem csupa nulla \( \theta_1, \ldots, \theta_k \) racionalis számok, amelyekre

\[ \varepsilon_0 + \varepsilon_1 \alpha_1 + \cdots + \varepsilon_k \alpha_k = 0. \tag{6}
\]

A (6) egyenlőséget a \( \varepsilon_j \)-k nevezőinek legkisebb közös többszörössévé beszorozva elérhető, hogy (6) egész \( \varepsilon_j \)-kkel is teljesüljön.

A megoldás kulcsa az, hogy az (5) alapján „kicsi” abszolút értékű \( n\alpha_j - v_j - \tau_j \) számoknak és \( \theta = n \cdot 1 - \nu \)-nek a \( \theta_1, \ldots, \theta_k \varepsilon_j \)-számokkal vett lineáris kombinációja is kicsi abszolút értékű lesz:

\[ |c_1(n\alpha_1 - v_1 - \tau_1)| + \sum_{j=1}^{k} |c_j(n\alpha_j - v_j - \tau_j)| < \varepsilon \sum_{j=1}^{k} |\tau_j| = \varepsilon'. \tag{7}
\]

Másrészt (7) bal oldala az abszolút érték nélkül

\[ n(c_0 + \sum_{j=1}^{k} c_j \alpha_j) - \sum_{j=1}^{k} c_j v_j - M \tag{8}
\]

alakba írható, ahol \( M \) egész szám. A (6), (7) és (8) alapján

\[ \sum_{j=1}^{k} c_j v_j + M \leq \varepsilon',
\]

603
adódnak, tehát
\[
\sum_{j=1}^{k} r_j \geq \varepsilon' \quad \text{vagy} \quad \sum_{j=1}^{k} c_j \geq 1 - \varepsilon'.
\]

Ez tetszőleges \( n_1, \ldots, n_k \) esetén nyilván lehetetlen, és így ellentmondásra jutottunk.

9. Algebrai és transzcendens számok

- **9.2.8 [298]** A feltétel szerint \( f \neq 0 \), továbbá \( f \) -nek létezik gyöke, tehát \( f \) nem lehet (nemnulla) konstans polinom.

Tegyük fel indirekt, hogy \( f \) irreducibilis \( \mathbb{Q} \) felett. Ekkor \( f \) a gyökei minimálpolinomja, azaz

\[
f = m_\alpha = m_\beta.
\]

Mivel \( g(\alpha) = 0 \), ezért \( m_\alpha = f \mid g \). Ekkor viszont \( f \) minden gyöke \( g \) -nek is gyöke, tehát \( g(\beta) = 0 \).
Az így kapott ellentmondás bizonyítja, hogy \( f \) reducibilis \( \mathbb{Q} \) felett.

(A feltételek ből \( g \) reducibilitására vagy irreducibilitására nem tudunk következtetni, mindkét eset megvalósulhat.)

- **9.3.6 [302]** Tegyük fel, hogy \( r \) és \( \cos \varphi \) algebrai. Ekkor \( \sin \varphi = \pm \sqrt{1 - \cos^2 \varphi} \) és \( i \) is algebrai, tehát az \( r \), \( \cos \varphi \), \( \sin \varphi \) és \( i \) számokból az összeadás és szorzás segítségével képzett \( \alpha \) is algebrai.

Megfordítva, tegyük fel, hogy \( \alpha \) algebrai. A T 9.3.3 Tétel alapján ekkor \( r \cos \varphi \) és \( r \sin \varphi \) is algebrai.
Innen \( r = \sqrt{(r \cos \varphi)^2 + (r \sin \varphi)^2} \) is algebrai. Ezt felhasználva kapjuk, hogy \( \cos \varphi = (r \cos \varphi)/r \) is algebrai.

- **9.4.1 [307]** (a) Legyen \( \tilde{h} = a/b \), ahol \( b > 0 \) és \( \alpha \) egész számok. Mivel \( \alpha \) Liouville-szám, ezért tetszőleges \( n \) -hez létezik olyan \( \tilde{f} \) tört, amelyre

\[
|\alpha - \tilde{f} b| < \frac{1}{s^2n}.
\]

A már többször alkalmazott meggondolás szerint \( n \to \infty \) mellett a megfelelő \( s \) értékek is a végtelemhez tartanak, így feltehetjük, hogy \( s > b \).

Az (1) egyenlőtlenség átírható

\[
|\tilde{h} - a/b| - \left( \frac{\alpha}{b} - \frac{r}{s} \right) < \frac{1}{s^2n}
\]

alakba, és így az \( s > b \) feltételt is felhasználva

\[
|\tilde{h} + \alpha| - \frac{as + br}{ls} < \frac{1}{s^2n} < \frac{1}{(ls)^2}
\]

adódik. Ez azt jelenti, hogy az

\[
\frac{R}{S} = \frac{as - br}{ls}
\]
törtre

\[ \left| h \cdot \alpha - c \right| - \frac{R}{S} \leq \frac{1}{S^n} \]

teljesül. Ezzel beláttuk, hogy \(h + \alpha\) Liouville-szám.

- (a2) A \(h\alpha\) -ra vonatkozó állítást az előzőekhez hasonlóan igazolhatjuk.

- (a3) Megmutatjuk, hogy ha \(\tau / s\) „jól” közelíti \(\alpha\) -t, akkor \((\tau / s)^h\) „majdnem ilyen jól” közelíti \(\alpha^k\) -t. Induljunk ki az

\[ \alpha^k - \left( \frac{\tau}{s} \right)^k = \left( \alpha - \frac{\tau}{s} \right) \left( \alpha^{k-1} + \alpha^{k-2} \left( \frac{\tau}{s} \right) + \cdots + \left( \frac{\tau}{s} \right)^{k-1} \right) \]  

azonosságból. Ha \(\tau / s\) (bármilyen értelmen) közel van \(\alpha\) -hoz, akkor (2) második tényezőjének értéke közel van \(k\alpha^{k-1}\) -hez, tehát abszolút értékbén egy csak az \(\alpha\) -tól és \(\kappa\) -tól függő \(c\) korlát alatt marad. Ebből következik, hogy ha

\[ \left| \alpha - \frac{\tau}{s} \right| < \frac{1}{ck^\alpha}, \quad (3) \]

akkor

\[ \left| \alpha^k - \frac{\tau^k}{s^k} \right| < \frac{c}{(s^k)^{n}}. \quad (4) \]

Mivel \(\alpha\) Liouville-szám, ezért (3), és így (4) is tetszőleges \(\nu\) -re elérhető, azaz \(\alpha^k\) is Liouville-szám.

- (a4) Azt fogjuk igazolni, hogy ha \(\tau / s\) „jól” közelíti \(\alpha\) -t, akkor \(\tau / r\) „jól” közelíti \(1 / \nu\) -t. (Ha \(\tau < \Theta\), akkor \(\tau / r\) helyett a \((-\tau) / (-\nu)\) alakot vesszük.)

Az (1) egyenlőtlenség

\[ |\nu \alpha - r| < \frac{1}{s^{2n-1}} \]

alakját felhasználva

\[ \left| \frac{1}{\nu \alpha} - \frac{\tau}{s^\nu} \right| = \left| \frac{s - \nu \tau}{\nu \alpha \tau} \right| < \frac{1}{s^{2n-1} |\nu \alpha \tau|} \]

adódik (nyilván feltehető \(\nu \neq 0\)). Tudjuk, hogy ha \(\nu \to \infty\), akkor a megfelelő \(s\) értékek végletenhez és az \(\tau / s\) törték \(\alpha\) -hoz tartanak, ezért feltehető, hogy

\[ \left| \frac{\tau}{s} \right| < |\alpha| + 1 < s \quad \text{és} \quad s |\alpha| \geq 1. \]  

Az (5) és (6) egyenlőtlenségekből kapjuk, hogy

\[ \left| \frac{1}{\alpha} - \frac{s}{\tau} \right| < \frac{1}{|\tau|^\alpha}, \quad (7) \]

Mivel \(\alpha\) Liouville-szám, ezért (1), és így (7) is tetszőleges \(\nu\) -re elérhető, azaz \(1 / \alpha\) is Liouville-szám.
9.4.4 [308] Tegyük fel indirekt, hogy egy \( \alpha \) komplex szám többszörös gyöke az \( \bar{f} \) polinomnak. Ekkor \( \alpha \) gyöke az \( \bar{f} \) deriváltjának, \( \bar{f}' \)-nek is. Mivel \( \bar{f} \) irreducibilis \( \mathbb{Q} \) felett, ezért \( \bar{f} \) az \( \alpha \) (egyik) minimálpolinomja. Így \( \bar{f}'(\alpha) = 0 \)-ból következik, hogy \( f \mid \bar{f}' \). Ez azonban \( \bar{f}' \neq 0 \) és \( \deg \bar{f}' < \deg \bar{f} \) miatt lehetetlen.

9.6.5 [316](a) Az állítás igaz. Tegyük fel indirekt, hogy \( \bar{f} \) minden gyöke algebrai egész, azaz \( \bar{f} \) gyöktényezős alakja \( \mathbb{C}[x] \)-ben

\[
f = (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n),
\]

ahol mindegyik \( \alpha_j \) algebrai egész. A szorzást elvégezve kapjuk, hogy az \( \bar{f} \) együtthatói az \( \alpha_j \)-kből összeadás, kivonás és szorzás segítségével állnak elő. Mivel az algebrai egészek gyűrűt alkotnak, így \( \bar{f} \) minden együtthatója algebrai egész. Az együtthatók egyen racionális számok is, tehát szükségképpen egész számok, ami ellentmond az \( \bar{f} \)-re vonatkozó feltételnek.

(b) Az állítás hamis. Például az

\[
f = (x^2 - 6)(x^2 - 1/2) = x^4 - 13/2x^2 + 3
\]
polinom normált, racionális együtthatós, nem minden együtthatója egész, és mégis van olyan gyöke, a \( \sqrt[3]{6} \) (és a \( -\sqrt[3]{6} \)), amely algebrai egész.

(c) Az állítás igaz. Mivel \( \bar{f} \) irreducibilis \( \mathbb{Q} \) felett, ezért valamennyi gyökeinek minimálpolinomja. A D 9.6.1 Definíció alapján így egyik gyök sem lehet algebrai egész.

(d) Az állítás igaz. Legyen \( \alpha \) az \( \bar{f} \) polinom egyetlen olyan gyöke, amely nem algebrai egész. Mivel \( \bar{f}'(\alpha) = 0 \), ezért \( m_\alpha \mid \bar{f} \), és így \( m_\alpha \) minden gyöke \( \bar{f} \)-nek is gyöke. Az \( m_\alpha \) egyik gyöke sem algebrai egész, továbbá \( m_\alpha \)-nak (a 9.4.4 feladat [308] szerint) nem lehet többszörös gyöke, ezért a feladat feltétele csak úgy teljesülhet, ha \( m_\alpha \) elsőfokú. Ez azt jelenti, hogy \( \alpha \) racionális szám, tehát \( \bar{f} \)-nek valóban létezik racionális gyöke.

10. Algebrai számtestek

10.2.5 [325](a) Legyen \( \alpha = \sqrt[3]{7} + 3i \) és \( M = \mathbb{Q}(\alpha) \), ekkor \( \deg \alpha = \deg(M : \mathbb{Q}) \).

Tekintsük a következő bővítésláncot:

\[
\mathbb{Q} \subseteq K \subseteq L, \quad \text{ahol} \quad K = \mathbb{Q}(\sqrt[3]{7}) \quad \text{és} \quad L = K(i). \quad (1)
\]
Belátjuk, hogy \( M = L \) és így \( \deg \alpha \) meghatározásához az \( L : \mathbb{Q} \) bővítés fokát kell meghatározunk.

Az \( L \) definíciója alapján \( \sqrt[3]{7} \in L \) és \( 3i \in L \), továbbá \( L \) test, ezért \( \alpha = \sqrt[3]{7} + 3i \in L \), és így \( M \subseteq L \).

A másik irányú, \( L \subseteq M \) tartalmazásához azt kell igazolni, hogy \( \sqrt[3]{7} \in M \) és \( 3i \in M \). Mivel

\[
(\sqrt[3]{7} - 3i)(\sqrt[3]{7} + 3i) = 16, \quad \text{azaz} \quad m = \frac{16}{\alpha},
\]
ezért \( m \in M \), tehát
Rátérve \( \text{deg}(L : \mathbb{Q}) \) meghatározására, megmutatjuk, hogy az (1) bővítésláncban mindkét láncszem foka 2. Nyilván \( \text{deg}(K : \mathbb{Q}) = \text{deg}(\sqrt{7}) = 2 \). Mivel \( L \neq K \) (hiszen \( K \) minden eleme valós, \( L \) viszont tartalmazza az \( \sqrt{7} \)-t), ezért \( \text{deg}(L : K) \geq 2 \). Ugyanakkor \( \text{deg}(L : K) = \text{deg}_K \sqrt{7} \leq \text{deg}\sqrt{7} = 2 \), tehát valóban \( \text{deg}(L : K) = 2 \).

Ezután a fokszámtételből következik, hogy
\[
\text{deg}_{K} = \text{deg}(L : \mathbb{Q}) = \text{deg}(K : \mathbb{Q}) \cdot \text{deg}(L : K) = 4.
\]

- **10.2.7 [326]** Jelöljük \( Q(\sqrt{7}) \) valós elemeinek halmazát \( V \)-vel: \( V = Q(\sqrt{7}) \cap \mathbb{R} \).

  **(a)** Mivel \( \sqrt{7} = \sqrt{3}(\cos 144^\circ - i \sin 144^\circ) \) gyöke az \( x^5 - 3 \), a racionális test felett irreducibilis polinomnak, ezért \( Q(\sqrt{7}) \) bővítés foka 5.

  Tekintsük a \( \mathbb{Q} \subseteq V \subseteq Q(\sqrt{7}) \) bővitésláncot. A fokszámtétel alapján
\[
5 = \text{deg}(Q(\sqrt{7}) : \mathbb{Q}) = \text{deg}(Q(\sqrt{7}) : V) \cdot \text{deg}(V : \mathbb{Q}),
\]
és így \( \text{deg}(Q(\sqrt{7}) : V) = 1 \) vagy 5. Mivel \( V \) csak valós számokból áll, \( Q(\sqrt{7}) \) pedig tartalmaz nem valós komplex számokat is, ezért \( Q(\sqrt{7}) \neq V \). Ebből következik, hogy \( \text{deg}(Q(\sqrt{7}) : V) = 1 \), vagyis csak \( \text{deg}(Q(\sqrt{7}) : V) = 5 \) lehetséges. Ekkor \( \text{deg}(V : \mathbb{Q}) = 1 \), azaz \( V = \mathbb{Q} \).

  **(b)** Megmutatjuk, hogy \( V = Q(\sqrt[5]{3}) \).

Mivel \( \sqrt[5]{3} \) valós és
\[
\sqrt[5]{3} = -\left(i\sqrt[5]{3}\right)^2 = -\sqrt[5]{3} \in Q(\sqrt{7}),
\]
ezén \( Q(\sqrt{3}) \subseteq V \).

Tekintsük a
\[
\mathbb{Q} \subseteq Q(\sqrt[5]{3}) \subseteq V \subseteq Q(\sqrt{7})
\]
bővitésláncot.

Mivel \( \sqrt[5]{3} = i\sqrt[5]{3} \) gyöke az \( x^6 + 3 \), a racionális test felett irreducibilis polinomnak, ezért \( \text{deg}(Q(\sqrt[5]{3}) : \mathbb{Q}) = 6 \).

Hasonlóan adódik, hogy \( \text{deg}(Q(\sqrt[5]{3}) : \mathbb{Q}) = 3 \).

Így a fokszámtételelt a (2) bővitésláncra alkalmazva kapjuk, hogy
\[
2 = \text{deg}(Q(\sqrt[5]{3}) : Q(\sqrt[5]{3})) = \text{deg}(Q(\sqrt{7}) : V) \cdot \text{deg}(V : Q(\sqrt[5]{3})).
\]
Az (a) résznel látott módon adódik, hogy \( Q(\sqrt{7}) \neq Q(\sqrt[5]{3}) \), és így

\[
\sqrt{7} = \Re e^{i \epsilon} = \frac{\alpha + \sqrt{7}}{2} \in M
eq \Re e^{i \epsilon} = \frac{\alpha - \sqrt{7}}{2} \in M.
\]
MEGOLDÁSOK

\[ \deg(\sqrt{2} : Q(\sqrt{2})) = 1, \quad \text{azaz} \quad V = Q(\sqrt{2}). \]

\( \blacksquare (c) \) Mivel a \( \sqrt{i} \) két értéke egymás negatívja, ezért ugyanahhoz a bővítéshez jutunk bármelyik érték esetén. Válasszuk például a

\[ \hat{\theta} = \sqrt{i} = \frac{1 + i}{\sqrt{2}} \quad (3) \]

értéket.

Megmutatjuk, hogy \( V = Q(\sqrt{2}) \).

Első megoldás: Mivel

\[ i = (\sqrt{i})^2 = \hat{\theta}^2 \in Q(\hat{\theta}), \]

ezért (3)-ból következik, hogy

\[ \sqrt{2} \in Q(\hat{\theta}), \quad \text{tehát} \quad Q(\sqrt{2}) \subseteq V. \]

Tekintsük a

\[ Q \subseteq Q(\sqrt{2}) \subseteq V \subseteq Q(\hat{\theta}) \]

bővítésláncot. Az előző részekhez hasonlóan adódik, hogy

\[ \deg(\hat{\theta} : Q) = 1, \quad \deg(Q(\sqrt{2}) : Q) = 2 \quad \gg \quad V \neq Q(\hat{\theta}). \]

Ebből a fokszámtétel felhasználásával kapjuk, hogy

\[ \deg(V : Q(\sqrt{2})) = 1, \quad \text{azaz} \quad V = Q(\sqrt{2}). \]

Második megoldás: A T. 10.2.3 Tétel szerint \( Q(\hat{\theta}) \) elemei egyértelműen felirhatók racionális \( a_i \) számokkal

\[ \alpha = a_0 + a_1 \sqrt{i} + a_2 (\sqrt{i})^2 + a_3 (\sqrt{i})^3 = a_0 + a_1 \frac{1 + i}{\sqrt{2}} + a_2 i + a_3 \frac{-1 + i}{\sqrt{2}} \quad (4) \]

alakban.

Az \( \alpha \) akkor és csak akkor valós, ha a képzetes része 0, azaz

\[ \frac{a_4 - a_3}{\sqrt{2}} + a_2 = 0. \]

Mivel \( \sqrt{2} \) iracionális, ez pontosan akkor teljesül, ha

\[ a_4 = -a_1 \quad \gg \quad a_2 = 0. \]

Ezt (4)-be visszahelyettesítve kapjuk, hogy \( \alpha \) akkor és csak akkor valós, ha

\[ \alpha = a_0 + a_1 \sqrt{2}, \quad \text{azaz} \quad \alpha \in Q(\sqrt{2}). \]

Ezzel beláttuk, hogy \( V = Q(\sqrt{2}) \).

Harmadik megoldás: Az állítás a 10.2.8 feladatból [326] is következik.
10.2.8 [326] Mivel $|\vec{v}| = 1$, ezért $\bar{\vec{v}} = \frac{-1}{\vec{v}}$, és így

$$\text{Re} \cdot \bar{\vec{v}} = \frac{\vec{v} + \bar{\vec{v}}}{2} = \frac{1}{2} \left( \vec{v} + \frac{1}{\vec{v}} \right).$$

Ebből következik, hogy $\text{Re} \cdot \bar{\vec{v}} \in \mathbb{Q}(\vec{v})$, és így $\mathbb{Q}(\text{Re} \cdot \vec{v}) \subseteq \mathbb{Q}(\vec{v})$. Mivel nyilván $\mathbb{Q}(\text{Re} \cdot \vec{v}) \subseteq \mathbb{R}$, ezért

$$\mathbb{Q}(\text{Re} \cdot \vec{v}) \subseteq \mathbb{Q}(\vec{v}) \cap \mathbb{R}.$$ \hspace{1cm} (5)

A másik irányú tartalmazáshoz legyen $c$ a $\mathbb{Q}(\vec{v})$ tetszőleges valós eleme: $c = \frac{g(\vec{v})}{h(\vec{v})}$ (ahol $g, h \in \mathbb{Q}[x], h(\vec{v}) \neq 0$). Ekkor

$$h(\vec{v})c = g(\vec{v}).$$ \hspace{1cm} (6)

A (7) egyenlőséget konjugálva, $c \in \mathbb{R}$ alapján

$$h(\vec{v})c = g(\bar{\vec{v}}).$$ \hspace{1cm} (7)

adódik. Tegyük fel egyelőre, hogy $h(\vec{v}) + h(\bar{\vec{v}}) \neq 0$. Ekkor (7)-et és (8)-at összeadva, majd $c$-t kifejezve azt kapjuk, hogy

$$c = \frac{g(\vec{v}) + g(\bar{\vec{v}})}{h(\vec{v}) + h(\bar{\vec{v}})} = \frac{g(\vec{v}) + g(1/\vec{v})}{h(\vec{v}) + h(1/\vec{v})}. \hspace{1cm} (9)$$

Felhasználva, hogy $\vec{v}^k + \vec{v}^{-k}$ felírható $\vec{v} + (1/\vec{v})$, azaz $2\text{Re} \cdot \vec{v}$ racionális együtthatós polinomjaként, (9)-ből azt nyerjük, hogy $c \in \mathbb{Q}(\text{Re} \cdot \vec{v})$. Ezzel beláttuk, hogy

$$\mathbb{Q}(\vec{v}) \cap \mathbb{R} \subseteq \mathbb{Q}(\text{Re} \cdot \vec{v}).$$

Hátván még a

$$h(\vec{v}) + h(\bar{\vec{v}}) = h(\vec{v}) + h(1/\vec{v}) = 0 \hspace{1cm} (10)$$

eset vizsgálata. Ekkor azonnal adódik, hogy $\vec{v}$ algebrai szám. Az alábbi gondolatmenet nemcsak (10) fennállása, hanem tetszőleges $\vec{v}$ algebrai szám esetén érvényes.

Felhasználva (6)-ot, tekintsük a

$$\mathbb{Q}(\text{Re} \cdot \vec{v}) \subseteq \mathbb{Q}(\vec{v}) \cap \mathbb{R} \subseteq \mathbb{Q}(\vec{v}), \hspace{1cm} (11)$$

bővítésláncot. A feladat állítása $\vec{v} = \pm 1$ esetén nyilvánvaló, így feltehetjük, hogy $\vec{v}$ nem valós szám. Megmutatjuk, hogy ekkor (11)-ben az egész lánc is, és a második láncszem is másodfokú bővítés, ezért a főszámértékel alapján az első láncszem elsőfokú, azaz a két szóban forgó bővítés megegyezik.

Mivel a (11) lánc első két eleme csak valós számokból áll, a harmadik viszont nem, ezért az egész lánc és a második láncszem is legalább másodfokú. Így elég belátni, hogy az egész lánc (legfeljebb) másodfokú bővítés.

A $|\vec{v}| = 1$ feltétel miatt $\text{Im} \cdot \vec{v} = \pm 1$, így feltehetjük, hogy $\vec{v}$ nem valós szám. Megmutatjuk, hogy ekkor (11)-ben az egész lánc is, és a második láncszem is másodfokú bővítés, ezért a főszámértékel alapján az első láncszem elsőfokú, azaz a két szóban forgó bővítés megegyezik.

Mivel a (11) lánc első két eleme csak valós számokból áll, a harmadik viszont nem, ezért az egész lánc és a második láncszem is legalább másodfokú. Így elég belátni, hogy az egész lánc (legfeljebb) másodfokú bővítés.

$$\mathbb{Q}(\text{Re} \cdot \vec{v}) \subseteq \mathbb{Q}(\vec{v}) \cap \mathbb{R} \subseteq \mathbb{Q}(\vec{v}).$$

bővítésláncot. A feladat állítása $\vec{v} = \pm 1$ esetén nyilvánvaló, így feltehetjük, hogy $\vec{v}$ nem valós szám. Megmutatjuk, hogy ekkor (11)-ben az egész lánc is, és a második láncszem is másodfokú bővítés, ezért a főszámértékel alapján az első láncszem elsőfokú, azaz a két szóban forgó bővítés megegyezik.
MEGOLDÁSOK

( \ln \theta \neq 0 \) miatt pontosan) másodfokú elen \( Q(\Re \theta) \) felett. Így valóban \( \deg Q(\theta) : Q(\Re \theta) = 2 \).

- 10.2.11 [326] Megmutatjuk, hogy az egységkörön a \( \pm 1 \)-en kívül nincs páratlan fokú algebrai szám.

- Első bizonyítás: A 10.2.8 feladat [326] megoldása során beláttuk, hogy ha \( \theta \) algebrai szám és \( |\theta| = 1 \), akkor
  \[
  Q(\Re \theta) \subseteq Q(\theta),
  \]
  és \( \theta \neq \pm 1 \) esetén a bővítés foka 2.

Ez azt jelenti, hogy a
  \[
  Q \subseteq Q(\Re \theta) \subseteq Q(\theta)
  \]
bővítéslánc második láncszemének a foka 2, és így a fokszámtétel szerint
  \[
  \deg \theta = \deg Q(\theta) : Q(\theta) \]-árós.

- Második bizonyítás: Egy valós együtthatós polinomnak egy komplex szám és a konjugáltja ugyanannyiszoros gyöke, ezért \( |\theta| = 1 \) esetén \( 1/\theta - \bar{\theta} \) is gyöke a \( \theta \) minimálpolinomjának. Ebből \( \nu_{\theta} \) irreducibilitása miatt következik, hogy
  \[
  \nu_{\theta} = \nu_{1/\theta}, \tag{12}
  \]
Könnyen adódik (lásd például a 9.1.2c feladathoz [294] fűzött útmutatást), hogy ha \( \theta \) minimálpolinomja
  \[
  \nu_{\theta} = a_0 + a_1 x + \cdots + a_n x^n \quad (a_n \neq 0), \tag{13a}
  \]
akkor \( 1/\theta \) (egyik) minimálpolinomja
  \[
  \nu_{1/\theta} = a_n + a_{n-1} x + \cdots + a_0 x^n \quad (a_0 \neq 0). \tag{13b}
  \]
A (12) feltételből következik, hogy a (13b) polinom a (13a) polinomnak egy \( c \) racionális számszorosa. A konstans tagok és a főegyütthatók összehasonlításából kapjuk, hogy
  \[
  a_m = ca_0 \quad \text{és} \quad a_n = ca_n,
  \]
és így \( c = \pm 1 \). Ennek felhasználásával a többi együttható összehasonlításából az adódik, hogy vagy
  \[
  a_j = a_{n-j}, \quad j = 0, 1, \ldots, n,
  \]
vagy pedig
  \[
  a_j = -a_{n-j}, \quad j = 0, 1, \ldots, n.
  \]
Ha \( \deg \theta = n \) páratlan, akkor az első esetben
  \[
  \nu_{\theta}(-1) = \sum_{j=0}^{n} a_j(-1)^j = \sum_{j=0}^{(n-1)/2} a_j((-1)^j + (-1)^{n-j}) = 0,
  \]
a a második esetben pedig

610
\[ m_p(1) = \sum_{j=0}^{\infty} a_j - \sum_{j=0}^{\infty} (a_j + a_{n-j}) = 0. \]

Ez azt jelenti, hogy \( m.a \)-nak a \(-1\) vagy az \(1\) racionális szám gyöke. Mivel \( m.a \) irreducibilis \( \mathbb{Q} \) felett, ezért ez csak úgy lehetséges ha \( \vartheta = -1 \), illetve 1.

- **10.3.5 [338]** Ha \( t \) négyzetmentes összetett szám, akkor létezik olyan \( p > 2 \) prím szám, amelyre \( p \mid t \).

Indirekt tegyük fel, hogy \( F(\sqrt{t}) \)-ben igaz a számelméleti alaptétele. Ekkor a T 10.3.8 Tétel (vii) állítása szerint \( p \) felbonlhat \( F(\sqrt{t}) \)-ben, és így létezik olyan \( \alpha = a + b\sqrt{t} \), amelyre \( N(\alpha) = a^2 + t b^2 = p \). Itt \( a \) és \( b \) egész vagy 2 nevezőjű törtek, tehát \( \alpha = ka \), \( \gamma = \beta b \) biztosan egész, és
\[ \gamma^2 + t |\gamma|^2 = 4p. \tag{14} \]
Ha \( \gamma = 0 \), akkor \( \gamma^2 = 4p \), ami lehetetlen.

Legyen \( |t| = kp \). Mivel \( k \geq 2 \), ezért \( |\gamma| \geq 2 \) esetén (14) bal oldala nagyobb a jobb oldalnál.

Maradt a \( |\gamma| = 1 \) eset. Ekkor \( \gamma^2 = (4-k)p \), ami \( k = 3 \) és \( k \geq 5 \) mellett nyilván lehetetlen, továbbá \( t \) négyzetmentessége miatt \( k \neq 4 \).

Ezzel megmutattuk, hogy (14) nem teljesülhet, és így ellentmondásra jutottunk.

- **10.3.6 [338]** Az útmutatásban jelzett gondolatmenetet követjük.

Legyen \( t = -4k+1 \) és \( \alpha_n = n + (1 + \sqrt{t})/2 \). Ekkor
\[ N(\alpha_n) = N\left(n + \frac{1 + \sqrt{t}}{2}\right) = \left(n + \frac{1 + \sqrt{t}}{2}\right)\left(n + \frac{1 - \sqrt{t}}{2}\right) = n^2 + \nu + k. \tag{15} \]

Megmutatjuk, hogy \( 0 \leq \nu \leq k - 2 \) esetén \( \alpha_n \) felbonthatatlan. Tegyük fel indirekt, hogy (valamely \( n \)-re) \( \alpha_n = \beta \gamma \), ahol \( \beta \) és \( \gamma \) egyike sem egység. Mivel \( \alpha_n \)-nek nem lehet \( \pm 1 \)-től különböző olyan osztója, amely egész szám, ezért
\[ \beta = b_0 + b_1 \frac{1 + \sqrt{k}}{2}, \quad \gamma = c_0 - c_1 \frac{1 + \sqrt{k}}{2}, \quad \text{ahol} \quad b_0, c_1 \in \mathbb{Z}, \quad \text{és} \quad b_0, c_1 \neq 0. \]

Ebből következik, hogy
\[ N(\beta) = b_0^2 - b_0 b_1 - b_1^2 k = \left(b_0 + b_1 \frac{1}{2}\right)^2 + b_1^2 \left(k - \frac{1}{4}\right) \geq k, \]
és ugyanígy \( N(\gamma) \geq k \). Ekkor azonban
\[ k^2 \leq N(\beta)N(\gamma) = N(\alpha_n) < N(\alpha_{n-1}) = (k - 1)^2 + (k - 1) + k = k^2, \]
ami ellentmondás.

Ezzel beláttuk, hogy \( 0 \leq \nu \leq k - 2 \) esetén \( \alpha_n \) felbonthatatlan. Ebből következik, hogy \( \overline{\alpha_n} \) is felbonthatatlan.

Tegyük fel most indirekt, hogy valamely \( 0 \leq \nu \leq k - 2 \)-re \( f(\nu) \) nem prím szám, azaz
A (15) és (16) összefüggésekből ekkor
\[
\left( u + \frac{1 + \sqrt{7}}{2}\right) \left( u + \frac{1 - \sqrt{7}}{2}\right) = rs
\]
adódik. A (17) bal oldalán két felbonthatatlan szám szorzata áll. Így a számelmélet alaptétele szerint a jobb oldalon álló két, egységtől különböző tényező is felbonthatatlan, mégpedig valamelyik bal oldali tényező egységszerese kell hogy legyen. Ez azonban lehetetlen, hiszen a ± 1-től különböző \( r \) egész szám nem lehet osztója \( \alpha_n \)-nek vagy \( \alpha_n \)-nak.

- 10.3.9 [338] (e) Az útmutatásnak megfelelően azt fogjuk igazolni, hogy ha \( r \equiv 1 \) vagy 9 (mod 20), akkor van olyan \( a, b \) egész, amelyre
\[
p = a^2 + 5b^2 = (a + b\sqrt{-5})(a - b\sqrt{-5}).
\]
Erre két bizonyítást adunk. Mindkettőben felhasználjuk, hogy \( \left( \frac{-2}{p} \right) \equiv 1 \) miatt létezik olyan \( c \) egész, amelyre \( p \mid c^2 + 5 \).

- Első bizonyítás: A T 8.2.4 Tétel bizonyításának gondolatmenetét követjük. Tekintsük a síkon az \( x = pa + cv \) , \( y = v \) koordinátájú pontokat, ahol \( u \) és \( v \) egymástól függetlenül befutják az egész számokat. Ezek a pontok egy paralelogrammarácsot alkotnak, amelyben az alapparalelogramma területe \( \Delta = p \).

Bármely rácsponst esetén
\[
x^2 + 5y^2 = (pa + cv)^2 + 5n^2 = p(pa^2 + 2cvn) + c^2(5 - 5) = 0 \pmod{p},
\]
azaz \( p \mid x^2 + 5y^2 \).

Alkalmazzuk Minkowski tételét az \( x^2 + 5y^2 \leq 4\sqrt{5}p/\pi \) egyenletű, origó körüli \( 4p = 4\Delta \) területű (záró) ellipszisre. A tétel szerint ez az ellipszis az origón kívül is tartalmaz legalább egy \((x, y)\) rácsponst. Így erre a rácspontra teljesül
\[
p \mid x^2 + 5y^2 \quad \text{és} \quad x^2 + 5y^2 \leq \frac{4\sqrt{5}p}{\pi} < 3p,
\]
teht \( x^2 + 5y^2 = p \) vagy \( 2p \).

Az \( x^2 + 5y^2 = 2p \) egyenlőség azonban nem állhat fenn, mert 5-tel osztva a bal oldal lehetséges maradéka 0 és ± 1 , a jobb oldal pedig ± 2 , hiszen \( p = \pm 1 \pmod{5} \). Ezért szükségképpen \( x^2 + 5y^2 = p \).

- Második bizonyítás: Legyen \( p \mid c^2 + 5 \). Belátjuk, hogy a \( cv \equiv x \pmod{p} \) kongruenciának létezik olyan \( x \) , \( v \) megoldása, ahol \( 0 < |x|, |y| < \sqrt{p} \). Ez a 7.5.21a feladatban [242] szereplő Thue-lemmából következik, a \( k = 1 \) , \( x = v = \left[ \sqrt{p} \right] \) és \( C = c \) szereposztással.

Ekkor
\[
x^2 + 5y^2 \equiv c^2x^2 + 5y^2 \equiv (c^2 + 5)y^2 \equiv 0 \pmod{p} \quad \text{és} \quad x^2 + 5y^2 < 6p.
\]
Megmutatjuk, hogy van olyan $a$, $b$ egész, amelyre $a^2 + 5b^2 = p$.

Ha $x^2 + 5y^2 = 5p$, akkor $5 \mid x$, azaz $x = 5x_1$, és így $25x_1^2 + 5y^2 = 5p$, vagyis $5x_1^2 + y^2 = p$.

Ha $x^2 + 5y^2 = 4p$, akkor a modulo 4 maradékok alapján $x$ és $y$ is páros, $x = 2a_1$, $y = 2b_1$, és így $4a_1^2 + 20b_1^2 = 4p$, azaz $a_1^2 + 5b_1^2 = p$.

Az $x^2 + 5y^2 = 3p$ vagy $2p$ egyenlőség a két oldal modulo 5 maradékinak különbözősége miatt nem teljesülhet.

Végül, az $x^2 + 5y^2 = p$ eset azonnal a kívánt állítást jelenti.

**10.5.6 [349]** Tekintsünk egy általános $Q(\sqrt{5})$ másodfokú bővítést, ahol $t$ négyzetmentes egész szám és $t \not= 1$. Megmutatjuk, hogy $Q(\sqrt{5})$-ben akkor és csak akkor létezik a kívánt tulajdonságú egész bázis, ha $t = 1 \mod 4$.

Elégségesség: Ha $t \equiv 1 \mod 4$, akkor az

$$\omega_1 = \frac{1 + \sqrt{t}}{2} \quad \text{és} \quad \omega_2 = \frac{1 - \sqrt{t}}{2}$$

választás megfelel.

Ehhez azt alábbiakat kell megmutatni:

(i) minden $a \in Q(\sqrt{5})$ egyértelműen felírható racionális $c_i$ számokkal

$$a = c_1 \omega_1 + c_2 \omega_2 \quad (18)$$

alakban;

(ii) $a$ akkor és csak akkor algebrai egész, ha $c_1$ és $c_2$ egész szám;

(iii) $\omega_1$-nek és $\omega_2$-nek ugyanaz a minimálpolinomja.

(i) Tudjuk, hogy $a$ egyértelműen előáll

$$a = a + b\sqrt{5} \quad (19)$$

alakban, ahol $a$ és $b$ racionális számok. Hasonlóan össze (18)-at és (19)-et:

$$a + b\sqrt{5} = c_1 \frac{1 + \sqrt{t}}{2} + c_2 \frac{1 - \sqrt{t}}{2} = c_1 + c_2 + \frac{c_1 - c_2}{2} \sqrt{5}.$$  

A (19) előállítás egyértelműségéből látszik, hogy (18) pontosan akkor teljesül, ha

$$a = \frac{c_1 + c_2}{2} \quad \text{és} \quad b = \frac{c_1 - c_2}{2}, \quad (20a)$$

azaz

$$c_1 = a + b \quad \text{és} \quad c_2 = a - b. \quad (20b)$$

Ezzel a megfelelő (racionális) $c_1$ és $c_2$ létezését és egyértelműségét beláttuk.
(ii) A T 10.3.2 Tétel szerint a \( t \equiv 1 \pmod{4} \) esetben \( \alpha \) akkor és csak akkor algebrai egész, ha
\[
\begin{align*}
  a &= \frac{n}{2} \quad b = \frac{v}{2}, \quad \text{ahol} \quad n, v \in \mathbb{Z} \quad \text{és} \quad u \equiv v \pmod{2}.
\end{align*}
\]
Azt kell igazolnunk, hogy a (21) feltétel ekvivalens azzal, hogy \( c_1 \) és \( c_2 \) egész számok.

Ha \( a \) és \( b \) a (21)-ben előírt alakú, akkor (20b)-ből következik, hogy
\[
\begin{align*}
  c_1 &= \frac{n + v}{2} \quad \text{és} \quad c_2 = \frac{n - v}{2}
\end{align*}
\]
egész számok.

Megfordítva, ha \( c_1 \) és \( c_2 \) egész, akkor \( a = c_1 + c_2 \) és \( v = c_1 - c_2 \) azonos paritású, és így (20a) szerint \( a \) és \( b \) eleget tesz (21)-nek.

(iii) A két szám közös minimálpolinomja
\[
(x - \omega_1)(x - \omega_2) = x^2 - x + \frac{1 - t}{4}.
\]

Szükségesség: Indirekt tegyük fel, hogy valamely \( t \not\equiv 1 \pmod{4} \) esetén létezik a megadott tulajdonságú \( \omega_1, \omega_2 \) egész bázis.

Az \( \omega_1 \) és \( \omega_2 \) egyéb \( \mathbb{Q} \) feletti konjugáltai, tehát
\[
\omega_1 = r + s\sqrt{t} \quad \text{és} \quad \omega_2 = r - s\sqrt{t}, \quad r, s \in \mathbb{Q}.
\]

Mivel \( \omega_1 \) és \( \omega_2 \) algebrai egész és \( t \not\equiv 1 \pmod{4} \), ezért (a T 10.3.2 Tétel alapján) \( r \) és \( s \) egész számok, továbbá \( \omega_1 \) és \( \omega_2 \) lineáris függetlensége miatt \( s \neq 0 \).

Az 1 algebrai egész, tehát alkalmas \( c_1 \) és \( c_2 \) egész számokkal elő kell állnia
\[
1 = c_1\omega_1 + c_2\omega_2 = (c_1 + c_2)r + (c_1 - c_2)s\sqrt{t}
\]
alakban. Ez pontosan akkor teljesül, ha
\[
(c_1 + c_2)r = 1 \quad \text{és} \quad (c_1 - c_2)s = 0.
\]
Az \( s \neq 0 \) feltételből kapjuk, hogy \( c_1 = c_2 \), és így
\[
1 = (c_1 + c_2)r = 2c_1r,
\]
ami egész \( c_1 \) és \( r \) értékekre lehetetlen.

11. Ideálok

- 11.1.8 [355(a)] Először megmutatjuk, hogy az a1 és a3 gyűrű nem test, mivel található bennük nullosztó.

Jelöljük \( I \) -vel \( \mathbb{R}[x]/I \) -ben az \( x^2 - 2 \) által generált főideált: \( I = (x^2 - 2) \). Ekkor az \( \mathbb{R}[x]/I \) faktorgyűrűben az \( x + \sqrt{2} \) és \( x - \sqrt{2} \) polinomok által reprezentált (nemnulla) maradékosztályok szorzata a nulla maradékosztály:

614
MEGOLDÁSOK

\[ [x + \sqrt{2} + I] \cdot [x - \sqrt{2} + I] = [x + \sqrt{2}] [x - \sqrt{2}] + I = x^2 - 2 + I = 0 + I. \]

Ez azt jelenti, hogy \( x + \sqrt{2} + I \) és \( x - \sqrt{2} + I \) nullosztók \( \mathbb{R}[x]/I \)-ben, és így \( \mathbb{R}[x]/I \) nem lehet test.

Hasonló a helyzet a \( \mathbb{C}[x]/(x^2 + 1) \) faktorgyűrűben: itt az \( x + i \) és \( x - i \) polinomok által reprezentált (nemnulla) maradékosztályok szorzata nulla.

Most megmutatjuk, hogy az \( a^2 \)-ben megadott \( \mathbb{R}[x]/(x^2 + 1) \) faktorgyűrű test, mégpedig a komplex számtesttel izomorf.

A T 11.1.6 Tétel utáni példa gondolatmenetét követjük. Most azok a (valós együtthatós) polinomok kerülnek az \( \langle x^2 + 1 \rangle \) főideál szerint egy maradékosztályba, amelyek ugyanazt a maradéket adják \( x \)-gyel osztva. Ily módon minden maradékosztály egyértelműen jellemzhető egy „maradékkal”, azaz egy legfeljebb elsőfokú \( a + bx \) (valós együtthatós) polinommal (idesorolva a 0 polinomot is, amely magát az ideált reprezentálja).

A maradékosztálygyűrűben tulajdonképpen ezekkel a maradékokkal számolunk, azaz pl. két maradékosztály szorzásakor ezeket a maradékokat összeszorozzuk és vesszük a szorzatnak az \( x^2 + 1 \) -gyel való osztási maradékát. Ennek megfelelően az összeadást az

\[ [a + bx] + [c + dx] = [a + c] + [b + d]x, \]

a szorzást pedig az

\[ [a + bx][c + dx] = ac + adx + bce + bd\cdot x^2 = \]

\[ cm + \frac{bc + bd}{x - 1}x + \frac{bd}{x - 1} = \]

szabály szerint kell végezni, azaz pontosan ugyanúgy, ahogyan a komplex számoknál (képzeljünk az „\( \cdot \)” betű helyére mindenhol „\( \cdot \)” betütt).

Ezzel beláttuk, hogy az \( \mathbb{R}[x]/(x^2 + 1) \) maradékosztálygyűrű test és izomorf \( \mathbb{C} \)-vel.

• (b) Bebizonyítsuk, hogy az \( R = T[x]/(f) \) faktorgyűrű akkor és csak akkor test, ha \( f \) irreducibilis \( T \)-felett.

Szükségesség: Tegyük fel indirekt, hogy \( f \) nem irreducibilis \( T \)-felett. Ekkor \( f = 0 \), vagy \( f \) egység, vagy pedig \( f \) reducibilis \( T \)-felett. Megmutatjuk, hogy \( R \) egyik esetben sem test.

Ha \( f \) egység, akkor \( \langle f \rangle = \langle 1 \rangle = T[x] \), tehát \( R \)-nak csak egy eleme van, ha pedig \( f = 0 \), akkor \( \langle f \rangle = \langle 0 \rangle \), tehát \( R \) azonosnak tekinthető \( T[x] \)-szel, vagyis \( R \) ezekben az esetekben nyilván nem test.

Ha \( f \) reducibilis, azaz létezik olyan \( g \) és \( h \) nemkonstans polinom, amelyre \( f = gh \), akkor \( R \)-ben a \( g \) és \( h \) polinomok által reprezentált maradékosztályok szorzata a nulla maradékosztály:

\[ [g + fh][h + fh] = gh + (f) = f + (f) = 0 + (f). \]

Ugyanakkor \( g + (f) \) és \( h + (f) \) egyike sem a nulla maradékosztály, hiszen \( f \nmid g \) és \( f \nmid h \).

Ez azt jelenti, hogy reducibilis \( f \) esetén \( R \)-ben találhatók nullosztók, és így \( R \) nem lehet test.
Elégségesség: Azt kell igazolni, hogy ha \( f \) irreducibilis \( T \)-felett, akkor az \( R = T[x]/(f) \) faktorgyűrű test.

Az \( R \) gyűrű kommutatív, továbbá az \( 1 + (f) \) maradékosztály egységelem (a szorzásra nézve). Azt kell még belátni, hogy minden nem nulla elemnek létezik inverze.

A T 10.2.3 Tétel bizonyításának I. részéhez hasonló gondolatmenetet alkalmazunk.

Legyen \( a + (f) \) egy tetszőleges nem nulla maradékosztály, azaz \( f \nmid a \). A \( v + (f) \) maradékosztály pontosan akkor lesz az \( a + (f) \) inverze, ha

\[
[a + (f)][v + (f)] = uv + (f) = 1 + (f),
\]

vagyis \( f \mid 1 - uv \).

Ez azt jelenti, hogy létezik olyan \( w \in T[x] \) polinom, amelyre

\[
1 = uv + fw.
\] (1)

Az (1) egyenletben \( u \) és \( f \) adottak, \( u \) és \( v \) pedig az ismeretlenek; így az invertálhatóság kérdését egy polinomokra vonatkozó „diofantikus” egyenlet megoldhatóságára fogalmaztuk át.

Amint a T 10.2.3 Tétel bizonyításában már megindokoltuk, az (1) diofantikus egyenlet (az egész számokra vonatkozó T 1.3.6 Tétellel összhangban) akkor és csak akkor oldható meg, ha \( u \) és \( f \) legnagyobb közös osztója osztója az 1-nek, azaz \( u \) és \( f \) relatív prímek. Mivel \( f \) irreducibilis és \( f \nmid a \), ezért ez valóban teljesül.

(c) Az \( I = (2, x^2 + x + 1) \) ideál szerinti maradékosztályok reprezentálásához a polinomoknak az ideál mindkét generátoreleme szerint vesszük a maradékát. (Mivel \( g = x^2 + x + 1 \) normált polinom, ezért az egész együtthatós polinomok körében is el tudunk osztani bármely polinomot maradékosan \( g \)-vel.)

Ennek megfelelően minden maradékosztálynak van olyan reprezentánsa, amely legfeljebb elsőfokú (vagy a 0 polinom) és valamennyi együtthatója 0 vagy 1. Így az alábbi négy polinomot kapjuk:

\[
0, \ 1, \ x, \ 1 + x.
\]

Könnyen adódik, hogy ezek közül már semelyik kettő sem esik ugyanabba a maradékosztályba (azaz semelyik két polinom különbsége sem eleme az \( I \) ideálnak).

Ez azt jelenti, hogy az \( R = Z[x]/(2, x^2 + x + 1) \) faktorgyűrűnek négy eleme van, és ezek rendre a fenti négy polinommal reprezentálhatók.

Az \( R \) gyűrű nyílván kommutatív és az \( 1 + I \) maradékosztály egység- elem. Az egységelem inverze önmaga, a másik két nem nulla elem pedig egymás inverze:

\[
[x + I][1 + x + I] = x[1 + x] + I = 1 + [x^2 + x + 1 - 2] + I = 1 + I,
\]

hiszen \( x^2 + x + 1 - 2 \in I \).

Ezzel beláttuk, hogy az \( R \) gyűrű test.

Egy másik lehetséges bizonyítást a feladathoz adott útmutatásnál vázoltunk.

(c) Az \( R \) test, akkor \( R[x] \) (a fokszám szerinti maradékos osztásra nézve) euklideszi gyűrű, és így a T 11.3.5 Tétel alapján fölideálgyűrű is.
A megfordításhoz tegyük fel, hogy $\mathbb{R}[x]$ főideálgyűrű. Azt kell igazolni, hogy $\mathbb{R}$- test, azaz bármely $a \neq 0$ elemnek létezik inverze.

Tekintsük $\mathbb{R}[x]$-ben az $a$ nemnulla konstans polinom és az $x$ által generált $I = (a, x)$ ideált. A feltétel szerint $I$ főideál, azaz alkalmas $g \in \mathbb{R}[x]$ polinommal $I = (g)$.

Mivel $x \in (a, x) = (g)$, ezért $g \mid x$. Így $g = \varepsilon$ vagy $g = \varepsilon x$, ahol $\varepsilon$ egység (azaz olyan konstans polinom, amelynek létezik inverze $\mathbb{R}[x]$-ben, vagy ami ugyanaz, az $\varepsilon$-nak mint $\mathbb{R}$-beli elemnek létezik inverze $\mathbb{R}$-ben). A $g \mid \varepsilon$ feltétel miatt $g \neq \varepsilon x$, azaz csak $g = \varepsilon$ lehetséges. Ekkor $(g) = (1)$.

Mivel $(a, x) = (1)$, ezért alkalmas $h$, $\varepsilon \in \mathbb{R}[x]$ polinomokkal $1 = ah + xt$. Ebből következik, hogy $h$ konstans tagjának és az $a$-nak a szorzata 1, tehát $a$-nak valóban létezik inverze.

**11.3.9 [365][a]** A 11.1.10b feladathoz [355] adott útmutatás alapján azonnal adódik, hogy $\mathbb{R}$ minden ideálja végesen generált.

Ha $(a, b, c) = (d)$, akkor $(a, b, c) = (d, c)$. Ennek megfelelően elég azt belátni, hogy bármely, két elemmel generált $(a, b)$ ideál főideál.

Ha itt valamelyik generátor elem 0, akkor az állítás nyilvánvaló. Így feltehetjük, hogy $a$ és $b$ egyike sem 0.

A számelmélet alaptételéből következik, hogy létezik $\mathbb{N}_{\text{egyel}}(a, b)$, jelöljük ezt $d$-vel. A T 11.2.2/ (iii) Tétel szerint $(a, b) = (d)$ fennállásához $d = \mathbb{N}_{\text{egyel}}(a, b)$ mellett azt kell még megmutatni, hogy alkalmas $u$, $v \in \mathbb{R}$ elemekre $d = au + bv$. Ezt $d$-vel osztva a vele ekvivalens

$$1 = au + bv,$$  

egyenlőségehez jutunk, ami más megfogalmazásban azt jelenti, hogy alkalmas $u$-val az 1 és $a_1u$ elemek ugyanabba a $(b_1)$ szerinti maradékosztályba esnek. Ezt kell tehát belátnunk.

Vegyünk a $(b_1)$ szerinti véges sok maradékosztály mindengyikéből egy-egy elemet (azaz egy teljes maradékkrendszert modulo $b_1$), legyen ez $\mathbb{r}_1, \ldots, \mathbb{r}_n$. Megmutatjuk, hogy ekkor $\mathbb{a}_1\mathbb{r}_1, \ldots, \mathbb{a}_1\mathbb{r}_n$ is teljes maradékkrendszert modulo $b_1$.

Ha $a_1\mathbb{r}_i$ és $a_1\mathbb{r}_j$ ugyanabba a $(b_1)$ szerinti maradékosztályba esnek, akkor $a_1\mathbb{r}_i - a_1\mathbb{r}_j \in (b_1)$, azaz $b_1 \mid a_1(r_i - r_j)$. Mivel $a_1$ és $b_1$ relatív prímek, ezért a számelmélet alaptételéből következik, hogy ekkor $b_1 \mid r_i - r_j$. Ez azt jelenti, hogy $r_i - r_j \in (b_1)$, vagyis $i = j$.

Ezzel igazoltuk, hogy az $a_1\mathbb{r}_1, \ldots, a_1\mathbb{r}_n$ elemek különböző maradékosztályokba esnek, és így valóban minden maradékosztályt reprezentálhának. Ebből speciálisan az is következik, hogy van olyan $i$, amelyre $a_1\mathbb{r}_i$ ugyanabba a maradékosztályba esik, mint az 1, és ezt kellett igazolni.

**11.3.10 [366]** A megadott öt $t$ érték esetén $\mathbb{E}(\sqrt{t})$-ben a norma szerint elvégezhető a maradékos osztás, ennek igazolását a 10.3.4 feladathoz [338] adott útmutatásban vázoltuk.

A megfordításhoz tegyük fel, hogy $\mathbb{F}(\sqrt{t})$ euklideszi gyűrű. Nyilván elég a $k < -3$ esettel foglalkozni, ekkor a $\pm 1$-en kívül nincs más egység $\mathbb{F}(\sqrt{t})$-ben.
Legyen $\beta$ egy olyan, a 0-tól és az egységektől (azaz $\pm 1$-től) különböző elem, amelyre $f(\beta) = 0$ és az $f(\pm 1)$ értékektől eltekintve a legkisebb.

A $\beta$ kiválasztásából következik, hogy bármely $\xi \in \mathbb{F}(\sqrt{t})$ elemet $\beta$-val maradékosan osztva a maradék csak 0 vagy $\pm 1$ lehet. Ez más megfogalmazásban azt jelenti, hogy bármely $\xi$ esetén $\xi$, $\xi + 1$ vagy $\xi - 1$ osztható $\beta$-val.

Speciálisan, ha $\xi = 2$, akkor azt kapjuk, hogy $\beta \mid 2$ vagy $\beta \mid 3$ vagy $\beta \mid 1$. Az utolsó eset nem fordulhat elő, hiszen $\beta \neq \pm 1$.

Ha $\beta \mid 2$, akkor $N(\beta) \mid N(2) = 4$, azaz $N(\beta) = 2$ vagy $N(\beta) = 4$. Beláthatjuk, hogy csak $N(\beta) = 2$ lehetséges.

A $N(\beta) = 4$ feltétel (a $\beta \mid 2$ oszthatósággal együtt) azt jelenti, hogy a $\beta$ a 2 egységszerése. Ennek az esetében a kizárásokhoz így elég egy olyan $\xi$-t mutatni, amelyre a $2$ a $\xi$, $\xi - 1$ és $\xi - 1$ elemek egyikének sem osztója.

Ha $t \neq \pm 1$ ($\text{mod } 4$), akkor $\xi = \sqrt{t}$, ha pedig $t = 1$ ($\text{mod } 4$), akkor $\xi = (1 + \sqrt{5})/2$ nyilván ilyen tulajdonságú. (Felhasználtuk az $E(\sqrt{t})$ elemeinek előállítására vonatkozó T 10.3.2 Tételt.)

Ezzel megmutattuk, hogy ha $\beta \mid 2$, akkor $N(\beta) = 2$. Teljesen hasonlóan kapjuk, hogy a $\beta \mid 3$ esetben $N(\beta) = 3$.

Legyen először $t \neq 1$ ($\text{mod } 4$). Ekkor $\beta = c + d\sqrt{t}$, ahol $c$ és $d$ egész. Mivel $N(\beta)$ nem négyzetes, ezért $d \neq 0$, és így

\[ 3 \geq N(\beta) = c^2 + |t| \cdot d^2 \geq 0 + |t| \cdot 1 = |t|, \]

azaz $t \geq -3$, amit kizártunk.

Ha $t = 1$ ($\text{mod } 4$), akkor $\beta = c + d(1 + \sqrt{5})/2$ alakú, ahol $c$ és $d$ egész. Most is $d \neq 0$, és így

\[ 3 \geq N(\beta) = (c - \frac{d}{2})^2 + |t| \cdot \frac{d^2}{4} \geq 1 + |t| \cdot \frac{1}{4}, \]

azaz $t \geq -11$, vagyis ($t < -3$-at és $t \equiv 1$ ($\text{mod } 4$)-et figyelembe véve) $t = -7$ vagy $t = -11$, amit állítottuk.

11.4.8 [372](a) Az alábbi két tényt többször is fel fogjuk használni:

(i) $E(\sqrt{-5})$ ideáljaiba teljesül az oszthatóság és a fordított irányú tartalmazás ekvivalenciája, ezért elég azt megvizsgálnunk, hogy a megadott ideálok tartalmazzák.

(ii) $-5 \equiv 3$ ($\text{mod } 4$), ezért a T 10.3.2 Tétel szerint $E(\sqrt{-5})$ elemei $u + v\sqrt{-5}$ alakúak, ahol $u$ és $v$ egész számok.

(a): a1 Először megmutatjuk, hogy

\[ a - b\sqrt{-5} \in \{2, 1 + \sqrt{-5}\} \iff a \equiv b (\text{mod } 2). \]

(Ennek a feladatnak a megoldásánál számok helyett más jeleket használunk a képletszámokhoz, annak érdekében, hogy mondjuk a (2) főideál és a (2) képlet azonos jelölése ne okozhasson zavart.)
Ha \( a \) és \( b \) páros, akkor

\[
\begin{align*}
\alpha + b \sqrt{-5} &= 2 \left( \frac{a}{2} + \frac{b}{2} \sqrt{-5} \right) \in (2) \subseteq (2, 1 + \sqrt{-5}),
\end{align*}
\]

ha pedig \( a \) és \( b \) páratlan, akkor

\[
\begin{align*}
\alpha + b \sqrt{-5} &= 2 \left( \frac{a-1}{2} + \frac{b-1}{2} \sqrt{-5} \right) + \left( 1 + \sqrt{-5} \right) \in (2, 1 + \sqrt{-5}).
\end{align*}
\]

Tegyük fel megfordítva, hogy \( a + b \sqrt{-5} \in (2, 1 + \sqrt{-5}) \), azaz alkalmas \( \alpha \), \( \beta \in E(\sqrt{-5}) \) elemekek

\[
\alpha + b \sqrt{-5} = 2\alpha + \left( 1 + \sqrt{-5} \right) \beta.
\]

A (+) egyenlőséget \( 1 - \sqrt{-5} \)-tel beszorozva kapjuk, hogy

\[
\left[ a + b \sqrt{-5} \right] \left[ 1 - \sqrt{-5} \right] = 2 \left[ 1 - \sqrt{-5} \right] \alpha + 6\beta.
\]

Ebből következik, hogy

\[
2 \left\lfloor a + b \sqrt{-5} \right\rfloor \left\lfloor 1 - \sqrt{-5} \right\rfloor = \left\lfloor a + 5b \right\rfloor + \left\lfloor b - a \right\rfloor \sqrt{-5}.
\]

Ez azt jelenti, hogy \( a + 5b \) és \( b - a \) páros szám, vagyis \( a \) és \( b \) azonos paritású.

Ezzel (\( \times \))-ot beláttuk.

Térjünk rá most az \( I = (2, 1 + \sqrt{-5}) \) ideál osztóiira. Nyilván \( I \mid I \) és \( \langle 1 \rangle \mid I \). Megmutatjuk, hogy \( I \)-nek nincs több osztója (vagyis \( I \) felbonthatatlan ideál, és így prímideál).

Tegyük fel, hogy egy \( A \) ideálra \( A \mid I \) és \( A \neq I \). Ekkor \( I \subset A \) szigorú tartalmazással. Azt kell igazolnunk, hogy \( A = \langle 1 \rangle \), azaz \( 1 \in A \).

Legyen \( c + d \sqrt{-5} \in A \setminus I \). Ekkor (\( \ast \)) miatt \( c \) és \( d \) különböző paritású.

Ha \( c \) páratlan és \( d \) páros, akkor ismét (\( \ast \)) alapján kapjuk, hogy

\[
c - 1 + d \sqrt{-5} \in I \subset A,
\]

és így

\[
1 = \left\lfloor c + d \sqrt{-5} \right\rfloor - \left\lfloor c - 1 + d \sqrt{-5} \right\rfloor \in A.
\]

Ha \( d \) páratlan és \( c \) páros, akkor hasonló módon adódik, hogy

\[
\sqrt{-5} = \left\lfloor c + d \sqrt{-5} \right\rfloor - \left\lfloor c + d - 1 \right\rfloor \sqrt{-5} \in A,
\]

és így

\[
1 = \left\lfloor \sqrt{-5} \right\rfloor \left\lfloor \sqrt{-5} \right\rfloor + 3 \cdot 2 \in A.
\]

\( \blacksquare \) a2 \( (2) \)-ideálának nyilván osztója önmaga és az \( (1) \) ideál. Emellett (\( \ast \)) alapján a \( (2, 1 + \sqrt{-5}) \) ideál egy nemtriviális osztó. Megmutatjuk, hogy \( (2) \)-nek nincs több osztója.

619
Tegyük fel, hogy egy $B$ ideálra $B \mid (2)$ és $B \not= (2)$. Ekkor $(2) \subseteq B$ szigorú tartalmazással.

Legyen $u + v\sqrt{-5} \in B \setminus (2)$.

Ha $u$ páratlan és $v$ páros, akkor $u - 1 + v\sqrt{-5} \in (2)$, és így

$$1 = |u + v\sqrt{-5}| = |u - 1 + v\sqrt{-5}| \subseteq B,$$

teológ $B = (1)$.

Ha $u$ páros és $v$ páratlan, akkor hasonló módon adódik, hogy

$$\sqrt{-5} = |u + v\sqrt{-5}| = |u + |v|\sqrt{-5}| \subseteq B,$$

ami ból ismét

$$1 = \sqrt{-5} + 3 \cdot 2 \subseteq B,$$

azaz $B = (1)$

következik.

Végül, ha $u$ és $v$ is páratlan, akkor

$$1 + \sqrt{-5} = |u + v\sqrt{-5}| = |u - 1 + \frac{v - 1}{2} + \frac{u - 1}{2} + \sqrt{-5}| \subseteq B.$$

Ez azt jelenti, hogy $(2, 1 + \sqrt{-5}) \subseteq B$, ami ból az $a$ rész felhasználásával következik, hogy $B = (2, 1 + \sqrt{-5})$ vagy $B = (1)$.

- A3 Megmutatjuk, hogy az $(1 + \sqrt{-5})$ főideálaknak az alábbi négy (különböző) osztója van:

$$(1), \quad (1 + \sqrt{-5}), \quad (2, 1 + \sqrt{-5}) \quad \text{és} \quad (3, 1 + \sqrt{-5}).$$

Ezek valamennyien osztók, hiszen tartalmazzák az $(1 + \sqrt{-5})$ főideált.

A $(2, 1 + \sqrt{-5})$ ideál nemtriviális osztó, ugyanis egyrészt

$$1 + \sqrt{-5} \not\mid 2 \implies (2, 1 + \sqrt{-5}) \not= (1 + \sqrt{-5}),$$

másrészt az $a$-beli $(x)$ képlet szerint $(2, 1 + \sqrt{-5}) \not= (1)$.

Ugyanig például, hogy $(3, 1 + \sqrt{-5})$ nemtriviális osztó, ekkor $(x)$ helyett a hasonló módon igazolható

$$a + b\sqrt{-5} \in (3, 1 + \sqrt{-5}) \iff a = b \text{ (mod } 3).$$

Összefüggést érdemes felhasználni.

Végül (például) $(x)$-ből és $(x \ast)$-ből kapjuk, hogy

$$(2, 1 + \sqrt{-5}) \not= (3, 1 + \sqrt{-5}).$$

Most belátjuk, hogy ha a $C'$ ideál osztója az $(1 + \sqrt{-5})$ főideáknak, akkor $C'$ a fenti négy ideál valamelyikével egyenlő.
Tegyük fel, hogy $C \mid (1 + \sqrt{-5})$ és $C \not\mid (1 + \sqrt{-5})$, ekkor $(1 + \sqrt{-5}) \subseteq C$ szigorú tartalmazással. Legyen

$$\tau + s\sqrt{-5} \in C \setminus (1 + \sqrt{-5}).$$

Ekkor egyrészt

$$\tau - s = [\tau + s\sqrt{-5}] - s[1 + \sqrt{-5}] \subseteq C,$$

másrészt

$$\delta = [1 + \sqrt{-5}][1 - \sqrt{-5}] \in (1 + \sqrt{-5}) \subseteq C.$$  

Jelöljük $d$-vel a $6$ és $\tau - s$ egész számok legnagyobb közös osztóját. Ekkor alkalmas $t$ és $\ell$ egész számokra $d = 6t + \{r - s\sqrt{-5}\}$, és így $(\tau)$ és $(\ell)$ alapján $d \in C$.

Ha $d = 1$, akkor $1 \in C$, tehát $C = \{1\}$.

Ha $d = 2$, akkor $2 \in C$, és így $(2, 1 + \sqrt{-5}) \subseteq C$. Az a1 rész alapján ebből következik, hogy $C = (2, 1 + \sqrt{-5})$ vagy $C = \{1\}$.

Ha $d = 3$, akkor $3 \in C$, és így $(3, 1 + \sqrt{-5}) \subseteq C$. Az a1 részhez hasonlóan, $(*)$ felhasználásával könnyen igazolható, hogy ekkor $C = (3, 1 - \sqrt{-5})$ vagy $C = \{1\}$.

Végül belátjuk, hogy $d \neq 6$. Ha ugyanis $d = 6$, azaz $6 \mid \tau - s$ , akkor

$$\tau + s\sqrt{-5} = [\tau - s] + s[1 + \sqrt{-5}] \subseteq (1 + \sqrt{-5}),$$

ami ellentmond $(\nabla)$-nak.

\textbf{11.4.9 [372](a)} Az állítás hamis, például $E(\sqrt{-5})$-ben a 2 felbonthatatlan elem, azonban a (2) nem felbonthatatlan ideál. \textbf{(b)} Az állítás igaz. A feltétel alapján $\alpha$ nem lehet egység vagy 0. Tegyük fel, hogy $\alpha = \beta\gamma$. Ekkor $(\alpha) = (\beta)(\gamma)$, és így $(\alpha)$ felbonthatatlansága miatt $(\beta) = (1)$ vagy $(\gamma) = (1)$, azaz $\beta$ vagy $\gamma$ egység.

\textbf{11.4.9 (c) és (d)} Mindkét állítás igaz. Mivel

$$(\alpha) \neq (0) \iff \alpha \neq 0 \quad \text{és} \quad (\alpha) \neq (1) \iff \alpha \text{ leg egység,}$$

ezért a továbbiakban feltehetjük, hogy $(\alpha)$ nemtrivialis ideál.

Felhasználjuk az oszthatóság és a fordított irányú tartalmazás ekvivalenciáját. Ennek megfelelően

$$(\alpha) \text{ prímideál} \iff [\beta\gamma \in (\alpha) \implies \beta \in (\alpha) \text{ vagy } \gamma \in (\alpha)] \iff [\alpha \mid \beta \gamma \implies \alpha \mid \beta \text{ vagy } \alpha \mid \gamma] \iff \alpha \text{ prímidelem}.$$

\textbf{11.5.7 [383](c)} Megmutatjuk, hogy egy $p > 0$ primszámhoz akkor és csak akkor található olyan $\alpha$ egész szám, amelyre a $(p, \alpha + \sqrt{-5})$ ideál prímideál, ha $p = 2$, $p = 5$, vagy pedig $p$ a 20-szal oszta 1, 3, 7, illetve 9 maradékot ad.

Először azt igazoljuk, hogy a felsorolt $p$ értékek valóban rendelkeznek az előírt tulajdonsággal.
MEGOLDÁSOK

- A $p = 2$ esetben $a = 1$ megfelel: $I_2 = (2, 1 + \sqrt{-5})$ prímideál (lásd a 11.4.8 feladatot [372]).
- A $p = 5$ esetben $a = 0$ megfelel: $I_5 = (5, \sqrt{-5}) = (\sqrt{-5})$ prímideál. Ez a 11.4.9c–d feladat [372] alapján azzal ekvivalens, hogy $\sqrt{-5}$ primelem $E(\sqrt{-5})$-ben. Így azt kell igazolnunk, hogy

$$\sqrt{-5} \mid [a + b\sqrt{-5}] \left( c + d\sqrt{-5} \right) \Rightarrow \sqrt{-5} \mid a + b\sqrt{-5} \text{ vagy } \sqrt{-5} \mid c + d\sqrt{-5}. \quad (2)$$

Mivel $\sqrt{-5}$ önmagának osztója, ezért (2) ekvivalens az alábbi feltétel teljesülésével:

$$\sqrt{-5} \mid \omega c \Rightarrow \sqrt{-5} \mid a \text{ vagy } \sqrt{-5} \mid c. \quad (3)$$

Egy egész szám könnyen láthatóan pontosan akkor osztható $\sqrt{-5}$-tel, ha 5-tel osztható, tehát (3) átírható a következő alakba:

$$5 \mid \omega c \Rightarrow 5 \mid a \text{ vagy } 5 \mid c. \quad (4)$$

Az 5 az egész számok körében prim, ezért (4), és így (2) is valóban teljesül.

(Célhoz érhetünk volna a 10.3.7b feladat [338] felhasználásával is.)

- Legyen most $P$ egy $20k + 1$, $20k + 3$, $20k + 7$ vagy $20k + 9$ alakú pozitív primszám. A Legendre-szimbólum tulajdonságainak a felhasználásával könnyen adódik, hogy ezek éppen azok a prímek, amelyekre $\left(\frac{-5}{p}\right) = 1$. Ez azt jelenti, hogy az

$$x^2 \equiv -5 \text{ (mod } p)$$

kongruencia megoldható, vagyis létezik olyan $a$ egész szám, amelyre

$$p \mid a^2 + 5. \quad (5)$$

Megmutatjuk, hogy az $I_p = (p, a + \sqrt{-5})$ ideál felbonthatatlan ideál, és így prímideál. Ehhez azt kell igazolni, hogy $I_p \not= (1)$, $I_p \not= (0)$, továbbá $I_p$ csak triviális módon bontható két ideál szorzatára. Ez utóbbi teljesüléséhez a D 11.4.6 Definíció után adott ekvivalens átfogalmazások szerint elég azt belátni, hogy bármely $A$ ideálra

$$I_p \subseteq A \subseteq E(\sqrt{-5}) \Rightarrow A = I_p \text{ vagy } A = E(\sqrt{-5}). \quad (6)$$

Nyilván $I_p \not= (0)$.

Ha $I_p = (1)$ teljesülne, akkor alkalmas $\alpha$, $\beta \in E(\sqrt{-5})$ elemekkel az 1 előállna

$$1 = \alpha p + \beta [a + \sqrt{-5}] \quad (7)$$

alakban. A (7) egyenlőséget $a - \sqrt{-5}$-tel beszorozva kapjuk, hogy

$$a - \sqrt{-5} = \alpha [a - \sqrt{-5} p + \beta [c^2 + 5]. \quad (8)$$

Mivel (5) alapján (8) jobb oldala osztható $P$-vel, ezért a bal oldal is, vagyis

$$\frac{a}{p} - \frac{1}{p} \sqrt{-5} \in E(\sqrt{-5}),$$

622
ami nyilván lehetetlen. Ezzel beláttuk, hogy $I_p \neq (1)$.

A (6) tulajdonság igazolásához tegyük fel, hogy egy $A$ ideál valódi módon tartalmazza az $I_p$ ideált. Megmutatjuk, hogy $1 \in A$, azaz $A = E(\sqrt[5]{-5})$.

Vegyük egy tetszőleges

$$c + d\sqrt[5]{-5} \in A \setminus I_p$$

elemet. Ekkor

$$[c - d\sqrt[5]{-5}] - d[a - \sqrt[5]{-5}] = c - da \in A.$$  \hspace{1cm} (9)

Ha $p \mid c - da$, azaz alkalmas $u$ egész számmal

$$c = du + up,$$

akkor

$$c + d\sqrt[5]{-5} = d[a + \sqrt[5]{-5}] + up \in I_p,$$

ami ellentmond (9)-nek.

Ebből következik, hogy $c - da$ nem lehet osztható a $P$ prímszámmal, vagyis $c - da$ és $P$ (az egész számok körében) relatív prímek. Ekkor alkalmas $u'$ és $v'$ egész számokkal

$$1 = v'[c - du] + up'.$$ \hspace{1cm} (11)

Mivel $p \in A$ és (10) alapján $c - du \in A$, ezért (11) szerint $1 \in A$, amint állítottuk.

Most megmutatjuk, hogy a felsorolásból kínált, azaz a $20k + 11, 20k + 13, 20k + 17$ és $20k + 19$ alakú (pozitív) $P$ prímszámmokhoz nem található olyan $a$ egész szám, amelyre $(p, a + \sqrt[5]{-5})$ prímideál.

Ezekre a $P$ prímszámakra $(\frac{-5}{p}) = -1$, és így a T 10.3.7 Tétel alapján ezek a $P$ értékek $E(\sqrt[5]{-5})$-ben is primek. A 11.4.9c feladat [372] szerint ekkor $(p^l)$ primideál.

Tegyük fel indirekt, hogy alkalmas $a$ egész számra $(p, a + \sqrt[5]{-5})$ prímideál lenne. Mivel

$$(p) \subseteq (p, a + \sqrt[5]{-5}),$$

és így

$$(p, a + \sqrt[5]{-5}) \subseteq (p),$$

továbbá $(p, a + \sqrt[5]{-5})$ és $(p)$ is primideál, ezért csak $(p, a + \sqrt[5]{-5}) = (p)$ lehetséges. Ez azt jelenti, hogy $a + \sqrt[5]{-5} \in (p)$, és így

$$p \mid a + \sqrt[5]{-5};$$

és ezért

$$\frac{a}{p} + \frac{1}{p}\sqrt[5]{-5} \in E(\sqrt[5]{-5}),$$

ami lehetetlen.

• **11.5.9 [383]** Előre bocsátjuk, hogy a T 11.5.1 Tétel érvényes marad akkor is, ha algebrai egész helyett mindenhol egész számot írunk. Ez abból következik, hogy ha $u$ és $v$ egész számok, akkor az $u \mid v$ oszthatóság pontosan akkor teljesül az algebrai egészek körében, mint amikor az egész számok körében. Tekintsük ugyanis az $uv = v$ egyenlőséget. Ha $v$ egész szám, akkor nyilván $v$ algebrai egész is. Megfordítva, ha $v$ algebrai egész, akkor mivel $(u \neq 0$ esetén) $w = v/u$ racionális is, ezért $v$ szükségképpen egész szám.

A továbbiakban a T 11.5.1 Tételnek ezt az egész számokra vonatkozó speciális esetét fogjuk használni.
(a) Legyen a két primitív polinom
\[ f(x) = a_0 + a_1 x + \cdots + a_m x^m \quad \text{és} \quad g(x) = b_0 + b_1 x + \cdots + b_n x^n; \]
ez a szorzatuk
\[ f(x)g(x) = c_0 + c_1 x + \cdots + c_{m+n} x^{m+n}. \]
Tegyük fel indirekt, hogy \( f(x)g(x) \) nem primitív polinom, azaz létezik olyan \( p \) primszám, amelyre
\[ p \mid c_k, \quad k = 0, 1, \ldots, m + n. \]
Ekkor a T 11.5.1 Tétel (fent jelzett speciális esete) szerint
\[ p \mid a_i, \quad i = 0, 1, \ldots, m, \quad j = 0, 1, \ldots, n. \]
Mivel \( f \) és \( g \) is primitív polinom, ezért van olyan \( i \), illetve \( j \), amelyre
\[ p \mid a_i \quad \text{és} \quad p \mid b_j. \]
Ebből \( p \) primitulajdonsága szerint következik, hogy \( p \mid a_i b_j \), ami ellentmondás.

(b) Legyen az \( F \), illetve \( G \) polinomban az együtthatók nevezőinek legkisebb közös többszöröse \( r \), illetve \( s \). A \( H = \mathbb{F}_q \) egyenlőséget \( t = r s \)-sel beszorozva kapjuk, hogy
\[ t H(x) = F_2(x) G_2(x), \quad \text{ahol} \quad F_2(x), G_2(x) \in \mathbb{Z}[x]. \quad (12) \]
Ha \( t = 1 \), akkor készen vagyunk. Ha \( t > 1 \), akkor legyen \( p \) a \( t \) egy tetszőleges prímosztója. Ekkor \( p \) osztója az \( F_2(x) G_2(x) \) polinom minden együtthatójának.

Ha \( p \) nem osztója sem az \( F_2(x) \) polinom minden együtthatójának, sem pedig \( G_2(x) \) minden együtthatójának, akkor az (a) részben láttott módon ellentmondásba kerülünk a T 11.5.1 Tétellel. Így \( p \) osztója mondjuk \( F_2(x) \) minden együtthatójának, \( F_2(x) = p F_3(x) \).

A (12) egyenletet \( p \)-vel egyszerűsítve
\[ t H(x) = F_3(x) G_3(x), \quad F_3(x), G_3(x) \in \mathbb{Z}[x], \quad t_1 = \frac{t}{p}, \]
adódik. Ha \( t_1 = 1 \), akkor készen vagyunk, egyébként ismételjük meg az eljárást mindaddig, amíg a \( H \) polinom egy kívánt előállítását kapjuk.

11.6.3 [387](a) Mivel \( k \) és \( h \) relatív primek, ezért léteznek olyan \( \alpha \) és \( \psi \) pozitív egészek, amelyekre \(\bar{k}u = 1 + i\bar{\psi} \). Ekkor
\[ A^k \sim B^h \Rightarrow A^{k u} \sim B^{h u}, \]
az alkalmaz \( (\alpha) \) és \( (\beta) \) nemnulla főideálokra
\[ (\alpha) A^{k u} = (\beta) B^{h u}. \quad (13) \]
Írjuk be (13)-ban \( A^{k u} \), illetve \( B^{h u} \) helyére az \( A^{k \psi} \), illetve \( B^{h \psi} \) előállítást, és használjuk fel, hogy \( A^{k \psi} \) és \( B^{h \psi} \) főideál, legyen \( A^{k \psi} = (\gamma) \), \( B^{h \psi} = (\delta) \). Innen kapjuk, hogy
MEGOLDÁSOK

\[(cr) A = (35) B, \quad \text{azaz} \quad A \sim B.\]

- (b) Az (a) részt speciálisan \( B = (1) \)-ra alkalmazva \( A \sim (1) \) adódik, és így a 11.6.2/(iv) Tétel alapján \( A \) fölideál.

- **11.6.4 [387](d)** Megmutatjuk, hogy az \( x^2 + 35 = y^3 \) diofantikus egyenlet összes megoldása

\[x = \pm 36, \quad y = 11.\]

A T 11.6.5 Tétel bizonyításának a gondolatmenetét követjük. Fel fogjuk használni, hogy \( E(\sqrt{-35}) \) -ben az ideálosztályok száma \( h(\sqrt{-35}) = 2 \) (lásd a T 11.6.4 Tétel előtt megadott táblázatot). Ebből az is következik, hogy \( E(\sqrt{-35}) \)-ben nem érvényes a számmelélet alaptétele.

Az egyenlet bal oldalát \( E(\sqrt{-35}) \)-ben szorzattá bontjuk:

\[\left[ x - \sqrt{-35} \right] \left[ x + \sqrt{-35} \right] = y^3. \quad (14)\]

Mivel \( E(\sqrt{-35}) \)-ben nem érvényes a számmelélet alaptétele, ezért (14)-ről át kell térni a megfelelő fölideálok közötti egyenletre:

\[(x + \sqrt{-35})(x - \sqrt{-35}) = (y)^3. \quad (15)\]

Megmutatjuk, hogy az \((x + \sqrt{-35})\) és \((x - \sqrt{-35})\) ideálok relatív prímek. Tegyük fel indirekt, hogy van egy \( P \) primideál közös osztójuk. Ekkor \( P \) osztója \((y)^3\)-nak is, és mivel \( P \) primideál, ezért \((y)\)-nak is. Az oszthatóságoknak megfelelő tartalmazások alapján

\[\sqrt{-35} \left[ x - \sqrt{-35} \right] = 2 \cdot 35 = 70 \in P\]

is igaz.

Megmutatjuk, hogy \( y/7 \) és 70 relatív prímek (az egész számok körében).

Ha \( 7 \mid y \), akkor az eredeti egyenletből kapjuk, hogy \( x \) is osztható 7-tel, ekkor azonban a 7-nek \( x^2 + 35 \) pontosan az első, \( y^3 \) viszont legalább a harmadik hatványával osztható, ami lehetetlen.

Ugyanígy kapjuk, hogy \( 5 \mid y \).

Ha \( 2 \mid y \), akkor \( x \) páratlan, és az egyenlet bal oldala 4, a jobb oldala viszont 0 maradékot ad 8-cal osztva, ami szintén lehetetlen.

Ezzel beláttuk, hogy \( y \) és 70 relatív prímek. Ekkor alkalmaz \( r \) és \( s \) egész számokra \( 1 = 7r + 10s \).

Mivel \( 7 \) és \( y \) is eleme \( P \)-nek, ezért az \( 1 \) is eleme \( P \)-nek, azaz \( P = (1) \), ami ellentmond annak, hogy \( P \) primideál.

Így a (15) egyenlőség bal oldalán szereplő két (fő)ideál valóban relatív prim. Az ideálokra vonatkozó egyértelmű prímfaktorizációból (T 11.5.8 Tétel) következik, hogy mindkét ideál egy alkalmaz ideál köbe, azaz (például)

\[(x + \sqrt{-35}) \equiv A^3. \quad (16)\]
Mivel $E(\sqrt{-35})$-ben az ideálosztályok száma $\hat{n}(\sqrt{-35}) = 2$, ezért a T 11.6.4 Tétel szerint $A^2$ főideál, $A^2 = (\gamma)$. Ezt a (16) egyenlősége beírva

$$(x + \sqrt{-35}) = (\gamma).$$

adódik, amiből a 11.4.3b feladat [371] alapján kapjuk, hogy $A$ főideál, azaz $A = (\alpha)$. Ekkor (16) átírható az

$$(x + \sqrt{-35}) = (\alpha^2), \quad \text{ez felül} \quad x + \sqrt{-35} = \varepsilon \alpha^2$$

alakba, ahol $\varepsilon$ egység $E(\sqrt{-35})$-ben. Az $E(\sqrt{-35})$ egységei csak a $\pm 1$, és ezek maguk is köbszámok. Ezért (17) tovább ekvivalens azzal, hogy

$$x + \sqrt{-35} = \beta^3 = [a + b\sqrt{-35}]^3,$$  \hspace{1cm} (17)

ahol $-35 \equiv 1 \text{ (mod 4)}$ miatt $a$ és $b$ egész számok vagy pedig $a = u/2$ és $b = v/2$, ahol $u$ és $v$ páratlan egészek.

A köbre emelést elvégezve és a képzetes részeket összehasonlitva

$$1 = 3a^2b - 35b^2 = 5[3a^2 - 35b^2]$$

adódik.

Ha $a$ és $b$ egész számok, akkor innen $b = \pm 1$, azonban $a$-ra nem kapunk egész értéket.

Ha $a = n/2$ és $b = v/2$, ahol $n$ és $v$ páratlan, akkor (19)-et 8-cal szorozva adódik, hogy

$$8 = \varepsilon[3n^2 - 35v^2].$$

Mivel $\varepsilon$ páratlan, ezért

$$v = \pm 1 \quad \text{és} \quad 3n^2 - 35v^2 = 3n^2 - 35 = \pm 8.$$  \hspace{1cm} (18)

Innen $u = \pm 3$ és $v = -1$. Ezeket az értékeket (18)-ba visszahelyettesítve és a valós részeket összehasonlitva kapjuk, hogy

$$x = \frac{u[n^2 - 15v^2]}{8} = \pm 3\beta \quad \text{és} \quad y = \sqrt{2x^2 + 35} = 11.$$  \hspace{1cm} (19)

12. Kombinatorikus számelmélet

- **12.1.3 [395]** Először egy konstrukciót adunk arra, hogy a megoldásszám elérhető $[k/2]$-t. Legyen $k = 2j - 1$ vagy $2j$, ekkor $[k/2] = j$. Az útmutatásban javasoltaknak megfelelően legyen

$$q > j, a_1 = q + 1, a_2 = q + 2, \ldots, a_j = q + j \quad \text{és} \quad t = a_1 + a_2 + \cdots + a_j.$$  \hspace{1cm} (20)

Ezután legyen $a_{j+1} = a_1 + a_2$, ekkor

$$t = a_3 + a_4 + \cdots + a_j + a_{j+1}.$$  \hspace{1cm} (21)
is igaz. Hasonlóan folytatva legyen \( a_{j+2} = a_5 + a_4 \), ekkor a
\[
l = a_5 + a_6 + \cdots + a_{j+1} + a_{j+2}
\]
előállítás is érvényes.

Általában legyen \( a_{j+\tau} = a_{2\tau-1} + a_{2\tau} \), ha \( \tau \leq j - 1 \) (és \( k = 2j \) esetén legyen \( a_{2j} \) tetszőleges, \( a_{2j-1} \)-nél nagyobb szám). Ekkor
\[
l = a_{2\tau+1}1 + a_{2\tau+2}2 + \cdots + a_{j+\tau}
\]
ily módon \( a_s < a_{s+1} \) minden \( s \) esetén fennáll: \( s < j \) -re az \( a_s \) -eket így választottuk, \( s = j \) -re \( a_{j+1} = a_1 + a_2 = 2q + 3 > a_j = q + j \) (hiszen \( q > j \)), \( j < s \leq 2j - 2 \) -re pedig \( a_{s+1} \) mindig két későbbi \( a_i \) -nek az összege, mint \( a_s \).

Az eljárást végigvive \( l \) előállítás, \( j \), \( j = 1 \ldots \ldots \) szomszédos \( a_i \) összegekért, míg végül egytagú összegként is megjelenik, ami összesen a kívánt \( j \) számú előállítás.

Most megmutatjuk, hogy ennél nagyobb előállításszám nem lehetséges. Vegyünk egy tetszőleges \( a_1 \ldots \ldots a_k \) rendszer és egy \( l \) számot, és tekintük \( l \) -nek azt az előállítását, amelyben az utolsó (azaz a legnagyobb) tag a lehető legkisebb, legyen az indexe \( v \).

Ha \( v > j \), akkor legfeljebb \( k - (v - 1) \leq j - j \) előállítás lehetséges, hiszen mindegyiknek szükségképpen az utolsó tagja.

Ha \( v \leq j \), akkor mivel minden előállítás tagszáma más és minden tagszám legfeljebb \( v \), tehát legfeljebb \( v \leq j \) előállítás lehetséges.

- **12.2.3 [404]** Tekintsük a \( P^2 \) elemű \( T_2 \) véges testet és ebben a \( P \) elemű \( T_1 \) résztestet. Mivel egy véges test multilikatív csoportja ciklikus, így van \( T_2 \) -nek olyan \( \Delta \) eleme, amelynek a hatványai \( T_2 \) minden nemnulla elemét előállítják.

Vegyünk egy tetszőleges \( \Theta \in T_2 \setminus T_1 \) elemet, és legyenek \( T_1 \) elemei \( \gamma_1 \ldots \gamma_n \).Írjuk fel a \( \Theta + \gamma_i \) elemeiket \( \Theta + \gamma_i = \Delta^u \) alakban, ezzel kijelöltünk \( P \) darab \( a_i \) egész számot 1 és \( p^2 - 1 \) között.

Megmutatjuk, hogy ezek eleget tesznek a feltételnek, azaz az \( a_i + a_j \) összegek páronként különböző maradékokat adnak modulo \( p^2 - 1 \).

Tegyük fel, hogy \( a_i + a_j = a_k + a_q \ (\text{mod} \ p^2 - 1) \). Ekkor az \( a_i \) -k definíciója alapján
\[(\Theta + \gamma_i)(\Theta + \gamma_j) - (\Theta + \gamma_i)(\Theta + \gamma_j) = 0 \]
adódnak. A bal oldal \( \Theta \) -nak legfeljebb elsőfokú polinomja \( T_1 \) -beli együttthatók, hiszen \( \Theta^2 \) kiesik. Elsőfokú azonban nem lehet, mert akkor \( \Theta \in T_1 \) következne, így — mivel a \( \Theta \) gyöké — csak az azonosan nulla polinom lehet. Ekkor azonban pl. a polinomok gyöktényezős alakjának az egyértelműsége miatt \( \{\gamma_i, \gamma_j\} \rightleftharpoons \{\gamma_k, \gamma_l\} \), és így ugyanez áll az \( a_i \) -kre is, ami éppen a bizonyítandó állítás volt.

- **12.2.4 [404]** Az útmutatást követve vegyünk egy \( \tilde{g} \) primitív gyököt modulo \( P \), és legyen \( a_i \ az \ x \equiv i \ (\text{mod} \ p - 1) \), \( x \equiv g^i \ (\text{mod} \ p) \) szimultán kongruenciarendszer megoldása modulo \( p(p - 1), i = 1, 2, \ldots, p - 1 \). Nyilván elég azt megmutatnunk, hogy bármely \( c \) -re a \( c = a_i + a_j \ (\text{mod} \ p(p - 1)) \) kongruencia legfeljebb egyetlen \( \{i, j\} \) -vel teljesülhet. Az \( a_i \) definíciója alapján ez a kongruencia a \( c \equiv i + \tilde{g} \ (\text{mod} \ p - 1) \), \( c \equiv g^i + g^j \ (\text{mod} \ p) \) szimultán...
kongruenciarendszerrel ekvivalens. Itt az első kongruencia átírható a \( g^e \equiv g^i \pmod{d} \) alakba, vagyis a \( g^i \) és \( g^j \) számok összegét és szorzatát is ismerjük modulo \( d \). A gyökök és együtthatók közötti összefüggés alapján a \( g^i \) és \( g^j \) maradékosztályok a \( z^2 - cz + g^e \equiv 0 \pmod{d} \) másodfokú kongruencia egyértelműen meghatározott gyökei (\( P \) prim), és így \( i \) és \( j \) is egyértelmű.

- **12.3.6 [414]** Az útmutatást követve legyen \( |C| = |D| = n < p \), \( C = \{c_1, \ldots, c_n\} \), \( A_1 = \cdots = A_n = D \) és

\[
F(x_1, \ldots, x_n) = \prod_{1 \leq j < i \leq n} (x_i - x_j)(x_i + c_i - x_j - c_j).
\]

Ekkor \( F \) foka \( n(n-1) \), így ha \( \prod_{i=1}^{n} x_i^{n-1} \) együthatója nem nulla, akkor a 12.3.5b feladat [414] alapján van olyan \( d_1, \ldots, d_n \in D \), amelyre

\[
F(d_1, \ldots, d_n) = \prod_{1 \leq j < i \leq n} (d_i - d_j)(d_i + c_i - d_j - c_j) = 0.
\]

Ekkor szükségképpen \( d_i \neq d_j \), ha \( i \neq j \), vagyis \( d_1, \ldots, d_n \) kiadják a \( D \) összes elemét, továbbá \( c_i + d_i \neq c_j + d_j \), ha \( i \neq j \), azaz \( c_i \leftrightarrow d_i \) egy megfelelő párba állítás a \( C \) és \( D \) halmaz elemei között. Most igazoljuk, hogy \( F \) -ben a \( \prod_{i=1}^{n} x_i^{n-1} \) tag együthatója nem nulla. \( F \) -ben a \( \deg F = n(n-1) \)-edfokú tagokat \( \prod_{1 \leq i < j \leq n} (x_i - x_j)^2 \) adj (a többi tag ennél alacsonyabb fokú). Ez a rész nem más, mint a

\[
V(x_1, \ldots, x_n) = \begin{vmatrix}
1 & x_1 & \ldots & x_1^{n-1} \\
1 & x_2 & \ldots & x_2^{n-1} \\
\vdots & \vdots & \ddots & \vdots \\
1 & x_n & \ldots & x_n^{n-1}
\end{vmatrix}
\]

Vandermonde-determináns négyszöge. Írjuk fel \( V(x_1, \ldots, x_n) \) -et a determináns definíciója szerint, és vizsgáljuk meg, mi lesz az önmagával való szorzatában a kérdéses \( \prod_{i=1}^{n} x_i^{n-1} \) tag együthatója. Ilyen tagot akkor kapunk, ha az egyik determinánsból a

\[
(-1)^{\ell(j_1, \ldots, j_n)} x_{j_1}^{j_1} \cdots x_{j_n}^{j_n}
\]

tagot a másik determinánsból a

\[
(-1)^{\ell(u-1-j_1, \ldots, n-1-j_n)} x_{u-1-j_1}^{j_1} \cdots x_{n-1-j_n}^{j_n}
\]

tagtával szorozzuk össze (ahol \( \ell() \) a megfelelő oszlopindex-permutációk inverziózását jelölő, az oszlopokat 0-tól \( n-1 \)-ig számozottuk). Mivel az előjelet meghatározó két permutáció éppen egymás „komplementere”, ezért

\[
I(j_1, \ldots, j_n) + I(u-1-j_1, \ldots, n-1-j_n) = \binom{\ell_i}{2}.
\]

vagyis minden ilyen szorzat

\[
(-1)^{\binom{\ell_i}{2}} x_1^{n-1} \cdots x_n^{n-1}.
\]
Mivel $n!$ ilyen sorzat képezhető, így $F_n$-ben a $\prod_{i=1}^{n} x_i^{a-1}$ tag együtthatója $(-1)^{\binom{n}{2}} n!$, ami $n < p$ miatt valóban nem nulla, amint állítottuk.

- **12.4.11 [419]b** Tegyük fel indirekt, hogy az útmutatás szerinti színezésben az $1 \leq b < b + d < b + 2d < \cdots < b + pd \leq p(2^d - 1)$ számok mind azonos színűek. Legyen $\Theta = \Delta^b$, $\Psi = \Delta^d$. A feltétel szerint ekkor a $\Theta, \Theta \Psi, \ldots, \Theta \Psi^p$ „vektorok” vagy valamennyien a $W$ altérbe esnek, vagy pedig egymük sem esik $W$-be.

Ha a számú sorozat piros, akkor tehát ezek a vektorok egy $p - 1$-dimenziós altér elemei. Ezért közülük már az első $P$ darab is lineárisan összefüggő, azaz alkalmas $\gamma \in \mathbb{Z}_2$ együtthatókkal $\sum_{i=0}^{p-1} \gamma_i (\Theta \Psi^i) = 0$ nemtriviálisan teljesül. Az egyenlőséget $\Theta$-val elosztva azt kapjuk, hogy $\Psi$ gyöke egy $p$-nél alacsonyabb fokú $\mathbb{Z}_2$ feletti polinomnak. Mivel $\Psi$ foka osztója $\Theta$ fokának, vagyis $p$-nek, ezért $\Psi$ foka csak 1 lehet, azaz $\Psi \in \mathbb{Z}_2$. Ez azonban ellentmondás, hiszen nyilván $\Psi \neq 0$ és $d < 2^p - 1$ miatt $\Psi \neq 1$.

Ha a számú sorozat kék, akkor a $\Theta \Psi - \Theta, \Theta \Psi^2 - \Theta \Psi, \ldots, \Theta \Psi^p - \Theta \Psi^{p-1}$ vektorokra kell megismételni az előző gondolatmenetet (csak $\Theta$ helyett most $\Psi$-gyel kell a megfelelő egyenlőséget elosztani).

- **12.4.12 [420]** Az útmutatást követve tekintsük azokat a számokat $u$-ig, amelyeket a $d$ alapú számrendszerben felírva minden számjegy $< d/2$ és a számjegyek négyzetösszege egy adott $Q$ érték. Ha három ilyen szám számú sorozatot alakítottak, akkor minden számjegyükre ugyanez áll fenn, mert a jegyekre adott korlátozás miatt két szám összeadása során sohasem képződik átvitel a következő helyiértékre. Így a középső szám valamennyi jegye a másik két szám megfelelő jegyeinek számtani középe. Felirva, hogy mindhárom szám jegyeinek négyzetösszege $Q$, egyszerű számolással adódik, hogy a számok szükségképpen egyenlők. (Más megfogalmazásban: ha a három számt a számjegyeikből alkotott vektoroknak tekintjük, akkor a harmadik vektor az első kettő összegének a fele, továbbá mindhárom vektor euklideszi normája egyenlő. Ez csak úgy lehet, ha maguk a vektorok is megegyeznek.)

Adott $d$ mellett a felírásban szereplő számjegyek száma $u \approx (\log d)/(\log d)$, és $Q$-nak legfeljebb $u^2p/4$-féle értéke lehet. Ha a halmazainkat minden lehetséges $Q$-ra egyesítjük, akkor az összes olyan számot megkapjuk, amelyek valamennyi jegye $d/2$-nél kisebb. Ez összesen kb. $n^{2n}$ szám. Ezért biztosan van olyan $Q$, amelynek megfelelő halmaz elemszáma legalább $n^{(2n-2)pd^2}$. Ez akkor veszi fel a maximumát ha $\log d \approx \sqrt{\log n}$, és ez a maximum éppen a feladat állításában előírt érték.

---

629
15. fejezet - TÖRTÉNETI NÉVTÁR

A könyv során több helyen kitértünk a számelmélet történetének néhány vonatkozására. A következő összefoglalóban megadjuk a könyvbén név szerint említett legtöbb matematikus születési és halálozási évszámát, nemzetiségét, valamint röviden utalunk számelméleti munkásságukra. Ez a könyv történeti kitekintés szükségszerűen szubjektív, több okból is. Először is, csak olyan matematikusok szerepelnek benne, akik a könyvben tárgyalt fejezeteivel kapcsolatba hozhatók, azok történetében szerepet játszottak. Ebből az is következik, hogy a számelmélet sok jelentős kutatója kimaradt. Másodszor, a felsorolt matematikusoknak sem feltétlenül a legjelentősebb eredményeit tudjuk említeni, még kevésbé méltatni, nem beszélve a matematika egyéb területein végzett munkásságukról. Így az alábbi összefoglaló semmiképpen sem tekinthető az adott matematikusok fontosságát, szerepét bemutató elemző értékelésnek, hanem csak olyan változatnak, amely a könyvben tárgyalt számelméleti anyaghoz némi történeti hátteret kölcsönöz.


Diophantosz, i.sz. 250 körül élt Alexandriában, görög. Róla nevezték el az olyan (általában) egész együtthatós algebrai egyenleteket, amikor a megoldásokat az egész (esetleg a racionális) számok körében keressük. Az ó nevét őrzi a diofantikus egyenletek vizsgálatában fontos szerepet játszó diofantikus approximáció is.

Dirichlet, Peter Lejeune (ejtsd: dirislé vagy dirichlé), 1805–1859, német. Hatékonyan alkalmazta az analízis módszeiret a számelméletben. Bebizonyította azt a később róla elnevezett tételt, hogy ha egy számú sorozat első eleme és differenciája relatív prímek, akkor a sorozat végtelen sok prímszámot tartalmaz. A Dirichlet-sorok a számelméleti függvények vizsgálatának ma is fontos eszközei.


Gauss, Carl Friedrich, 1777–1855, német. Minden idők talán legnagyobb, legsokoldalúbb matematikusa. 1801-ben jelent meg Disquisitiones arithmeticae c. könyve, amelyben többek között a másodfokú kongruenciák elméletének részletes tárgyalása szerepel. Gauss vezette be a kongruenciáknál ma is használatos jelölésszedzert, valamint a róla elnevezett Gauss-egészeket, amelyek később mintául szolgáltak az algebrai számtástek vizsgálatához. Gauss-tól származik a háromnégyzetszám-tétel, valamint a szabályos sokszögek euklideszi szerkeszthetőségére vonatkozó tétel is.

Gelfond, Alekszandr Oszipovics, 1906–1968, orosz. ő és Schneider igazolták (egyidejüleg, de egymástól függetlenül) Hilbertnek azt a sejtését, hogy egy (0-tól és 1-től különböző) algebrai szám irracionális algebrai kitevős hatványa mindig transzcendens.


Hadamard, Jacques (ejtsd: ádámár), 1865–1963, francia. ő és de la Vallée Poussin igazolták elsőként (egyidejüleg, de egymástól függetlenül) a prímszámtételt.


Hilbert, David, 1862–1943, német. Az 1900-as párizsi matematikai kongresszuson tartott híres előadásában 23 problémakört vázolt fel, amelyeket a matematikai kutatások szempontjából kiemelkedő fontosságúaknak tartott, és ezzel (is) óriási hatást gyakorolt a huszadik század matematikájára. A Hilbert-problémák között több számtanbeli is található. Hilbert bizonyította be elsőként a Waring-problémákban szereplő \(g(k)\) létezését.

Jacobi, Carl, 1804–1851, német. A számelméletben a Legendre-szimbólum általánosításaként kapott Jacobi-szimbólum őrzi a nevét.


Kronecker, Leopold, 1823–1891, német. Az algebrai bővítések ideáljaival kapcsolatban ért el jelentős eredményeket.


Lamé, Gabriel, 1795–1870, francia. Az utókor számára leginkább egy, a Fermat-sejtésre adott hibás bizonyítása által vált híressé.
Legendre, Adrien-Marie (ejtsd: lőzsandr), 1752–1833, francia. Nevét űrzi a másodfokú kongruenciáknál szereplő Legendre-szimbólum, valamint az \( \tau \) kanonikus alakjára vonatkozó Legendre-formula.

Lindemann, Ferdinand, 1852–1939, német. Bebizonyította 1882-ben, hogy \( \pi \) transzcendens, és ezzel lezárta \( \alpha(z \text{ euklideszi értelmemben vett}) \) körmûszögesítés kétézer éves problémáját.


Mersenne, Marin (ejtsd: merszen), 1588–1648, francia. Kiváló tudományosvezető, aki kiterjedt levelezést folytatott Fermat-val, Descartes-tal és a kor számos más kiemelkedő tudósával. A később róla elnevezett primek elsősorban a tökéletes számokkal való kapcsolatuk miatt érdekeltek. Az ilyen primekről 1644-ben közzétett listája meglepően kevés hibát tartalmaz (a lista ellenőrzésének matematikai és technikai eszközeire több, mint kétszáz évet kellett kellett várni).


Möbius, Ferdinand, 1790–1868, német. Az általa bevezetett \( \mu \)-függvény igen fontos szerepet játszik a szármeléleti függvények vizsgálatánál, valamint a prímszármelméletben (emellett a Möbius-szalag is az ő nevét viseli).

Poussin, Charles de la Vallée (ejtsd: pusszen, dö la valé), 1866–1962, belga. Ő és Hadamard igazolták elsőként (egyidejűleg, de egymástól függetlenül) a prímszámtételt.


Riemann, Bernhard, 1826–1866, német. A prímszámtétel bizonyításához vezető út kidolgozója, az ő elvei alapján igazolta a tételt egymástól függetlenül Hadamard és de la Vallée Poussin 1896-ban. Euler gondolatait továbbfejleszte Riemann rámutatott a róla elnevezett zétafüggvény központi jelentőségére a prímszámok eloszlásának vizsgálatában. Ehhez a függvényhez kapcsolódik a ma is megoldatlan Riemann-sejtés.

Schneider, Theodor, 1911–1988, német. Ő és Gelfond igazolták (egyidejűleg, de egymástól függetlenül) Hilbertnek az algebrai számok irracionalis algebrai kitevős hatványaira vonatkozó problémáját.

Schur, Issai, 1875–1941, (a náci által zsidó származása miatt elűzött) német. Híres tétele, hogy véges sok színnel kiszínezve a természetes számok elég nagy kezdőszekletet, mindig lesz az \( z \equiv y \equiv z \) egyenletnek egyszínű megoldása.

Thue, Axel, 1863–1922, norvég. Fontos eredményeket ért el a diofantikus approximációban és a diofantikus egyenletek területén.


Wilson, John, 1741–1793, angol. Nevét a $(p - 1)!$ modulo $p$ maradékáról szóló tétel őrzi.
### 16. fejezet - Táblázatok

#### Prímszámok 2–1733

<p>| | | | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>127</td>
<td>283</td>
<td>467</td>
<td>661</td>
<td>877</td>
<td>1087</td>
<td>1297</td>
<td>1523</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>131</td>
<td>293</td>
<td>479</td>
<td>673</td>
<td>881</td>
<td>1091</td>
<td>1301</td>
<td>1531</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>137</td>
<td>307</td>
<td>487</td>
<td>677</td>
<td>883</td>
<td>1093</td>
<td>1303</td>
<td>1543</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>139</td>
<td>311</td>
<td>491</td>
<td>683</td>
<td>887</td>
<td>1097</td>
<td>1307</td>
<td>1549</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>149</td>
<td>313</td>
<td>499</td>
<td>691</td>
<td>907</td>
<td>1103</td>
<td>1319</td>
<td>1553</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>151</td>
<td>317</td>
<td>503</td>
<td>709</td>
<td>911</td>
<td>1109</td>
<td>1321</td>
<td>1559</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>157</td>
<td>331</td>
<td>509</td>
<td>709</td>
<td>919</td>
<td>1117</td>
<td>1327</td>
<td>1567</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>163</td>
<td>337</td>
<td>521</td>
<td>719</td>
<td>929</td>
<td>1123</td>
<td>1361</td>
<td>1571</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>167</td>
<td>347</td>
<td>523</td>
<td>727</td>
<td>937</td>
<td>1129</td>
<td>1367</td>
<td>1579</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>173</td>
<td>349</td>
<td>541</td>
<td>733</td>
<td>941</td>
<td>1151</td>
<td>1373</td>
<td>1583</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| | | | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
<td>179</td>
<td>353</td>
<td>547</td>
<td>739</td>
<td>947</td>
<td>1153</td>
<td>1381</td>
<td>1597</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>181</td>
<td>359</td>
<td>557</td>
<td>743</td>
<td>953</td>
<td>1163</td>
<td>1399</td>
<td>1601</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>41</td>
<td>191</td>
<td>367</td>
<td>563</td>
<td>751</td>
<td>967</td>
<td>1171</td>
<td>1409</td>
<td>1607</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>43</td>
<td>193</td>
<td>373</td>
<td>569</td>
<td>757</td>
<td>971</td>
<td>1181</td>
<td>1423</td>
<td>1609</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>197</td>
<td>379</td>
<td>571</td>
<td>761</td>
<td>977</td>
<td>1187</td>
<td>1427</td>
<td>1613</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>53</td>
<td>199</td>
<td>383</td>
<td>577</td>
<td>769</td>
<td>983</td>
<td>1193</td>
<td>1429</td>
<td>1619</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>59</td>
<td>211</td>
<td>389</td>
<td>587</td>
<td>773</td>
<td>991</td>
<td>1201</td>
<td>1433</td>
<td>1621</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>61</td>
<td>223</td>
<td>397</td>
<td>593</td>
<td>787</td>
<td>997</td>
<td>1213</td>
<td>1439</td>
<td>1627</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>67</td>
<td>227</td>
<td>401</td>
<td>599</td>
<td>797</td>
<td>1009</td>
<td>1217</td>
<td>1447</td>
<td>1637</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>71</td>
<td>229</td>
<td>409</td>
<td>601</td>
<td>809</td>
<td>1013</td>
<td>1223</td>
<td>1451</td>
<td>1657</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| | | | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>73</td>
<td>233</td>
<td>419</td>
<td>607</td>
<td>811</td>
<td>1019</td>
<td>1229</td>
<td>1453</td>
<td>1663</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>79</td>
<td>239</td>
<td>421</td>
<td>613</td>
<td>821</td>
<td>1021</td>
<td>1231</td>
<td>1459</td>
<td>1667</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>83</td>
<td>241</td>
<td>431</td>
<td>617</td>
<td>823</td>
<td>1031</td>
<td>1237</td>
<td>1471</td>
<td>1669</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>89</td>
<td>251</td>
<td>433</td>
<td>619</td>
<td>827</td>
<td>1033</td>
<td>1249</td>
<td>1481</td>
<td>1693</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>97</td>
<td>257</td>
<td>439</td>
<td>631</td>
<td>829</td>
<td>1039</td>
<td>1259</td>
<td>1483</td>
<td>1697</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>101</td>
<td>263</td>
<td>443</td>
<td>641</td>
<td>839</td>
<td>1049</td>
<td>1277</td>
<td>1487</td>
<td>1699</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>103</td>
<td>269</td>
<td>449</td>
<td>643</td>
<td>853</td>
<td>1051</td>
<td>1279</td>
<td>1489</td>
<td>1709</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>107</td>
<td>271</td>
<td>457</td>
<td>647</td>
<td>857</td>
<td>1061</td>
<td>1283</td>
<td>1493</td>
<td>1721</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>109</td>
<td>277</td>
<td>461</td>
<td>653</td>
<td>859</td>
<td>1063</td>
<td>1289</td>
<td>1499</td>
<td>1723</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>113</td>
<td>281</td>
<td>463</td>
<td>659</td>
<td>863</td>
<td>1069</td>
<td>1291</td>
<td>1511</td>
<td>1733</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Prímszámok 1741–3907

<table>
<thead>
<tr>
<th>Prím</th>
<th>Prím</th>
<th>Prím</th>
<th>Prím</th>
<th>Prím</th>
<th>Prím</th>
<th>Prím</th>
<th>Prím</th>
</tr>
</thead>
<tbody>
<tr>
<td>1741</td>
<td>1993</td>
<td>2221</td>
<td>2437</td>
<td>2689</td>
<td>2909</td>
<td>3187</td>
<td>3433</td>
</tr>
<tr>
<td>1747</td>
<td>1997</td>
<td>2237</td>
<td>2441</td>
<td>2693</td>
<td>2917</td>
<td>3191</td>
<td>3449</td>
</tr>
<tr>
<td>1753</td>
<td>1999</td>
<td>2239</td>
<td>2447</td>
<td>2699</td>
<td>2927</td>
<td>3203</td>
<td>3457</td>
</tr>
<tr>
<td>1759</td>
<td>2003</td>
<td>2243</td>
<td>2459</td>
<td>2707</td>
<td>2939</td>
<td>3209</td>
<td>3461</td>
</tr>
<tr>
<td>1777</td>
<td>2011</td>
<td>2251</td>
<td>2467</td>
<td>2711</td>
<td>2953</td>
<td>3217</td>
<td>3463</td>
</tr>
<tr>
<td>1783</td>
<td>2017</td>
<td>2267</td>
<td>2473</td>
<td>2713</td>
<td>2957</td>
<td>3221</td>
<td>3467</td>
</tr>
<tr>
<td>1787</td>
<td>2027</td>
<td>2269</td>
<td>2477</td>
<td>2719</td>
<td>2963</td>
<td>3229</td>
<td>3469</td>
</tr>
<tr>
<td>1789</td>
<td>2029</td>
<td>2273</td>
<td>2503</td>
<td>2729</td>
<td>2969</td>
<td>3251</td>
<td>3491</td>
</tr>
<tr>
<td>1801</td>
<td>2039</td>
<td>2281</td>
<td>2521</td>
<td>2731</td>
<td>2971</td>
<td>3253</td>
<td>3499</td>
</tr>
<tr>
<td>1811</td>
<td>2053</td>
<td>2287</td>
<td>2531</td>
<td>2741</td>
<td>2999</td>
<td>3257</td>
<td>3511</td>
</tr>
<tr>
<td>1823</td>
<td>2063</td>
<td>2293</td>
<td>2539</td>
<td>2749</td>
<td>3001</td>
<td>3259</td>
<td>3517</td>
</tr>
<tr>
<td>1831</td>
<td>2069</td>
<td>2297</td>
<td>2543</td>
<td>2753</td>
<td>3011</td>
<td>3271</td>
<td>3527</td>
</tr>
<tr>
<td>1847</td>
<td>2081</td>
<td>2309</td>
<td>2549</td>
<td>2767</td>
<td>3019</td>
<td>3299</td>
<td>3529</td>
</tr>
<tr>
<td>1861</td>
<td>2083</td>
<td>2311</td>
<td>2551</td>
<td>2777</td>
<td>3023</td>
<td>3301</td>
<td>3533</td>
</tr>
<tr>
<td>1867</td>
<td>2087</td>
<td>2333</td>
<td>2557</td>
<td>2789</td>
<td>3037</td>
<td>3307</td>
<td>3539</td>
</tr>
<tr>
<td>1871</td>
<td>2089</td>
<td>2339</td>
<td>2579</td>
<td>2791</td>
<td>3041</td>
<td>3313</td>
<td>3541</td>
</tr>
<tr>
<td>1873</td>
<td>2099</td>
<td>2341</td>
<td>2591</td>
<td>2797</td>
<td>3049</td>
<td>3319</td>
<td>3547</td>
</tr>
<tr>
<td>1877</td>
<td>2111</td>
<td>2347</td>
<td>2593</td>
<td>2801</td>
<td>3061</td>
<td>3323</td>
<td>3557</td>
</tr>
<tr>
<td>1879</td>
<td>2113</td>
<td>2351</td>
<td>2609</td>
<td>2803</td>
<td>3067</td>
<td>3329</td>
<td>3559</td>
</tr>
<tr>
<td>1889</td>
<td>2129</td>
<td>2357</td>
<td>2617</td>
<td>2819</td>
<td>3079</td>
<td>3331</td>
<td>3571</td>
</tr>
<tr>
<td>1901</td>
<td>2131</td>
<td>2371</td>
<td>2621</td>
<td>2833</td>
<td>3083</td>
<td>3343</td>
<td>3581</td>
</tr>
<tr>
<td>1907</td>
<td>2137</td>
<td>2377</td>
<td>2633</td>
<td>2837</td>
<td>3089</td>
<td>3347</td>
<td>3583</td>
</tr>
<tr>
<td>1913</td>
<td>2141</td>
<td>2381</td>
<td>2647</td>
<td>2843</td>
<td>3109</td>
<td>3359</td>
<td>3593</td>
</tr>
<tr>
<td>1931</td>
<td>2143</td>
<td>2383</td>
<td>2657</td>
<td>2851</td>
<td>3119</td>
<td>3361</td>
<td>3607</td>
</tr>
<tr>
<td>1933</td>
<td>2153</td>
<td>2389</td>
<td>2659</td>
<td>2857</td>
<td>3121</td>
<td>3371</td>
<td>3613</td>
</tr>
<tr>
<td>1949</td>
<td>2161</td>
<td>2393</td>
<td>2663</td>
<td>2861</td>
<td>3137</td>
<td>3373</td>
<td>3617</td>
</tr>
<tr>
<td>1951</td>
<td>2179</td>
<td>2399</td>
<td>2671</td>
<td>2879</td>
<td>3163</td>
<td>3389</td>
<td>3623</td>
</tr>
<tr>
<td>1973</td>
<td>2203</td>
<td>2411</td>
<td>2677</td>
<td>2887</td>
<td>3167</td>
<td>3391</td>
<td>3631</td>
</tr>
<tr>
<td>1979</td>
<td>2207</td>
<td>2417</td>
<td>2683</td>
<td>2897</td>
<td>3169</td>
<td>3407</td>
<td>3637</td>
</tr>
<tr>
<td>1987</td>
<td>2213</td>
<td>2423</td>
<td>2687</td>
<td>2903</td>
<td>3181</td>
<td>3413</td>
<td>3643</td>
</tr>
</tbody>
</table>

Prímtényezős felbontás

Az alábbi táblázatban megadjuk az 1100-nál kisebb, 2-vel, 3-mal és 5-tel nem osztható pozitív összetett számok prímtényezős felbontását.
Mersenne-számok

Mersenne-számoknak az \( M_p = 2^p - 1 \) alakú számokat nevezzük, ahol \( p > 0 \) primszám. Ezekkel részletesen foglalkozunk az 5.2 pontban, és ott megtalálható a 2005-ben ismert 43 ilyen alakú prim listája is.

Az alábbi táblázatban megadjuk a 10 és 100 közötti kitevőkhöz tartozó Mersenne-számok prímtényezős felbontását.
Fermat-számok

Fermat-számoknak az $F_n = 2^{2^n} + 1$ alakú számokat nevezzük, ahol $n \geq 0$ egész, ezekkel részletesen foglalkozunk az 5.2 pontban.

A $0 \leq n \leq 4$ értékekre $F_n$ prím:

\[
F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537.
\]

Egyelőre $n > 5$-re nem találtak prímet a Fermat-számok között.

Az $F_5$, $F_6$ és $F_7$ primitívgyökök felbontása a következő:

\[
F_5 = 641 \cdot 6700417 \\
F_6 = 274177 \cdot 67289421310721 \\
F_7 = 59649589127437217 \cdot 5704689200685129054721
\]

Ezeken kívül 2005-ben még $8 \leq n \leq 11$ esetén ismert az $F_n$ primitívgyökök felbontása.
$F_{14}$-ről megmutatták, hogy összetett, de nem tudták még egyetlen nemtriviális osztóját sem meghatározni.

$F_{33}$ a legkisebb olyan Fermat-szám, amelyről nem ismert, hogy prim-e vagy összetett.
A tárgymutató elsődleges célja, hogy segítséget nyújtson a könyvben (több helyen) előforduló fogalmak, elnevezések, jelölések magyarázatának visszakeresésében.

Ennek megfelelően a tárgymutatóban (általában) csak az első előfordulási hely adatai szerepelnek. A fogalom, elnevezés után megadjuk a könyvben használt tipikus jelölését (ha van ilyen), majd annak a definíciójának, tételeknél stb. a számát, ahol a fogalom, elnevezés, jelölés magyarázata megtalálható, végül zárójelben odaírjuk az oldalszámot is.

A definíció kívül gyakran a szóban forgó fogalomhoz kapcsolódó fontos tételeket is jelzünk, például „\(\sigma(n)\)” esetében a D 6.2.1 Definíció mellett a függvény képletét tartalmazó T 6.2.2 Tételre is utalunk. Más esetekben a fogalomhoz kapcsolódó tételeket külön sorokban listázzuk, például az „átlagérték”-nél rendre megadjuk, hogy a nevezetesebb származéki függvények átlagértékeiről mely tételek szólnak.

Ha egy fontos fogalom több területen is előjön, akkor általában ezek mindegyikét felsoroljuk, lásd például az „egység” vagy a „norma” esetében. (Ha a jelölésben nincs eltérés, akkor azt nem ismételjük meg minden sorban.)

A definíciószám, tétszám stb. után egy „−”, illetve „+” jel szerepel, ha az adott fogalmat nem a jelzett definícióban, tételeben stb., hanem (közvetlenül) azt megelőzően, illetve követően a szövegben (külön számozás nélkül) vezetjük be. Így pl. a „triviális osztó”-nél D1.4.1 − arra utal, hogy a triviális osztó értelmezése az D 1.4.1 Definíció előtt (az előző oldal alján) történik.

A tárgymutatóban D3.2.1 jelenti a 3.2.1 Definíciót, és a D betű helyett T, L, F rendre a megfelelő számú tételel, lemmára, feladatra utal. Az 1.3.3 Tétel bizonyítását B1.3.3-mal, az 1.2 pontban szereplő 3. példát 1.2.P3-mal, az 5.8 pontot 5.8-cal jelezzük. Ez utóbbi jelentheti akár az egész pontot, akár annak egy részét, az eligazodásban ilyenkor a megelőző oldalszámok segíthetnek. Például a „titkosírás” esetén az 5.8 pont (feladatok nélkül) teljes 5.8–6 oldalsáma fel van tüntetve, ugyanakkor a „Diffie–Hellman-elv”-nél csak a 1–2 oldal szerepel. Az „RSA-séma” konkrétan össze van foglalva az 5.8.1 Tételben, így az tárgymutató is azt jelzi.

A \(\sigma(n)\) függvényre vonatkozó „átlagos nagyságrend”-nél T6.7.3+ azt mutatja, hogy a magyarázat a tétel kimondása után (még a bizonyítás előtt) található, ugyanakkor az „algebrailag zárt test” esetében B9.3.6+ arra utal, hogy az értelmezés a 9.3.6 Tétel bizonyítása után keressendő.

A jelölésekkel kapcsolatos legfontosabb információkat a „Technikai tudnivalók” [ix] c. rész is tartalmazza, de az alábbiakban ezeket is megismételjük.

A definíciók stb. számozásánál az első szám mindig a fejezetet, a második a fejezeten belül a pontot, a harmadik pedig a ponton belül a sorszámont jelöli. A definíciók és tételek sorszámozása egy ponton belül folyamatos, tehát pl. az 1.1.2 Definíció után az 1.1.3 Tétel következik. Az illusztrációs példák, képletek stb. (simá, egy számmal történő) számozása pontonként újrakezdődik.

Külön is kiemelünk néhány fontos jelölést, amelyek a könyvben leggyakrabban szereplő fogalmakat érintik. Megkülönböztetjük a (valós) számok alsó és felső egészrészét, és ezeket \(\lfloor \cdot \rfloor\), illetve \(\lceil \cdot \rceil\) jelöli, így pl. \(\lfloor x \rfloor = 3, \lceil x \rceil = 4\), a \(\lfloor x \rfloor\) jelölést nem használjuk. A számok törtrészét \(\{ \cdot \}\) jelöli, tehát \(\{c\} = c - \lfloor c \rfloor\) . Az oszthatóságra, a legnagyobb közös osztóra és a legkisebb közös többszörössére a szokásos jelöléseket használjuk, tehát pl. \(7 \mid 42\), \(9, 15 \mid 3\), \(9, 15 \mid 45\). A \(\mathbb{Z}\) szögesletes zárójel legkisebb közös többszöröse, zárt intervallumot vagy egyszerűen zárőjelet jelöl (ez utóbbi különösen a 11. fejezetben jellemző, ahol a \(\left\{ \infty \right\}\) kerek zárójel ideált jelent; a megkülönböztetés érdekében itt a legnagyobb közös osztóra is az lnko \(\left\{a, b\right\}\) jelölést használjuk).
A polinomok és függvények jelölésére többnyire az (argumentum nélküli) $f$, $g$ stb. jelölés szerepel, de helyenként az $f(x)$, $g(x)$ stb. írásmóds is előfordul. A polinomok fokszámát (az angol degree szónak megfelelően) „deg”-gel jelöljük, tehát pl. $\deg(x^3 + x) = 3$. A szokásos módon $\mathbb{Q}$, $\mathbb{R}$, illetve $\mathbb{C}$ rendre a racionális, a valós, illetve a komplex számok testét jelöli. 

$\mathbb{Z}$, $\mathbb{N}$, illetve $\mathbb{T}[x]$ pedig az egész számok, a modulo $\mathbb{n}$ maradékosztályok, illetve a $\mathbb{T}$ feletti polinomok gyűrjét jelenti. A testbővítések és a $\mathbb{Q}(\theta)$, illetve $\mathbb{E}(\theta)$ racionális test $\theta$-val való egyszerű bővítését, illetve (algebrai $\theta$ esetén) az ebben található algebrai egészek gyűrjét jelenti, $\mathbb{F}$-vel pedig az összes algebrai egész gyűrjét jelöli. 

A $\mathbb{P}$ betűt szinte kizárólag a pozitív prímszámok jelölésére használjuk, a sima (index nélküli) log jelölés a természetes ($\mathbb{e}$ alapú) logaritmust jelenti.

A (véges vagy végtelen) sorozatok és összegek jelölésére gyakran használjuk a $\prod$ és $\sum$ jeleket, például

$$\prod_{i=1}^{n} p_i^{a_i}, \quad \prod_{p \leq x} p, \quad \sum_{\nu \leq \alpha} \frac{1}{p^2}$$

rendre a $p_1^{a_1} \cdots p_n^{a_n}$ szorzatot, az $n$-nel nem nagyobb (pozitív) prímszámok szorzatát, illetve a (pozitív) prímszámok négyzetének reciprokösszegét jelenti.

Megemlítjük még, hogy a könyvben a definíciók, illetve a tételek megfogalmazásának a végén ◆ áll, a bizonyítások befejezését pedig ■ jelzi. A feladatok kitűzésénél szereplő *, **, illetve M jelek rendre arra utalnak, hogy a feladat nehéz, kiemelkedően nehéz, illetve részletes megoldás található a c. fejezetben.
<table>
<thead>
<tr>
<th>— — relatív konjugálta</th>
<th>( f(x_{ij}) )</th>
<th>D10.4.2, T10.4.3 (D 10.4.2– T 10.4.3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>algebrai számtest = ( \mathbb{Q} )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>egyszerű algebrai bővítése</td>
<td></td>
<td></td>
</tr>
<tr>
<td>algebrailag zárt test</td>
<td></td>
<td></td>
</tr>
<tr>
<td>álprím (( a ) alapú)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>— (univerzális)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>alsó egészrezsz</td>
<td></td>
<td></td>
</tr>
<tr>
<td>approximáció (diofantikus)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>—, algebrai számé</td>
<td>T9.4.1 (390), T9.4.3 (T 9.4.3)</td>
<td></td>
</tr>
<tr>
<td>—, irrationális számé</td>
<td>8.1 (S8.1– S8.2)</td>
<td></td>
</tr>
<tr>
<td>—, racionális számé</td>
<td>T8.1.3, T8.1.4 (T 8.1.3– T 8.1.4)</td>
<td></td>
</tr>
<tr>
<td>—, szimultán</td>
<td>F8.1.1 (f8.1.1 [274])</td>
<td></td>
</tr>
<tr>
<td>átlagérték, átlagértékfüggvény</td>
<td>D6.7.1 (D 6.7.1)</td>
<td></td>
</tr>
<tr>
<td>—, ( \ell(n) ) -( \cdot )</td>
<td>T6.4.3 (T 6.4.3), T6.4.4 (T 6.4.4)</td>
<td></td>
</tr>
<tr>
<td>—, ( \varphi(n) ) -( \cdot )</td>
<td>T6.7.4 (T 6.7.4)</td>
<td></td>
</tr>
<tr>
<td>—, ( \omega(n) ) -( \cdot )</td>
<td>T6.7.6 (T 6.7.6)</td>
<td></td>
</tr>
<tr>
<td>—, ( \Omega(n) ) -( \cdot )</td>
<td>F6.7.5 (f6.7.5 [211])</td>
<td></td>
</tr>
<tr>
<td>—, ( \sigma(n) ) -( \cdot )</td>
<td>T6.7.3 (T 6.7.3)</td>
<td></td>
</tr>
<tr>
<td>átlagos nagyságrend, ( \varphi(n) ) -( \cdot )</td>
<td>T6.7.4+ (T 6.7.4)</td>
<td></td>
</tr>
<tr>
<td>— —, ( \sigma(n) ) -( \cdot )</td>
<td>T6.7.3+ (T 6.7.3)</td>
<td></td>
</tr>
</tbody>
</table>

barátságos számok | F6.3.7 (f6.3.7 [181]) |
| bázis (additív) | T12.3.3 – (520), F12.3.10 (T 12.3.3 f12.3.10 [415]) |
| Bertrand-posztulátum (Csebisev-tétel) | T5.5.3+ (T 5.5.3) |
| binom kongruencia | T3.5.1 (T 3.5.1) |
| bövelkedő szám | F6.3.3 (f6.3.3 [180]) |

<p>| ( \mathbb{C} ) = komplex számok |
| Carmichael-szám | D5.7.3 (D 5.7.3) |
| Cauchy–Davenport–Chowla-tétel | T12.3.1 (T 12.3.1) |
| Chevalley-tétel | T3.6.1 (T 3.6.1) |
| cinkos | B5.7.4 (B5.7.4) |
| Csebisev-egyenlőtlenség | B6.7.7+ (B6.7.7), B12.1.1 (B12.1.1) |
| Csebisev-tétel | T5.5.3 (T 5.5.3) |</p>
<table>
<thead>
<tr>
<th>csoport</th>
<th>csupaegy</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>F1.3.12 (f1.3.12 [14])</td>
</tr>
<tr>
<td>$d(n) = \tau_1$ (pozitív) osztóinak a száma</td>
<td>T1.6.3 (T 1.6.3)</td>
<td></td>
</tr>
<tr>
<td>$d_\Delta(n)$</td>
<td>D6.2.6, T6.2.7 (D 6.2.6, T 6.2.7)</td>
<td></td>
</tr>
<tr>
<td>$\deg = \text{fok(szám)}$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Diffie–Hellman-elv</td>
<td>5.8 (DH1– DH2)</td>
<td></td>
</tr>
<tr>
<td>diofantikus approximáció</td>
<td>8.1 (S8.1– S8.2)</td>
<td></td>
</tr>
<tr>
<td>--- egyenlet</td>
<td>T1.3.6 (T 1.3.6)</td>
<td></td>
</tr>
<tr>
<td>--- , lineáris</td>
<td>T1.3.6 (T 1.3.6), T7.1.1 ( T 7.1.1)</td>
<td></td>
</tr>
<tr>
<td>Dirichlet-sor</td>
<td>$\mathcal{F}(s)$</td>
<td></td>
</tr>
<tr>
<td>Dirichlet-tétel (prímszámok számtani sorozatokban)</td>
<td>D6.6.3 (D 6.6.3)</td>
<td></td>
</tr>
<tr>
<td>diszjunkt fedőrendszer (DFR)</td>
<td>F12.5.6 (f12.5.6 [423])</td>
<td></td>
</tr>
<tr>
<td>diszkrét logaritmus $= \text{index}$</td>
<td>D3.4.1 (D 3.4.1)</td>
<td></td>
</tr>
<tr>
<td>diszkrimináns $\left( \mathcal{Q}(\mathfrak{d}) \right)$</td>
<td>B10.5.4+ (B10.5.4)</td>
<td></td>
</tr>
<tr>
<td>--- $\left( \mathcal{Q}(\mathfrak{d}) \right)$ -beli elem- $\mathfrak{n}$ - eseké $\Delta(\alpha_1, \ldots, \alpha_n)$</td>
<td>D10.5.2 (D 10.5.2)</td>
<td></td>
</tr>
</tbody>
</table>

$\mathcal{F} = \text{összes algebrai egész gyűrűje}$

$\mathfrak{e}$ irracionalitása

$\mathfrak{e}$ transzcendenciája

$\mathcal{E}(\mathfrak{d}) = \text{a } \mathcal{Q}(\mathfrak{d}) \text{ bővítés algebrai egészeinek gyűrűje}$

egész bázis $\left( \mathcal{Q}(\mathfrak{d}) \right)$ -ban $\omega_1, \ldots, \omega_r$

egészrész (alsó) $[ \ ]$

egészrész (felső) $[ \ ]$

eyenletes eloszlás D8.4.3, T8.4.4 (D 8.4.3– T 8.4.4)

eyértelmű primfaktorizáció,
eyértelmű primfélbontás — számelmélet alaptétele
eyiptomi tört F7.3.6 (f7.3.6 [227])

eyegység $\mathfrak{e}$

$\left( \text{egész számoknál} \right)$ D1.1.2, T1.1.3 (D 1.1.2– T 1.1.3)
<table>
<thead>
<tr>
<th>Tárgymutató</th>
</tr>
</thead>
<tbody>
<tr>
<td>— (Euler-egészeknél)</td>
</tr>
<tr>
<td>— (Gauss-egészeknél)</td>
</tr>
<tr>
<td>— (másodfokú bővítésekknél)</td>
</tr>
<tr>
<td>egységelem (szorzásnál)</td>
</tr>
<tr>
<td>— bővítés</td>
</tr>
<tr>
<td>— bővítés</td>
</tr>
<tr>
<td>— bővítés</td>
</tr>
<tr>
<td>ekvivalenciareláció</td>
</tr>
<tr>
<td>— bővítés</td>
</tr>
<tr>
<td>elemi szimmetrikus polinom</td>
</tr>
<tr>
<td>eratosztenes szita</td>
</tr>
<tr>
<td>euklideszi algoritmus</td>
</tr>
<tr>
<td>— gyűrű</td>
</tr>
<tr>
<td>Euler-egész</td>
</tr>
<tr>
<td>Euler-féle (\varphi) -függvény</td>
</tr>
<tr>
<td>Euler–Fermat-tétel</td>
</tr>
<tr>
<td>Euler partíciós tétele</td>
</tr>
<tr>
<td>Euler-prím</td>
</tr>
<tr>
<td>Euler-racionális</td>
</tr>
<tr>
<td>faktorgyűrű = maradékosztálygyűrű</td>
</tr>
<tr>
<td>fedőrendszer</td>
</tr>
<tr>
<td>—, diszjunkt (DFR)</td>
</tr>
<tr>
<td>felbonthatatlan ideál</td>
</tr>
<tr>
<td>— szám</td>
</tr>
<tr>
<td>felső egészrész</td>
</tr>
<tr>
<td>Fermat-prím</td>
</tr>
<tr>
<td>Fermat-sejtés</td>
</tr>
<tr>
<td>— a 3 kitevőre</td>
</tr>
<tr>
<td>— a 4 kitevőre</td>
</tr>
<tr>
<td>Fermat-szám</td>
</tr>
<tr>
<td>— (prim)osztói</td>
</tr>
<tr>
<td>— primetzjte</td>
</tr>
<tr>
<td>Fermat-tétel („kis”)</td>
</tr>
<tr>
<td>(\varphi(n) = \text{Euler-féle } \varphi) -függvény</td>
</tr>
<tr>
<td>Fibonacci-szám</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Tárgymutató</td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>fok, fokszám (algebrai elemé)</td>
</tr>
<tr>
<td>— (algebrai számé)</td>
</tr>
<tr>
<td>— (polinomé modulo ( n ))</td>
</tr>
<tr>
<td>fok (testbővítésé)</td>
</tr>
<tr>
<td>fokszámtest</td>
</tr>
<tr>
<td>főideál</td>
</tr>
<tr>
<td>főideálgyűrű</td>
</tr>
<tr>
<td>Frobenius-probléma</td>
</tr>
</tbody>
</table>

| \( g(k) \) |  | D7.6.1 (D 7.6.1) |
| \( G(k) \) |  | D7.6.3 (D 7.6.3) |
| Gauss-egész | \( \alpha = a + bi \) | D7.4.1 (D 7.4.1) |
| Gauss-felbonthatatlan | \( \pi \) | D7.4.10 (D 7.4.10) |
| Gauss-lemma (másodfokú kongruenciánál) |  | T4.2.1 (T 4.2.1) |
| — (primitív polinomoknál) |  | F11.5.9 (F11.5.9 [383]) |
| Gauss-prim | \( \pi \) | D7.4.11 (D 7.4.11), T7.4.15 (T 7.4.15) |
| Gauss-racionális |  | 9.6.P3 (9.6.P3) |
| Gelfond–Schneider-tétel |  | T9.3.5 (T 9.3.5) |
| generátorfüggvény (partícióknál) |  | 7.9 (S7.9– S8.1) |
| Goldbach-sejtés |  | 5.1 (S5.1) |

| Gyűrű | \( \mathbb{R} \) | B2.8.2+ (B2.8.2) |
| — , alaptételes |  | T11.3.1 (T 11.3.1) |
| — , euklideszi |  | D11.3.4(D 11.3.4), T11.3.5 (T 11.3.5) |

<p>| Hányados (maradékos osztásnál) | ( \varphi ) | B1.2.1+ (B1.2.1) |
| Hardy–Ramanujan-tétel |  | T6.7.7, T6.7.7A (T 6.7.7, T 6.7.7A) |
| harmonikus szám |  | F6.3.6 (F6.3.6 [181]) |
| három-négyzetszám-tétel |  | T7.5.2 (T 7.5.2) |
| hatványmaradék (( k )-adik) |  | D3.5.2, T3.5.3 (D 3.5.2, T 3.5.3) |
| hatvány-nemmaradék (( k )-adik) |  | D3.5.2 (D 3.5.2) |
| hatványozás ismételt négyzetre emeléssel |  | 3.2.P (3.2.P), B5.7.1 (B5.7.1) |</p>
<table>
<thead>
<tr>
<th>Tárgymutató</th>
</tr>
</thead>
<tbody>
<tr>
<td>hegytétel</td>
</tr>
<tr>
<td>hégag a szomszédos prímek között</td>
</tr>
<tr>
<td>hiányos szám</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ideál</th>
<th>( I )</th>
<th>D11.1.1 (D 11.1.1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>—, elem(ek) által generált</td>
<td>((a_1, \ldots, a_k))</td>
<td>D11.1.2, D11.1.4 (D 11.1.2– D 11.1.4)</td>
</tr>
<tr>
<td>—, felbonthatatlan</td>
<td>D11.4.6 (D 11.4.6)</td>
<td></td>
</tr>
<tr>
<td>—, legszűkebb</td>
<td>T11.1.3 (T 11.1.3), T11.1.5 (T 11.1.5)</td>
<td></td>
</tr>
<tr>
<td>—, maximális</td>
<td>D11.4.6+ (D 11.4.6)</td>
<td></td>
</tr>
<tr>
<td>—, triviális</td>
<td>11.1.P4 (11.1.P4)</td>
<td></td>
</tr>
<tr>
<td>—, végesen generált</td>
<td>D11.1.4 (D 11.1.4)</td>
<td></td>
</tr>
</tbody>
</table>

| ideál szerinti maradékosztály | \( a + I \) | T11.1.6 (T 11.1.6) |
| ideállok ekvivalenciája | | D11.6.1 (D 11.6.1) |
| — legkisebb közös többszöröse | F11.4.5 (f11.4.5 [372]) |
| — legnagyobb közös osztója | \((A, B)\) | D11.4.4, T11.4.5 (D 11.4.4, T 11.4.5) |
| — oszthatósága | \( B \mid A \) | D11.4.3 (D 11.4.3) |
| — összege | \( A + B \) | F11.4.4b (f11.4.4 [371]) |
| — szorzata | \( AB \) | D11.4.1, T11.4.2 (D 11.4.1– T 11.4.2) |

| ideálosztály | | T11.6.3 – (T 11.6.3) |

| ikerprímek | | 5.1 (S5.1) |

<p>| Im = képzetes rész (komplex számé) | | |
| index | ( \text{inc}: a, \text{inc}: \varphi \alpha ) | D3.4.1 (D 3.4.1) |
| inkongruens = nem kongruens | ( \not\equiv ) | D2.1.1+ (D 2.1.1) |
| integritási tartomány | F1.1.23 (f1.1.23 [5]) |
| inverz (szorzásnál) | T2.8.3 – (T 2.8.3) |
| irracionális szám approximációja | 8.1 (S8.1– S8.2) |
| irrationalitás bizonyítása, ( \varepsilon ) | T9.5.1 (T 9.5.1) |
| — —, ( \sqrt{n} ) | F1.6.33a (f1.6.33 [31]) |
| — —, ( \log_{_{\text{eu}}} b ) | F1.6.33b (f1.6.33 [31]) |
| — —, ( \sqrt{2} ) (geometriailag) | F1.3.17e (f1.3.17 [15]) |
| — —, ( \pi ) | T9.5.2 (T 9.5.2) |
| irreducibilis = felbonthatatlan | | |
| ismételt négyzetre emelés módszere | 3.2.P (3.2.P), B5.7.1 (B5.7.1) |</p>
<table>
<thead>
<tr>
<th>izolált prim</th>
<th>T5.5.2 (T 5.5.2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jacobi-szimbólum</td>
<td>D4.3.1 (D 4.3.1)</td>
</tr>
<tr>
<td>( k ) -adik hatványmaradék</td>
<td>D3.5.2, T3.5.3 (D 3.5.2, T 3.5.3)</td>
</tr>
<tr>
<td>( k ) -adik hatvány-nemmaradék</td>
<td>D3.5.2 (D 3.5.2)</td>
</tr>
<tr>
<td>kanonikus alak</td>
<td>T1.6.1 (42 T 1.6.1)</td>
</tr>
<tr>
<td>— — (Gauss-egészeknél)</td>
<td>B7.5.1 (B7.5.1)</td>
</tr>
<tr>
<td>— — (ideálóknál)</td>
<td>T11.5.9 — (T 11.5.9)</td>
</tr>
<tr>
<td>— — (legkisebb közös többszörösé)</td>
<td>T1.6.6 (T 1.6.6)</td>
</tr>
<tr>
<td>— — (legnagyobb közös osztóé)</td>
<td>T1.6.4 (T 1.6.4)</td>
</tr>
<tr>
<td>— — (módosított)</td>
<td>T1.6.1+ (T 1.6.1)</td>
</tr>
<tr>
<td>— — ( ( n! )-é)</td>
<td>T1.6.8 (T 1.6.8)</td>
</tr>
<tr>
<td>— — (osztóé)</td>
<td>T1.6.2 (T 1.6.2)</td>
</tr>
<tr>
<td>karakterizáció (additív szármeléleti függvényeké)</td>
<td>T6.8.1 (T 6.8.1)</td>
</tr>
<tr>
<td>képzetes másodfokú bővítés</td>
<td>T10.3.6 — (T 10.3.6)</td>
</tr>
<tr>
<td>két-négyetszám-tétel</td>
<td>T7.5.1 (T 7.5.1)</td>
</tr>
<tr>
<td>kínai maradéktétel</td>
<td>T2.6.2 (T 2.6.2)</td>
</tr>
<tr>
<td>kis Fermat-tétel</td>
<td>T2.4.1A, T2.4.1B (T 2.4.1A, T 2.4.1B)</td>
</tr>
<tr>
<td>kitüntetett közös osztó</td>
<td>D1.3.2 (D 1.3.2)</td>
</tr>
<tr>
<td>kommutatív csoport</td>
<td>B2.8.5+ (B2.8.5)</td>
</tr>
<tr>
<td>— test</td>
<td>T2.8.3+ (T 2.8.3)</td>
</tr>
<tr>
<td>komplementum (additív)</td>
<td>12.6 (S12.6)</td>
</tr>
<tr>
<td>— , teljesen gazdaságos (TGK)</td>
<td>T12.6.2 — (T 12.6.2)</td>
</tr>
<tr>
<td>kongruencia</td>
<td>D2.1.1 (D 2.1.1)</td>
</tr>
<tr>
<td>— ( ( a + b\sqrt{b} ) alakú számoknál)</td>
<td>B5.2.4 (B5.2.4)</td>
</tr>
<tr>
<td>— (Euler-egészeknél)</td>
<td>D7.7.8 (T 7.7.8)</td>
</tr>
<tr>
<td>— , binom</td>
<td>T3.5.1 (T 3.5.1)</td>
</tr>
<tr>
<td>— , lineáris</td>
<td>D2.5.1, T2.5.3—T2.5.5 (D 2.5.1, T 2.5.3—T 2.5.5)</td>
</tr>
<tr>
<td>— , másodfokú</td>
<td>D4.1.1 (D 4.1.1)</td>
</tr>
<tr>
<td>— , primhatvány modulusú</td>
<td>T3.7.1 (T 3.7.1)</td>
</tr>
<tr>
<td>kongruencia fedőrendszer</td>
<td>12.5 (S12.5—S12.6)</td>
</tr>
<tr>
<td>kongruencia megoldásszáma</td>
<td>D2.5.2 (D 2.5.2)</td>
</tr>
<tr>
<td>konjugált (( \mathbb{Q} ) feletti)</td>
<td>D10.4.1 (D 10.4.1)</td>
</tr>
<tr>
<td>— (relatív)</td>
<td>D10.4.2, T10.4.3 (D 10.4.2—T 10.4.3)</td>
</tr>
</tbody>
</table>
### Tárgymutató

<table>
<thead>
<tr>
<th>Konvolúció</th>
<th>$f * g$</th>
<th>D6.6.1 (D 6.6.1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>König–Rados-tétel</td>
<td></td>
<td>T3.6.2 (T 3.6.2)</td>
</tr>
<tr>
<td>Körösségi polinom</td>
<td>$\Phi_m$</td>
<td>B5.3.4 (B5.3.4)</td>
</tr>
<tr>
<td>Középérték (függyveny) = átlagérték (függyveny)</td>
<td></td>
<td>D6.7.1 (D 6.7.1)</td>
</tr>
<tr>
<td>Közös osztó, legnagyobb</td>
<td>$(a, b)$, $\text{lko}(a, b)$</td>
<td>D1.3.1 (D 1.3.1), D7.4.9 (D 7.4.9)</td>
</tr>
<tr>
<td>— — , kitüntetett</td>
<td>$(a, b)$</td>
<td>D1.3.2 (D 1.3.2)</td>
</tr>
<tr>
<td>Közös többszörös, legkisebb</td>
<td>$[a, b], \text{lkt}(a, b)$</td>
<td>D1.6.5 (D 1.6.5)</td>
</tr>
<tr>
<td>Kronecker-tétel (ideálokknál)</td>
<td></td>
<td>T11.5.5 (T 11.5.5)</td>
</tr>
<tr>
<td>Kvadratikus maradék</td>
<td></td>
<td>D4.1.1 (D 4.1.1)</td>
</tr>
<tr>
<td>— nemmaradék</td>
<td></td>
<td>D4.1.1 (D 4.1.1)</td>
</tr>
<tr>
<td>— reciprocitási tétel</td>
<td></td>
<td>T4.2.3 (T 4.2.3)</td>
</tr>
<tr>
<td>Kváziítőkéletes szám</td>
<td></td>
<td>F6.3.4 (f6.3.4 [180])</td>
</tr>
</tbody>
</table>

<p>| Lánctört | | 8.3 (S8.3) |
| Lánctörtjegy | | D8.3.1 (D 8.3.1) |
| Legendre-formula = $n!$ kanonikus alakja | | T1.6.8 (T 1.6.8) |
| Legendre-szimbólum | $(a)$ | D4.1.3 (D 4.1.3) |
| Legkisebb abszolút értékű maradék | $\tau$ | T1.2.1A+ (T 1.2.1A) |
| — közös többszörös | $[a, b], \text{lkt}(a, b)$ | D1.6.5 (D 1.6.5) |
| — — — kanonikus alakja | | T1.6.6 (T 1.6.6) |
| Legkisebb nemnegatív maradék | $\tau$ | B1.2.1+ (B1.2.1) |
| Legnagyobb közös mérték | | F1.3.17d (f1.3.17 [15]) |
| — osztó | $(a, b), \text{lko}(a, b)$ | D1.3.1 (D 1.3.1), D7.4.9 (D 7.4.9) |
| — — (egész számoknál) | $(a, b), \text{lko}(a, b)$ | D1.3.1 (D 1.3.1) |
| — — (Gauss-egészeknél) | $(a, b)$ | D7.4.9 (D 7.4.9) |
| — — (ideálokknál) | $(A, B)$ | D11.4.4, T11.4.5 (D 11.4.4, T 11.4.5) |
| — — kanonikus alakja | | T11.1.3 (T 11.1.3), T11.1.5 (T 11.1.5) |
| Legszűkebb ideál | | T10.2.2 (T 10.2.2) |
| Lineáris diofantikus egyenlet | $ax + by = c$ | T1.3.6 (T 1.3.6), T7.1.1 (T 7.1.1) |
| — kongruencia | $ax \equiv b \pmod{m}$ | D2.5.1, T2.5.3–T2.5.5 (D 2.5.1, T 2.5.3–T 2.5.5) |
| Liouville approximációs tétel | | T9.4.1 (T 9.4.1) |
| Liouville-szám | | F9.4.1 (f9.4.1 [307]) |</p>
<table>
<thead>
<tr>
<th>Lucas-Lehmer-teszt ≡ Mersenne-számok prímtesztje</th>
<th>T5.2.4 (T 5.2.4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>maradék (maradékos osztásnál) &amp; ( r ) &amp; B1.2.1+ (B1.2.1)</td>
<td></td>
</tr>
<tr>
<td>—, kvadratikus &amp; &amp; D4.1.1 (D 4.1.1)</td>
<td></td>
</tr>
<tr>
<td>—, legkisebb abszolút értékű &amp; &amp; T1.2.1A+ (T 1.2.1A)</td>
<td></td>
</tr>
<tr>
<td>—, legkisebb nemnegatív &amp; &amp; B1.2.1+ (B1.2.1)</td>
<td></td>
</tr>
<tr>
<td>maradékos osztás (egész számonkéről) &amp; &amp; T1.2.1, T1.2.1A (T 1.2.1–T 1.2.1A)</td>
<td></td>
</tr>
<tr>
<td>— (euklideszi gyűrűben) &amp; &amp; D11.3.4 (D 11.3.4)</td>
<td></td>
</tr>
<tr>
<td>— (Gauss-egészeknél) &amp; &amp; T7.4.8 (T 7.4.8)</td>
<td></td>
</tr>
<tr>
<td>maradékosztály (faktorgegyűrűnél) &amp; &amp; T11.1.6 (T 11.1.6)</td>
<td></td>
</tr>
<tr>
<td>— (kongruenciánál) &amp; &amp; D2.2.1 (D 2.2.1)</td>
<td></td>
</tr>
<tr>
<td>—, redukált &amp; &amp; D2.2.6 (D 2.2.6)</td>
<td></td>
</tr>
<tr>
<td>maradékosztálygyűrű (ideál szerinti) &amp; &amp; T11.1.6 (T 11.1.6)</td>
<td></td>
</tr>
<tr>
<td>— (modulo ( n ) ) &amp; ( \mathbb{Z}_{nR} ) &amp; T2.8.2 (T 2.8.2)</td>
<td></td>
</tr>
<tr>
<td>maradékrendszer, redukált &amp; &amp; D2.2.8, T2.2.9 (D 2.2.8, T 2.2.9)</td>
<td></td>
</tr>
<tr>
<td>—, teljes &amp; &amp; D2.2.2, T2.2.3 (D 2.2.2–T 2.2.3)</td>
<td></td>
</tr>
<tr>
<td>maradékszámrendszer &amp; &amp; 2.6.P2 – (2.6.P2)</td>
<td></td>
</tr>
<tr>
<td>másodfokú bővítés &amp; &amp; ( \mathbb{Q} (\sqrt{r}) ) &amp; 10.3 (S10.3–S10.4)</td>
<td></td>
</tr>
<tr>
<td>—, képzetes &amp; &amp; T10.3.6 – (T 10.3.6)</td>
<td></td>
</tr>
<tr>
<td>—, valós &amp; &amp; T10.3.6 – (T 10.3.6)</td>
<td></td>
</tr>
<tr>
<td>másodfokú bővítés algebrai egészeki &amp; &amp; T10.3.2 (T 10.3.2)</td>
<td></td>
</tr>
<tr>
<td>— kongruencia &amp; &amp; D4.1.1 (D 4.1.1)</td>
<td></td>
</tr>
<tr>
<td>másodrendű additív bázis &amp; &amp; T12.3.3 – (T 12.3.3)</td>
<td></td>
</tr>
<tr>
<td>maximális ideál &amp; &amp; D11.4.6+ (D 11.4.6)</td>
<td></td>
</tr>
<tr>
<td>megfordítási formula &amp; &amp; T6.5.3 (T 6.5.3)</td>
<td></td>
</tr>
<tr>
<td>— függvény &amp; &amp; T6.5.2 (T 6.5.2)</td>
<td></td>
</tr>
<tr>
<td>megoldásszám (kongruenciál) &amp; &amp; ( \tilde{f} )</td>
<td></td>
</tr>
<tr>
<td>Mersenne-prím &amp; &amp; ( \mathcal{M}_p ) &amp; F1.4.4 (F1.4.4 [17]), 5.2 (S5.2)</td>
<td></td>
</tr>
<tr>
<td>Mersenne-szám &amp; &amp; ( \mathcal{M}_p ) &amp; 5.2 (S5.2)</td>
<td></td>
</tr>
<tr>
<td>— (prim)osztói &amp; &amp; T5.2.3 (T 5.2.3)</td>
<td></td>
</tr>
<tr>
<td>— prímtesztje &amp; &amp; T5.2.4 (T 5.2.4)</td>
<td></td>
</tr>
<tr>
<td>Miller–Lenstra–Rabin-teszt &amp; &amp; T5.7.5 (T 5.7.5)</td>
<td></td>
</tr>
<tr>
<td>minimálpolinom (algebrai elemé) &amp; &amp; ( \mathcal{M}_{\theta} ) &amp; D10.1.5 (D 10.1.5)</td>
<td></td>
</tr>
<tr>
<td>— (algebrai számé) &amp; &amp; ( \mathcal{M}_{\alpha} ) &amp; D9.2.1 (D 9.2.1)</td>
<td></td>
</tr>
<tr>
<td>Tárgymutató</td>
<td>T8.2.1 (T 8.2.1)</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Minkowski-tétel</td>
<td>T8.2.1 (T 8.2.1)</td>
</tr>
<tr>
<td>modulus (kongruenciák)</td>
<td>D2.1.1+ (D 2.1.1)</td>
</tr>
<tr>
<td>Möbius-féle megfordítási formula</td>
<td>T6.5.3 (T 6.5.3)</td>
</tr>
<tr>
<td>Möbius-függvény</td>
<td>D6.2.3 (D 6.2.3)</td>
</tr>
<tr>
<td>multiplikatív inverz</td>
<td>T2.8.3 – (T 2.8.3)</td>
</tr>
<tr>
<td>— számléleti függvény</td>
<td>D6.1.2 (D 6.1.2)</td>
</tr>
<tr>
<td>( \mu(n) ) = Möbius-függvény</td>
<td>D6.2.3 (D 6.2.3)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( \tau! ) kanonikus alakja (Legendre-formula)</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1.6.8 (T 1.6.8)</td>
</tr>
<tr>
<td>négy-négyzetszám-tétel</td>
</tr>
<tr>
<td>négyzetmentes szám</td>
</tr>
<tr>
<td>négyzetteljes szám</td>
</tr>
<tr>
<td>norma (egyszerű algebrai bővítésben)</td>
</tr>
<tr>
<td>— (Euler-egészé)</td>
</tr>
<tr>
<td>— (Gauss-egészé)</td>
</tr>
<tr>
<td>— (kvaternióé)</td>
</tr>
<tr>
<td>— (másodfokú bővítésben)</td>
</tr>
<tr>
<td>nullmértékú halmaz</td>
</tr>
<tr>
<td>nullosztó</td>
</tr>
</tbody>
</table>

| nyilvános jelkulsú titkosírás                   | 5.8 (S5.8– Ch6) |

<table>
<thead>
<tr>
<th>( \omega(n) = \tau ) különböző (pozitív) primosztóinak a száma</th>
</tr>
</thead>
<tbody>
<tr>
<td>D6.2.5 (D 6.2.5)</td>
</tr>
<tr>
<td>( \Omega(n) = \tau ) „összes” (pozitív) primosztóinak a száma</td>
</tr>
<tr>
<td>D6.2.5 (D 6.2.5)</td>
</tr>
</tbody>
</table>

<p>| Ore-szám                                                      | F6.3.6 (f6.3.6 [181]) |
| osztályszám                                                  | T11.6.3 (T 11.6.3) |
| osztható(ság), osztó                                         | D1.1.1 (D 1.1.1), D7.4.4 (D 7.4.4) |
| — , — (egész számoknál)                                      | D1.1.1 (D 1.1.1) |
| — , — (Gauss-egészeknél)                                     | D7.4.4 (D 7.4.4) |
| — , — (ideáloknál)                                           | D11.4.3 (D 11.4.3) |
| osztók összege                                               | D6.2.1, T6.2.2 (D 6.2.1, T 6.2.2) |
| — száma                                                     | T1.6.3 (T 1.6.3) |
| osztókra vonatkozó összegési függvény                        | D6.5.1 (D 6.5.1) |</p>
<table>
<thead>
<tr>
<th>összegzési függvény</th>
<th>$f^+$</th>
<th>D6.5.1 (D 6.5.1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>összemérhetőség</td>
<td></td>
<td>F1.3.17 (f1.3.17 [15])</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$P_n$ : általában az $n$ -edik prímszámot jelöli</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$\varphi(n) = n$ -edik prícióinak a száma</td>
<td>D7.9.1 (D 7.9.1)</td>
</tr>
<tr>
<td>páronként relatív prim</td>
<td>D1.3.8 (D 1.3.8)</td>
</tr>
<tr>
<td>páros számok számmelélete</td>
<td>B1.1.3+ (B1.1.3), B1.4.3+ (B1.4.3), B1.5.1 — (B1.5.1)</td>
</tr>
<tr>
<td>partíció</td>
<td>D7.9.1 (D 7.9.1)</td>
</tr>
<tr>
<td>Pell-egyenlet</td>
<td>T7.8.1 (T 7.8.1), T7.8.2 (T 7.8.2)</td>
</tr>
<tr>
<td>Pepin-teszt = Fermat-számok prímtesztje</td>
<td>T5.2.2 (T 5.2.2)</td>
</tr>
<tr>
<td>$\pi$ irracionalitása</td>
<td>T9.5.2 (T 9.5.2)</td>
</tr>
<tr>
<td>$\pi(x)$</td>
<td>T5.4.1 — (T 5.4.1)</td>
</tr>
<tr>
<td>— alsó és felső becslése</td>
<td>T5.4.3 (T 5.4.3)</td>
</tr>
<tr>
<td>pitagorasi számhármas</td>
<td>T7.2.1 (T 7.2.1)</td>
</tr>
<tr>
<td>polinom, körösztási</td>
<td>$\Phi_m$</td>
</tr>
<tr>
<td>— , primitív</td>
<td>F11.5.9 (f11.5.9 [383])</td>
</tr>
<tr>
<td>polinom deriváltja</td>
<td>$f'$</td>
</tr>
<tr>
<td>— fok(szám)a modulo $m$</td>
<td>D3.1.1 (D 3.1.1)</td>
</tr>
<tr>
<td>— többszörös gyöke</td>
<td>B5.3.4 (B5.3.4)</td>
</tr>
<tr>
<td>prím, prímszám</td>
<td>$\rho$</td>
</tr>
<tr>
<td>primhatvány modulisú kongruencia megoldása</td>
<td>T3.7.1 (T 3.7.1)</td>
</tr>
<tr>
<td>primideál</td>
<td>D11.4.7 (D 11.4.7)</td>
</tr>
<tr>
<td>primitív gyök (modulo $m$ )</td>
<td>$y$</td>
</tr>
<tr>
<td>— pitagorasi számhármas</td>
<td>T7.2.1 (T 7.2.1)</td>
</tr>
<tr>
<td>— polinom</td>
<td>F11.5.9 (f11.5.9 [383])</td>
</tr>
<tr>
<td>prímsgépletek</td>
<td>5.1 (S5.1)</td>
</tr>
<tr>
<td>prímszámok száma („különböző”)</td>
<td>$\omega(n)$</td>
</tr>
<tr>
<td>— — („összes”)</td>
<td>$\Omega(n)$</td>
</tr>
<tr>
<td>prímszámok számtani sorozatokban</td>
<td>5.1 (S5.1), T5.3.1 (T 5.3.1)</td>
</tr>
<tr>
<td>primszámtétel</td>
<td>T5.4.1 (T 5.4.1)</td>
</tr>
<tr>
<td>primteszt (Agrawal–Kayal–Saxena)</td>
<td>5.7(S5.7–S5.8)</td>
</tr>
<tr>
<td>— (Fermat-számé)</td>
<td>T5.2.2(T 5.2.2)</td>
</tr>
<tr>
<td>— (kis Fermat-tétel alapján)</td>
<td>T5.7.2 (T 5.7.2)</td>
</tr>
</tbody>
</table>
— (Mersenne-számé) | T5.2.4 (T 5.2.4)
— (Miller–Lenstra–Rabin) | T5.7.5 (T 5.7.5)
— (Solovay–Strassen) | T5.7.4 (T 5.7.4)
pszeudoprím = álprim | D5.7.3 (D 5.7.3)

| Q = racionális számok | |
|—— egyszerű (algebrai) bővítése | Q(\varphi)
|—— feletti konjugált (algebrai számé) | Q(\varphi_j)
| | D10.2.1, T10.2.2, T10.2.3 (D 10.2.1– T 10.2.3)
| | D10.4.1 (D 10.4.1)

| Ē = valós számok | |
|—— racionális szám approximációja | F8.1.1 (f8.1.1 [274])
|—— Ramsey-számok | T12.4.1 (T 12.4.1)
|—— Ramsey tétele | T12.4.1 (T 12.4.1)
|—— Re=valós rész (komplex számé) | |
|—— reciprocitási tétel | T4.2.3 (T 4.2.3)
|—— redukált maradékosztály | D2.2.6 (D 2.2.6)
|—— maradékrendszer | D2.2.8, T2.2.9 (D 2.2.8, T 2.2.9)
|—— relatív konjugált (Q(\varphi) -ban) | f(\varphi_j)
|—— prim | D1.3.7 (D 1.3.7)
|—— , páronként | D1.3.8 (D 1.3.8)
|—— relatív prímség valószínűsége | T6.7.5 (T 6.7.5)
|—— rend (modulo m ) | \varphi(a), \varphi_i(a)
|—— Riemann-féle zéta-függvény | \zeta(s)
|—— Riemann-sejtés | T6.6.4 – (T 6.6.4)
|—— Roth approximációs tétele | T9.4.3 (T 9.4.3)
|—— RSA-séma | T5.8.1 (T 5.8.1)

| Schur-számok | T12.4.2+ (T 12.4.2)
|—— Schur tétele | T12.4.2 (T 12.4.2)
|—— Sidon-sorozat | 12.2 (S12.2 – S12.3)
|—— Smith-determináns | T6.5.4 (T 6.5.4)
|—— Solovay–Strassen-teszt | T5.7.4 (T 5.7.4)

| szakaszok összemérhetősége | F1.3.17 (f1.3.17 [15])
|—— számmelmélet alaptétele | T1.5.1 (T 1.5.1), T7.4.13 (T 7.4.13), 11.3 (S11.3–S11.4)
|—— (egész számnál) | T1.5.1 (T 1.5.1)
<table>
<thead>
<tr>
<th>Tárgymutató</th>
<th>T7.4.13 (T 7.4.13)</th>
</tr>
</thead>
<tbody>
<tr>
<td>— (Gauss-egészeknél)</td>
<td>T7.4.13 (T 7.4.13)</td>
</tr>
<tr>
<td>— (gyűrűben általában)</td>
<td>11.3 (S11.3– S11.4)</td>
</tr>
<tr>
<td>— (ideálokknál)</td>
<td>T11.5.8 (T 11.5.8)</td>
</tr>
<tr>
<td>— (másodfokú bővítések algebrai egészeire)</td>
<td>T10.3.5 (T 10.3.5), T10.3.6 (T 10.3.6)</td>
</tr>
<tr>
<td>szármeléleti algoritmusok lépésszáma</td>
<td>T5.7.1 (T 5.7.1)</td>
</tr>
<tr>
<td>— függvény</td>
<td>D6.1.1 (D 6.1.1)</td>
</tr>
<tr>
<td>számrendszeres felírás</td>
<td>T1.2.2 (T 1.2.2)</td>
</tr>
<tr>
<td>számtani sorozatok prímzámái</td>
<td>5.1 (S5.1), T5.3.1 (T 5.3.1)</td>
</tr>
<tr>
<td>$\sigma(n) = n$ (pozitív) osztóinak az összege</td>
<td>D6.2.1, T6.2.2 (D 6.2.1, T 6.2.2)</td>
</tr>
<tr>
<td>szimmetrikus polinom</td>
<td>T9.3.1+ (T 9.3.1)</td>
</tr>
<tr>
<td>— polinomok alaptétele</td>
<td>T9.3.2 (T 9.3.2)</td>
</tr>
<tr>
<td>szimultán approximáció</td>
<td>T8.1.3, T8.1.4 (T 8.1.3– T 8.1.4)</td>
</tr>
<tr>
<td>— kongruenciarendszer</td>
<td>2.6 (S2.6– S2.7)</td>
</tr>
<tr>
<td>szupertökéletes szám</td>
<td>F6.3.5 (f6.3.5 [181])</td>
</tr>
</tbody>
</table>

\[T\] : általában kommutatív testet jelöl
\[T[x] = a\] T test feletti polinomok gyűrűje
tanú                                                                 | B5.7.4 (B5.7.4) |
teljes maradékrrendszer                                         | D2.2.2, T2.2.3 (D 2.2.2– T 2.2.3) |
teljesen additív szármeléleti függvény                           | D6.1.5 (D 6.1.5) |
| — gazdaságos komplementum(TGK)                               | T12.6.2 – (T 12.6.2) |
| — multiplikatív szármeléleti függvény                         | D6.1.3 (D 6.1.3) |
test                                                                 | T2.8.3+ (T 2.8.3) |
| — , algebrailag zárt                                          | B9.3.6+ (B9.3.6) |
testbővítés                                                  | D10.1.1 (D 10.1.1) |
| — , egyszerű                                                 | D10.2.1, T10.2.2 (D 10.2.1, T 10.2.2) |
| — , egyszerű algebrai                                         | D10.2.1 (D 10.2.1), T10.2.3 (T 10.2.3) |
| — , másodfokú                                                | 10.3 (S10.3– S10.4) |
| — , véges                                                    | D10.1.2 (D 10.1.2) |
testbővítés foka                                              | D10.1.2 (D 10.1.2) |
testbővítések fokszámántelete                                  | T10.1.3 (T 10.1.3) |
Thue approximációs tétele                                      | T9.4.3 (T 9.4.3) |
<table>
<thead>
<tr>
<th>Tárgymutató</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Thue-lemma</td>
<td>F7.5.21a (f7.5.21 [242])</td>
</tr>
<tr>
<td>titkosírás</td>
<td>5.8 (55.8– Ch6)</td>
</tr>
<tr>
<td>tízédes tört</td>
<td>F3.2.20 (f3.2.20 [76])</td>
</tr>
<tr>
<td>totálisan additív szármeléleti függvény</td>
<td>D6.1.5 (D 6.1.5)</td>
</tr>
<tr>
<td>— multiplikatív szármeléleti függvény</td>
<td>D6.1.3 (D 6.1.3)</td>
</tr>
<tr>
<td>tőbbszörös</td>
<td>D1.1.1 (15), D7.4.4 (D 7.4.4)</td>
</tr>
<tr>
<td>tőkéletes szám</td>
<td>D6.3.1, T6.3.2 (T 6.3.2)</td>
</tr>
<tr>
<td>törtrész</td>
<td>{ }</td>
</tr>
<tr>
<td>transzcendencia bizonyítása, ε</td>
<td>T9.5.3 (T 9.5.3)</td>
</tr>
<tr>
<td>— — , $\log n$</td>
<td>F9.3.7 (f9.3.7 [302])</td>
</tr>
<tr>
<td>transzcendens szám</td>
<td>D9.1.2 (D 9.1.2)</td>
</tr>
<tr>
<td>— — létezése</td>
<td>T9.1.3 (T 9.1.3), T9.4.2 (T 9.4.2)</td>
</tr>
<tr>
<td>triviális ideál</td>
<td>11.1.P4 (11.1.P4)</td>
</tr>
<tr>
<td>— osztó</td>
<td>D1.4.1 — (D 1.4.1)</td>
</tr>
</tbody>
</table>

| univerzális álprim                                                        | D5.7.3 (D 5.7.3) |

| valós másodfokú bővítés                                                   | T10.3.6 — (T 10.3.6) |
| Van der Waerden-számok                                                    | T12.4.4A+ (T 12.4.4) |
| Van der Waerden tétele                                                    | T12.4.4, T12.4.4A (T 12.4.4, T 12.4.4A) |
| véges bővítés                                                             | D10.1.2 (D 10.1.2) |
| végtelen leszállás                                                        | B7.5.3+ (B7.5.3) |
| — szorzat                                                                  | F5.6.6, F5.6.7 (f5.6.7 [149]) |
| völgytétel                                                                 | T6.4.1 (T 6.4.1) |

| Waring-problémakör                                                       | 7.6 (S7.6– S7.7) |
| Weyl tétele                                                                | T8.4.4 (T 8.4.4) |
| Wiles tétele (Fermat-sejtés)                                               | T7.7.1 (T 7.7.1) |
| Wilson-tétel                                                               | T2.7.1 (93), B3.1.2+ (B3.1.2) |

| $\mathbb{Z}$ = egész számok                                                |                |
| $\mathbb{Z}_m = \text{modulo } m$, maradékosztálygyűrű                  | T2.8.2 (T 2.8.2) |
| zéta-függvény                                                             | $\zeta(s)$ |
|                                                                            | F5.6.6 (f5.6.6 [149]), T6.6.4 — (T 6.6.4) |