Sárközy András

számelmélet

dla

MK

510
S 19

SÁRKÖZY ANDRÁS

SZÁMELMÉLET

SÁRKÖZY ANDRÁS

SZÁMELMÉLET

PÉLDATÁR

MŰSZAKI KÖNYVKIADÓ, BUDAPEST, 1976

Lektorálta:

DR. GYARMATI EDIT
egy. adjunktus

228

JATE Móra Ferenc Kollégium
KÖNYVTÁRA
LM. 82 LM. 2582

© Dr. Sárközy András, 1976

ETO: 511 (076)

ISBN 963 10 0915 7

Felelős kiadó: Solt Sándor igazgató
Felelős szerkesztő: Oláh Gyuláné tanár

TARTALOMJEGYZÉK

Bevezetés 7

I. A számelmélet alapjai 9

1. Maradékos osztás. Az $[x]$ függvény 9
2. Számrendszerek 11
3. Oszthatóság 16
4. A legnagyobb közös osztó. A legkisebb közös többszörös. Lineáris diofantikus egyenletek 19
5. Prímszámok. A számelmélet alaptétele 28
6. Osztók. A $d(n)$ függvény 34

Feladatok 38

Az I. fejezetben kitűzött feladatok megoldásai 46

II. Kongruenciák 81

1. A kongruencia fogalma. Alaptulajdonságok 81
2. Redukált maradékosztályok. Az Euler-féle φ függvény. Az Euler—Fermat-tétel 87
3. Lineáris kongruenciák és kongruencia-rendszerek 92
4. Magasabbfokú kongruenciák 104
5. Binom kongruenciák. Primitív gyökök 114
6. Kvadratikus maradékok 121

Feladatok 128

A II. fejezetben kitűzött feladatok megoldásai 140

III. Számelméleti függvények 189

1. A $\sigma(n)$ függvény. A prímosztók száma 189
2. Összegezési függvény. A Möbius-függvény 193
3. Számelméleti függvények értékeinek eloszlása. Számelméleti függvények középértékei 198

Feladatok 204

A III. fejezetben kitűzött feladatok megoldásai 210

IV. A prímszámelmélet elemei 220
1. A prímszámok száma. Következmények 220
2. Additív prímszámelmélet. Prímdifferenciák 232
3. Dirichlet tétele 237
Feladatok 240
A IV. fejezetben kitűzött feladatok megoldásai 246

V. Diofantikus egyenletek 267
1. A diofantikus egyenletekről általában 267
2. Az $x^2+y^2=n$ diofantikus egyenlet megoldhatóságának szükséges és elégséges feltétele. A „descente infinie" módszer 273
3. Az $x^2+y^2=n$ diofantikus egyenlet megoldhatóságának vizsgálata a Thue-lemma segítségével 279
4. Az $x^2+y^2=n$ diofantikus egyenlet megoldhatóságának vizsgálata Gauss-egészek segítségével. Az algebrai számelmélet elemei 281
5. A geometriai számelmélet elemei. Az $x^2+y^2=n$ diofantikus egyenlet megoldhatóságának vizsgálata Minkowski tétele segítségével 289
6. A három- és négy négyzetszámtétel. A Waring-probléma 293
7. A pithagoraszi számhármasok. A Fermat-sejtés 298
Feladatok 301
Az V. fejezetben kitűzött feladatok megoldásai 307

VI. Diofantikus approximációelmélet 325
1. A diofantikus approximációelmélet elemei 325
2*. Lánctörtek 334
Feladatok 344
A VI. fejezetben kitűzött feladatok megoldásai 347

VII*. Az analitikus számelmélet elemei 363
1. A generátorfüggvény-elv 363
2. Trigonometrikus módszerek (exponenciális összegek) 366
3. Dirichlet-sorok. A Riemann-féle ζ-függvény 373
Feladatok 379
Útmutatások a VII*. fejezetben kitűzött feladatok megoldásához 385

BEVEZETÉS

A könyv első fele (az első két fejezet) tartalmazza azokat a bevezető számelmélet ismereteket, amelyek a matematika más területein (sőt esetenként a számítástechnikában, fizikában és egyes műszaki tudományokban is) leggyakrabban alkalmazhatók, és amelyek tárgyalhatók a középiskolai tananyag alapján. Ennek megfelelően e két fejezet olvasásához elegendő a középiskolai tananyag ismerete, eltekintve néhány olyan feladattól, melynek megoldása során bizonyos kombinatorikai alapfogalmakat is felhasználunk; ezeket a feladatokat — a nehezebb feladatokhoz hasonlóan — csillaggal jelöltük. A könyv e részek elhagyásával is kerek egész.

A könyv második felében (a III. fejezettől kezdve) a modern számelmélet egyes speciális területeit tárgyaljuk (nagyjából a tudományegyetemeken előadásra kerülő számelmélet-tananyagnak megfelelően). E fejezetek olvasása — a téma jellegénél fogva — már általában bizonyos matematikai előismereteket igényel (például némi analízisbeli jártasságot vagy a komplex számok ismeretét). A nehezebb, valamint a komolyabb matematikai (például analízisbeli) felkészültséget igénylő feladatokat, ill. fejezeteket itt is csillaggal jelöltük.

A formulák, példák, ill. feladatok számozását minden fejezetben újra kezdjük. Ha valahol például a 3. pontra, a 17. feladatra vagy (23) képletre utalunk, akkor mindig ugyanazon fejezet 3. pontjáról, 17. feladatáról, ill. (23) képletéről van szó; ellen-

kező esetben megnevezzük azt a fejezetet is, amelyben a szóban forgó pont, feladat, ill. képlet található.

Általában a leginkább elterjedt jelölést fogjuk alkalmazni. Ha azonban egy-egy esetben több egyaránt elterjedt jelölésmód is használatos (például egyes számelméleti függvények esetében), akkor az általunk kiválasztott jelölés mellett a többi jelölésre is fogunk utalni. A b szám a alapú logaritmusát $\overset{a}{\smile}\log b$*-vel, „természetes" logaritmusát (vagyis* $\overset{e}{\smile}\log b$*-t)* $\log b$*-vel fogjuk jelölni.*

A szerző

I. A SZÁMELMÉLET ALAPJAI

1. MARADÉKOS OSZTÁS. AZ $[x]$ FÜGGVÉNY

Az egész és racionális számok, valamint a velük végezhető műveletek alaptulajdonságait itt nem részletezzük, azokat ismerteknek tételezzük fel. Kiemeljük azonban e tulajdonságok közül a *maradékos osztás tételét*, melyre még többször fogunk utalni:

Legyen az a tetszőleges, b pedig 0-tól különböző egész szám. Ekkor léteznek olyan egyértelműen meghatározott q, r egész számok, melyekre

$$a = qb + r$$

és

$$0 \leqq r < |b|$$

teljesül. Itt q-t az $a:b$ osztás *hányadosának*, r-et *maradékának* nevezzük.

A számelméletben gyakran előnyös a maradékos osztás tételét a következő, kissé módosított formában alkalmazni:

Tetszőleges a egész számot és 0-tól különböző b egész számot megadva, léteznek olyan s, t egész számok, melyekre

$$a = sb + t$$

és

$$|t| \leqq \frac{|b|}{2}$$

teljesül. Egy ilyen t egész számot az $a:b$ osztás *abszolút legkisebb maradékának* nevezünk.

Megjegyezzük, hogy itt s és t már nem feltétlenül vannak egyértelműen meghatározva, amint ezt a következő példa mutatja: legyen c 0-tól különböző egész szám, k tetszőleges egész szám, $b=2c$, $a=(2k+1)c$. Ekkor

$$a = (2k+1)c = k \cdot 2c + c = kb + c,$$

másrészt

$$a = (2k+1)c = (k+1)2c - c = (k+1)b - c,$$

ahonnan látható, hogy a fenti feltételek mind $s=k$, $t=c$, mind $s=k+1$, $t=-c$ választással teljesülnek. Igazolható azonban, hogy ettől a kivételtől eltekintve, s és t már mindenkor egyértelműen vannak meghatározva.

Legyen x tetszőleges valós szám. Ekkor létezik olyan egyértelműen meghatározott k természetes szám, melyre

$$k \leqq x < k+1$$

teljesül. Ezt a k számot x egész részének nevezzük, és $[x]$-szel jelöljük. Ezzel a jelöléssel gyakran fogunk e könyvben találkozni. Továbbá az $x-[x]$ számot x *tört részének* nevezzük, és $\{x\}$-szel jelöljük, tehát

$$(1) \qquad x = [x] + \{x\}.$$

E jelöléseket használva, az $a:b$ osztás elvégzése során fellépő q hányados és r maradék a következőképpen fejezhető ki a és b segítségével:

$$q = \left[\frac{a}{b}\right]$$

és

$$\frac{r}{b} = \left\{\frac{a}{b}\right\}.$$

Az $[x]$ függvény nyilvánvalóan *monoton*, azaz $x \leqq y$ esetén szükségképpen $[x] \leqq [y]$.

$[x]$ egy további fontos tulajdonsága: tetszőleges a, b valós számokra

$$(2) \qquad [a]+[b] \leqq [a+b] \leqq [a]+[b]+1$$

(l. a 2. példát).

Példák

1. Számítsuk ki $-\frac{10}{3}$ egész részét és tört részét!

Megoldás:

$$-\frac{10}{3}=-\frac{12}{3}+\frac{2}{3}=-4+\frac{2}{3}.$$

Így nyilván

$$\left[-\frac{10}{3}\right]=-4 \quad \text{és} \quad \left\{-\frac{10}{3}\right\}=\frac{2}{3}.$$

2. Bizonyítsuk be, hogy a (2) összefüggés tetszőleges a, b valós számokra teljesül!

Megoldás:

(1)-re tekintettel

$$a+b=([a]+\{a\})+([b]+\{b\})=[a]+[b]+\{a\}+\{b\}\geqq[a]+[b],$$

hiszen az $\{x\}$ függvény nyilván mindig nemnegatív. Így az $[a]+[b]$ egész szám nem nagyobb, mint $a+b$, tehát — az $[x]$ függvény definíciójára tekintettel — $[a]+[b]$ legfeljebb akkora, mint $a+b$ egész része:

(3) $\quad [a]+[b]\leqq[a+b].$

Másrészt

$$a+b=([a]+\{a\})+([b]+\{b\})=[a]+[b]+\{a\}+\{b\}<[a]+[b]+2,$$

hiszen $\{x\}$ nyilván minden x-re kisebb 1-nél. Mivel az $[x]$ függvény definíciója szerint bármely x-re $[x]\leqq x$, ezért

$$[a+b]<[a]+[b]+2.$$

Mindkét oldalon egész szám áll, innen következik tehát, hogy

(4) $\quad [a+b]\leqq([a]+[b]+2)-1=[a]+[b]+1.$

(3)-ból és (4)-ből adódik az állítás.

2. SZÁMRENDSZEREK

A számítógépek és a számítástechnika széles körű elterjedése indokolja, hogy e könyvben viszonylag részletesen foglalkozzunk a különböző alapszámú számrendszerekkel is. A számítógépek ugyanis technikai okokból rendszerint a 2-es vagy 8-as számrendszert használják. Itt csak *pozitív egész* számok különböző számrendszerekben való felírásával fogunk foglalkozni.

A különböző számrendszerek használata az alábbi tételen alapul:

Legyen $a>1$, n pedig tetszőleges természetes szám. Ekkor léteznek olyan egyértelműen meghatározott $b_0, b_1, \ldots, b_k$ egész számok, melyekre az alábbi feltételek teljesülnek:

$$(5) \qquad n = b_0 a^k + b_1 a^{k-1} + \ldots + b_{k-1} a + b_k$$

és

$$(6) \qquad 1 \leqq b_0 \leqq a-1, \; 0 \leqq b_1 \leqq a-1, \; \ldots,$$

$$0 \leqq b_{k-1} \leqq a-1, \; 0 \leqq b_k \leqq a-1.$$

Ha az n természetes számot előállítjuk az (5) alakban, akkor azt mondjuk, hogy *n-et felírtuk az a alapú számrendszerben*, és erre e könyvben a következő jelölést használjuk:

$$n = b_0 b_1 \overset{a}{\ldots} b_{k-1} b_k.$$

(Más jelölések is használatosak, pl. 3142_6. Ha $a=10$, vagyis a tízes számrendszerről van szó, akkor a szokásos írásmódot használjuk.) A $b_0, b_1, \ldots, b_k$ számokról azt mondjuk, hogy azok az n szám *jegyei* az a alapú számrendszerben. (6) szerint valamely számot felírva a alapú számrendszerben, a jegyek a $0, 1, 2, \ldots, a-1$ számok közül kerülnek ki.

Valamely n természetes szám felírása a alapú számrendszerben, vagyis az (5) és (6) feltételeket kielégítő $b_0, b_1, \ldots, b_k$ jegyek megkeresése a gyakorlatban *a maradékos osztás tételére építve* a következőképpen történhet:

Első lépésként elosztjuk n-et a-val. A kapott maradék adja az utolsó jegyet, b_k-t. A következő lépésben az előző osztás során kapott hányadost osztjuk el a-val; a kapott maradék adja az utolsó előtti jegyet, b_{k-1}-et. Ezután ennek az osztásnak a hányadosát osztjuk el a-val s í.t. Ez az algoritmus akkor ér véget, amikor valamely osztás során a-nál kisebb hányadost kapunk; ez a hányados adja b_0-t.

Megjegyezzük, hogy ezen az úton a számrendszerek fenti alaptétele teljes általánosságban is bebizonyítható; célszerű a bizonyítást n-re vonatkozó teljes indukcióval végezni.

Ha több műveletet kell elvégeznünk valamilyen adott a alapú számrendszerben, akkor célszerű ehhez a számrendszerhez „egy-meg-egy" és „egyszeregy" táblázatot készítenünk (ez az $i+j$ összeadás, ill. az ij szorzás eredményét tartalmazza minden, a $0 \leqq i \leqq a-1$, $0 \leqq j \leqq a-1$ feltételt kielégítő i, j számpárra; az eredményt természetesen a alapú számrendszerben kell felírnunk).

Példák

3. Írjuk fel 10-es számrendszerben az alábbi számokat:

a. $\overset{6}{\smile}314$,

b. $\overset{8}{\smile}475$.

Megoldás:

a. $\overset{6}{\smile}314 = 2\cdot 6^3+3\cdot 6^2+1\cdot 6+4 = 2\cdot 216+3\cdot 36+1\cdot 6+4 =$

$= 432+108+6+4 = 550.$

Eljárhatunk másképpen is:

$\overset{6}{\smile}314 = 2\cdot 6^3+3\cdot 6^2+1\cdot 6+4 = [(2\cdot 6+3)6+1]6+4 =$

$= [(12+3)6+1]6+4 = (15\cdot 6+1)6+4 = (90+1)6+4 =$

$= 91\cdot 6+4 = 546+4 = 550.$

(Ez a módszer annak a fent ismertetett eljárásnak a megfordítása, melylyel *tízes* számrendszerben megadott számok írhatók fel más számrendszerben.)

b. $\overset{8}{\smile}475 = 4\cdot 8^2+7\cdot 8+5 = 4\cdot 64+7\cdot 8+5 = 256+56+5 = 317.$

4. Írjuk fel 6-os számrendszerben az alábbi számokat:

a. 346,

b. 830.

Megoldás:

a. $346:6 = 57$, $\quad 57:6 = 9$, $\quad 9:6 = 1.$

$\underline{46}$ $\quad \underline{3}$ $\quad \underline{3}$

4

A jegyek tehát sorrendben 1 (az utolsó, 6-nál kisebb hányados), valamint 3, 3 és 4 (a maradékok fordított sorrendben). Így

$$346 = \overset{6}{\breve{1}}334.$$

A gyakorlatban az egyes osztásokat rendszerint fejben végezzük (különösen, ha az alapszám kicsi), és csupán a hányadosokat és maradékokat tüntetjük fel, azokat egy alábbi típusú sémában elrendezve:

$$\begin{array}{r|l} 376 & 4 \\ 57 & 3 \\ 9 & 3 \\ \hline 1 & \end{array}$$

A bal oldali oszlopban állnak tehát az osztandók (melyek egyúttal hányadosok is), míg a jobb oldali oszlopban a maradékok (melyek a legalul álló számmal együtt a jegyeket adják, fordított sorrendben). A fenti sémát természetesen felülről lefelé, illetve azonos soron belül balról jobbra haladva készítjük el.

b.
$$\begin{array}{r|l} 830 & 2 \\ 138 & 0 \\ 23 & 5 \\ \hline 3 & \end{array}$$

Így $830 = 3\overset{6}{\breve{5}}02.$

5. Készítsünk „egymegegy" és „egyszeregy" táblázatot a 6-os számrendszerben!

Megoldás:

Az „egymegegy" táblázat:

	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	10
2	2	3	4	5	10	11
3	3	4	5	10	11	12
4	4	5	10	11	12	13
5	5	10	11	12	13	14

Az „egyszeregy” táblázat:

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	10	12	14
3	0	3	10	13	20	23
4	0	4	12	20	24	32
5	0	5	14	23	32	41

(Például a $4 \cdot 5$ szorzat értékét a következőképpen kereshetjük ki: a második táblázat első oszlopában kikeressük a 4-et, első sorában az 5-öt. A megfelelő sor, ill. oszlop kereszteződésénél áll a szorzat 6-os számrendszerben felírt értéke: 32. Valóban, $4 \cdot 5 = 20 = 3 \cdot 6 + 2 = \overset{6}{32}$.)

6. Az előző példa megoldása során készített táblázatokat felhasználva, végezzük el a kijelölt műveleteket:

a. $\overset{6}{3154} + \overset{6}{4215} = ?$

b. $\overset{6}{4201} - \overset{6}{2135} = ?$

c. $\overset{6}{2354} \cdot \overset{6}{1343} = ?$

Megoldás:

Az „egymegegy”, ill. az „egyszeregy” táblázat alapján (a szereplő számokat 6-os számrendszerben felírt számoknak tekintve):

a.
$$\begin{array}{r} 3154 \\ +\ 4215 \\ \hline 11413 \end{array}$$

b.
$$\begin{array}{r} 4201 \\ -\ 2135 \\ \hline 2022 \end{array}$$

c.
$$\begin{array}{l} 2354 \cdot 1343 \\ 11550 \\ \ \ 14344 \\ \ \ \ \ 11550 \\ \hline 4152430 \end{array}$$

3. OSZTHATÓSÁG

A számelmélet nagyrészt az oszthatóság fogalmára épül.

Ha adott a, b egész számokhoz található olyan c egész szám, hogy

$$a = bc,$$

akkor azt mondjuk, hogy *a osztható b-vel* (vagy másképpen: *b osztója a-nak*), és ezt a következőképpen jelöljük: $b|a$. (A definícióból speciálisan következik, hogy $0|0$.)

A maradékos osztás tételét felhasználva, ez a definíció a következőképpen fogalmazható át:

Ha az a egész szám, b pedig 0-tól különböző egész szám, és a-t b-vel osztva 0 maradékot kapunk, akkor azt mondjuk, hogy a osztható b-vel. A 0-t oszthatónak tekintjük 0-val.

Könnyen igazolhatók az oszthatóság alábbi tulajdonságai:

A) Bármely a egész számra $a|a$. (Az oszthatóság *reflexív*.)

B) Ha az a, b, c egész számokra $a|b$ és $b|c$ teljesül, akkor szükségképpen $a|c$ is fennáll. (Az oszthatóság *tranzitív*.) Másképpen: ha $a|b$, akkor tetszőleges d egész számra $a|bd$. (L. a 16. feladatot.)

C) Valamely a egész szám akkor és csak akkor osztója *minden* egész számnak, ha $a=-1$ vagy $a=+1$.

Ha $a|b$ minden b egész számra teljesül, akkor a-t *egységnek* nevezzük. (Ez a definíció elsősorban a racionális egész számok számelméletének különböző általánosításaiban játszik fontos szerepet.) A racionális egész számok körében tehát két egység van: -1 és $+1$.

D) $a|b$ akkor és csak akkor teljesül, ha $a|(-b)$, $(-a)|b$ és $(-a)|(-b)$ is fennáll.

E) Ha $a|b$ és $b|a$ egyidejűleg fennáll, akkor szükségképpen $a=b$ vagy $a=-b$.

F) A 0 osztható bármely egész számmal (beleértve a 0-t is!).

G) Ha az a, b, c egész számokra $a|b$ és $a|c$ teljesül, akkor tetszőleges d, e egész számokra: $a|(db+ec)$. (Rögzített b és c mellett a $db+ec$ alakú számok összességét b és c *lineáris kombinációinak* mondjuk. Ezt a terminológiát használva, e tulajdonság a következőképpen fogalmazható meg: ha két egész szám osztható valamely a egész számmal, akkor a *lineáris*

kombinációik is oszthatók a-val.) Speciálisan: ha $a|b$ és $a|c$, akkor $a|(b+c)$ és $a|(b-c)$. (L. a 7. példát.)

Oszthatósági feladatok megoldása során gyakran hivatkozunk az a^n-b^n, $a^{2k+1}+b^{2k+1}$ algebrai kifejezések szorzattá alakítására vonatkozó azonosságokra:

$$(7) \quad a^n-b^n = (a-b)(a^{n-1}+a^{n-2}b+\ldots+ab^{n-2}+b^{n-1}),$$

$$(8) \quad a^{2k}-b^{2k} = (a+b)(a^{2k-1}-a^{2k-2}b+\ldots+ab^{2k-2}-b^{2k-1})$$

és

$$(9) \quad a^{2k+1}+b^{2k+1} = (a+b)(a^{2k}-a^{2k-1}b+\ldots-ab^{2k-1}+b^{2k}),$$

ahol a, b tetszőleges valós számok, n 1-nél nagyobb, k pedig tetszőleges természetes szám. Például a (7) összefüggésből következik, hogy ha a, b egész számok, akkor $(a-b)|(a^n-b^n)$.

Egy másik elemi tény, melyre gyakran hivatkozunk: tetszőleges k természetes számot megadva, bármely k számú egymást követő egész szám valamelyike osztható k-val. Következésképpen: k számú egymást követő egész szám szorzata mindig osztható k-val.

Az oszthatósági feladatok rendszerint lényegesen könnyebben oldhatók meg *kongruenciák* segítségével, melyekkel a következő fejezetben fogunk foglalkozni.

Példák

7. Igazoljuk az oszthatóság *G)* tulajdonságát!

Megoldás:

Feltevésünk szerint $a|b$ és $a|c$ tehát alkalmas f, g egész számokra $b=af$ és $c=ag$. Így tetszőleges d, e egész számokra

$$db+ec = d(af)+e(ag) = a(df+eg),$$

tehát $db+ec$ az a-nak *egészszámszorosa*, és így $a|(db+ec)$ valóban fennáll.

8. Bizonyítsuk be, hogy ha egy háromjegyű természetes számot (mondjuk $\overset{10}{\smile}abc$-t) kétszer egymás mellé írunk, akkor az így kapott hatjegyű szám (tehát $\overset{10}{\smile}abcabc$) osztható 7-tel, 11-gyel és 13-mal!

Megoldás:

$$\overset{10}{\overbrace{abcabc}} = a\cdot 10^5+b\cdot 10^4+c\cdot 10^3+a\cdot 10^2+b\cdot 10+c =$$

$$= a\cdot 10^2(10^3+1)+b\cdot 10(10^3+1)+c(10^3+1) =$$

$$= (10^3+1)(100a+10b+c) = 1001\,(100a+10b+c) =$$

$$= 7\cdot 11\cdot 13(100a+10b+c),$$

ahonnan következik az állítás.

9. Bizonyítsuk be, hogy ha n természetes szám, akkor

$$f(n) = 3^{2n+1}+2^{n+2}$$

osztható 7-tel!

I. Megoldás:

$$f(n) = 3\cdot 3^{2n}+2^2\cdot 2^n = 3\cdot 9^n+4\cdot 2^n =$$

$$= 3\cdot 9^n+(7-3)\cdot 2^n = 3\cdot 9^n+7\cdot 2^n-3\cdot 2^n = 3(9^n-2^n)+7\cdot 2^n.$$

Itt az első tagban szereplő 9^n-2^n tényező a (7) azonosság értelmében osztható az alapok különbségével, azaz $9-2=7$-tel. Így a kapott összeg mindkét tagjának van 7-tel osztható tényezője, tehát az oszthatóság *G)* tulajdonsága értelmében ezek lineáris kombinációja, $f(n)$ is osztható 7-tel.

II. Megoldás:

Teljes indukcióval fogunk bizonyítani. Nyilván

$$f(1) = 3^{2\cdot 1+1}+2^{1+2} = 3^3+2^3 = 27+8 = 35 = 5\cdot 7$$

osztható 7-tel.

Most tegyük fel, hogy

(10) $\quad 7|f(k).$

Ekkor

$$f(k+1) = 3^{2(k+1)+1}+2^{(k+1)+2} = 3^{2k+3}+2^{k+3} =$$

$$= 3^2\cdot 3^{2k+1}+2\cdot 2^{k+2} = 9\cdot 3^{2k+1}+2\cdot 2^{k+2} =$$

$$= (7+2)\cdot 3^{2k+1}+2\cdot 2^{k+2} = 7\cdot 3^{2k+1}+2(3^{2k+1}+2^{k+2} =$$

$$= 7\cdot 3^{2k+1}+2f(k),$$

ahonnan (10)-re és az oszthatóság *G)* tulajdonságára tekintettel következik az állítás.

(Az indukció alkalmazása hasonló típusú feladatok megoldása során azért jelent könnyebbséget, mert $f(k+1)$ átalakítását megszabja az a tény, hogy $f(k)$-nak fel kell lépnie).

4. A LEGNAGYOBB KÖZÖS OSZTÓ. A LEGKISEBB KÖZÖS TÖBBSZÖRÖS. LINEÁRIS DIOFANTIKUS EGYENLETEK

A számelméletnek, ill. a racionális számelmélet különböző általánosításainak felépítése során alapvető szerepet játszik a *legnagyobb közös osztó* fogalma. Két szám legnagyobb közös osztóját a legegyszerűbben a következőképpen definiálhatjuk:

Ha az a, b egész számok közül legalább az egyik 0-tól különböző, akkor a két szám közös osztói közül a legnagyobb abszolút értékűeket a és b legnagyobb közös osztójának nevezzük; $a=b=0$ esetén pedig a és b legnagyobb közös osztója legyen 0. Bármely a, b számokat is tekintünk, azoknak mindig van közös osztójuk, hiszen például az 1 közös osztó. Másrészt, ha a és b közül legalább az egyik 0-tól különböző, akkor a közös osztók egyike sem lehet nagyobb, mint $|a|$ és $|b|$ közül a nagyobbik. Ebből a két tényből következik, hogy *bármely két egész számnak van legnagyobb közös osztója.* Nyilvánvaló az is, hogy két szám legnagyobb közös osztójának negatívja is legnagyobb közös osztója a két számnak; további legnagyobb közös osztója azonban nincs a két számnak. Ezt a tényt úgy szoktuk megfogalmazni, hogy *a legnagyobb közös osztó lényegében* (azaz, előjeltől eltekintve) *egyértelműen van meghatározva.*

A legnagyobb közös osztó fogalma másféleképpen is definiálható:

Legyenek a, b adott egész számok. A D egész számot akkor nevezzük a és b legnagyobb közös osztójának, ha az rendelkezik az alábbi tulajdonságokkal:

A) $D|a$ és $D|b$ teljesül;

B) ha valamely d egész számra $d|a$ és $d|b$ teljesül, akkor szükségképpen $d|D$ is fennáll.

(Ez utóbbi definíció tehát abban különbözik az előbbitől, hogy a *B)* pótolja azt a feltételt, mely szerint a közös osztók közül a legnagyobb abszolút értékűeket nevezzük legnagyobb közös osztónak.)

E definíciót alkalmazva, felmerül az a nehézség, hogy a legnagyobb közös osztót így definiálva, annak létezése és egyértelműsége távolról sem magától értetődő tény. Ezért a nehézségért azonban bőven kárpótol az, hogy ez a definíció az előbbihez viszonyítva a legnagyobb közös osztónak

lényegesen mélyebb, számelméleti szempontból fontosabb tulajdonságait fejezi ki. Másrészt ha a racionális számelmélet (a racionális egész számok elméletének) különböző általánosításai során (l. az V. fejezet 4. pontját), ill. különböző rokon területeken be akarjuk vezetni a legnagyobb közös osztó megfelelőjét, akkor csupán a második definíció vihető át.

A fentiek miatt a továbbiakban *a legnagyobb közös osztó második definícióját vesszük alapul.*

E definícióból kiindulva ekkor bizonyításra szorul, hogy bármely a, b egész számoknak létezik a legnagyobb közös osztója. Ez a tény az ún. *euklideszi algoritmus* segítségével igazolható, mely egyúttal konkrét számok legnagyobb közös osztójának meghatározására is alkalmas. Ez az algoritmus *a maradékos osztás tételére* épül, melyet az 1. pontban már említettünk. E tételt felhasználva, valamely a, b egész számok legnagyobb közös osztója a következőképpen határozható meg az euklideszi algoritmus segítségével:

Ha $b=0$, akkor könnyen látható, hogy a legnagyobb közös osztó létezik és a-val egyenlő.

Ha viszont $b\neq 0$, akkor az euklideszi algoritmus első lépésként osszuk el a-t b-vel. Jelöljük a hányadost q_1-gyel, a maradékot r_1-gyel:

$$a = q_1 b + r_1.$$

Ha $r_1=0$, akkor itt megállunk, vége az eljárásnak.

Ha viszont $r_1\neq 0$, akkor az előbbi osztót, b-t elosztjuk az előbbi maradékkal, r_1-gyel. Jelöljük a hányadost q_2-vel, a maradékot r_2-vel:

$$b = q_2 r_1 + r_2.$$

Ha $r_2=0$, akkor befejezzük az eljárást; ha viszont $r_2\neq 0$, akkor az előbbi osztót osztjuk az előbbi maradékkal:

$$r_1 = q_3 r_2 + r_3.$$

Ezt az eljárást így folytatjuk tovább, amíg valamely osztásnál 0 maradékot nem kapunk. Ennek véges sok lépés után be kell következnie, hiszen a maradékok nyilván szigorúan fogyó sorozatot alkotnak: $(|b|>)r_1>r_2>r_3>\ldots$. Nemnegatív egész számok szigorúan fogyó sorozata azonban csak véges hosszú-

ságú lehet. (Sőt, innen az is látható, hogy az algoritmus legfeljebb $|b|$ lépésből állhat.)

Tegyük fel, hogy az utolsó 0-tól különböző maradékot az n-edik osztás során kapjuk:

$$r_{n-2} = q_n r_{n-1} + r_n,$$

és az utolsó osztás:

$$r_{n-1} = q_{n+1} r_n.$$

Igazolható, hogy *az utolsó 0-tól különböző maradék*, r_n rendelkezik a legnagyobb közös osztót definiáló *A)*, *B)* tulajdonságokkal (l. a 35*. feladatot). Ezzel beláttuk, hogy *bármely két egész számnak létezik a legnagyobb közös osztója.*

Bármely két szám legnagyobb közös osztója lényegében — azaz előjeltől eltekintve — egyértelműen van meghatározva. Részletezve: ha D_1 és D_2 is legnagyobb közös osztója az a, b egész számoknak, akkor szükségképpen $D_2 = D_1$ vagy $D_2 = -D_1$. A második definíciót alkalmazva, ez a tény bizonyításra szorul; meglehetősen egyszerű, közvetlen bizonyítás adható, az euklideszi algoritmus felhasználása nélkül (l. a 34. feladatot).

Végeredményben tehát akár az első, akár a második definíciót alkalmazzuk, bármely a, b egész számok legnagyobb közös osztója lényegében egyértelműen van meghatározva. Könnyen igazolható, hogy a kétféleképpen definiált legnagyobb közös osztó megegyezik, vagyis *a két definíció ekvivalens.*

Az a, b egész számok lényegében egyértelműen meghatározott legnagyobb közös osztóját (a, b)-vel jelöljük; mégpedig (a, b)-n. rendszerint a legnagyobb közös osztó *pozitív* értékét értjük. (Nem szabad azonban elfelejtenünk, hogy (a, b)-vel együtt $-(a, b)$ is legnagyobb közös osztó.)

Fontos speciális eset, amikor $(a, b) = 1$; ilyenkor azt mondjuk, hogy az a, b egész számok egymáshoz *relatív prímek.*

Az euklideszi algoritmus segítségével levezethető a legnagyobb közös osztó következő fontos tulajdonsága is:

C) Bármely a, b egész számok legnagyobb közös osztója felírható a két szám *lineáris kombinációjaként*, azaz

$$au + bv = (a, b)$$

alakban, ahol u, v egész számok.

Az euklideszi algoritmus segítségével nem csupán ilyen u, v egész számok létezése igazolható, hanem ezek konkrétan meg is határozhatók (l. a 36*. feladatot).

Megjegyezzük, hogy akár (a, b) kiszámítása, akár (11)-et kielégítő u, v számok meghatározása a célunk, a gyakorlatban az euklideszi algoritmust kissé módosított formában alkalmazzuk. Nevezetesen az euklideszi algoritmus egyes osztásainak elvégzése során a maradékos osztás tétele helyett célszerű azt az 1. pontban említett módosított formában alkalmazni, vagyis célszerű az *abszolút legkisebb maradékok* felhasználásával osztani. Könnyen látható, hogy ekkor az euklideszi algoritmusról fent elmondottak változatlanul érvényben maradnak, másrészt az így módosított euklideszi algoritmus általában kevesebb lépésből áll, tehát kevesebbet kell számolnunk.

Foglaljuk össze az eddigieket: *bármely a, b egész számoknak létezik legnagyobb közös osztója, mely lényegében egyértelműen van meghatározva, és az euklideszi algoritmusban fellépő utolsó, 0-tól különböző maradékkal azonos.* Továbbá *bármely két szám legnagyobb közös osztója felírható a két szám lineáris kombinációjaként.*

A legnagyobb közös osztó két további fontos tulajdonsága levezethető a *C)* tulajdonságból:

D) Tetszőleges a, b, c egész számokra $(ac, bc) = c(a, b)$ (l. a 39*. feladatot).

E) Ha a, b, c egész számok, és $(b, c) = 1$ teljesül, akkor $(ab, c) = (a, c)$. Speciálisan, ha $(b, c) = 1$ mellett $(a, c) = 1$ is teljesül, akkor $(ab, c) = 1$ (l. a 43*. feladatot).

Ugyancsak a legnagyobb közös osztó *C)* tulajdonságából vezethető le a következő két, alapvető fontosságú tétel:

F) Ha az a, b, c egész számokra $a|bc$ és $(a, b) = 1$ teljesül, akkor szükségképpen $a|c$ is fennáll (l. a 41*. feladatot).

G) Ha az a, b, c egész számokra $a|c$, $b|c$ és $(a, b) = 1$ teljesül, akkor szükségképpen $ab|c$ is fennáll (l. a 42*. feladatot).

Kettőnél több szám legnagyobb közös osztója ugyanúgy definiálható, mint két számé:

Legyenek $a_1, a_2, \ldots, a_k$ adott egész számok (k tetszőleges, 1-nél nagyobb természetes szám). A D egész számot akkor nevezzük az $a_1, a_2, \ldots, a_k$ számok legnagyobb közös osztójának, ha az kielégíti az alábbi két feltételt:

A') $D|a_1, D|a_2, \ldots, D|a_k$ teljesül.

B') Ha valamely d egész számra $d|a_1, d|a_2, \ldots, d|a_k$ teljesül, akkor szükségképpen $d|D$ is fennáll.

Igazolható, hogy bármely $a_1, a_2, \ldots, a_k$ számoknak létezik legnagyobb közös osztója, és az lényegében (egységszorzótól, azaz előjeltől eltekintve) egyértelműen van meghatározva; ezt a legnagyobb közös osztót $(a_1, a_2, \ldots, a_k)$-val jelöljük. Mind ennek a tételnek a bizonyítása, mind konkrét számok legnagyobb közös osztójának meghatározása visszavezethető *két* szám legnagyobb közös osztójának vizsgálatára, az

$$(12) \quad (a_1, a_2, \ldots, a_n) = ((a_1, a_2, \ldots, a_{n-1}), a_n)$$

összefüggés révén.

Példák

10. Számítsuk ki *a.* az euklideszi algoritmus segítségével; *b.* a módosított euklideszi algoritmus révén (vagyis az egyes osztásokat az abszolút legkisebb maradékok segítségével végezve) 504 és 372 legnagyobb közös osztóját!

Megoldás:

a. $504 = 1 \cdot 372 + 132,$

$372 = 2 \cdot 132 + 108,$

$132 = 1 \cdot 108 + 24,$

$108 = 4 \cdot 24 + 12,$

$24 = 2 \cdot 12.$

A legnagyobb közös osztó tehát az utolsó, 0-tól különböző maradék, a 12.

b. $504 = 1 \cdot 372 + 132,$

$372 = 3 \cdot 132 - 24.$

Nyilván nem változik a legnagyobb közös osztó, ha negatív maradék esetén a következő lépésben annak abszolút értékével osztunk:

$$132 = 5 \cdot 24 + 12,$$

$$24 = 2 \cdot 12.$$

A legnagyobb közös osztó tehát az utolsó, 0-tól különböző maradék, 12.

11. Igazoljuk a legnagyobb közös osztó *F)* tulajdonságát (ha $a|bc$ és $(a, b) = 1$, akkor szükségképpen $a|c$)!

Megoldás:

A legnagyobb közös osztó *C)* tulajdonsága szerint léteznek olyan u, v egész számok, melyekre

$$au + bv = (a, b) = 1.$$

Mindkét oldalt c-vel szorozva:

$$a(cu) + (bc)v = c.$$

Feltevésünk szerint $a|bc$, tehát a bal oldal mindkét tagjának első tényezője osztható a-val. Így az oszthatóság *G)* tulajdonsága szerint ezek lineáris kombinációja, a bal oldal is osztható a-val, és így a jobb oldal, azaz c is.

Két szám *legkisebb közös többszörösét* is kétféleképpen definiálhatjuk. *Az első definíció:*

Az a, b egész számok közös többszörösei közül a legkisebb abszolút értékűeket a és b legkisebb közös többszörösének nevezzük.

A másik definíció:

Legyenek a, b adott egész számok. Az M egész számot akkor nevezzük a és b legkisebb közös többszörösének, ha az rendelkezik az alábbi két tulajdonsággal:

A'') $a|M$ és $b|M$ teljesül.

B'') Ha valamely m egész számra $a|m$ és $b|m$ teljesül, akkor szükségképpen $m|M$ is fennáll.

Akár az első, akár a második definícióból indulunk ki, igazolható, hogy

bármely a, b egész számoknak létezik a legkisebb közös többszörösük, és az lényegében (egységszorzótól, azaz előjeltől eltekintve) egyértelműen van meghatározva; továbbá

a kétféleképpen definiált legkisebb közös többszörösök megegyeznek.

Az a, b számok legkisebb közös többszörösét a következőképpen jelöljük: $[a, b]$. (Kettőnél több szám legkisebb közös többszöröse analóg módon definiálható, annak létezésére hasonló tétel igaz, és (12)-höz hasonló formula segítségével határozható meg.)

Bizonyítható, hogy bármely a, b egész számokra

(13) $ab = (a, b)[a, b]$.

Ennek az összefüggésnek az alapján két szám legkisebb közös többszörösének vizsgálata, ill. konkrét számok legkisebb közös többszörösének meghatározása visszavezethető a legnagyobb közös osztó vizsgálatára, ill. annak kiszámítására.

Példa

12. Számítsuk ki 504 és 372 legkisebb közös többszörösét!

Megoldás:
Már láttuk az előzőkben, hogy $(504,372)=12$. Így (13) alapján

$$[504,372] = \frac{504 \cdot 372}{(504,372)} = 504 \cdot 31 = 15624.$$

A legnagyobb közös osztó *C)* tulajdonsága alapján tárgyalhatók a *lineáris diofantikus egyenletek* is. *Kétismeretlenes lineáris diofantikus egyenleten*

(14) $ax+by = c$

alakú egyenletet értünk, ahol a, b, c adott egész számok, és az egyenletnek x, y *egész* megoldásait keressük.

Állítjuk, hogy a (14) *egyenlet megoldhatóságának szükséges és elégséges feltétele az*, hogy $(a, b)|c$ teljesüljön. E feltétel szükségessége következik az oszthatóság *G)* tulajdonságából. Másrészt, ha feltesszük, hogy $(a, b)|c$, akkor $k=\frac{c}{(a, b)}$ egész szám. A legnagyobb közös osztó *C)* tulajdonsága szerint léteznek olyan u, v egész számok, melyekre (11) teljesül. (11) mindkét oldalát k-val megszorozva, látható, hogy $x=uk, y=vk$ kielégítik (14)-et. Továbbá ez a bizonyítás egyúttal módszert is ad (14) egy konkrét megoldásának meghatározására.

Könnyen igazolható továbbá, hogy ha ismerjük a (14) diofantikus egyenletnek *egy* x_0, y_0 megoldását, akkor az egyenlet *összes megoldását* a következőképpen állíthatjuk elő:

$$(15)\quad x = x_0 + \frac{b}{(a, b)} t, \quad y = y_0 - \frac{a}{(a, b)} t, \quad \text{ahol}$$

$$t = 0, \pm 1, \pm 2, \ldots .$$

Az ugyanis könnyen ellenőrizhető, hogy ezek az x, y (egész számokból álló) számpárok kielégítik (14)-et. Másrészt, tegyük fel, hogy x, y és x_0, y_0 is megoldás, vagyis (14) és

$$ax_0 + by_0 = c$$

teljesül. Ezt az egyenlőséget kivonva (14)-ből:

$$a(x - x_0) + b(y - y_0) = 0.$$

$(a, b) = 0$-ból $a = b = 0$ következne, ami nyilván érdektelen eset; így feltehető, hogy $(a, b) \neq 0$. Ekkor (a, b)-vel osztva:

$$(15')\quad \frac{a}{(a, b)}(x - x_0) = \frac{b}{(a, b)}(y - y_0).$$

Innen következik, hogy $\frac{b}{(a, b)}$ osztója a bal oldalon álló szorzatnak. Nyilván $\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = 1$, tehát az *F)* tulajdonság szerint szükségképpen $\frac{b}{(a, b)}$ osztója a második tényezőnek:

$$\frac{b}{(a, b)} \,\Big|\, (x - x_0).$$

Más szóval, létezik olyan t egész szám, hogy

$$x - x_0 = \frac{b}{(a, b)} t,$$

vagyis

$$x = x_0 + \frac{a}{(a, b)} t,$$

(15′)-be helyettesítve és y-t kifejezve, nyerjük, hogy

$$y = y_0 - \frac{a}{(a, b)} t,$$

tehát valóban minden megoldás a (15) alakban írható.

A *lineáris diofantikus egyenletek általános alakja* a következő:

$$a_1x_1 + a_2x_2 + \ldots + a_kx_k = b.$$

ahol $a_1, a_2, \ldots, a_k, b$ adott egész számok, és az egyenletnek $x_1, x_2, \ldots, x_k$ *egész* megoldásait keressük. Ennek az egyenletnek a megoldása visszavezethető *kétismeretlenes* lineáris diofantikus egyenletek megoldására. *A megoldhatóság szükséges és elégséges feltétele* az, hogy $(a_1, a_2, \ldots, a_k)|b$ teljesüljön.

Példák

13. Állapítsuk meg, hogy a

$$33x + 21y = 24$$

lineáris diofantikus egyenlet megoldható-e? Ha az egyenlet megoldható, adjuk is meg egy megoldását!

Megoldás:

Először számítsuk ki 33 és 21 legnagyobb közös osztóját a módosított euklideszi algoritmus segítségével:

$$33 = 2 \cdot 21 - 9,$$

$$21 = 2 \cdot 9 + 3,$$

$$9 = 3 \cdot 3.$$

A legnagyobb közös osztó tehát az utolsó, 0-tól különböző maradék, $3 : (33,21) = 3$. A vizsgált egyenlet jobb oldala, 24 osztható 3-mal, és így az egyenlet megoldható.

(Természetesen 33 és 21 legnagyobb közös osztóját közvetlenül, az euklideszi algoritmus felhasználása nélkül is könnyen meghatározhatnánk; a továbbiakban azonban — az egyenlet egy megoldásának meghatározása során — még szükségünk lesz a két számra vonatkozó euklideszi algoritmusra.)

Egy konkrét megoldás meghatározása céljából ki kell fejeznünk 33 és 21 legnagyobb közös osztóját, 3-at a két szám lineáris kombinációjaként. Ezt a következőképpen végezzük:

Először az euklideszi algoritmus első egyenlőségéből kifejezzük a maradékot (33 és 21 lineáris kombinációjaként):

$$9 = -1\cdot 33+2\cdot 21.$$

A kapott összefüggést felhasználva, kifejezzük az euklideszi algoritmus második egyenlőségéből a maradékot (33 és 21 lineáris kombinációjaként):

$$3 = 21-2\cdot 9 = 21-2\cdot(-1\cdot 33+2\cdot 21) = 21+2\cdot 33-4\cdot 21 =$$

$$= 2\cdot 33-3\cdot 21.$$

Ezzel (33,21)=3-at kifejeztük 33 és 21 lineáris kombinációjaként:

$$2\cdot 33-3\cdot 21 = (33,21) = 3.$$

Mindkét oldalt megszorozva $\frac{24}{(33,21)}=\frac{24}{3}=8$-cal:

$$33\cdot(2\cdot 8)-21\cdot(3\cdot 8) = 3\cdot 8,$$

vagyis

$$33\cdot 16+21\cdot(-24) = 24.$$

Így $x=16$, $y=-24$ megoldása a vizsgált lineáris diofantikus egyenletnek.

5. PRÍMSZÁMOK. A SZÁMELMÉLET ALAPTÉTELE

A prímszámok alapvető szerepet játszanak a számelméletben. Ennek oka a számelmélet alaptételében rejlik, melyet alább ismertetünk.

A *prímszám* vagy *törzsszám* fogalmát kétféleképpen is definiálhatjuk:

A) Valamely egységtől (azaz, -1-től és $+1$-től) különböző p egész számot akkor nevezünk prímszámnak, ha $p=ab$ esetén — ahol a, b egész számok — szükségképpen a vagy b egység (más szóval akkor, ha p csak ± 1-gyel és $\pm p$-vel osztható).

B) Valamely 0-tól és egységtől (azaz, -1-től és $+1$-től) különböző p egész számot akkor nevezünk prímszámnak, ha

$p|ab$ esetén — ahol a, b egész számok — szükségképpen a $p|a$ és $p|b$ relációk közül legalább az egyik teljesül.

Alapvető fontosságú az a tény, hogy a fenti két definíció ekvivalens.

Azaz, ha egy p egész szám prímszám a *B)* értelemben, akkor az *A)* értelemben is az (ennek bizonyítása viszonylag könnyű; l. a 64. feladatot), másrészt megfordítva, ha p prímszám az *A)* értelemben, akkor a *B)* értelemben is az. Ez utóbbinak a bizonyítása nehezebb (l. a 16. példát), és — közvetve vagy közvetlenül — a legnagyobb közös osztó létezésére és annak *C)* tulajdonságára, ezen keresztül az *euklideszi algoritmusra*, még tovább menve, a *maradékos osztás tételére* épül.

Ha valamely 0-tól és egységtől különböző természetes szám nem prímszám, akkor *összetett számnak* nevezzük.

Az adott definíciókból kitűnik, hogy ha p prímszám, akkor $-p$ is az. Mégis, a kialakult konvenciónak megfelelően, a következő ponttól kezdve prímszámon mindig *pozitív* prímszámot fogunk érteni.

A 63. feladat kapcsán igazolni fogjuk, hogy *végtelen sok prímszám* létezik. A prímszámokkal kapcsolatos mélyebb problémákkal a IV. fejezetben foglalkozunk.

Már utaltunk a *számelmélet alaptételére:*

Bármely, a 0-tól és az egységtől (azaz, -1-től és $+1$-től) különböző egész szám felírható prímszámok szorzataként, éspedig sorrendtől és egységszorzóktól (azaz előjelektől) eltekintve, egyértelműen.

Annak bizonyítása, hogy bármely, a 0-tól és a ± 1-től különböző egész szám felírható prímszámok szorzataként, viszonylag könnyebb, és a prímszámok *A)* definíciójára épül. Nehezebb az egyértelműség bizonyítása, melynek során fel kell használnunk a prímszámok *B)* definíciójában szereplő tulajdonságot is; így fel kell használnunk azt a tényt, hogy ha egy egész szám prímszám az *A)* értelemben, akkor a *B)* értelemben is az. Itt tehát közvetve építünk az euklideszi algoritmusra, még tovább menve, a maradékos osztás tételére.

Ha egy 1-nél nagyobb n természetes számot felírunk prímszámok szorzataként és az azonos tényezőket összegyűjtjük, akkor n-nek a következő típusú előállítását kapjuk:

$$(16) \quad n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r},$$

ahol $p_1, p_2, \dots, p_r$ páronként különböző pozitív prímszámok

(a pozitivitás $n>0$ miatt nyilván feltehető) és $\alpha_1, \alpha_2, \ldots, \alpha_r$ pozitív egész számok. A számelmélet alaptételéből következik, hogy *n-nek ez az előállítása a tényezők sorrendjétől eltekintve egyértelmű.* Ezt az előállítást az n szám *kanonikus vagy törzstényezős alakjának* nevezzük.

Legyen $r=\frac{a}{b}$ pozitív racionális szám, ahol a, b pozitív egész számok. Itt $a>1, b>1$ esetén a-t és b-t kanonikus alakban felírva (ha a, b valamelyike 1, változatlanul hagyjuk), és a nevezőben szereplő prímhatványokat negatív kitevők segítségével felírva, majd az azonos alapú prímhatványokat összevonva, $r\neq 1$ esetén r-nek

$$(17) \quad r = q_1^{\beta_1} q_2^{\beta_2} \ldots q_s^{\beta_s}$$

alakú előállítását nyerjük, ahol $q_1, q_2, \ldots, q_s$ páronként különböző (pozitív) prímszámok, $\beta_1, \beta_2, \ldots, \beta_s$ 0-tól különböző egész számok (utóbbiak természetesen lehetnek negatív számok is). Igazolható, hogy *r-nek ez az előállítása a tényezők sorrendjétől eltekintve egyértelmű.* Ezt az előállítást r *kanonikus alakjának* nevezzük.

(Ha n vagy r negatív, akkor a (16), ill. (17) kanonikus alak természetesen csak annyiban módosul, hogy a jobb oldalon mínusz jelet írunk.)

Felmerülhet az a kérdés, hogy hogyan tudjuk valamely *adott n természetes szám kanonikus alakját meghatározni?* E feladat megoldásához elegendő a következő problémát megoldani: *meghatározandók az n-nél nem nagyobb prímszámok.* (Ha ugyanis ez utóbbi feladatot meg tudjuk oldani, akkor már nyilván az előbbi feladat megoldása sem jelent elvi nehézséget, csupán némi számolásra van szükség.) A második feladat viszont az ún. *eratoszthenészi szita* révén oldható meg.

Ennek első lépéseként felírjuk 2-től n-ig a természetes számokat:

$$2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, \ldots, n.$$

E sorozatban az első helyen álló szám, a 2 prímszám; ezt a számot bekarikázzuk. Ezután kihúzzuk („kiszitáljuk") a sorozat 2-nél nagyobb, 2-vel osztható elemeit:

$$2, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, 9, \cancel{10}, 11, \cancel{12}, \ldots.$$

Ezután bekarikázzuk a sorozat első, eddig be nem karikázott és át nem húzott elemét (a 3-at), majd áthúzzuk ennek nála nagyobb többszöröseit (tehát a 3-mal osztható, 3-nál nagyobb, eddig át nem húzott számokat):

②, ③, 4, 5, 6, 7, 8, 9, 10, 11, 12, ...

Az első be nem karikázott és át nem húzott szám, az 5 ismét prímszám; ezt bekarikázzuk, majd áthúzzuk 5-nél nagyobb többszöröseit s í.t.

Ezt az eljárást addig folytatjuk, amíg végül valamennyi felírt számot bekarikázzuk vagy áthúzzuk. Könnyen látható, hogy ekkor a bekarikázott számok az n-nél nem nagyobb prímszámokkal azonosak, míg az áthúzott számok az n-nél nem nagyobb összetett számokkal.

Ez az eljárás kissé rövidíthető az alábbi megjegyzés segítségével (melyre még többször fogunk hivatkozni):

Legyen n adott természetes szám, és legyen az a pozitív egész szám osztója n-nek. Ekkor $b=\frac{n}{a}$ szintén pozitív egész szám, és

(18) $n=ab$,

tehát b is osztója n-nek. A (18)-at kielégítő osztópárokat *n komplementer osztóinak* nevezzük. Legyen a, b n-nek egy komplementer osztópárja. Feltehető, hogy $a \leqq b$. Ekkor $a \leqq \sqrt{n}$, hiszen ellenkező esetben

$$(n =)ab \geqq a^2 > (\sqrt{n})^2 = n$$

teljesülne. Ezzel igazoltuk, hogy *komplementer osztók kisebbike nem nagyobb* $\sqrt{n}$-nél.

Ebből az is következik, hogy *ha n összetett szám, akkor van olyan d osztója, melyre $2 \leqq d \leqq \sqrt{n}$ teljesül*, és így még inkább van e feltételt *kielégítő prímosztója*. Így az eratoszthenészi szitát a következőképpen rövidíthetjük le: ha már valamennyi, $\sqrt{n}$-nél nem nagyobb prímszám többszöröseit „kiszitáltuk", akkor megállunk, és valamennyi megmaradt számot bekarikázzuk, hiszen ezek már szükségképpen mind prímszámok.

Példák

14. Határozzuk meg azokat a p prímszámokat, melyekre $p+10$ és $p+14$ is prímszám!

Megoldás:

A $p-1$ $p, p+1$ számok valamelyikének oszthatónak kell lennie 3-mal, hiszen három egymást követő szám valamelyike biztosan osztható 3-mal. Ha továbbá $p-1$ osztható 3-mal, akkor $p+14=(p-1)+15=(p-1)+3\cdot 5$ is, ha pedig $p+1$ osztható 3-mal, akkor $p+10=(p+1)+9=(p+1)+3\cdot 3$ is. Így a $p, p+10, p+14$ számok valamelyike biztosan osztható 3-mal. Ez a szám csak abban az esetben lehet prímszám, ha -3-mal vagy $+3$-mal egyenlő. Így hat lehetőséget kell megvizsgálnunk: $p=-3$ vagy $+3$, $p+10=$ $=-3$ vagy $+3$ és $p+14=-3$ vagy $+3$. Az innen p-re adódó értékek rendre $p=-3, +3, -13, -7, -17, -11$. E hat eset közül csupán négyben teljesül, hogy $p+10$ és $p+14$ is prímszám, nevezetesen $p=-17, -7, -3$ és $+3$ esetén.

15. Bizonyítsuk be, hogy ha valamely p egész szám prímszám az *A)* értelemben, akkor a *B)* értelemben is az!

Megoldás:

Legyen p prímszám az *A)* értelemben. Ekkor $p\neq\pm 1$ és $p\neq 0$ (utóbbi könnyen következik az *A)* definícióból), továbbá (kissé átfogalmazva a definíció követelményeit) p összes osztói $-1, +1, -p$ és $+p$.

Tegyük fel most, hogy valamely a, b egész számokra $p|ab$. Ha $p|a$, készen vagyunk; elég tehát a $p\nmid a$ esetre szorítkozni.

Mivel az eddigiek szerint $p\nmid a$, és p összes osztói $-1, +1, -p$ és $+p$, szükségképpen $(a, p)=1$. Így a legnagyobb közös osztó *C)* tulajdonsága szerint léteznek olyan u, v egészek, hogy

$$au+pv = 1.$$

Mindkét oldalt b-vel szorozva:

$$(ab)u+p(bv) = b.$$

Feltevésünk szerint $p|ab$, tehát p osztója a bal oldalon álló mindkét tag első tényezőjének, így az oszthatóság *G)* tulajdonsága szerint osztója ezek lineáris kombinációjának, az egész bal oldalnak és így a jobb oldalnak, b-nek is; és ezzel az állítást igazoltuk.

(A bizonyítás második részében hivatkozhattunk volna a 11. példára is.)

16. Bizonyítsuk be, hogy valamely $n>1$ egész szám akkor és csak akkor teljes k-adik hatvány (azaz pozitív egész szám k-adik hatványa), ha kanonikus alakjában valamennyi kitevő osztható k-val! (k tetszőleges természetes szám.)

Megoldás:

Legyen k kanonikus alakja

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}.$$

Tegyük fel, hogy itt valamennyi kitevő osztható k-val, azaz $\alpha_1 = k\beta_1$, $\alpha_2 = k\beta_2, \ldots, \alpha_r = k\beta_r$, ahol $\beta_1, \beta_2, \ldots, \beta_r$ pozitív egész számok. Ekkor

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} = p_1^{k\beta_1} p_2^{k\beta_2} \ldots p_r^{k\beta_r} = (p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r})^k = m^k,$$

ahol $m = p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}$ pozitív egész szám; és ezt kellett igazolnunk.

Másrészt tegyük fel, hogy n teljes k-adik hatvány, azaz valamely t pozitív egész számra

(19) $\quad n = t^k.$

Mivel $n > 1$, innen $t > 1$ következik. Legyen t kanonikus alakja

$$t = q_1^{\gamma_1} q_2^{\gamma_2} \ldots q_s^{\gamma_s}$$

(ahol tehát $q_1, q_2, \ldots, q_s$ páronként különböző pozitív prímszámok, a kitevők pozitív egész számok). (19)-be helyettesítve:

$$n = t^k = (q_1^{\gamma_1} q_2^{\gamma_2} \ldots q_s^{\gamma_s})^k = q_1^{k\gamma_1} q_2^{k\gamma_2} \ldots q_s^{k\gamma_s}.$$

n így kapott előállítása kielégíti a kanonikus alakkal szemben támasztott követelményeket (hiszen itt $q_1, q_2, \ldots, q_s$ páronként különböző prímszámok, a kitevők pedig pozitív egész számok). Minthogy a kanonikus alak egyértelmű, n-nek a fenti előállítása szükségképpen azonos n kanonikus alakjával, és itt nyilván minden kitevő osztható k-val. Ezzel az állítást igazoltuk.

(Ugyanígy igazolható, hogy egy 1-től különböző pozitív racionális szám akkor és csak akkor racionális szám k-adik hatványa, ha kanonikus alakjában valamennyi kitevő osztható k-val. Ebből például következik, hogy $\sqrt{2}$ irracionális szám.)

17. Határozzuk meg a 36-nál kisebb prímszámokat az eratoszthenészi szita segítségével!

Megoldás:

Írjuk fel 2-től 36-ig a természetes számokat:

2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22,

23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36.

A sorozat első eleme, a 2 prímszám. Ezt bekarikázzuk és áthúzzuk 2-nél nagyobb többszöröseit:

②, 3, ~~4~~, 5, ~~6~~, 7, ~~8~~, 9, ~~10~~, 11, ~~12~~, 13, ~~14~~, 15, ~~16~~, 17, ~~18~~, 19, ~~20~~, 21,

~~22~~, 23, ~~24~~, 25, ~~26~~, 27, ~~28~~, 29, ~~30~~, 31, ~~32~~, 33, ~~34~~, 35, ~~36~~.

Az első olyan szám, amelyik nincs áthúzva, vagyis a 3 prímszám. Karikázzuk ezt be és „szitáljuk ki" a többszöröseit:

②, ③, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21,

22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36.

Most az 5-öt karikázzuk be és ennek többszöröseit szitáljuk ki:

②, ③, 4, ⑤, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21,

22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36.

Az eljárást nem szükséges tovább folytatnunk, hiszen a következő prímszám, a 7 már nagyobb lenne, mint $\sqrt{36}=6$. Így a 36-nál kisebb prímszámok az utolsóként felírt számsor azon számai, melyek nincsenek áthúzva: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31.

18. Határozzuk meg 19649 kanonikus alakját!

Megoldás:

Az ismert oszthatósági szabályok szerint 19649 nem osztható 2, 3, 5 egyikével sem. A következő prímszám, a 7 azonban osztója 19649-nek: $19649=7\cdot 2807$. A kanonikus alak meghatározása céljából 2807-et kell tovább bontanunk. Mivel 19649 nem volt osztható 2-vel, 3-mal és 5-tel, így osztója, 2807 sem osztható ezekkel a prímekkel. 7-tel azonban osztható a vizsgált szám: $2807=7\cdot 401$. Így $19649=7^2\cdot 401$. Most a 401 tényezőt kell tovább bontanunk. Ez a szám az eddigiek szerint nem osztható 2, 3, 5 egyikével sem. A soron következő prímszámokkal, 7-tel, 11-gyel, 13-mal, 17-tel és 19-cel osztva, rendre a következőt kapjuk: $401=57\cdot 7+2$, $401=36\cdot 11+5$, $401=30\cdot 13+11$, $401=23\cdot 17+10$ és $401=21\cdot 19+2$. Tovább nem szükséges az eljárást folytatnunk, hiszen ha 401 összetett szám lenne, akkor lenne 2 és $\sqrt{401}<21$ közti prímosztója. Minthogy ilyen prímosztó nincs, a 401 szükségképpen prímszám. Végeredményben tehát 19649 kanonikus alakja: $19649=7^2\cdot 401$.

6. OSZTÓK. A $d(n)$ FÜGGVÉNY

Ebben a pontban a számelmélet alaptételének néhány további következményét fogjuk tárgyalni.

Legyen az n természetes szám kanonikus alakja

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}.$$

A számelmélet alaptételére hivatkozva, könnyen igazolható, hogy *valamely d természetes szám akkor és csak akkor osztója*

n-nek, ha

$$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$$

alakban írható, ahol $\beta_1, \beta_2, \dots, \beta_r$ olyan egész számok, melyekre

$$(20) \quad 0 \leqq \beta_1 \leqq \alpha_1,\ 0 \leqq \beta_2 \leqq \alpha_2,\ \dots,\ 0 \leqq \beta_r \leqq \alpha_r.$$

Valamely n természetes szám pozitív osztóinak a számát d(n)-nel szoktuk jelölni (a $\tau(n)$ jelölés is használatos). Ez a függvény a természetes számok halmazán van definiálva. Az olyan függvényeket, melyek értelmezési tartománya a természetes számok összessége, *számelméleti függvényeknek* nevezzük. Könnyen látható, hogy a (20)-at kielégítő $\beta_1, \beta_2, \dots, \beta_r$ (egész számokból álló) szám-r-esek száma $(\alpha_1+1)(\alpha_2+1)\dots(\alpha_r+1)$. Így a $d(n)$ számelméleti függvény $n>1$ esetén a következő képlet segítségével számítható ki:

$$(21) \quad d(n) = d(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}) = (\alpha_1+1)(\alpha_2+1)\dots\alpha_r+1)$$

és nyilván $d(1)=1$. Megjegyezzük, hogy ez a képlet akkor is érvényben marad, ha az $\alpha_1, \alpha_2, \dots, \alpha_r$ kitevők közt a 0 is előfordul.

Igazolható, akár a (21) képletet felhasználva, akár közvetlenül, hogy ha az m, n természetes számokra $(m, n)=1$ teljesül, akkor szükségképpen

$$d(mn) = d(m)d(n).$$

Ha valamely $f(n)$ számelméleti függvényre $(m, n)=1$ esetén

$$f(mn) = f(m)f(n)$$

teljesül, akkor *multiplikatív számelméleti függvénynek*, ha ez az összefüggés *bármely m, n* természetes számokra teljesül, akkor *totálisan multiplikatív számelméleti függvénynek* nevezzük $f(n)$-et. Így például az $f(n)=n^c$ (ahol c rögzített valós szám) számelméleti függvény totálisan multiplikatív. *A d(n) számelméleti függvény tehát multiplikatív*, de könnyen látható, hogy nem totálisan multiplikatív. (A $d(n)$ függvény multiplikativitására még vissza fogunk térni a III. fejezet 2. pontjában.)

Az osztók kanonikus alakjáról előbb elmondottakat (vagyis végső soron a számelmélet alaptételét) felhasználva, két szám kanonikus alakjának ismeretében a *két szám legnagyobb közös osztójának, ill. legkisebb közös többszörösének kanonikus alakja* könnyen meghatározható.

Legyen ugyanis az $a>1$, $b>1$ egész számok kanonikus alakja

$$a = p_1^{\alpha_1} \dots p_s^{\alpha_s} q_1^{\beta_1} \dots q_t^{\beta_t},$$

ill.

$$b = p_1^{\gamma_1} \dots p_s^{\gamma_s} r_1^{\delta_1} \dots r_u^{\delta_u},$$

ahol $p_1, \dots, p_s, q_1, \dots, q_t, r_1, \dots, r_u$ páronként különböző pozitív prímszámok, $\alpha_1, \dots, \alpha_s, \beta_1, \dots, \beta_t, \gamma_1, \dots, \gamma_s, \delta_1, \dots, \delta_u$ pozitív egész számok. (A két szám nyilván felírható ilyen alakban; pusztán arról van szó, hogy különválasztjuk a és b közös prímosztóit.) Jelöljük továbbá $i=1, 2, \dots, s$ esetén α_i, γ_i kisebbikét μ_i-vel, a nagyobbikat ω_i-vel. Igazolható, hogy ekkor a és b legnagyobb közös osztójának, ill. legkisebb közös többszörösének kanonikus alakja az alábbi:

$$(a, b) = p_1^{\mu_1} p_2^{\mu_2} \dots p_s^{\mu_s}$$

ill.

$$[a, b] = p_1^{\omega_1} \dots p_s^{\omega_s} q_1^{\beta_1} \dots q_t^{\beta_t} r_1^{\delta_1} \dots r_u^{\delta_u}.$$

Példák

19. Írjuk fel 72 pozitív osztóit!

Megoldás:
Először 72 kanonikus alakját kell meghatároznunk:

$$72 = 2\cdot 36 = 2\cdot 2\cdot 18 = 2\cdot 2\cdot 2\cdot 9 = 2\cdot 2\cdot 2\cdot 3\cdot 3 = 2^3\cdot 3^2.$$

Így 72 pozitív osztói $2^\alpha 3^\beta$ alakúak, ahol $0\leqq\alpha\leqq 3$ és $0\leqq\beta\leqq 2$. A keresett osztók tehát a következők:

$$2^0\cdot 3^0=1\cdot 1=1,\quad 2^1\cdot 3^0=2\cdot 1=2,\quad 2^2\cdot 3^0=4\cdot 1=4,\quad 2^3\cdot 3^0=8\cdot 1=8,$$

$$2^0\cdot 3^1=1\cdot 3=3,\quad 2^1\cdot 3^1=2\cdot 3=6,\quad 2^2\cdot 3^1=4\cdot 3=12,\quad 2^3\cdot 3^1=8\cdot 3=24,$$

$$2^0\cdot 3^2=1\cdot 9=9,\quad 2^1\cdot 3^2=2\cdot 9=18,\quad 2^2\cdot 3^2=4\cdot 9=36 \text{ és } 2^3\cdot 3^2=8\cdot 9=72$$

20. Határozzuk meg az $n=2^2\cdot 3^3\cdot 4^4\cdot 5^5\cdot 6^6$ szám pozitív osztóinak a számát!

Megoldás:
Először n kanonikus alakját kell meghatároznunk:

$$n = 2^2 \cdot 3^3 \cdot 4^4 \cdot 5^5 \cdot 6^6 = 2^2 \cdot 3^3 \cdot (2^2)^4 \cdot 5^5 \cdot (2 \cdot 3)^6 =$$

$$= 2^2 \cdot 3^3 \cdot 2^8 \cdot 5^5 \cdot 2^6 \cdot 3^6 = 2^{16} \cdot 3^9 \cdot 5^5.$$

Így

$$d(n) = (16+1)(9+1)(5+1) = 17 \cdot 10 \cdot 6 = 1020.$$

21. Bizonyítsuk be, hogy tetszőleges n természetes számra

$$d(n) \leqq 2\sqrt{n}.$$

Megoldás:
Alkossunk n pozitív osztóiból rendezett párokat a következőképpen („rendezett" páron azt értjük, hogy a sorrendre is tekintettel vagyunk): egy-egy párba tegyük n komplementer osztóit (azaz, a (19)-et kielégítő osztópárokat), mégpedig úgy, hogy az első helyre a két osztó kisebbike kerüljön. Így például $n=72$ esetén ezek a párok a következők: 1, 72; 2, 36; 3, 24; 4, 18; 6,12; 8, 9. Minthogy minden osztó szerepel valamelyik párban, $d(n)$ legfeljebb akkora, mint e párok számának kétszerese. (Sőt, $d(n)$ általában egyenlő e párok számának kétszeresével. Az egyetlen kivételes eset az, amikor n négyzetszám; ekkor ugyanis egy $\sqrt{n}$, $\sqrt{n}$; alakú pár is szerepel, tehát ekkor a $\sqrt{n}$ osztót kétszer számoljuk.) Azonban e rendezett párokban első helyen álló számok páronként különbözők, és 1 és $\sqrt{n}$ közé esnek (hiszen az előző pontban mondottak szerint komplementer osztók kisebbike nem lehet nagyobb $\sqrt{n}$-nél). Így e számok legfeljebb $\sqrt{n}$-féleképpen választhatók, tehát a párok száma is legfeljebb ennyi. $d(n)$ pedig — mint mondtuk — legfeljebb akkora, mint e párok számának kétszerese, tehát legfeljebb $2\sqrt{n}$, és ezzel az állítást igazoltuk.

22. Határozzuk meg az $a=5^2 \cdot 6^3 \cdot 11^4 \cdot 21^5$ és $b=7^2 \cdot 9^3 \cdot 10^4 \cdot 13^5$ számok legnagyobb közös osztóját, ill. legkisebb közös többszörösét!

Megoldás:
Határozzuk meg először a és b kanonikus alakját:

$$a = 5^2 \cdot 6^3 \cdot 11^4 \cdot 21^5 = 5^2 \cdot (2 \cdot 3)^3 \cdot 11^4 \cdot (3 \cdot 7)^5 =$$

$$= 5^2 \cdot 2^3 \cdot 3^3 \cdot 11^4 \cdot 3^5 \cdot 7^5 = 2^3 \cdot 3^8 \cdot 5^2 \cdot 7^5 \cdot 11^4$$

és

$$b = 7^2 \cdot 9^3 \cdot 10^4 \cdot 13^5 = 7^2 \cdot (3^2)^3 \cdot (2 \cdot 5)^4 \cdot 13^5 =$$

$$= 7^2 \cdot 3^6 \cdot 2^4 \cdot 5^4 \cdot 13^5 = 2^4 \cdot 3^6 \cdot 5^4 \cdot 7^2 \cdot 13^5.$$

Így

$$(a, b) = (2^3 \cdot 3^8 \cdot 5^2 \cdot 7^5 \cdot 11^4,\ 2^4 \cdot 3^6 \cdot 5^4 \cdot 7^2 \cdot 13^5) = 2^3 \cdot 3^6 \cdot 5^2 \cdot 7^2$$

és

$$[a, b] = [2^3 \cdot 3^8 \cdot 5^2 \cdot 7^5 \cdot 11^4,\ 2^4 \cdot 3^6 \cdot 5^4 \cdot 7^2 \cdot 13^5] = 2^4 \cdot 3^8 \cdot 5^4 \cdot 7^5 \cdot 11^4 \cdot 13^5.$$

FELADATOK

1. Számítsuk ki

a. $\frac{25}{4}$,

b. $-3{,}2$

egész részét és tört részét!

2. Legyen a tetszőleges valós szám, n természetes szám. Bizonyítsuk be, hogy

$$\left[\frac{[a]}{n}\right] = \left[\frac{a}{n}\right].$$

3. Legyenek $a_1, a_2, \ldots, a_k, b$ tetszőleges valós számok, melyekre

$$a_1 + a_2 + \ldots + a_k \leqq b.$$

Bizonyítsuk be, hogy ekkor

$$[a_1] + [a_2] + \ldots + [a_k] \leqq [b].$$

4. Legyen a tetszőleges valós szám, n tetszőleges természetes szám. Bizonyítsuk be, hogy

$$[a] + \left[a + \frac{1}{n}\right] + \left[a + \frac{2}{n}\right] + \ldots + \left[a + \frac{n-1}{n}\right] = [na].$$

5. Írjuk fel a $\overset{7}{\smile}{30514}$ számot 9 alapú számrendszerben!

6. Milyen x természetes számra teljesül az

a. $\overset{x}{\smile}{231} = 190$,

b. $\overset{x}{\smile}{1182} = 884$

egyenlőség?

7. Bizonyítsuk be, hogy minden számrendszerben az alapot megelőző szám kétszerese és négyzete ugyanazokkal a számjegyekkel írható, csupán a számjegyek sorrendje fordított!

8. Egy háromjegyű szám a tízes számrendszerben $\overset{10}{\overset{\smile}{aaa}}$ alakú. Ugyanazon szám számjegyei egy másik számrendszerben sorrendben $4a$, $2a$, a. Melyik ez a szám, és mennyi a másik számrendszer alapszáma?

9. Bizonyítsuk be, hogy az

$$a = 123456\overset{16}{\overset{\smile}{789}}ABCDEF$$

szám osztható 15-tel! (Az $A, B, \ldots, F$ betűk a 10, 11, ..., 15 számjegyeket jelölik.)

10. Bizonyítsuk be, hogy $m > n$ esetén az

$$123\ldots(n-1)\overset{m}{\overset{\smile}{n}}(n-1)\ldots 321$$

szám teljes négyzet!

11. Valamely x természetes számra $4\overset{x}{\overset{\smile}{465}}$-öt $6\overset{x}{\overset{\smile}{92}}$-vel osztva, a hányados 7, a maradék $5\overset{x}{\overset{\smile}{23}}$. Határozzuk meg x értékét!

12. Bizonyítsuk be, hogy egy pozitív egész szám a tízes számrendszerben akkor és csak akkor osztható 8-cal, ha az utolsó három számjegye által alkotott háromjegyű szám osztható 8-cal!

13. Bizonyítsuk be, hogy egy (tízes számrendszerben felírt) pozitív egész szám akkor és csak akkor osztható 9-cel, ha a számjegyeinek összege osztható 9-cel!

14. Bizonyítsuk be, hogy egy (tízes számrendszerben felírt) pozitív egész szám akkor és csak akkor osztható 11-gyel, ha a páratlan sorszámú helyeken álló számjegyek összegéből kivonva a páros sorszámú helyeken álló számjegyek összegét, 11-gyel osztható számot kapunk!

15. Bizonyítsuk be a 7-tel való oszthatóságra vonatkozó következő szabályt: vonjuk ki az adott szám utolsó jegyének elhagyásával keletkező (eggyel kevesebb jegyű) számból az elhagyott számjegy 9-szeresét. Akkor a kapott szám akkor és csak akkor osztható 7-tel, ha az adott szám is osztható volt

7-tel. Alkalmazzuk ezt az eljárást annak eldöntésére, hogy a 32968 szám osztható-e 7-tel?

16. Igazoljuk az oszthatóság *B)* tulajdonságát (az oszthatóság tranzitivitását)!

17. Bizonyítsuk be, hogy ha az a, b, c, d egész számokra $a|c$ és $b|d$ teljesül, akkor szükségképpen $ab|cd$ is fennáll!

18. Bizonyítsuk be, hogy ha az m, n, a, b egész számokra $(m-n)|(am+nb)$ teljesül, akkor szükségképpen $(m-n)|(bm+an)$ is fennáll!

19. Bizonyítsuk be, hogy az $m=\overset{10}{\smile}{abc}$ szám akkor és csak akkor osztható 27-tel vagy 37-tel, ha az $n=\overset{10}{\smile}{bca}$ szám is!

20. Bizonyítsuk be, hogy páratlan szám négyzete 8-cal osztva 1 maradékot ad!

21. Bizonyítsuk be, hogy $(n^2+3n+1)^2-1$ osztható 24-gyel (n tetszőleges egész szám)!

22. Bizonyítsuk be, hogy n^5-5n^3+4n osztható 120-szal (n tetszőleges egész szám)!

23. Bizonyítsuk be, hogy ha n páratlan szám, akkor n^4-18n^2+17 osztható 64-gyel!

24. Bizonyítsuk be, hogy $n(n^2+5)$ osztható 6-tal, ha n tetszőleges természetes szám!

25. Bizonyítsuk be, hogy ha n egész szám, akkor $\frac{n}{6}+\frac{n^2}{2}+\frac{n^3}{3}$ szintén egész szám!

26. Keressük meg mindazokat az n egész számokat, melyekre n^2+2 osztható $n+1$-gyel!

27. Bizonyítsuk be, hogy ha n egész szám, akkor n^2+n+4 *nem osztható* 9-cel!

28. Bizonyítsuk be, hogy három egymás után következő egész szám köbének összege osztható

a. a középső szám 3-szorosával,

b. 9-cel!

29. Bizonyítsuk be, hogy $4^{90}+1$ osztható 17-tel!

30. Bizonyítsuk be, hogy $333^{444}+444^{333}$ osztható 7-tel!

31. Bizonyítsuk be, hogy $3^{3n+2}+4$ osztható 13-mal (n tetszőleges nemnegatív egész szám)!

32. Határozzuk meg mindazokat az n természetes számokat, melyekre 2^n+1 osztható 3-mal!

33. Bizonyítsuk be, hogy $2^{2n}-3n-1$ osztható 9-cel (n tetszőleges nemnegatív egész szám)!

34. Bizonyítsuk be, hogy bármely két egész számnak a 2. módon definiált legnagyobb közös osztója lényegében (előjeltől eltekintve) egyértelmű!

35*. Igazoljuk, hogy az euklideszi algoritmus által szolgáltatott utolsó, 0-tól különböző maradék a két szám legnagyobb közös osztója!

36*. Igazoljuk a legnagyobb közös osztó *C)* tulajdonságát!

37. Számítsuk ki az euklideszi algoritmus, majd a módosított euklideszi algoritmus segítségével 861 és 567 legnagyobb közös osztóját, és írjuk fel azt a két szám lineáris kombinációjaként! Határozzuk meg továbbá e két szám legkisebb közös többszörösét!

38. Számítsuk ki euklideszi algoritmus segítségével 1232, 1008 és 819 legnagyobb közös osztóját!

39*. Igazoljuk a legnagyobb közös osztó *D)* tulajdonságát!

40*. Igazoljuk a legnagyobb közös osztó *E)* tulajdonságát!

41*. Igazoljuk a 4. pont *F)* állítását!

42*. Igazoljuk a 4. pont *G)* állítását!

43. Határozzuk meg az alábbi legnagyobb közös osztókat (a, b tetszőleges egész számok):

a. $(a, 1)$, (a, a), $(a, 0)$;

b. $(a, 3a+1)$;

c. $(9a+4b, 11a+5b)$.

44. Legyenek a, b egész számok, melyekre $a|b$. Határozzuk meg az alábbi legnagyobb közös osztókat:

a. $(b, a+b)$;

b. $(b, 2a-3b)$;

c. $(11a+5b, 24a+11b)$.

45*. Bizonyítsuk be, hogy tetszőleges n természetes számra

$$(n!+1, (n+1)!+1) = 1.$$

46. Bizonyítsuk be, hogy tetszőleges n egész számra

$$(n^3+3n^2+5n+3,\ n^2+2n+2) = 1.$$

47*. Bizonyítsuk be, hogy ha m páratlan természetes szám, n tetszőleges természetes szám, akkor

$$(2^m-1,\ 2^n+1) = 1.$$

48*. Legyen $a_0=2^{2^0}+1\ (=3)$, $a_1=2^{2^1}+1\ (=5)$, ..., $a_k=$ $=2^{2^k}+1$, ... Az így definiált számokat *Fermat-számoknak*, az ilyen alakú prímszámokat *Fermat-prímeknek* nevezzük.

Fermat ugyanis azt sejtette, hogy az ilyen alakú számok mind prímszámok. Ezt a sejtést azóta megcáfolták. Igazolható ugyanis, hogy például $641|2^{2^5}+1$. Nem ismeretes azonban, hogy a Fermat-számok közt van-e végtelen sok prímszám, ill. összetett szám. A Fermat-számokra vonatkozóan l. még alább a 62. és 63. feladatokat, valamint a II. fejezet 62*. és 74. feladatát.

Bizonyítsuk be, hogy a Fermat-számok páronként relatív prímek!

49. Bizonyítsuk be, hogy

a. négy,

b. hat

egymást követő természetes szám közül mindig kiválasztható egy úgy, hogy az összes többihez relatív prím legyen!

50*. Legyen k tetszőleges természetes szám, m, n egész számok, melyekre $(m, n)=1$. Bizonyítsuk be, hogy

$$(m, n^k)=1!$$

51*. Legyenek a, b egész számok, k természetes szám. Bizonyítsuk be, hogy $(a^k, b^k)=(a, b)^k$!

52. Bizonyítsuk be, hogy ha az a, b egész számokra $(a, b)=1$ teljesül, akkor

$$(a^3-b^3,\ a^2-b^2) = a-b.$$

53. Határozzuk meg a

$$98x-77y = 14$$

lineáris diofantikus egyenlet összes egész megoldásait!

54. Bontsuk fel 463-at két természetes szám összegére úgy, hogy az egyik szám osztható legyen 14-gyel, a másik 23-mal!

55. Bizonyítsuk be, hogy az

$$(5a+4)x-(9a+7)y = b$$

lineáris diofantikus egyenlet tetszőleges a, b egész számokra megoldható!

56. Bizonyítsuk be, hogy ha az a, b, n pozitív egész számokra $(a, b)=1$ és $n>ab$ teljesül, akkor az

$$ax+by = n$$

lineáris diofantikus egyenletnek van *pozitív* egész számokból álló x, y megoldása!

57. Határozzuk meg a

$$273x+210y-165z = 18$$

lineáris diofantikus egyenlet *egy* megoldását!

58. Határozzuk meg mindazon p prímszámokat, melyekre $2p-1$ és $2p+1$ is prímszám!

59. Mely p prímszámokra teljesül, hogy p^2+2 is prímszám?

60. Milyen n egész számokra prímszám n^4+4?

61. *a.* Bizonyítsuk be, hogy ha 2^n-1 (az n természetes szám) prímszám, akkor n is prímszám!

b. Keressünk 2^p-1 (p prímszám) alakú összetett számot!

(A 2^p-1 alakú prímszámokat *Mersenne-féle prímszámoknak* nevezzük; nem ismeretes, hogy létezik-e végtelen sok ilyen.)

62. Bizonyítsuk be, hogy ha valamely k természetes számra 2^k+1 prímszám, akkor $k=2^n$, ahol n nemnegatív egész szám! (L. a 48. feladatot.)

63. Bizonyítsuk be a 48. feladat felhasználásával, hogy végtelen sok prímszám létezik! Bizonyítsuk be továbbá, hogy az

n-edik prímszámot p_n-nel jelölve (tehát $p_1=2, p_2=3, p_3=5, \ldots$),

(22) $p_n < 2^{2^n}$ $(n=1, 2, \ldots)$.

64. Bizonyítsuk be, hogy ha egy p egész szám prímszám a *B)* értelemben, akkor az *A)* értelemben is az!

65. Állapítsuk meg, hogy

a. 437,

b. 457

prímszám-e?

66. Határozzuk meg 5271 kanonikus alakját!

67. Bizonyítsuk be, hogy ha

$$ab = k^n$$

(a, b, k és n természetes számok) és $(a, b)=1$, akkor a és b is természetes számok n-edik hatványai!

68. Egy q egész számot négyzetmentesnek nevezünk, ha nem létezik olyan 1-nél nagyobb a egész szám, melyre $a^2|q$ teljesül. Bizonyítsuk be, hogy minden n természetes szám egyértelműen felírható $n=k^2q$ alakban, ahol k természetes szám, q pedig négyzetmentes szám!

69. Legyen $n>1$ tetszőleges természetes szám. Bizonyítsuk be, hogy

$$1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{n}$$

nem egész szám!

70. Írjuk fel 84 pozitív osztóit!

71. Határozzuk meg $6^5 \cdot 10^4 \cdot 14^3 \cdot 15^2$ pozitív osztóinak a számát!

72. Állapítsuk meg, hogy az $n=2^5 \cdot 3^4 \cdot 5^3 \cdot 7^2$ számnak hány olyan pozitív osztója van, mely nem osztható 28-cal?

73. Keressük meg azt a legkisebb n természetes számot, melyre $d(n)=9$.

74. Állapítsuk meg, hogy mi a szükséges és elégséges feltétele annak, hogy $d(n)$ páratlan legyen?

75. Számítsuk ki az

a. 180,

b. 900

szám pozitív osztóinak a szorzatát!

76. Bizonyítsuk be, hogy végtelen sok n természetes számra

$$d(n+1) \geqq 2d(n).$$

77. Bizonyítsuk be, hogy létezik olyan n_0 szám, hogy $n \geqq n_0$ esetén

$$d(n) \leqq n-5,$$

és keressük meg a legkisebb ilyen n_0 természetes számot!

78. Bizonyítsuk be, hogy tetszőleges n természetes számra

$$d(n) \leqq \frac{n}{3}+2.$$

79. Bizonyítsuk be, hogy létezik olyan c pozitív állandó, hogy végtelen sok n egész számra

$$d(n) > c \log n.$$

80*. Bizonyítsuk be, hogy tetszőleges k természetes számot megadva, létezik végtelen sok n természetes szám, melyre

$$d(n) > (\log n)^k.$$

AZ I. FEJEZETBEN KITŰZÖTT FELADATOK MEGOLDÁSAI

1.

a. $\frac{25}{4} = 6 + \frac{1}{4}$.

Így

$$\left[\frac{25}{4}\right] = 6 \quad \text{és} \quad \left\{\frac{25}{4}\right\} = \frac{1}{4}.$$

b. $-3{,}2 = -4 + 0{,}8$.

Így

$$[-3{,}2] = -4 \quad \text{és} \quad \{-3{,}2\} = 0{,}8.$$

2. Az $[x]$ függvény monotonitása miatt

$$\left[\frac{[a]}{n}\right] \leqq \left[\frac{a}{n}\right]. \tag{23}$$

Másrészt az $[x]$ függvény definíciója szerint

$$x < [x] + 1. \tag{24}$$

Írjuk itt x helyére $\frac{[a]}{n}$-et:

$$\frac{[a]}{n} < \left[\frac{[a]}{n}\right] + 1.$$

Mindkét oldalt n-nel szorozva:

$$[a] < n\left[\frac{[a]}{n}\right] + n.$$

Itt mindkét oldalon egész szám áll, tehát innen következik, hogy

$$[a] + 1 \leqq n\left[\frac{[a]}{n}\right] + n. \tag{25}$$

Másrészt (24) szerint

(26) $a < [a]+1.$

(25)-ből és (26)-ból adódik, hogy

$$a < n\left[\frac{[a]}{n}\right]+n.$$

Mindkét oldalt n-nel osztva:

(27) $$\frac{a}{n} < \left[\frac{[a]}{n}\right]+1.$$

Az $[x]$ függvény definíciójára tekintettel

(28) $$\left[\frac{a}{n}\right] \leqq \frac{a}{n}.$$

(27)-ből és (28)-ból nyerjük, hogy

$$\left[\frac{a}{n}\right] < \left[\frac{[a]}{n}\right]+1.$$

Mivel mindkét oldalon egész szám áll, innen következik, hogy

(29) $$\left[\frac{a}{n}\right] \leqq \left(\left[\frac{[a]}{n}\right]+1\right)-1 = \left[\frac{[a]}{n}\right].$$

(23) és (29) együtt adja a bizonyítandó állítást.

3. Ismételten alkalmazva a (2) egyenlőtlenség első felét:

(30) $$\begin{aligned}[a_1+a_2+\ldots+a_k] &= [a_1+(a_2+\ldots+a_k)] \geqq \\ &\geqq [a_1]+[a_2+\ldots+a_k] = [a_1]+[a_2+(a_3+\ldots+a_k)] \geqq \\ &\geqq [a_1]+[a_2]+[a_3+\ldots+a_k] \geqq \ldots \geqq \\ &\geqq [a_1]+[a_2]+\ldots+[a_{k-2}]+[a_{k-1}+a_k] \geqq \\ &\geqq [a_1]+[a_2]+\ldots+[a_{k-2}]+[a_{k-1}]+[a_k].\end{aligned}$$

Másrészt az $[x]$ függvény monotnitására tekintettel az $a_1+a_2+\ldots+a_k \leqq b$ feltételből következik, hogy

(31) $[a_1+a_2+\ldots+a_k] \leqq [b].$

(30)-ból és (31)-ből adódik a bizonyítandó egyenlőtlenség.

4. Legyen

(32) $[na] = qn+r,$

ahol q, r egész számok, és

(33) $0 \leqq r \leqq n-1.$

Legyen továbbá a rövidség kedvéért

$$\{na\} = \Theta;$$

ekkor az $\{x\}$ függvény definíciója szerint

(34) $0 \leqq \Theta < 1.$

A fenti jelöléseket bevezetve, na a következő alakban írható:

(35) $na = [na] + \{na\} = qn + r + \Theta,$

vagy mindkét oldalt n-nel osztva:

$$a = q + \frac{r}{n} + \frac{\Theta}{n}.$$

Ha most $i = 0, 1, 2, \ldots, n-r-1$, akkor (33)-ra, (34)-re és (35)-re tekintettel

(36) $$a + \frac{i}{n} = q + \frac{r}{n} + \frac{\Theta}{n} + \frac{i}{n} = q + \frac{(r+i)+\Theta}{n} \leqq$$

$$\leqq q + \frac{(n-1)+\Theta}{n} < q + \frac{(n-1)+1}{n} = q+1,$$

másrészt

(37) $a + \frac{i}{n} \geqq a \geqq q.$

Mivel q egész szám, az $[x]$ függvény definíciójára tekintettel (36)-ból és (37)-ből következik, hogy az ilyen i-kre

$$\left[a + \frac{i}{n}\right] = q.$$

A bizonyítandó összefüggés bal oldalán álló első $n-r$ tag értéke tehát q.

Ha viszont $i = n-r, n-r+1, \ldots, n-1$, akkor (33)-ból, (34)-ből és (35)-ből hasonlóan nyerjük, hogy

(38) $$a + \frac{i}{n} = \left(q + \frac{r}{n} + \frac{\Theta}{n}\right) + \frac{i}{n} = q + \frac{(r+i)+\Theta}{n} \geqq$$

$$\geqq q + \frac{n+0}{n} \geqq q+1,$$

másrészt

$$(39)\quad a+\frac{i}{n}=\left(q+\frac{r}{n}+\frac{\Theta}{n}\right)+\frac{i}{n}<q+\frac{n-1}{n}+\frac{1}{n}+\frac{n-1}{n}=$$

$$=q+\frac{2n-1}{n}<q+2.$$

Mivel q egész szám, (38)-ból és (39)-ből következik, hogy az ilyen i-kre (melyek száma r)

$$\left[a+\frac{i}{n}\right]=q+1.$$

Végeredményben tehát a vizsgált összefüggés bal oldala:

$$(n-r)\cdot q+r\cdot(q+1)=nq-rq+rq+r=nq+r,$$

ami (32) szerint egyezik a jobb oldallal.

5. Először áttérünk a 10-es számrendszerre:

$$30\overset{7}{\breve{5}}14=\{[(3\cdot 7+0)7+5]7+1\}7+4=[(21\cdot 7+5)7+1]7+4=$$

$$=[(147+5)7+1]7+4=(152\cdot 7+1)7+4=(1064+1)7+4=$$

$$=1065\cdot 7+4=7455+4=7459.$$

Most meghatározzuk a szám 9-es számrendszerbeli alakját:

$$\begin{array}{l} \underline{7459}:9=828, \\ \underline{25} \\ \underline{79} \\ 7 \end{array} \qquad \begin{array}{l} \underline{828}:9=92, \\ \underline{18} \\ 0 \end{array} \qquad \begin{array}{l} \underline{92}:9=10, \\ \underline{2} \\ 2 \end{array} \qquad \begin{array}{l} \underline{10}:9=1. \\ 1 \end{array}$$

Így $\quad 30\overset{7}{\breve{5}}14=11\overset{9}{\breve{2}}07.$

6. *a.* Részletezve az adott feltételt:

$$2x^2+3x+1=190,$$

vagyis

$$2x^2+3x-189=0.$$

Innen

$$x_{1,2}=\frac{-3\pm\sqrt{9+8\cdot 189}}{4}=\frac{-3\pm\sqrt{1521}}{4}=\frac{-3\pm 39}{4},$$

tehát az egyetlen pozitív gyök $x=9$.

b. Ha úgy járnánk el, mint az *a.* feladat megoldása során, x-re harmadfokú egyenletet kellene megoldanunk; gyorsabban célhoz érhetünk azonban más módszerrel.

Ugyanis $\overset{x}{\smile}{1182}$ számjegyei közül a legnagyobb 8, tehát az alapszámnak ennél nagyobbnak kell lennie:

(40) $x \geqq 9.$

Másrészt ha $x \geqq 10$ lenne, akkor

$$\overset{x}{\smile}{1182} = 1\cdot x^3+1\cdot x^2+8\cdot x+2 \geqq 1\cdot 10^3+1\cdot 10^2+8\cdot 10+2 =$$

$$= 1182 > 884$$

teljesülne, ellentétben az adott $\overset{x}{\smile}{1182}=884$ feltétellel. Így szükségképpen csak

(41) $x \leqq 9$

lehetséges. (40)-et és (41)-et egybevetve, nyerjük, hogy az egyetlen lehetséges megoldás $x=9$. Valóban, ekkor

$$\overset{x}{\smile}{1182} = \overset{9}{\smile}{1182} = [(1\cdot 9+1)9+8]9+2 = (10\cdot 9+8)9+2 =$$

$$= 98\cdot 9+2 = 882+2 = 884,$$

tehát $x=9$ megoldása a feladatnak.

7. Jelöljük az alapszámot n-nel. Ekkor az alapot megelőző szám kétszerese:

(42) $2(n-1) = 2n-2 = 1\cdot n+(n-2) = 1\overset{n}{\smile}{(n-2)}.$

Az alapot megelőző szám négyzete:

(43) $(n-1)^2 = n^2-2n+1 = (n-2)n+1 = (n-\overset{n}{\smile}{2})1.$

(42) és (43) adja a feladat állítását.

8. A másik számrendszer alapszámát x-szel jelölve, a feladat feltételei szerint

$$\overset{10}{\smile}{aaa} = (4a)\overset{x}{\smile}{(2a)}a,$$

vagyis

$$100a+10a+a = 4a\cdot x^2+2a\cdot x+a.$$

Átrendezve:

$$4ax^2+2ax-110a = 0.$$

Minthogy nyilván $a \neq 0$, oszthatjuk mindkét oldalt $2a$-val:

$$2x^2 + x - 55 = 0.$$

Innen

$$x_{1,2} = \frac{-1 \pm \sqrt{1 + 4 \cdot 2 \cdot 55}}{4} = \frac{-1 \pm \sqrt{441}}{4} = \frac{-1 \pm 21}{4}.$$

Így az egyetlen pozitív gyök:

$$x = \frac{-1 + 21}{4} = 5.$$

A másik számrendszer alapszáma tehát 5. Minthogy egy 5 alapú számrendszerben felírt szám legnagyobb számjegye nem lehet nagyobb 4-nél, szükségképpen a $(4a)\overset{x}{(2a)}a$ legnagyobb számjegye, $4a$ sem lehet nagyobb 4-nél: $4a \leqq 4$. Innen következik, hogy a egyetlen lehetséges értéke: $a = 1$. Végeredményben tehát az adott háromjegyű szám $\overset{10}{aaa} = 111$, és a másik számrendszer alapszáma 5.

9. $$123456789\overset{16}{A}BCDEF =$$

$$= \sum_{i=1}^{15} i \cdot 16^{15-i} = \sum_{i=1}^{15} i(16^{15-i} - 1) + \sum_{i=1}^{15} i =$$

$$= \sum_{i=1}^{15} i(16^{15-i} - 1) + \frac{15 \cdot 16}{2} = \sum_{i=1}^{15} i(16^{15-i} - 1) + 15 \cdot 8.$$

A (7) összefüggésre tekintettel a $16^{15-i} - 1$ tényezők mindegyike osztható $16 - 1 = 15$-tel. Minthogy az utolsó tag, $15 \cdot 8$ is osztható 15-tel, az oszthatóság *G)* tulajdonsága értelmében az egész összeg, vagyis a is osztható 15-tel.

10. $$123\ldots(n-1)\overset{m}{n}(n-1)\ldots321 =$$

$$= 1 \cdot m^{2n-2} + 2 \cdot m^{2n-3} + 3 \cdot m^{2n-4} \ldots + (n-1)m^n + n \cdot m^{n-1} +$$

$$+ (n-1)m^{n-2} + \ldots + 3m^2 + 2m + 1 =$$

$$= (m^{2n-2} + m^{2n-3} + \ldots + m^n + m^{n-1}) + (m^{2n-3} + m^{2n-4} +$$

$$+ \ldots + m^{n-1} + m^{n-2}) + \ldots + (m^{n-1} + m^{n-2} + \ldots + m + 1) =$$

$$= m^{n-1}(m^{n-1} + m^{n-2} + \ldots + m + 1) + m^{n-2}(m^{n-2} + m^{n-2} + \ldots +$$

$$+ m + 1) + \ldots + (m^{n-1} + m^{n-2} + \ldots + m + 1) =$$

$$= (m^{n-1} + m^{n-2} + \ldots + m + 1)(m^{n-1} + m^{n-2} + \ldots + m + 1) =$$

$$= (m^{n-1}+m^{n-2}+\ldots+m+1)^2 = (\overset{m}{\smile}11\ldots11)^2,$$

ahol a jegyek (1-esek) száma n.

11. A feltételek szerint

$$4\overset{x}{\smile}55 = 7\cdot\overset{x}{\smile}92+5\overset{x}{\smile}23,$$

vagyis

$$(44)\qquad 4x^3+4x^2+6x+5 = 7(6x^2+9x+2)+(5x^2+2x+3).$$

Összevonva és átrendezve:

$$4x^3-43x^2-59x = 12.$$

A bal oldalon x-et kiemelve:

$$x(4x^2-43x-59) = 12.$$

Innen következik, hogy $x|12$. Másrészt a $6\overset{x}{\smile}92$ hányadosban szerepel a 9-es számjegy, tehát szükségképpen $x\geqq 10$. A 12-nek azonban nyilván csak egyetlen olyan x osztója van, mely az $x\geqq 10$ feltételt is kielégíti, nevezetesen $x=12$; így x egyetlen lehetséges értéke $x=12$. (44)-be helyettesítve, ellenőrizhető, hogy ez az x érték valóban megoldás.

12. $n = a_0a_1\ldots\overset{10}{\smile}a_{k-2}a_{k-1}a_k =$

$$= a_0 10^k+a_1 10^{k-1}+\ldots+a_{k-3}10^3+a_{k-2}10^2+a_{k-1}10+a_k =$$

$$= 10^3(a_0 10^{k-3}+a_1 10^{k-4}+\ldots+a_{k-3})+(a_{k-2}10^2+a_{k-1}10+a_k) =$$

$$= 8\cdot 125(a_0 10^{k-3}+a_1 10^{k-4}+\ldots+a_{k-3})+a_{k-2}\overset{10}{\smile}a_{k-1}a_k.$$

Mivel ennek az összegnek az első tagja osztható 8-cal, az összeg, vagyis n akkor és csak akkor osztható 8-cal (az osztathatóság G) tulajdonsága szerint), ha a második tag is osztható 8-cal.

13. $a_0a_1\ldots\overset{10}{\smile}a_{k-1}a_k = a_0 10^k+a_1 10^{k-1}+\ldots+a_{k-1}10+a_k =$

$$= a_0(10^k-1)+a_1(10^{k-1}-1)+\ldots+a_{k-1}(10-1)+a_k(1-1)+$$

$$+(a_0+a_1+\ldots+a_{k-1}+a_k).$$

A (7) összefüggés szerint ennek az összegnek az első $k+1$ tagja osztható $10-1=9$-cel, tehát az egész összeg, vagyis az adott szám akkor és csak akkor osztható 9-cel, ha az utolsó tag, vagyis a számjegyek összege is osztható 9-cel.

14. $a_0 a_1 \ldots \overset{10}{\smile} a_{k-2} a_{k-1} a_k =$

$$= a_0 10^k + a_1 10^{k-1} + \ldots + a_{k-2} 10^2 + a_{k-1} 10 + a_k =$$

$$= a_0[10^k + (-1)^{k+1}] + a_1[10^{k-1} + (-1)^k] + \ldots + a_{k-2}(10^2 - 1) +$$

$$+ a_{k-1}(10 + 1 + a_k(1-1) + (-1)^{k+1}[a_0 - a_1 + a_2 -$$

$$\ldots + (-1)^{k-2} a_{k-2} + (-1)^{k-1} a_{k-1} + (-1)^k a_k].$$

Ennek az összegnek az első $k+1$ tagja osztható 11-gyel, nevezetesen a $10^{2l}-1$ alakú tagok a (8), míg a $10^{2l+1}+1$ alakúak a (9) összefüggés alapján. Így az egész összeg, vagyis az adott szám akkor és csak akkor osztható 11-gyel, ha az utolsó tag is osztható 11-gyel, és ezt kellett igazolnunk.

15. Legyen az adott szám $n=10a+b$. Azt kell bizonyítanunk, hogy $7|n$ akkor és csak akkor teljesül, ha $7|m=a-9b$. Azonban

$$n=3m = (10a+b)-3(a-9b) = 7a+28b = 7(a+4b)$$

osztható 7-tel, tehát n akkor és csak akkor osztható 7-tel, ha $3m$ is osztható 7-tel. $(3,7)=1$-re tekintettel viszont $3m$ akkor és csak akkor osztható 7-tel, ha m is osztható 7-tel, és ezzel az állítást igazoltuk. Annak vizsgálata céljából, hogy 32 968 osztható-e 7-tel, alkalmazzuk ismételten a leírt redukciós szabályt:

$$3296-9\cdot 8 = 3224, \quad 322-9\cdot 4 = 286, \quad 28-9\cdot 6 = -26,$$

ami nem osztható 7-tel, tehát a vizsgált szám sem osztható 7-tel.

16. Ha $a|b$ és $b|c$, akkor léteznek olyan d,e egész számok, melyekre $b=ad$ és $c=be$. Ekkor

$$c = be = (ad)e = a(de),$$

tehát c felírható úgy, mint a-nak egészszámszorosa, és így $a|c$.

17. Ha $a|c$ és $b|d$, akkor léteznek olyan m, n egész számok, melyekre $c=am$ és $d=bn$. Ekkor

$$cd = (am)\cdot(bn) = (ab)\cdot(mn),$$

tehát cd felírható úgy, mint ab-nek és egy egész számnak a szorzata, és így $ab|cd$.

18. Az állítás leolvasható a

$$bm+an = (bm-am-bn+an)+(am+bn) =$$

$$= [m(b-a)-n(b-a)]+(am+bn) = (m-n)(b-a)+(am+bn)$$

azonos átalakításból.

19. Induljunk ki a következő összefüggésből:

$$10m-n = 10(100a+10b+c)-(100b+10c+a) = 999a = 27\cdot 37a.$$

Innen következik, hogy n akkor és csak akkor osztható 27-tel, ill. 37-tel, ha $10m$ is osztható 27-tel, ill. 37-tel. Azonban mivel $(10,27)=(10,37)=1$, ezért $10m$-nek 27-tel, ill. 37-tel való oszthatósága ekvivalens m-nek 27-tel, ill. 37-tel való oszthatóságával. Ezzel az állítást igazoltuk.

20. Azt kell bizonyítanunk, hogy tetszőleges k egész számra

$$(2k+1)^2-1 = (4k^2+4k+1)-1 = 4k^2+4k = 4k(k+1)$$

osztható 8-cal. Ez következik abból, hogy k és $k+1$ valamelyike páros, tehát a kapott szorzat osztható $4\cdot 2=8$-cal.

21. Az $a^2-b^2=(a-b)(a+b)$ azonosság alapján:

$$(n^2+3n+1)^2-1 = [(n^2+3n+1)-1][(n^2+3n+1)+1] =$$

$$= (n^2+3n)(n^2+3n+2) = n(n+3)(n+1)(n+2) =$$

$$= n(n+1)(n+2)(n+3).$$

Itt négy egymást követő szám szorzata áll, tehát a tényezők valamelyike osztható 3-mal. Másrészt a tényezők valamelyike osztható 4-gyel, és található egy ettől különböző páros tényező is, tehát a szorzat osztható $4\cdot 2=8$-cal is. Mivel 3 és 8 egymáshoz relatív prímek, a vizsgált kifejezés osztható ezek szorzatával, $3\cdot 8=24$-gyel is. (L. a 4. pontban a *G)* állítást.)

22. $n^5-5n^3+4n = n(n^4-5n^2+4) = n(n^2-1)(n^2-4) =$

$$= n(n-1)(n+1)(n-2)(n+2) = (n-2)(n-1)n(n+1)(n+2).$$

Itt öt egymást követő szám szorzata áll, tehát a szorzat osztható 5-tel. Másrészt az előző feladat megoldása során mondottak szerint a szorzat osztható 3-mal és 8-cal is. Mivel 3, 5 és 8 páronként relatív prímek, a szorzat osztható $3\cdot 5\cdot 8=120$-szal is.

23. $n^4-18n^2+17 = (n^2-1)(n^2-17) = (n^2-1)[(n^2-1)-16].$

Az előző feladat értelmében itt mindkét tényező osztható 8-cal, tehát a szorzat osztható $8\cdot 8=64$-gyel.

24. $n(n^2+5) = n[(n^2-1)+6] = n(n^2-1)+6n = (n-1)n(n+1)+6.$

Az első tag három egymást követő szám szorzata, tehát osztható 2-vel és 3-mal is, és így — $(2,3)=1$ miatt — $2\cdot 3=6$-tal is. Innen következik az állítás.

25. Közös nevezőre hozva:

$$\frac{n}{6}+\frac{n^2}{2}+\frac{n^3}{3} = \frac{2n^3+3n^2+n}{6}. \tag{45}$$

Azt kell tehát bizonyítanunk, hogy

$$6|2n^3+3n^2+n = (2n^3-2n)+(3n^2+3n) =$$

$$= 2(n^3-n)+3(n^2+n) = 2(n-1)n(n+1)+3n(n+1).$$

Az első tagban három egymást követő szám szorzata áll, tehát az előző feladat megoldása során mondottak szerint osztható 6-tal. A második tagban álló $n(n+1)$ szorzat osztható 2-vel (hiszen egyik tényezője páros); így ez a tag is osztható $3 \cdot 2 = 6$-tal. Minthogy mindkét tag osztható 6-tal, összegük, a (45) jobb oldalán álló tört számlálója is osztható 6-tal.

26. $n^2+2 = (n^2-1)+3 = (n-1)(n+1)+3.$

Így ez a szám akkor és csak akkor osztható $n+1$-gyel, ha a második tag, 3 is osztható $n+1$-gyel. Azonban 3 összes osztói ± 1, ± 3, tehát $n+1$-nek ezek közül kell kikerülnie:

$$n+1 = -3, \quad n+1 = -1, \quad n+1 = +1 \quad \text{vagy} \quad n+1 = +3.$$

Ezeket az egyenleteket n-re megoldva, nyerjük, hogy n lehetséges értékei: $n = -4, -2, 0$ és 2.

27. $n^2+n+4 = (n^2+n-2)+6 = (n-1)(n+2)+6 =$

$$= (n-1)[(n-1)+3]+6.$$

Tegyük fel, hogy az állítással ellentétben ez a szám osztható 9-cel; ekkor szükségképpen osztható 3-mal is. Minthogy a második tag osztható 3-mal, az első tagnak is oszthatónak kell lennie 3-mal. Ekkor az első tag valamelyik tényezője is osztható 3-mal (hiszen a 3 prímszám). Ha azonban e tag egyik tényezője osztható 3-mal, akkor nyilván a másik is; így az első tag osztható $3 \cdot 3 = 9$-cel. Így a kapott összeg és annak első tagja is osztható 9-cel, tehát a második tagnak, 6-nak is oszthatónak kell lennie 9-cel. Azonban nyilván $9 \nmid 6$, tehát az indirekt feltevésből ellentmondásra jutottunk.

28. *a.* A középső számot n-nel jelölve, a vizsgált összeg:

$$(n-1)^3+n^3+(n+1)^3 = (n^3-3n^2+3n-1)+n^3+(n^3+3n^2+3n+1) =$$

$$= 3n^3+6n = 3n(n^2+2),$$

ahonnan azonnal látható, hogy a vizsgált összeg osztható a középső szám 3-szorosával.

b. A kapott $3n^3+6n$ kifejezést átalakítva:

$$3n^3+6n = (3n^3-3n)+9n = 3n(n^2-1)+9n = 3(n-1)n(n+1)+9n.$$

Ez az összeg nyilván osztható 9-cel, hiszen az $(n-1)n(n+1)$ szorzat osztható 3-mal.

29. $4^{90}+1 = (4^2)^{45}+1 = 16^{45}+1^{45}.$

Innen a (9) összefüggés értelmében következik, hogy a vizsgált kifejezés osztható $16+1=17$-tel.

JATE Móra Ferenc Kollégium
KÖNYVTÁRA

30. $333^{444}+444^{333} = (444^{333}+333^{333})+(333^{444}-333^{333}) =$

$$= (444^{333}+333^{333})+333^{333}(333^{111}-1) =$$

$$= (444^{333}+333^{333})+333^{333}(333^{111}-4^{111})+333^{333}(4^{111}-1) =$$

$$= (444^{333}+333^{333})+333^{333}(333^{111}-4^{111})+333^{333}[(4^3)^{37}-1] =$$

$$= (444^{333}+333^{333})+333^{333}(333^{111}-4^{111})+333^{333}(64^{37}-1).$$

Az első tag a (9) összefüggés értelmében osztható $444+333=777=7\cdot 111$-gyel, a második (7) szerint $333-4=329=7\cdot 47$-tel, végül az utolsó ugyancsak (7) szerint $64-1=63=7\cdot 9$-cel. Így valamennyi tag, tehát összegük, a vizsgált kifejezés is osztható 7-tel.

31. $3^{3n+2}+4 = 3^2\cdot(3^3)^n+4 = (9\cdot 27^n-9)+13 = 9(27^n-1)+13.$

Az első tag a (7) összefüggés értelmében osztható $27-1=26=2\cdot 13$-mal, ahonnan következik az állítás.

32. Ha n páratlan, akkor (9) értelmében 2^n+1 osztható $2+1=3$-mal. Ha viszont n páros, azaz valamely k természetes számra $n=2k$, akkor

$$2^n+1 = 2^{2k}+1 = [(2^2)^k-1]+2 = (4^k-1)+2.$$

Az első tag a (7) összefüggés szerint osztható $4-1=3$-mal; a második tag azonban nem és így szükségképpen az egész összeg sem osztható 3-mal.

Végeredményben tehát 2^n+1 akkor és csak akkor osztható 3-mal, ha n páratlan szám.

33. Teljes indukcióval bizonyítunk. Legyen

$$f(n) = 2^{2n}-3n-1.$$

Nyilván

$$9|f(1) = 2^2-3-1 = 0.$$

Most tegyük fel, hogy

(46) $9|f(n);$

bizonyítanunk kell, hogy ebből következik, hogy

(47) $9|f(n+1)$

is teljesül. $f(n+1)$ a következő alakban írható:

$$f(n+1) = 2^{2(n+1)}-3(n+1)-1 = 2^{2n}\cdot 2^2-3n-4 =$$

$$= 4\cdot 2^{2n}-3n-4 = 4(2^{2n}-3n-1)+9n = 4f(n)+9n.$$

Innen (46)-ra tekintettel nyilván következik (47).

34. Legyenek a, b adott egész számok. Tegyük fel, hogy a-nak és b-nek legnagyobb közös osztója D_1 és D_2 is, azaz mind D_1, mind D_2 rendelkezik az *A)* és *B)* tulajdonságokkal.

Mivel D_1 *A)* tulajdonságú, $D_1|a$ és $D_1|b$ teljesül. Mivel D_2 *B)* tulajdonságú, ezért osztható a és b minden közös osztójával, így D_1-gyel is:

(48) $D_1|D_2$.

Ugyanígy igazolható, hogy

(49) $D_2|D_1$

is teljesül.

(48)-ból és (49)-ből az oszthatóság *E)* tulajdonsága alapján következik, hogy $D_2 = \pm D_1$, és ezt kellett igazolnunk.

35*. Ugyanazokat a jelöléseket fogjuk használni, mint a 4. pontban. Először azt igazoljuk, hogy r_n rendelkezik a legnagyobb közös osztót definiáló *A)* tulajdonsággal, azaz r_n közös osztó:

(50) $r_n|a$ és $r_n|b$.

Az euklideszi algoritmus utolsó egyenlősége:

$$r_{n-1} = q_{n+1} r_n.$$

Innen következik, hogy

(51) $r_n|r_{n-1}$.

Az utolsó előtti egyenlőség:

(52) $r_{n-2} = q_n r_{n-1} + r_n$.

Innen (51) alapján következik, hogy

(53) $r_n|r_{n-2}$.

Az algoritmus (52)-t megelőző egyenlőségéből (51) és (53) alapján következik, hogy $r_n|r_{n-3}$.

Így okoskodva tovább, nyerjük, hogy $r_n|r_{n-4}, \ldots, r_n|r_3$,

(54) $r_n|r_2$

és

(55) $r_n|r_1$.

Az algoritmus második egyenlősége:

(56) $b = q_2 r_1 + r_2$.

Innen (54) és (55) alapján következik, hogy

(57) $r_n | b$.

Végül az algoritmus első egyenlősége:

(58) $a = q_1 b + r_1$.

Innen (55) és (57) alapján következik, hogy

(59) $r_n | a$.

(57) és (59) szerint a bizonyítandó állítás, (50) teljesül.

Most áttérünk annak bizonyítására, hogy r_n rendelkezik a *B)* tulajdonsággal is, azaz ha

(60) $d | a$ és $d | b$

akkor

(61) $d | r_n$

is fennáll.

Az euklideszi algoritmus első egyenlőségéből, (58)-ból r_1-et kifejezve:

(62) $r_1 = q_1 b - a$.

Innen (60) alapján következik, hogy

(63) $d | r_1$.

Az euklideszi algoritmus második egyenlőségéből, (56)-ból r_2-t kifejezve:

(64) $r_2 = b - q_2 r_1$.

Innen (60) és (63) alapján következik, hogy $d | r_2$.

Így okoskodva tovább, nyerjük, hogy $d | r_3, \ldots, d | r_{n-3}$,

(65) $d | r_{n-2}$

és

(66) $d | r_{n-1}$.

Ekkor az algoritmus utolsó előtti egyenlőségéből, (52)-ből r_n-et kifejezve:

(67) $r_n = r_{n-2} - q_n r_{n-1}$.

Innen (65) és (66) alapján következik (61).

r_n-nek, az euklideszi algoritmus által szolgáltatott utolsó, 0-tól különböző maradéknak tehát megvan a legnagyobb közös osztó mindkét tulajdonsága, és így valóban azonos a legnagyobb közös osztóval.

36*. Lényegében ugyanúgy fogunk okoskodni, mint az előző feladat megoldásának második fele során.

(62)-ből, vagyis az euklideszi algoritmus első egyenlőségéből látható, hogy $u_1 = -1$, $v_1 = q_1$ választással

(68) $$r_1 = u_1 a + v_1 b$$

teljesül.

Ezt felhasználva, (64)-ből (vagyis az algoritmus második egyenlőségéből) nyerjük, hogy

(69) $$r_2 = b - q_2 r_1 = b - q_2 (u_1 a + v_1 b) =$$

$$= (-q_2 u_1) a + (1 - q_2 v_1) b = u_2 a + v_2 b,$$

ahol $u_2 = -q_2 u_1$ és $v_2 = 1 - q_2 v_1$ egész számok.

Ezután az algoritmus harmadik egyenlőségéből kifejezve r_3-at, és felhasználva (68)-at, és (69)-et, azt kapjuk, hogy léteznek olyan u_3, v_3 egész számok, melyekre

$$r_3 = u_3 a + v_3 b.$$

Így okoskodva tovább, végül nyerjük, hogy léteznek olyan u_{n-2}, v_{n-2}, u_{n-1}, v_{n-1} egész számok, hogy

(70) $$r_{n-2} = u_{n-2} a + v_{n-2} b$$

és

(71) $$r_{n-1} = u_{n-1} a + v_{n-1} b.$$

Így (67)-ből, vagyis az algoritmus utolsó előtti egyenlőségéből (70) és (71) felhasználásával nyerjük, hogy

$$(a, b) = r_n = r_{n-2} - q_n r_{n-1} = (u_{n-2} a + v_{n-2} b) - q_n (u_{n-1} a + v_{n-1} b) =$$

$$= (u_{n-2} - q_n u_{n-1}) a + (v_{n-2} - q_n v_{n-1}) b = u_n a + v_n b,$$

ahol $u_n = u_{n-2} - q_n u_{n-1}$ és $v_n = v_{n-2} - q_n v_{n-1}$ egész számok, és ezzel az állítást igazoltuk.

37. Az euklideszi algoritmust az eredeti formában alkalmazva:

$$861 = 1 \cdot 567 + 294,$$

$$567 = 1 \cdot 294 + 273,$$

$$294 = 1 \cdot 273 + 21,$$

$$273 = 13 \cdot 21.$$

Így $(861, 567) = 21$.

Az euklideszi algoritmust a módosított formában alkalmazva:

(72) $861 = 2 \cdot 567 - 273,$

(73) $567 = 2 \cdot 273 + 21,$

$273 = 13 \cdot 21.$

Ez utóbbi tehát eggyel kevesebb lépésből áll. (Természetesen most is (861, 567) = 21 adódik.)

Továbbá (72)-ből:

$$273 = 2 \cdot 567 - 861.$$

(73)-ból:

$$21 = 567 - 2 \cdot 273 = 567 - 2(2 \cdot 567 - 861) = 2 \cdot 861 - 3 \cdot 567.$$

Így (861, 567) = 21 kívánt típusú előállítása:

$$2 \cdot 861 - 3 \cdot 567 = 21.$$

A legkisebb közös többszöröst pedig (13) alapján határozhatjuk meg:

$$[861, 567] = \frac{861 \cdot 567}{(861, 567)} = \frac{861 \cdot 567}{21} = 861 \cdot 27 = 23247.$$

38. (12)-re tekintettel:

(74) $(1232, 1008, 819) = ((1232, 1008), 819).$

Így először 1232 és 1008 legnagyobb közös osztóját kell meghatároznunk:

$1232 = 1 \cdot 1008 + 224,$

$1008 = 4 \cdot 224 + 112,$

$224 = 2 \cdot 112,$

tehát

(75) $(1232, 1008) = 112.$

Most (74)-re tekintettel 819 és 112 legnagyobb közös osztóját kell meghatároznunk:

$819 = 7 \cdot 112 + 35,$

$112 = 3 \cdot 35 + 7,$

$35 = 5 \cdot 7,$

tehát

(76) $(112, 819) = 7.$

(74), (75) és (76) értelmében $(1232, 1008, 819) = 7.$

39*. Könnyen látható (a részleteket az Olvasóra bízzuk), hogy ha az euklideszi algoritmust az a, b számok helyett az ac, bc számokra alkalmazzuk, akkor valamennyi hányados és maradék c-vel szorzódik, így speciálisan az utolsó, 0-tól különböző maradék, vagyis a két szám legnagyobb közös osztója is, és ezt kellett igazolnunk.

40*. A legnagyobb közös osztó definíciója szerint $(a, c)|a$ és $(a, c)|c$, tehát léteznek olyan m, n egész számok, melyekre $a=m(a, c)$ és $c=n(a, c)$. Ekkor

$$ab = m(a, c)\cdot b = (a, c)\cdot mb,$$

tehát (a, c) közös osztója c-nek és ab-nek:

$$(a, c)|c \quad \text{és} \quad (a, c)|ab.$$

Igazolnunk kell még, hogy

$$(77) \qquad d|ab, \; d|c$$

esetén

$$(78) \qquad d|(a, c).$$

A legnagyobb közös osztó *C)* tulajdonsága szerint léteznek olyan x, y, u, v egész számok, melyekre

$$xa+yc = (a, c)$$

és

$$ub+vc = (b, c) = 1.$$

Összeszorozva ezt a két egyenlőséget:

$$(xu)\cdot(ab)+yub+xva+yvc)c = (a, c).$$

Ha (77) teljesül, akkor nyilván a bal oldal mindkét tagja osztható d-vel, tehát a jobb oldalnak, (a, c)-nek is oszthatónak kell lennie d-vel, vagyis (78) valóban teljesül.

Ezzel igazoltuk, hogy (a, c) rendelkezik a legnagyobb közös osztót definiáló mindkét tulajdonsággal, tehát $(ab, c)=(a, c)$.

41*. A legnagyobb közös osztó *C)* tulajdonsága szerint léteznek olyan u, v egész számok, melyekre

$$ua+vb = (a, b) = 1.$$

Mindkét oldalt c-vel szorozva:

$$uc\cdot a+v\cdot bc = c.$$

Feltevésünk szerint $a|bc$, tehát a bal oldal mindkét tagja osztható a-val. Így szükségképpen a jobb oldalnak, c-nek is oszthatónak kell lennie a-val, és ezt kellett igazolnunk.

42*. A legnagyobb közös osztó *C)* tulajdonsága szerint léteznek olyan u, v egész számok, amelyekre

$$ua+vb = (a, b) = 1.$$

Mindkét oldalt c-vel szorozva:

$$uac+vbc = c. \tag{79}$$

Mivel $a|c$, ill. $b|c$, léteznek olyan m, n egész számok, melyekre $c=am=bn$. (79)-be helyettesítve:

$$ua\cdot bn+vb\cdot am = c,$$

vagyis

$$(un+vm)ab = c,$$

ahonnan következik, hogy $ab|c$, és ezt kellett igazolnunk.

43. *a.* A legnagyobb közös osztó definíciójából könnyen következik, hogy

$$(a, 1) = 1, \quad (a, a) = a, \quad (a, 0) = a.$$

b. Ha d közös osztója a-nak és $3a+1$-nek, akkor az oszthatóság *G)* tulajdonsága szerint osztója e két szám lineáris kombinációinak is. Így speciálisan

$$d|1\cdot(3a+1)-3\cdot a = 1,$$

tehát ± 1-en kívül nincs közös osztó. Így $(a, 3a+1)=1$.

c. Ha d közös osztója $9a+4b$-nek és $11a+5b$-nek, akkor osztója e két szám lineáris kombinációinak is, így speciálisan

$$d|5(9a+4b)-4(11a+5b) = a$$

és

$$d|9(11a+5b)-11(9a+4b) = b.$$

Így $d|(a, b)$.

Másrészt nyilván $(a, b)|9a+4b$ és $(a, b)|11a+5b$, tehát (a, b) rendelkezik a legnagyobb közös osztót definiáló két tulajdonsággal. Így $(9a+4b, 11a+5b)=(a, b)$.

44. Legyen $b=ac$. A legnagyobb közös osztó *D)* tulajdonságát felhasználva:

a. $(b, a+b) = (ac, a+ac) = a\cdot(c, c+1)$.

($(c, c+1)=1$, hiszen szomszédos egész számok nyilván relatív prímek.) Így végeredményben $(b, a+b)=a$.

b. $(b, 2a-3b) = (ac, 2a-3ac) = a\cdot(c, 2-3c)$.

Ha d közös osztója c-nek és $2-3c$-nek, akkor osztója ezek lineáris kombinációinak is. Így speciálisan

$$d|3\cdot c+1\cdot(2-3c) = 2,$$

tehát $(c, 2-3c)$ 1-gyel vagy 2-vel egyenlő. $(c, 2-3c)=2$ nyilván akkor és csak akkor teljesül, ha c páros, hiszen ekkor $2-3c$ is páros. Végeredményben tehát $(b, 2a-3b)=a$, ha c páratlan, vagyis $2a\nmid b$, és $(b, 2a-3b)=2a$, ha c páros, vagyis $2a|b$.

c. $(11a+5b, 24a+11b) = (11a+5ac, 24a+11ac) =$

$$= a\cdot(11+5c, 24+11c).$$

Ha d közös osztója $11+5c$-nek és $24+11c$-nek, akkor

$$d|11(11+5c)-5(24+11c) = 1,$$

tehát $(11+5c, 24+11c)=1$. Így $(11a+5b, 24a+11b)=1$.

45*. Legyen d közös osztója $n!+1$-nek és $(n+1)!+1$-nek. Ekkor d osztója e két szám lineáris kombinációinak is, így speciálisan

$$d|(n+1)\cdot(n!+1)-1\cdot[(n+1)!+1] =$$

$$= (n+1)!+(n+1)-(n+1)!-1 = n.$$

Innen és $d|(n!+1)$-ből következik, hogy

$$d|1\cdot(n!+1)-(n-1)!\cdot n = n!+1-n! = 1.$$

Így nincs ± 1-től különböző közös osztó, tehát a legnagyobb közös osztó 1.

46. Legyen d közös osztó, azaz

$$d|n^3+3n^2+5n+3$$

és

(80) $d|n^2+2n+2.$

Ekkor d osztója e két szám lineáris kombinációinak is, tehát speciálisan

(81) $d|1\cdot(n^3+3n^2+5n+3)-n\cdot(n^2+2n+2) =$

$$= (n^3+3n^2+5n+3)-(n^3+2n^2+2n) = n^2+3n+3.$$

(80)-ból és (81)-ből:

(82) $d|1\cdot(n^2+3n+3)-1\cdot(n^2+2n+2) = n+1.$

(80)-ból és (82)-ből:

(83) $d|1\cdot(n^2+2n+2)-n\cdot(n+1) = (n^2+2n+2)-(n^2+n) = n+2.$

Végül (82)-ből és (83-ból):

$$d|1\cdot(n+2)-1\cdot(n+1) = 1.$$

Így ± 1-en kívül nincs közös osztó, tehát a két szám relatív prím.

47*. Legyen

(84) $D = (2^m-1,\ 2^n+1).$

A (7) összefüggésre tekintettel

(85) $2^m-1|(2^m)^n-1 = 2^{mn}-1.$

Másrészt a (9) összefüggésre és m páratlan voltára tekintettel

$$2^n+1|(2^n)^m+1 = 2^{mn}+1.$$

(84)-ből és (85)-ből az oszthatóság tranzitivitása miatt következik, hogy

(86) $D|2^{mn}-1,$

(84)-ből és (86)-ból pedig következik, hogy

(87) $D|2^{mn}+1.$

(86)-ból és (87)-ből nyerjük, hogy

$$D|(2^{mn}+1)-(2^{mn}-1) = 2.$$

Azonban D nyilván páratlan szám, így szükségképpen $D=1$.

48*. Legyenek m, n tetszőleges természetes számok, melyekre $m<n$; bizonyítanunk kell, hogy ekkor $(a_m, a_n)=1$, vagyis

(88) $d|a_m$ és $d|a_n$

esetén szükségképpen $d=-1$ vagy $+1$.

Induljunk ki a következő átalakításból:

$$a_n-2 = (2^{2^n}+1)-2 = 2^{2^n}-1 = 2^{2^m\cdot 2^{n-m}}-1 = (2^{2^m})^{2^{n-m}}-1.$$

Itt a 2^{n-m} kitevő $n>m$-re tekintettel páros szám, tehát a (8) azonosság alapján következik, hogy

$$a_m = 2^{2^m}+1|a_n-2.$$

Minthogy (88) szerint a_m osztható d-vel, innen az oszthatóság tranzitív tulajdonsága alapján nyerjük, hogy

(89) $d|a_n-2.$

(88) és (89) szerint mind a_n, mind a_n-2 osztható d-vel, tehát a különbségük is osztható d-vel:

$$d|a_n-(a_n-2) = 2.$$

Másrészt a_m és a_n nyilván páratlan számok, tehát (88)-ból következik, hogy d páratlan szám. Így végeredményben d páratlan osztója a 2 számnak, tehát nyilván csak $d=-1$ vagy $+1$ lehetséges, és ezzel az állítást igazoltuk.

49. Először gondoljuk meg a következőket: Ha $d|a$ és $d|b$, akkor $d|b-a$; így a és b közös osztói abszolút értékben nem nagyobbak $|b-a|$-nél. Ha tehát a-nak és b-nek nem közös osztója a 2, 3, ..., $|b-a|$ számok egyike sem, akkor $(a, b)=1$.

a. Négy egymást követő egész szám közül kettő páratlan. E két páratlan szám különbsége 2, tehát közülük csak az egyik lehet osztható 3-mal. A másik páratlan számot tekintve, ez nem osztható sem 2-vel, sem 3-mal, tehát — az előbb vázolt gondolatmenet szerint — relatív prím a többi számhoz.

b. Hat egymást követő szám közül három páratlan; legyenek ezek n, $n+2$ és $n+4$. Ezek közül nyilván pontosan egy osztható 3-mal (hiszen $n+4$ akkor és csak akkor osztható 3-mal, ha $n+1$ is osztható 3-mal), és legfeljebb egy osztható 5-tel (hiszen e három szám közül nem választható ki kettő úgy, hogy különbségük osztható legyen 5-tel). Így van köztük egy olyan, amely nem osztható sem 3-mal, sem 5-tel; mivel ez a szám nem osztható 2, 3, 5 egyikével sem, az előbbi gondolatmenet szerint relatív prím a többi öt szám mindegyikéhez.

50*. Mind ez a feladat, mind a következő viszonylag egyszerűen tárgyalható lenne a számelmélet alaptételének segítségével; itt olyan bizonyítást fogunk adni, mely nem használja fel e tételt.

Teljes indukcióval bizonyítunk. $k=1$ esetén az állítás az $(m, n)=1$ feltétel értelmében teljesül.

Most tegyük fel, hogy valamely k-ra ($k=1, 2, \ldots$)

$$(m, n^k) = 1. \tag{90}$$

Bizonyítanunk kell: ebből következik, hogy

$$(m, n^{k+1}) = 1. \tag{91}$$

Legyen $a=n$, $b=n^k$, $c=m$. Ekkor a feladat feltételei szerint $(a, c)=(n, m)=1$, a (90) indukciós feltétel szerint $(b, c)=(n^k, m)=1$. Így a legnagyobb közös osztó *E)* tulajdonságát felhasználva,

$$(ab, c) = (n \cdot n^k, m) = (n^{k+1}, m) = 1,$$

tehát (91) teljesül, és ezzel az állítást igazoltuk.

51*. A legnagyobb közös osztó *D)* tulajdonsága szerint

$$(a^k, b^k) = (ab)^k \left(\left(\frac{a}{(a, b)} \right)^k, \left(\frac{b}{(a, b)} \right)^k \right). \tag{92}$$

$u = \dfrac{a}{(a, b)}$, $v = \dfrac{b}{(a, b)}$-t írva, nyilván

$$(u, v) = 1; \tag{93}$$

(92)-re tekintettel elég azt igazolnunk, hogy ekkor

$$(u^k, v^k) = 1.$$

Az előző feladatból $m=u$, $n=v$ választással (93) alapján következik, hogy

$$(m, n^k) = (u, v^k) = 1.$$

Innen viszont ismét az előző feladat alapján következik $m=v^k$, $n=u$ választással, hogy

$$(m, n^k) = (v^k, u^k) = 1,$$

és ezt kellett igazolnunk.

52. A legnagyobb közös osztó *D)* tulajdonsága szerint

$$(a^3-b^3,\ a^2-b^2) = (a-b)(a^2+ab+b^2,\ a+b).$$

Így elég azt igazolni, hogy

$$(94) \qquad (a^2+ab+b^2,\ a+b) = 1.$$

Tegyük fel, hogy d közös osztója a^2+ab+b^2-nek és $a+b$-nek. Ekkor d osztója e két szám lineáris kombinációinak is, tehát

$$d \mid 1\cdot(a^2+ab+b^2)-b\cdot(a+b) = a^2$$

és

$$d \mid 1\cdot(a^2+ab+b^2)-a\cdot(a+b) = b^2,$$

következésképpen $d \mid (a^2, b^2)$. Azonban mivel $(a, b)=1$, így az előző feladat szerint

$$(a^2, b^2) = (a, 2)^2 = 1,$$

tehát végeredményben $d \mid 1$. Így a^2+ab+b^2-nek és $a+b$-nek nincs ± 1-től különböző közös osztója, és ezzel (94)-et igazoltuk.

53. Először határozzuk meg 98 és 77 legnagyobb közös osztóját a módosított euklideszi algoritmus segítségével:

$$98 = 1\cdot 77+21,$$

$$77 = 4\cdot 21-7,$$

$$21 = 3\cdot 7.$$

A legnagyobb közös osztó tehát 7; ez osztója a jobb oldalnak, 14-nek is és így a vizsgált diofantikus egyenlet megoldható.

Most 98 és 77 legnagyobb közös osztóját, 7-et kifejezzük a két szám lineáris kombinációjaként. Az euklideszi algoritmus első egyenlőségéből:

$$21 = 98-1\cdot 77.$$

A másodikból:

$$7 = 4\cdot 21-77 = 4\cdot(98-1\cdot 77)-77 = 4\cdot 98-5\cdot 77.$$

A $(98, 77)=7$ tehát a következőképpen írható fel 98 és 77 lineáris kombinációjaként:

$$4\cdot 98-5\cdot 77 = 7.$$

Mindkét oldalt 2-vel szorozva:

$$98\cdot 8-77\cdot 10 = 14.$$

Innen látható, hogy a vizsgált egyenlet egy megoldása: $x=8$, $y=10$. Így (15) szerint az összes megoldás:

$$x = 8+\frac{-77}{(98, 77)}t = 8-\frac{77}{7}t = 8-11t,$$

$$y = 10-\frac{98}{(98, 77)}t = 10-\frac{98}{7}t = 10-14t,$$

ahol $t=0, \pm 1, \pm 2, \ldots$.

54. A

(95) $14x+23y = 463$

diofantikus egyenlet pozitív egész megoldásait keressük.

14 és 23 legnagyobb közös osztója:

$$23 = 2\cdot 14-5,$$

$$14 = 3\cdot 5-1,$$

$$5 = 5\cdot 1.$$

A legnagyobb közös osztó tehát 1 (és így egész megoldás nyilván létezik). Az első két egyenlőségből rendre

$$5 = 2\cdot 14-23,$$

$$1 = 3\cdot 5-14 = 3\cdot(2\cdot 14-23)-14 = 5\cdot 14-3\cdot 23.$$

463-mal szorozva ez utóbbi egyenlőséget:

$$14\cdot(5\cdot 463)-23\cdot(3\cdot 463) = 463$$

vagyis

$$14\cdot 2315-23\cdot 1389 = 463.$$

Így (15) szerint (95) összes egész megoldása:

$$x = 2315 + \frac{23}{(14, 23)} t = 2315 + 23t,$$

$$y = -1389 - \frac{14}{(14, 23)} t = -1389 - 14t.$$

Hogy kisebb számokkal számolhassunk, vonjuk ki az x előállításában szereplő konstansból 23 legnagyobb, 2315-öt túl nem lépő többszörösét, és vezessünk be egy új változót:

$$x = \left(2315 - 23\left[\frac{2315}{23}\right]\right) + 23\left(\left[\frac{2315}{23}\right] + t\right) =$$

$$= (2315 - 23 \cdot 100) + 23(100 + t) = 15 + 23u,$$

ahol $u = 100 + t$ és

$$y = -1389 - 14t = -1389 - 14(u - 100) =$$

$$= -1389 + 1400 - 14u = 11 - 14u;$$

itt $u = 0, \pm 1, \pm 2, \ldots$.

Az x, y megoldás nyilván akkor és csak akkor *pozitív* egész megoldás, ha

$$0 \leqq 14x = 14(15 + 23u) = 210 + 322u \leqq 463;$$

ez nyilván csak $u = 0$-ra teljesül. Így az egyetlen megoldás: $x = 15$, $y = 11$, tehát 463 csak egyféleképpen bontható fel a mondott módon, és ekkor az egyik tag $14x = 14 \cdot 15 = 210$, a másik $23y = 23 \cdot 11 = 253$.

(Megjegyezzük, hogy az adott esetben gyorsabban célhoz érhettünk volna, ha 463-ból sorra kivonjuk 23 többszöröseit, és ellenőrizzük, hogy e különbségek közül melyek oszthatók 14-gyel. Az általunk alkalmazott módszer jelentősége abban áll, hogy általánosabb szituációban is használható.)

55. Azt kell bizonyítanunk, hogy

$$(5a + 4,\ 9a + 7) \mid b$$

bármely a, b egész számokra fennáll. Ehhez viszont nyilván elég igazolni, hogy bármely a egész számra

$$(96) \qquad (5a + 4,\ 9a + 7) = 1.$$

Tegyük fel, hogy valamely d egész szám közös osztója $5a + 4$-nek és $9a + 7$-nek. Ekkor d osztója e két szám lineáris kombinációinak is, tehát

$$d \mid 9(5a + 4) - 5(9a + 7) = 1.$$

Innen következik (96).

56. Az $(a, b)=1$ feltételből következik, hogy a vizsgált diofantikus egyenlet megoldható. Tekintsük az összes olyan x, y megoldást, melyben x pozitív; ilyen megoldások léteznek, hiszen x, y-nal együtt $x+bt$, $y-at$ $(t=1, 2, \ldots)$ is megoldás. Tekintsük ezen megoldások közül azt, melyben x a legkisebb; ilyen megoldás létezik, hiszen pozitív egész számok közt van egy legkisebb. Jelöljük ezt az egyértelműen definiált megoldást x_0, y_0-val. Állítjuk, hogy

(97) $x_0 \leqq b.$

Ha ugyanis x_0 nagyobb lenne b-nél, akkor $x_1=x_0-b$, $y_1=x_0+a$ szintén megoldása lenne a vizsgált egyenletnek, mégpedig olyan megoldása, melyre

$$x_0 > x_1 = x_0-b > b-b = 0;$$

ez azonban ellentmondana x_0 minimum tulajdonságának. Így (97) valóban teljesül.

(97)-ből és a vizsgált egyenletből az $n>ab$ feltételre tekintettel következik, hogy

$$by_0 = n-ax_0 > ab-ab = 0,$$

tehát $x_0>0$ mellett $y_0>0$ is teljesül, és ezzel az állítást igazoltuk.

57. Legyen x_0, y_0 egy megoldása a

(98) $273x+210y = (273, 210)$

lineáris diofantikus egyenletnek (feltéve, hogy ez megoldható). Ekkor valamely u egész számmal szorozva, nyerjük, hogy

(99) $273x_0u+210y_0u = (273, 210)u.$

Legyen továbbá u_0, z_0 egy megoldása a

(100) $(273, 210)u-165z = 18$

lineáris diofantikus egyenletnek (amennyiben ez megoldható), azaz tegyük fel, hogy

(101) $(273,210)u_0-165z_0 = 18.$

Ekkor (99)-ből és (101)-ből következik, hogy

(102) $x = x_0u_0, \quad y = y_0u_0, \quad z = z_0$

megoldása a vizsgált egyenletnek. Végeredményben tehát az adott *háromismeretlenes* lineáris diofantikus egyenlet megoldása a (98) és (100) *kétismeretlenes* lineáris diofantikus egyenletek megoldására redukálható.

(98) megoldása céljából határozzuk meg 273 és 210 legnagyobb közös osztóját:

$$273 = 1 \cdot 210 + 63,$$

$$210 = 3 \cdot 63 + 21,$$

$$63 = 3 \cdot 21.$$

Így

(103) $(273, 210) = 21,$

továbbá az első egyenlőségből:

$$63 = 273 - 1 \cdot 210,$$

a másodikból:

$$21 = 210 - 3 \cdot 63 = 210 - 3(273 - 1 \cdot 210) = 4 \cdot 210 - 3 \cdot 273.$$

Így (98)-nak egy megoldása:

(104) $x_0 = -3, \quad y_0 = 4.$

(103)-ra tekintettel a (100) egyenlet a következő alakot ölti:

(105) $21u - 165z = 18.$

Ennek megoldása céljából határozzuk meg 21 és 165 legnagyobb közös osztóját:

$$165 = 8 \cdot 21 - 3,$$

$$21 = 7 \cdot 3.$$

Így $(21, 165) = 3$, továbbá az első egyenlőségből:

$$8 \cdot 21 - 1 \cdot 165 = 3.$$

Ezt az egyenlőséget $\frac{18}{(21, 165)} = \frac{18}{3} = 6$-tal szorozva:

$$21 \cdot (8 \cdot 6) - 165 \cdot (1 \cdot 6) = 18,$$

vagyis

$$21 \cdot 48 - 165 \cdot 6 = 18.$$

Így

(106) $u_0 = 48, \quad z_0 = 6$

megoldása a (105) egyenletnek.

(102)-ből, (104)-ből és (106)-ból nyerjük, hogy a vizsgált egyenlet egy megoldása:

$$x = x_0u_0 = (-3)\cdot 48 = -144,$$

$$y = y_0u_0 = 4\cdot 48 = 192,$$

$$z = z_0 = 6.$$

58. $2p=1$, $2p$ és $2p+1$ valamelyike osztható 3-mal, hiszen három egymást követő egész szám egyike osztható 3-mal. $3|2p$ azonban $(3, 2)=1$-re tekintettel akkor és csak akkor teljesül, ha $3|p$; így $2p-1, p$ és $2p+1$ valamelyike is osztható 3-mal. Egy prímszám azonban csak akkor lehet osztható 3-mal, ha -3-mal vagy $+3$-mal egyenlő. Így hat lehetőséget kell megvizsgálnunk: $2p-1=-3$ vagy $+3$, $p=-3$ vagy $+3$ és $2p+1=-3$ vagy $+3$. Az innen p-re adódó értékek rendre $p=-1, 2, -3, +3, -2, 1$. E hat eset közül csupán négy esetben teljesül, hogy $p, 2p-1$ és $2p+1$ mindegyike prímszám, nevezetesen $p=-3, -2, 2$ és 3 esetén.

59. p^2+2 a következőképpen alakítható át:

(107) $p^2+2 = (p^2-1)+3 = (p-1)(p+1)+3.$

Nyilván

(108) $3|(p-1)p(p+1,$

hiszen három egymást követő egész szám szorzata osztható 3-mal. Ha

(109) $3\nmid p,$

akkor (108)-ból és a prímszámok *B)* definíciójából következik, hogy

$$3|(p-1)(p+1).$$

Ekkor (107)-ből következik, hogy $3|p^2+2$. Azonban az egyetlen 3-mal osztható pozitív prímszám a 3, tehát innen szükségképpen

$$p^2+2 = 3.$$

Innen $p=\pm 1$ következnék, ami nem prímszám, tehát (109)-et kielégítő megoldás nem létezik.

Így csak $3|p$, vagyis $p=-3$ vagy $+3$ lehetséges; ekkor

$$p^2+2 = 3^2+2 = 11$$

valóban prímszám. A feladat összes megoldásai tehát $p=-3$ és $+3$.

60. Az n^4+4 kifejezés szorzattá alakítható:

$$n^4+4 = (n^4+4n^2+4)-4n^2 = (n^2+2)^2-(2n)^2 =$$

$$= (n^2+2n+2)(n^2-2n+2) = [(n+1)^2+1][(n-1)^2+1].$$

Így n^4+4-et felírtuk két *pozitív egész* szám szorzataként. Ha n^4+4 prímszám, akkor az egyik tényezőnek $+1$-nek kell lennie, tehát

$$(n+1)^2+1 = 1$$

vagy

$$(n-1)^2+1 = 1.$$

Innen $n=-1$, ill. $n=1$ következik. Ekkor

$$n^4+4 = 1^2+4 = 5$$

valóban prímszám, tehát a feladat összes megoldásai $n=-1$ és $+1$.

61. *a.* Nyilván elegendő azt belátni, hogy ha az m pozitív egész szám összetett szám, akkor 2^m-1 is összetett szám. ($n=1$ esetén ugyanis $2^n-1=$ $=2\cdot 1=1$ nem prímszám.) Tegyük fel tehát, hogy

$$n = ab,$$

ahol a, b egész számok és

(110) $1 < a \leqq b < n.$

Ekkor a (7) összefüggésre tekintettel

$$2^a-1 | 2^{ab}-1 = 2^n-1,$$

továbbá (110)-re tekintettel

$$2^a-1 \geqq 2^2-1 = 3 > 1$$

és

$$2^a-1 < 2^{2a}-1 \leqq 2^{ab}-1 = n,$$

tehát a 2^a-1 szám 2^n-1-nek 1-nél nagyobb és 2^n-1-nél kisebb osztója; így 2^n-1 valóban összetett szám.

b. $2^{11}-1 = 2047 = 23\cdot 89.$

62. Ha k nem 2^n alakú, akkor $k=m\cdot 2^l$ alakban írható, ahol m páratlan szám és 1-nél nagyobb, l nemnegatív egész szám. Azt kell tehát bizonyítanunk, hogy ha $m>1$ páratlan szám, l tetszőleges nemnegatív egész szám, akkor

$$A = 2^{m\cdot 2^l}+1$$

összetett szám. A (9) összefüggésből következik, hogy

(111) $2^{2^l}+1 | (2^{2^l})^m+1 = A,$

másrészt

(112) $2^{2^l}+1 \geqq 2^{2^0}+1 = 2+1 = 3$

és

(113) $2^{2^l}+1 < 2^{3\cdot 2^l}+1 \leqq 2^{m\cdot 2^l}+1 = A.$

(111)-ből, (112)-ből és (113)-ból következik, hogy A összetett szám.

63. Jelöljük a 48. feladatban definiált a_k Fermat-szám legkisebb prímosztóját q_k-val ($k=0, 1, 2, \ldots$). Mivel az $a_0, a_1, \ldots, a_k, \ldots$ számok a 48. feladat szerint páronként relatív prímek, a $q_0, q_1, \ldots, q_k, \ldots$ prímszámok különbözők; így definiáltunk egy különböző prímszámokból álló *végtelen* sorozatot, tehát szükségképpen végtelen sok prímszám létezik.

A feladat második állításának bizonyításához induljunk ki abból, hogy az előzők alapján $q_k \leqq a_k$ ($k=0, 1, \ldots$), tehát a $q_0, q_1, \ldots, q_{n-1}$ prímszámok egyike sem nagyobb a_{n-1}-nél. Így az n-edik prímszám sem lépheti túl ezt a korlátot, tehát

$$p_n \leqq a_{n-1} = 2^{2^{n-1}}+1 < 2^{2^n} \quad (n = 1, 2, \ldots),$$

és ezzel (22)-t igazoltuk.

64. Tegyük fel, hogy p prímszám a *B)* értelemben; bizonyítanunk kell, hogy ekkor

(114) $p = ab$

(a, b egész számok) esetén a vagy b szükségképpen egység. A *B)* tulajdonság szerint (114)-ből következik, hogy $p|a$ vagy $p|b$; feltehető, hogy $p|a$ teljesül, vagyis valamely c egész-számra

$$a = pc.$$

(114)-be helyettesítve:

$$p = (pc)b = pbc.$$

A *B)* definíció szerint $p \neq 0$, ezért

$$1 = bc.$$

Mivel b, c egész számok, innen következik, hogy b egység (és c is az), és ezt kellett igazolnunk.

65. *a.* 437-et sorban elosztva a $\sqrt{437} < 21$-nél kisebb prímszámokkal:

$$437 = 2\cdot 218+1 = 3\cdot 145+2 = 5\cdot 87+2 = 7\cdot 62+3 =$$

$$= 11\cdot 39+8 = 13\cdot 33+8 = 17\cdot 25+12 = 19\cdot 23,$$

tehát $437 = 19\cdot 23$ összetett szám.

b. 457-et sorban elosztva a $\sqrt{457} < 22$-nél kisebb prímszámokkal:

$$457 = 2\cdot 228+1 = 3\cdot 152+1 = 5\cdot 91+2 = 7\cdot 65+2 =$$

$$= 11\cdot 41+6 = 13\cdot 35+2 = 17\cdot 26+15 = 19\cdot 24+1.$$

Mivel 457 nem osztható az említett prímszámok egyikével sem, szükségképpen prímszám.

66. 5271 osztható 3-mal, hiszen számjegyeinek összege (azaz 15) osztható 3-mal. 3-mal osztva:

$$5271 = 3 \cdot 1757.$$

1757 nem osztható 2, 3, 5 egyikével sem, viszont osztható 7-tel:

$$1757 = 7 \cdot 251,$$

tehát

$$(115) \quad 5271 = 3 \cdot 7 \cdot 251.$$

251 nem osztható a $\sqrt{251} < 16$-nál kisebb prímszámok egyikével sem:

$$251 = 2 \cdot 125 + 1 = 3 \cdot 83 + 2 = 5 \cdot 50 + 1 = 7 \cdot 35 + 6 = 11 \cdot 22 + 9 =$$
$$= 13 \cdot 19 + 4.$$

Így 251 prímszám, tehát 5271 kanonikus alakja a (115) alatti.

67. Legyen k kanonikus alakja

$$k = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}.$$

Ekkor

$$ab = k^n = p_1^{n\alpha_1} p_2^{n\alpha_2} \dots p_r^{n\alpha_r}.$$

Ebből következik, hogy mind a, mind b kanonikus alakjában csak a $p_1, p_2, \dots, p_r$ prímtényezők léphetnek fel. Továbbá $(a, b) = 1$ miatt bármelyik p_i prímszám a és b kanonikus alakja közül csak az egyikben szerepelhet, mégpedig pontosan $n\alpha_i$ kitevővel. Így az a és b kanonikus alakjában szereplő kitevők oszthatók n-nel, tehát mind a, mind b természetes szám n-edik hatványa (l. a 17. példát).

68. Legyen n kanonikus alakja

$$n = p_1^{2\alpha_1+1} \dots p_r^{2\alpha_r+1} q_1^{2\beta_1} \dots q_s^{2\beta_s}$$

(vagyis különválasztjuk a páratlan, ill. páros kitevővel szereplő prímtényezőket). Ekkor

$$k = p_1^{\alpha_1} \dots p_r^{\alpha_r} q_1^{\beta_1} \dots q_s^{\beta_s}, \quad q = p_1 \dots p_r$$

nyilván kielégítik a k-ra és q-ra előírt feltételeket.

Az egyértelmüség bizonyítása céljából tegyük fel indirekt módon, hogy valamely k_1, k_2, q_1, q_2 természetes számokra

$$(116) \quad k_1^2 q_1 = k_2^2 q_2,$$

de

$$k_1 \neq k_2 \text{ és } q_1 \neq q_2;$$

feltehető, hogy

$$k_1 > k_2.$$

Innen következik, hogy létezik olyan p^α prímhatvány, hogy $p^\alpha | k_1$, de $p^\alpha \nmid k_2$. Ekkor p kitevője (116) bal oldalának kanonikus alakjában legalább 2α, míg a jobb oldalában legfeljebb $2(\alpha-1)+1=2\alpha-1$, tehát az indirekt feltevésből ellentmondásra jutottunk, és ezzel az állítást igazoltuk.

69*. Definiáljuk k-t a

$$2^k \leqq n < 2^{k+1}$$

egyenlőtlenséggel.

Most bővítsük valamennyi törtet úgy, hogy az új nevező $[1, 2, \ldots, n]$ legyen, azaz hozzunk közös nevezőre. $[1, 2, \ldots, n]$, vagyis a közös nevező 2-nek nyilván pontosan k-adik hatványával osztható. Könnyen látható az is, hogy az $\frac{1}{2^k}$ törtet kivéve, egyetlen nevező sem osztható 2^k-nál. Így az összes többi törtet páros számmal bővítjük, tehát az új számlálók mindegyike páros, ezt az egyet kivéve. Az $\frac{1}{2^k}$ törtből bővítéssel keletkező tört számlálója viszont $\frac{[1, 2, \ldots, n]}{2^k}$, ami páratlan szám. Így, ha a közös nevezőre hozás után elvégezzük az összeadást, akkor a számlálóban valahány (pontosan $n-1$) páros számot adunk össze, valamint egy páratlan számot, tehát páratlan számot kapunk; másrészt a nevező $k \geqq 1$-re, vagyis $n \geqq 2$-re tekintettel páros (hiszen osztható 2^k-nal). Azonban egy páratlan számot egy páros számmal osztva, nem kaphatunk egész számot, és ezzel az állítást igazoltuk.

70. 84 kanonikus alakja:

$$84 = 2\cdot 42 = 2\cdot 2\cdot 21 = 2\cdot 2\cdot 3\cdot 7 = 2^2\cdot 3\cdot 7.$$

Így az összes pozitív osztók:

$$2^0\cdot 3^0\cdot 7^0 = 1,\ 2^1\cdot 3^0\cdot 7^0 = 2,\ 2^2\cdot 3^0\cdot 7^0 = 4,\ 2^0\cdot 3^1\cdot 7^0 = 3,$$

$$2^1\cdot 3^1\cdot 7^0 = 6,\ 2^2\cdot 3^1\cdot 7^0 = 12,\ 2^0\cdot 3^0\cdot 7^1 = 7,\ 2^1\cdot 3^0\cdot 7^1 = 14,$$

$$2^2\cdot 3^0\cdot 7^1 = 28,\ 2^0\cdot 3^1\cdot 7^1 = 21,\ 2^1\cdot 3^1\cdot 7^1 = 42 \text{ és } 2^2\cdot 3^1\cdot 7^1 = 84.$$

71. A kanonikus alak:

$$6^5\cdot 10^4\cdot 14^3\cdot 15^2 = (2\cdot 3)^5\cdot(2\cdot 5)^4\cdot(2\cdot 7)^3\cdot(3\cdot 5)^2 =$$

$$= 2^5\cdot 3^5\cdot 2^4\cdot 5^4\cdot 2^3\cdot 7^3\cdot 3^2\cdot 5^2 = 2^{12}\cdot 3^7\cdot 5^6\cdot 7^3.$$

Így

$$d(2^{12}\cdot 3^7\cdot 5^6\cdot 7^3) = (12+1)(7+1)(6+1)(3+1) = 13\cdot 8\cdot 7\cdot 4 = 2912.$$

72. A 28-cal nem osztható osztók számát megkaphatjuk, ha az összes osztók számából kivonjuk a 28-cal osztható osztók számát, azaz $\frac{n}{28}$ osztóinak a számát:

$$d(n)-d\left(\frac{n}{28}\right) = d(2^5\cdot 3^4\cdot 5^3\cdot 7^2)-d\left(\frac{2^5\cdot 3^4\cdot 5^3\cdot 7^2}{2^2\cdot 7}\right) =$$

$$= d(2^5\cdot 3^4\cdot 5^3\cdot 7^2)-d(2^3\cdot 3^4\cdot 5^3\cdot 7) =$$

$$= (5+1)(4+1)(3+1)(2+1)-(3+1)(4+1)(3+1)(1+1) =$$

$$= 6\cdot 5\cdot 4\cdot 3-4\cdot 5\cdot 4\cdot 2 = 360-160 = 200.$$

73. Legyen n kanonikus alakja

$$n = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r}.$$

Ekkor a keresett n-re

(117) $d(n) = (\alpha_1+1)(\alpha_2+1)\dots(\alpha_r+1) = 9.$

Mivel $\alpha_1, \alpha_2, \dots, \alpha_r$ természetes számok, $i=1, 2, \dots, r$ esetén

(118) $\alpha_i+1 \geqq 2.$

A 9-et csak kétféleképpen alakíthatjuk szorzattá úgy, hogy (117) és (118) teljesüljön; egyrészt 9-et felfoghatjuk egyetlen tényezőből álló szorzatként, másrészt $9=3\cdot 3$. Ekkor

$$r = 1 \quad \text{és} \quad \alpha_1+1 = 9,$$

ill.

$$r = 2 \quad \text{és} \quad \alpha_1+1 = \alpha_2+1 = 3.$$

Az első esetben $\alpha_1=8$, tehát

$$n = p_1^8,$$

a másodikban $\alpha_1=\alpha_2=2$, tehát

$$n = p_1^2p_2^2.$$

n lehető legkisebb értékét úgy nyerjük, hogy p_1, illetve p_1 és p_2 értékét a lehető legkisebbnek választjuk, azaz $p_1=2$, ill. $p_1=2$ és $p_2=3$. Ekkor n

értéke

$$n = 2^8 = 256,$$

ill.

$$n = 2^2 \cdot 3^2 = 4 \cdot 9 = 36.$$

E két szám közül az utóbbi a kisebb, tehát a feladat megoldása: $n=36$.

74. *I. megoldás:*
Legyen n kanonikus alakja

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}.$$

Ekkor

$$d(n) = (\alpha_1+1)(\alpha_1+1) \dots (\alpha_r+1).$$

Ez a szorzat akkor és csak akkor páratlan, ha valamennyi tényezője páratlan, vagyis $\alpha_1, \alpha_2, \dots, \alpha_r$ mindegyike páros. Ez a feltétel viszont a 17. példa szerint akkor és csak akkor teljesül, ha n négyzetszám.

II. megoldás:
Az n szám pozitív osztóiból alkossunk párokat úgy, hogy az a és b osztók akkor és csak akkor kerüljenek egy párba, ha

(119) $ab = n$

teljesül (azaz a és b komplementer osztók; l. a 22. példát), továbbá

(120) $a \neq b$.

Felírva az összes ilyen osztópárt, páros számú osztót írunk fel. Másrészt ilyen módon nyilván figyelembe vesszük valamennyi pozitív osztót, kivéve azt az esetet, amikor valamely a osztóra a (119) által definiált b-re a (120) feltétel nem teljesül, azaz

$$n = ab = a \cdot a = a^2,$$

vagyis n négyzetszám. Ilyen a osztó tehát csak akkor létezik, ha n négyzetszám, és akkor pontosan egy ilyen osztó van, nevezetesen $\sqrt{n}$. Így, ha n négyzetszám, akkor a pozitív osztók száma páratlan, ellenkező esetben páros.

75. Képezzük az n szám pozitív osztóinak a szorzatát úgy, hogy az osztókból olyan párokat alkotunk, hogy az egy párba sorolt a, b osztókra $ab=n$ és $a \neq b$ teljesüljön, és először az egy párba sorolt osztókat szorozzuk össze. Az előző feladat II. megoldása során mondottakból következik, hogy ha n nem négyzetszám, akkor $\frac{d(n)}{2}$-szer (a párok száma ennyi) kapunk n-et, tehát az osztók szorzata $n^{\frac{d(n)}{2}}$; ha viszont n négyzetszám,

akkor a szorzat értéke

$$n^{\frac{d(n)-1}{2}} \cdot \sqrt{n} = n^{\frac{d(n)-1}{2}} \cdot n^{\frac{1}{2}} = n^{\frac{d(n)}{2}}.$$

Végeredményben tehát mindkét esetben $n^{\frac{d(n)}{2}}$-et kapunk eredményül.

a. $d(n) = d(180) = d(2^2 \cdot 3^2 \cdot 5) = (2+1)(2+1)(1+1) = 3 \cdot 3 \cdot 2 = 18,$

tehát az osztók szorzata:

$$n^{\frac{d(n)}{2}} = 180^9.$$

b. $d(n) = d(900) = d(2^2 \cdot 3^2 \cdot 5^2) = (2+1)(2+1)(2+1) = 3^3 = 27,$

tehát az osztók szorzata:

$$n^{\frac{d(n)}{2}} = 900^{\frac{27}{2}} = \left(900^{\frac{1}{2}}\right)^{27} = 30^{27}.$$

76. Legyen n prímszám és 3-nál nagyobb (mint a 63. feladat megoldása során láttuk, végtelen sok prímszám létezik). Ekkor nyilván

(121) $d(n) = 2.$

Másrészt ekkor $n+1$ páros szám, tehát

$$1 \mid n+1, \quad 2 \mid n+1, \quad \frac{n+1}{2} \Big| n+1 \quad \text{és} \quad n+1 \mid n+1.$$

Mivel $n > 3$,

$$1 < 2 < \frac{n+1}{2} < n+1,$$

tehát $1, 2, \frac{n+1}{2}$ és $n+1$ négy különböző pozitív osztója $n+1$-nek. Így

(122) $d(n+1) \geqq 4.$

(121)-ből és (122)-ből következik a bizonyítandó egyenlőtlenség.

77. Az n szám valamennyi pozitív osztója az

$$1, 2, \ldots, n$$

számok közül kerül ki. Így a bizonyítandó egyenlőtlenség biztosan teljesül, ha e számok közt van öt olyan, mely nem osztója n-nek. Meg fogjuk mutatni, hogy $n \geqq 11$ esetén n nem osztható

(123) $n-1,\ n-2,\ n-3,\ n-4$ és $n-5$

egyikével sem. Valóban, ha n osztható $n-k$-val ($0 \leqq k < n$), akkor létezik olyan pozitív egész a szám, hogy

$$n = a(n-k).$$

Ha $a=1$, akkor innen $k=0$ következik. Ha viszont $a \geqq 2$, akkor innen

$$n = a(n-k) \geqq 2(n-k) = 2n-2k,$$

vagyis

$$2k \geqq n.$$

Minthogy feltevésünk szerint $n \geqq 11$, innen $k > 5$ következik, tehát n valóban nem osztható a (123) számok egyikével sem, és ezzel igazoltuk, hogy $n_0 = 11$ kielégíti a feladat feltételeit. Továbbá $n-d(n)$ értékét kiszámítva $n=10, 9$ és 8 esetén, kapjuk, hogy

$$10-d(10) = 10-4 = 6 > 5,$$

$$9-d(9) = 9-3 = 6 > 5$$

és

$$8-d(8) = 8-4 = 4 < 5,$$

ahonnan látható, hogy a legkisebb kívánt tulajdonságú n_0 szám $n_0=9$.

78. Legyen az a pozitív egész szám osztója n-nek. Ekkor létezik olyan b pozitív egész szám, melyre

$$n = ab,$$

vagyis

$$a = \frac{n}{b}. \tag{124}$$

Ha $b \geqq 3$, akkor innen

$$a \leqq \frac{n}{3}$$

következik. Az e feltételt kielégítő pozitív osztók az $1, 2, \ldots, \left[\frac{n}{3}\right]$ számok közül kerülnek ki, tehát számuk legfeljebb $\frac{n}{3}$. Ezeken kívül n-nek még legfeljebb két további pozitív osztója lehet, nevezetesen $b = 1$, ill. $b = 2$ esetén a-ra (124)-ből n, illetve $\frac{n}{2}$ adódik. n-nek tehát összesen legfeljebb $\frac{n}{3}+2$ pozitív osztója lehet, és ezt kellett igazolnunk.

79. Legyen $n=2^k$ (ahol $k=1, 2, \ldots$). Ekkor

$$\log n = k \log 2,$$

tehát

$$d(n) = k+1 > k = \frac{\log n}{\log 2},$$

tehát a kívánt egyenlőtlenség teljesül $c=\frac{1}{\log 2}$-vel.

80*. Jelöljük az i-edik prímszámot p_i-vel (tehát $p_1=2$, $p_2=3$, $p_3=5$, ...). Legyen

$$n = (p_1 p_2 \cdots p_{k+1})^j \tag{125}$$

(ahol $j=1, 2, \ldots$). Ekkor innen

$$\log n = j \log p_1 p_2 \cdots p_{k+1},$$

vagyis

$$j = \frac{\log n}{\log p_1 p_2 \cdots p_{k+1}}.$$

Így

$$d(n) = (j+1)^{k+1} > j^{k+1} = \left(\frac{\log n}{\log p_1 p_2 \cdots p_{k+1}}\right)^{k+1} = \tag{126}$$

$$= \frac{\log n}{(\log p_1 p_2 \cdots p_{k+1})^{k+1}} \cdot (\log n)^k.$$

$\log n$ nagyobbá válik tetszőleges előírt értéknél, ha (125)-ben j-t elég nagyra választjuk (hiszen $\log n$ végtelenhez tart, ha n tart a végtelenhez). Így elég nagy j-re

$$\log n > (\log p_1 p_2 \cdots p_{k+1})^{k+1},$$

ekkor pedig (126)-ból következik, hogy

$$d(n) > (\log n)^k.$$

II. KONGRUENCIÁK

1. A KONGRUENCIA FOGALMA. ALAPTULAJDONSÁGOK

A *kongruenciareláció* bevezetése igen nagy segítséget jelent a számelméletben. Kongruenciák felhasználásával sok tétel, definíció, bizonyítás lényegesen egyszerűbben fogalmazható.

Legyenek a, b egész számok, m pedig 0-tól különböző egész szám. Ha $a-b$ osztható m-mel (vagyis a és b ugyanazt a maradékot adják m-mel osztva), akkor azt mondjuk, hogy *a kongruens b-vel modulo m*, és ezt a tényt a következőképpen jelöljük:

$m \mid a-b$

(1) $a \equiv b \pmod{m}$.

(Olvasd: a kongruens b-vel modulo m.) Ezt az összefüggést *kongruenciának*, az m egész számot *modulusnak* nevezzük. Ha az (1) kongruencia nem teljesül, akkor azt mondjuk, hogy *a inkongruens b*-vel modulo m.

Megjegyezzük, hogy a kongruenciák vizsgálata $m=1$ esetén érdektelen, míg az $m<0$ eset vizsgálata visszavezethető az $m>0$ esetére. Ezért a továbbiakban az $m>1$ esetre fogunk szorítkozni (noha például az e pontban elmondottak teljes egészében vonatkoznak az $m=1$ és $m<0$ esetekre is).

Könnyen igazolható, hogy a kongruenciareláció rendelkezik az alábbi alaptulajdonságokkal:

(*A*) Tetszőleges a egész számra és m természetes számra

$$a \equiv a \pmod{m}.$$

(A kongruenciareláció *reflexív*.)

B) Ha (1) teljesül, akkor szükségképpen

$$\boxed{b \equiv a \pmod{m}}$$

is fennáll. (A kongruenciareláció *szimmetrikus.*)

C) Ha valamely a, b, c egész számokra és m természetes számra (1) és $a \equiv b \pmod{m}$

(2) $\boxed{b \equiv c \pmod{m}}$

teljesül, akkor szükségképpen

$$\boxed{a \equiv c \pmod{m}}$$

is fennáll. (A kongruenciareláció *tranzitiv.* — L. a 3. feladatot.)

Ha egy halmaz elemei (például bizonyos számok, geometriai alakzatok s í. t.) közt értelmezve van egy *A)*, *B)* és *C)* tulajdonságú reláció, akkor ezt a relációt *ekvivalenciarelációnak* nevezzük. (Ilyen ekvivalenciareláció például a valós számok között értelmezett egyenlőség, a sík háromszögei közt definiált egybevágóság vagy hasonlóság s í. t.).

Bebizonyítható, hogy ha egy halmaz elemei közt definiálva van egy ekvivalenciareláció, akkor a halmaz elemei csoportosíthatók — mégpedig egyértelműen — úgy, hogy két elem akkor és csak akkor kerül ugyanabba a csoportba, ha ekvivalensek egymással. Az így definiált csoportokat (részhalmazokat) *ekvivalenciaosztályoknak* nevezzük.

Rögzítsünk tehát valamely m természetes számot, és csoportosítsuk az egész számok összességét úgy, hogy az ugyanabba a csoportba sorolt egész számok egymással páronként kongruensek legyenek modulo m (más szóval: csoportosítsuk az egész számokat aszerint, hogy m-mel osztva, mennyi maradékot adnak). Az így keletkező csoportokat *maradékosztályoknak* — pontosabban *modulo m maradékosztályoknak* — nevezzük. Valamely maradékosztályt úgy jellemezhetünk, hogy megadjuk egy r elemét; ilyenkor azt mondjuk, hogy a szóban forgó maradékosztályt *r által reprezentáljuk*, és r-et e maradékosztály *reprezentánsának* mondjuk.

Ha bizonyos $a_1, a_2, \ldots, a_k$ egész számok olyan tulajdonságúak, hogy páronként különböző maradékosztályokat reprezentálnak, másrészt minden modulo m maradékosztályt reprezentál e számok valamelyike, akkor az $a_1, a_2, \ldots, a_k$ számokról azt mondjuk, hogy azok *teljes maradékrendszert alkotnak modulo m.* Egy teljes maradékrendszer elemeinek száma nyilván azonos a

modulo m maradékosztályok számával. Másrészt könnyen ellenőrizhető, hogy az $1, 2, \ldots, m$ számok teljes maradékrendszert alkotnak modulo m; így a *modulo m maradékosztályok száma m.* Az elmondottakból következik az alábbi, gyakran használt kritérium:

Bizonyos egész számok akkor és csak akkor alkotnak teljes maradékrendszert modulo m, ha páronként inkongruensek modulo m, és számuk m.

Két modulo m teljes maradékrendszerrel különösen gyakran találkozunk: az egyik a $0, 1, 2, \ldots, m-1$ számok, vagyis a *legkisebb nemnegatív maradékok*, a másik az $\left[\frac{m}{2}\right]-m+1$, $\left[\frac{m}{2}\right]-m+2, \ldots, -1, 0, 1, \ldots, \left[\frac{m}{2}\right]$ számok, vagyis az *abszolút legkisebb maradékok* által alkotott teljes maradékrendszer.

A kongruenciák néhány további fontos tulajdonsága:

D) Legyenek a, b, c, d egész számok, m természetes szám, melyekre (1) és $a \equiv b \pmod{m}$

(3) $\quad c \equiv d \pmod{m}$

teljesül. Ekkor szükségképpen

$$a+c \equiv b+d \pmod{m}$$

is fennáll. Speciálisan: (1)-ből következik, hogy

$$a+c \equiv b+c \pmod{m}$$

E) Legyenek a, b, c, d egész számok, m természetes szám, melyekre (1) és (3) teljesül. Ekkor szükségképpen

$$ac \equiv bd \pmod{m}$$

$a \equiv b \pmod{m}$
$c \equiv d \pmod{m}$

is fennáll. (L. az 1. példát.) Speciálisan: (1)-ből következik, hogy

$$ac \equiv bc \pmod{m}.$$

A *D)* és *E)* tulajdonság ismételt alkalmazásával igazolható a következő tulajdonság:

$a \equiv b \pmod{m}$

F) Legyenek a, b egész számok, m természetes szám, melyekre (1) teljesül. Legyen továbbá $f(x)$ tetszőleges, egész együtthatós polinom. Ekkor szükségképpen

$$f(a) \equiv f(b) \pmod{m}$$

is fennáll. Speciálisan: tetszőleges k természetes számra

$$a^k \equiv b^k \pmod{m}.$$

Már a kongruenciák fenti tulajdonságai is elégségesek ahhoz, hogy segítségükkel bizonyos problémák megoldását lényegesen egyszerűsíteni tudjuk.

Így például gyakran találkozunk a következő típusú oszthatósági feladatokkal:

Adott valamely konkrét $f(x)$ egész együtthatós polinom és valamely m természetes szám. Bizonyítandó, hogy bármely n egész számra $m|f(n)$. (Ilyenek például az I. fejezet 21., 22., 24. feladatai.) Az *F)* tulajdonságra tekintettel ennek az állításnak az igazolásához elég ellenőrizni, hogy az állítás teljesül $n=0, 1, 2, \ldots, m-1$ esetén, vagyis

(4) $\quad f(j) \equiv 0 \pmod{m}, \quad$ ahol $\quad j = 0, 1, \ldots, m-1.$

Ezek a számok ugyanis teljes maradékrendszert alkotnak modulo m, tehát bármely n természetes számot megadva, az modulo m kongruens az említett számok valamelyikével, mondjuk j-vel. Ebből az *F)* tulajdonságra tekintettel következik, hogy

(5) $\quad f(n) \equiv f(j) \pmod{m}.$

(4)-ből és (5)-ből a kongruenciák *C)* tulajdonságából (tranzitivitás) következik, hogy

$$f(n) \equiv 0 \pmod{m},$$

vagyis $m|f(n)$. Minthogy itt n tetszőleges egész számot jelölhet, ezzel az állítást igazoltuk. (L. a 2. példát.)

A kongruenciák további két olyan fontos tulajdonsága, melyre még hivatkozni fogunk: $a \equiv b \pmod{\ldots}$

G) Legyenek a, b egész számok, m természetes szám, melyekre (1) teljesül. Ekkor szükségképpen $(a, m)=(b, m)$. (L. a 4. feladatot.)

H) Legyenek a, b egész számok, c pedig 0-tól különböző egész szám, m természetes szám. Ekkor

(6) $\quad ac \equiv bc \pmod{m}$

akkor és csak akkor teljesül, ha

$$(7) \qquad a \equiv b \quad \left(\mathrm{mod}\ \frac{m}{(m, c)}\right)$$

is fennáll. Ha speciálisan $(m, c) = 1$ teljesül, akkor azt nyerjük, hogy (6) akkor és csak akkor teljesül, ha (1) is fennáll.

Megjegyezzük, hogy már az *E)* tulajdonság is adja, hogy (7)-ből következik (6). Ebben a megállapításban az az új, hogy „visszafelé" is következtethetünk: (6)-ból is következik (7).

Végül egy, a teljes maradékrendszerek transzformációjára vonatkozó tétel:

I) Legyen m tetszőleges természetes szám, $a_1, a_2, \ldots, a_m$ teljes maradékrendszer modulo m, b az m-hez relatív prím egész szám, c tetszőleges egész szám. Ekkor a $ba_1+c, ba_2+c, \ldots, ba_m+c$ számok is teljes maradékrendszert alkotnak modulo m.

Példák

1. Bizonyítsuk be a kongruenciák *E)* tulajdonságát!

Megoldás:
(1), ill. (3) szerint

$$m|a-b \quad \text{és} \quad m|c-d.$$

Innen következik, hogy m osztója $a-b$ és $c-d$ lineáris kombinációinak is, így speciálisan

$$m|a\cdot(c-d)+d\cdot(a-b) = ac-bd.$$

Ezt a relációt kongruencia alakban felírva:

$$ac \equiv bd \pmod{m},$$

és ezt kellett igazolnunk. $6 | n(n^2+5)$

2. Igazoljuk az I. fejezet 24. feladatának állítását az *F)* tulajdonság kapcsán ismertetett módszerrel!

Megoldás:
Azt kell bizonyítanunk, hogy bármely n egész számra

$$f(n) = n(n^2+5) \equiv 0 \pmod{6}.$$

Mint láttuk, az *F)* tulajdonságra tekintettel elég azt megmutatni, hogy ez a

kongruencia teljesül egy modulo 6 teljes maradékrendszer elemeire. Célszerű az abszolút legkisebb maradékok, azaz a $-2, -1, 0, 1, 2, 3$ számok által alkotott teljes maradékrendszer elemeit behelyettesítenünk. A számolás tovább egyszerűsíthető, figyelembe véve, hogy az $f(n)$ polinom páratlan, azaz tetszőleges n-re $f(-n) = -f(n)$:

$$f(0) = 0,$$

$$f(1) = -f(-1) = 1\cdot(1^2+5) = 6,$$

$$f(2) = -f(-2) = 2\cdot(2^2+5) = 2\cdot 9 = 18$$

és

$$f(3) = 3\cdot(3^2+5) = 3\cdot 14 = 42.$$

Minthogy e számok mindegyike osztható 6-tal, vagyis 0-val kongruens modulo 6, ezzel az állítást igazoltuk.

3. Állapítsuk meg, hogy $101^{102^{103}}$ milyen maradékot ad 51-gyel osztva?

Megoldás:

$$101^{102^{103}} = (2\cdot 51-1)^{102^{103}} \equiv (-1)^{102^{103}} =$$

$$= [(-1)^{102}]^{102^{102}} = 1^{102^{102}} = 1 \pmod{51},$$

tehát a keresett maradék 1.

4. Legyenek m, n tetszőleges egész számok. Bizonyítsuk be, hogy m^3-n^3 és $m-n$ 6-tal osztva ugyanazt a maradékot adják!

Megoldás:

Azt kell bizonyítanunk, hogy

$$m^3-n^3 \equiv m-n \pmod 6.$$

Mindkét oldalhoz n^3-m-et adva, az eredetivel ekvivalens kongruenciát kapunk:

$$m^3-m \equiv n^3-n \pmod 6,$$

vagyis

$$(m-1)m(m+1) \equiv (n-1)n(n+1) \pmod 6.$$

Ez a kongruencia viszont nyilván teljesül, hiszen mindkét oldalon három egymást követő szám szorzata áll, tehát mindkét oldal osztható 6-tal (vö. az I. fejezet 24. feladatának megoldásával), vagyis mindkét oldal 0-val kongruens modulo 6.

2. REDUKÁLT MARADÉKOSZTÁLYOK. AZ EULER-FÉLE φ FÜGGVÉNY. AZ EULER—FERMAT-TÉTEL

Az 1. pontban szereplő *G)* állításból következik, hogy ha egy modulo m maradékosztály valamelyik eleme relatív prím m-hez, akkor a maradékosztály valamennyi eleme relatív prím m-hez. Ha egy maradékosztály elemei relatív prímek a modulushoz, akkor a maradékosztályt *redukált maradékosztálynak* nevezzük.

A modulo m redukált maradékosztályok számát $\varphi(m)$-mel szoktuk jelölni, és $\varphi(1)$ értéke legyen definíció szerint 1. Az így definiált $\varphi(n)$ számelméleti függvényt *Euler-féle φ függvénynek* nevezzük. Könnyen látható, hogy a $\varphi(n)$ függvénynek ez a definíciója ekvivalens az alábbival:

Legyen n tetszőleges természetes szám. Az n-hez relatív prím, n-nél nem nagyobb pozitív egész számok számát $\varphi(n)$-nel jelöljük.

Igazolható, hogy a $\varphi(n)$ számelméleti függvény *multiplikatív*, azaz ha m, n egymáshoz relatív prím természetes számok, akkor

$$(8) \qquad \varphi(mn) = \varphi(m)\varphi(n) \quad (\text{ahol } (m, n) = 1).$$

(L. a 19*. feladatot.) Ezt az összefüggést felhasználva, *a $\varphi(n)$ függvény explicit alakja* könnyen meghatározható: ha az $n > 1$ természetes szám kanonikus alakja

$$(9) \qquad n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r},$$

akkor

$$(10) \qquad \varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right)$$

(l. a 20. feladatot).

Ha valamennyi redukált maradékosztályból kiválasztunk egy-egy reprezentáns elemet, akkor az így nyert számokról azt mondjuk, hogy azok *redukált maradékrendszert alkotnak modulo m*. Gyakran hivatkozunk az alábbi kritériumra:

Bizonyos $a_1, a_2, \dots, a_k$ egész számok akkor és csak akkor alkotnak redukált maradékrendszert modulo m, ha eleget tesz-

nek a következő három feltételnek: számuk $\varphi(m)$ (azaz $k=\varphi(m)$); páronként inkongruensek; relatív prímek m-hez.

Az 1. pontban szereplő *I)* tétel megfelelője redukált maradékrendszerekre:

Legyen m tetszőleges természetes szám, a az m-hez relatív prím egész szám, $b_1, b_2, \ldots, b_{\varphi(m)}$ redukált maradékrendszer modulo m. Ekkor az $ab_1, ab_2, \ldots, ab_{\varphi(m)}$ számok is redukált maradékrendszert alkotnak modulo m. (l. a 25. feladatot.)

Ezt a tételt felhasználva, nem nehéz bebizonyítani az ún. *Euler-tételt* (vagy Euler—Fermat-tételt):

Legyen m tetszőleges természetes szám, a az m-hez relatív prím egész szám. Ekkor

$$(11) \quad a^{\varphi(m)} \equiv 1 \pmod{m}, \quad \text{ahol } (a, m) = 1.$$

(L. a 26. feladatot.)

Írjunk itt m helyére valamely p prímszámot! Ekkor a bal oldalon álló $\varphi(p)$ kitevő értéke a $\varphi(n)$ függvény második definíciójából kiindulva könnyen kiszámítható: $\varphi(p)=p-1$.

E definíció szerint ugyanis $\varphi(p)$ értéke egyenlő a p-nél nem nagyobb, p-hez relatív prím pozitív egész számok számával. Az e feltételeket kielégítő pozitív egész számok nyilván $1, 2, \ldots, p-1$, tehát $\varphi(p)=p-1$. (Természetesen ezt az eredményt levezethettük volna a (10) formulából is.)

Így (11)-ből nyerjük az ún. *Fermat-tételt* (vagy „kis" Fermat-tételt):

Ha p (pozitív) prímszám, a pedig p-hez relatív prím egész szám, akkor

$$(12) \quad a^{p-1} \equiv 1 \pmod{p}, \quad \text{ahol } (a, p) = 1.$$

Mindkét oldalt a-val szorozva:

$$(13) \quad a^p \equiv a \pmod{p}.$$

Ez a kongruencia ((12)-vel ellentétben) nyilván $p|a$ esetén is teljesül (hiszen ekkor mindkét oldal 0-val kongruens modulo p). Így ez az összefüggés *bármely* a egész számra teljesül; ezért a Fermat-tételt a (12) alak helyett sokszor ebben a formában alkalmazzuk.

Példák

5. Számítsuk ki $\varphi(6!)$ értékét!

Megoldás:
6! kanonikus alakja:

$$6! = 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6 = 2\cdot 3\cdot 2^2\cdot 5\cdot 2\cdot 3 = 2^4\cdot 3^2\cdot 5.$$

Így a (10) formulát alkalmazva:

$$\varphi(6!) = \varphi(2^4\cdot 3^2\cdot 5) = 2^4\cdot 3^2\cdot 5\cdot\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) =$$

$$= 2^4\cdot 3^2\cdot 5\cdot\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5} = 2^3\cdot 3\cdot 1\cdot 2\cdot 4 = 2^3\cdot 3\cdot 2\cdot 2^2 = 2^6\cdot 3 =$$

$$= 64\cdot 3 = 192.$$

6. Állapítsuk meg, hogy $\varphi(n)$ értéke, mely n természetes számokra páratlan?

I. Megoldás:

$n = 1$ esetén $\varphi(1) = 1$ páratlan.

Tegyük fel most, hogy $n>1$, és legyen n kanonikus alakja

$$n = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r}.$$

Ekkor a (10) formulát alkalmazva:

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_r}\right) =$$

$$= p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_r}\right) =$$

$$= \left[p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right)\right]\cdot\left[p_2^{\alpha_2}\left(1-\frac{1}{p_2}\right)\right]\dots\left[p_r^{\alpha_r}\left(1-\frac{1}{p_r}\right)\right] =$$

$$= \left[p_1^{\alpha_1-1}(p_1-1)\right]\cdot\left[p_2^{\alpha_2-1}(p_2-1)\right]\dots\left[p_r^{\alpha_r-1}(p_r-1)\right].$$

Ez a szorzat akkor és csak akkor páratlan, ha a $p_i^{\alpha_i-1}(p_i-1)$ tényezők mindegyike páratlan. Ha azonban itt $p_i=2$ és $\alpha_i>1$, akkor az első, ha $p_i>2$, akkor a második tényező páros. Így a vizsgált szorzat csak akkor lehet páratlan, ha abban egyetlen tényező szerepel, és ebben $p=2$ és $\alpha=1$, azaz $n=2$. Végeredményben tehát $\varphi(n)$ akkor és csak akkor páratlan, ha $n=1$ vagy 2. (Mindkét esetben $\varphi(n)=1$.)

II. Megoldás:

Állítjuk, hogy ha n tetszőleges természetes szám és a egész szám, úgy $(a, n)=1$ akkor és csak akkor teljesül, ha $(n-a, n)=1$. Valóban, ha d közös osztója a-nak és n-nek, akkor d osztója e két szám különbségének, $n-a$-nak is; másrészt ha d osztója $n-a$-nak és n-nek is, akkor osztója különbségüknek, $n-(n-a)=a$-nak is. Innen következik az állítás.

Legyen tehát a az n-nél nem nagyobb, n-hez relatív prím pozitív egész szám; a $\varphi(n)$ függvény második definíciója szerint az ilyen a számok számát jelöltük $\varphi(n)$-nel. Ekkor — az előbbiek szerint — a-val együtt $n-a$ is relatív prím n-hez. Továbbá, ha $a<n$, akkor $n-a$ is *pozitív* egész szám; az $a=n$ szám viszont nyilván csak akkor lehet relatív prím n-hez, ha $n=1$. Végül $a=n-a$ csak akkor fordulhat elő, ha $a=\frac{n}{2}$ relatív prím n-hez; ez azonban nyilván csak $n=2$ esetén lehetséges. Így $n>2$ esetén a mondott tulajdonságú a számokat párokba sorolhatjuk úgy, hogy az egy párba sorolt a számok különbözők, ugyanígy a különböző párokba kerülő a számok is; innen viszont nyilván következik, hogy ekkor $\varphi(n)$ értéke páros.

Végül $\varphi(1)=\varphi(2)=1$ páratlan szám, tehát $\varphi(n)$ akkor és csak akkor páratlan, ha $n=1$ vagy 2.

7. Igazoljuk, hogy ha n tetszőleges egész szám, akkor $n^{13}+12n$ osztható 13-mal!

Megoldás:

$$n^{13}+12n = (n^{13}-n)+13n.$$

Minthogy a második tag osztható 13-mal, azt kell igazolnunk, hogy az első tag is osztható 13-mal:

$$13 \mid n^{13}-n.$$

Kongruencia alakban felírva:

$$n^{13}-n \equiv 0 \pmod{13},$$

vagyis

$$n^{13} \equiv n \pmod{13}.$$

Ez a kongruencia azonban a Fermat-tétel (13) alakja szerint teljesül.

8. Állapítsuk meg, hogy 173^{163} mennyi maradékot ad 17-tel osztva?

Megoldás:

$$173^{163} = (17\cdot 10+3)^{163} \equiv 3^{163} \pmod{17}.$$

Minthogy $(3, 17)=1$, a Fermat-tétel (12) alakja szerint

$$3^{16} \equiv 1 \pmod{17}.$$

Így

$$3^{163} = (3^{16})^{10} \cdot 3^3 \equiv 1^{10} \cdot 3^3 = 27 \equiv 10 \pmod{17},$$

a keresett maradék tehát 10.

9. Határozzuk meg a $37^{39^{42}}$ szám utolsó két számjegyét!

Megoldás:

Az utolsó két számjegy meghatározásához azt kell megállapítanunk, hogy a vizsgált szám 100-zal osztva mennyi maradékot ad.

$(37, 100) = 1$-re tekintettel az Euler-tétel szerint

$$(14) \qquad 37^{\varphi(100)} \equiv 1 \pmod{100}.$$

$a^{\varphi(100)} \equiv 1 \pmod{100}$

A (10) képlet szerint

$$\varphi(100) = \varphi(2^2 \cdot 5^2) = 2^2 \cdot 5^2 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) =$$

$$= 2^2 \cdot 5^2 \cdot \frac{1}{2} \cdot \frac{4}{5} = 2 \cdot 5 \cdot 4 = 40.$$

4

Így (14) a következő alakban írható:

$$37^{40} \equiv 1 \pmod{100}.$$

$a^4 \equiv 1 \pmod{10}$

Ha tehát k tetszőleges természetes szám, akkor mindkét oldalt k-adik hatványra emelve (vagyis a kongruenciák *F)* tulajdonságát alkalmazva), nyerjük, hogy

$$(15) \qquad 37^{40k} \equiv 1 \pmod{100} \quad (k = 1, 2, \ldots).$$

$a^{4k} \equiv 1 \pmod{10}$

Innen következik, hogy ha azt akarjuk megállapítani, hogy valamely 37^n alakú szám 100-zal osztva mennyi maradékot ad, akkor e maradék csupán attól függ, hogy n 40-nel osztva mennyi maradékot ad.

Jelen esetben

$$39^{42} = (40-1)^{42} \equiv (-1)^{42} = 1 \pmod{40},$$

$4 =$

tehát a 39^{42} kitevő $40k+1$ alakban írható, ahol k alkalmas természetes szám. Így (15)-re tekintettel

$$37^{39^{42}} = 37^{40k+1} = 37 \cdot 37^{40k} \equiv 37 \pmod{100}.$$

A vizsgált szám tehát 37-re végződik.

3. LINEÁRIS KONGRUENCIÁK ÉS KONGRUENCIA-RENDSZEREK

Lineáris kongruencián

(16) $ax \equiv b \pmod{m}$

alakú kongruenciát értünk, ahol a, b adott egész számok, m adott természetes szám, a nem osztható m-mel és azon x egész számokat keressük, melyek ezt a kongruenciát kielégítik; az ilyen x egész számokat (16) *megoldásainak* nevezzük.

Ha valamely x_0 egész szám kielégíti ezt a kongruenciát, akkor nyilván bármely, x_0-lal modulo m kongruens egész szám is, vagyis az x_0 által reprezentált modulo m maradékosztály valamennyi eleme is. Ezért elég, ha a (16)-ot kielégítő maradékosztályoknak csak egy-egy reprezentáns elemét határozzuk meg- Más szóval: elegendő a (16) kongruenciának olyan megoldásait meghatároznunk, melyek páronként inkongruensek modulo m — az ilyen megoldásokat *lényegesen különböző megoldásoknak* nevezzük —, mert (16) bármely más megoldása kongruens e megoldások valamelyikével.

Tegyük fel, hogy az x_0 egész szám megoldása (16)-nak, vagyis

(17) $m | ax_0 - b.$

Ekkor létezik olyan y_0 egész szám, melyre

(18) $ax_0 - b = my_0,$

vagyis

(19) $ax_0 - my_0 = b.$

x_0, y_0 tehát megoldása az

(20) $ax - my = b$

lineáris diofantikus egyenletnek.

Másrészt tegyük fel, hogy az x_0, y_0 egész számok kielégítik a (20) lineáris diofantikus egyenletet, azaz (19) teljesül. Innen

visszafelé következik (18), majd (17), azaz

$$ax_0 \equiv b \pmod{m},$$

tehát x_0 megoldása (16)-nak.

Ezzel igazoltuk, hogy *a* (16) *lineáris kongruencia ekvivalens a* (20) *lineáris diofantikus egyenlettel* abban az értelemben, hogy az x_0 egész szám akkor és csak akkor megoldása a (16) lineáris kongruenciának, ha található hozzá olyan y_0 egész szám, hogy x_0, y_0 megoldása a (20) lineáris diofantikus egyenletnek.

Ennek az ekvivalenciának, valamint a lineáris diofantikus egyenletekről az I. fejezet 4. pontjában mondottaknak az alapján könnyen igazolhatók az alábbiak:

A (16) lineáris kongruencia akkor és csak akkor oldható meg, ha $(a, m)|b$. Ha ez a feltétel teljesül, és x_0 megoldása a (16) kongruenciának, akkor (16) *összes megoldásai* az $x = x_0 + \frac{m}{(a, m)} t$ (ahol $t = 0, \pm 1, \pm 2, \ldots$) alakú egész számok, vagyis az

$$x \equiv x_0 \left(\mathrm{mod}\, \frac{m}{(a, m)}\right)$$

feltételt kielégítő x egész számok.

Innen látható, hogy a (16) lineáris kongruenciának *maximális számú lényegesen különböző megoldása* a következőképpen adható meg:

$$(21) \quad x_0, x_0 + \frac{m}{(a, m)}, x_0 + 2 \cdot \frac{m}{(a, m)}, \ldots, x_0 + [(a, m) - 1] \cdot \frac{m}{(a, m)}.$$

A lényegesen különböző megoldások száma tehát (a, m).

A fentiek alapján a (16) lineáris kongruencia összes megoldásának meghatározása egyetlen megoldás kiszámítására redukálható.

A mondottak értelmében egy ilyen megoldáshoz eljuthatunk, ha meghatározzuk a (20) lineáris diofantikus egyenlet egy x_0, y_0 megoldását; ekkor ugyanis x_0 megoldása (16)-nak. Kétismeretlenes lineáris diofantikus

egyenlet egy megoldásának meghatározására viszont az I. fejezet 4. pontjában adtunk eljárást, és így végeredményben a (16) lineáris kongruencia egy megoldásának meghatározására is van módszerünk.

Az Euler-tételt felhasználva, másik módszer is adható lineáris kongruenciák megoldására.

Mindenekelőtt megjegyezzük, hogy a kongruenciák 1. pontban említett *H)* tulajdonságát felhasználva, könnyen látható, hogy a (16) lineáris kongruencia megoldásai $(a, m)|b$ esetén (mint láttuk, ez a megoldhatóság feltétele) ugyanazok, mint az

$$(22) \qquad \frac{a}{(a, m)} x \equiv \frac{b}{(a, m)} \left(\mathrm{mod}\, \frac{m}{(a, m)}\right)$$

kongruenciának, vagyis a két kongruencia *ekvivalens*. Itt már x együtthatója és a modulus relatív prímek, tehát a (16) lineáris kongruencia megoldása *arra az esetre redukálható, amikor*

$$(23) \qquad (a, m) = 1;$$

a továbbiakban arra az esetre szorítkozunk. (Megjegyezzük, hogy a gyakorlatban ezután célszerű még egy redukciós lépést végrehajtanunk, nevezetesen a (22) kongruencia mindkét oldalát osztjuk x együtthatójának és a jobb oldalon álló konstansnak a legnagyobb közös osztójával, $\left(\frac{a}{(a, m)}, \frac{b}{(a, m)}\right)$-mel, mely már relatív prím az $\frac{m}{(a, m)}$ modulushoz.)

Az Euler-tétel szerint (23)-ból következik, hogy

$$(24) \qquad a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Szorozzuk meg a (16) lineáris kongruencia mindkét oldalát $a^{\varphi(m)-1}$-gyel (így $(a, m) = 1$ alapján ekvivalens kongruenciát nyerünk):

$$a^{\varphi(m)} x \equiv b a^{\varphi(m)-1} \pmod{m},$$

vagyis (24)-re tekintettel

$$(25) \qquad x \equiv b a^{\varphi(m)-1} \pmod{m}.$$

$(a, m) = 1$ esetén tehát a (16) *lineáris kongruencia összes megoldásai* a (25) feltételt kielégítő egész számok. Végül, ha a (16) lineáris kongruenciában $(a, m) > 1$, akkor a (22) kongruenciára alkalmazva a (25) képletet, meghatározhatjuk (22)-nek és így (16)-nak egy megoldását, ahonnan (16) összes megoldását a (21) képlet segítségével kaphatjuk meg.

Az elmondottakból látható, hogy a lineáris kongruenciák megoldására bemutatott két módszer — különösen az Euler-tételen alapuló — meglehetősen számolásigényes, ezért a gyakorlatban ezeket alig alkalmazzuk. Egy-egy konkrét lineáris kongruenciát rendszerint valamilyen más, „ad hoc" módszerrel oldunk meg. E módszerek rendszerint arra épülnek, hogy a (16) lineáris kongruenciában szereplő a, b számok helyett valamely más, velük modulo m kongruens számot írunk, esetleg mindkét oldalt megszorozzuk valamilyen egész számmal; így szerencsés esetben olyan, az eredetivel ekvivalens kongruenciát tudunk felírni, mely alkalmas egyszerűsítés után az eredetinél „egyszerűbbé" (például a értéke kisebbé) válik. (L. a 12. példát, valamint a 37., 38. és 39. feladatot.)

Az alábbiakban vázoljuk a lineáris kongruenciák elméletének egy fontos alkalmazását.

Legyen m tetszőleges természetes szám, a az m-hez relatív prím egész szám. Ekkor, az eddigiek szerint az

$$ax \equiv 1 \pmod{m}$$

lineáris kongruencia megoldható. Azokat az x egész számokat, melyek kielégítik ezt a kongruenciát, az a szám *multiplikatív inverzeinek* nevezzük (modulo m). Egy olyan egész számot, mely multiplikatív inverze a-nak, a^*-gal jelöljünk. A definícióból, ill. a lineáris kongruenciákról elmondottakból következnek a multiplikatív inverz alábbi tulajdonságai:

A) Legyen a^* multiplikatív inverze a-nak (modulo m). Ekkor a b egész szám akkor és csak akkor multiplikatív inverze a-nak, ha

$$b \equiv a^* \pmod{m}$$

teljesül. (Vagyis valamely a egész szám multiplikatív inverzei egy modulo m maradékosztályt alkotnak.)

B) Ha m tetszőleges természetes szám, a az m-hez relatív prím egész szám, és a^* multiplikatív inverze a-nak, akkor $(a^*, m) = 1$.

C) Ha

$$a \not\equiv b \pmod{m},$$

és a^* multiplikatív inverze a-nak, b^* b-nek, akkor

$$a^* \not\equiv b^* \pmod{m}.$$

D) Ha a^* multiplikatív inverze a-nak, akkor a is a^*-nak, azaz $(a^*)^*$ akkor és csak akkor multiplikatív inverze a^*-nak, ha

$$(a^*)^* \equiv a \pmod{m}.$$

E) Ha a egy modulo m redukált maradékrendszer elemein fut végig, akkor tekintve ezen a számoknak egy-egy a^* multiplikatív inverzét, az a^* számok szintén redukált maradékrendszert alkotnak modulo m.

F) Az a szám multiplikatív inverzei az

$$a^* \equiv a^{\varphi(m)-1} \pmod{m}$$

kongruenciás kielégítő a^* egész számok.

Megjegyezzük, hogy elegánsabb és a lényegre jobban rámutató fogalmazás válna lehetővé azáltal, hogy definiálnánk a modulo m maradékosztályok szorzatát, és egy szám multiplikatív inverze helyett maradékosztály multiplikatív inverzéről beszélnénk; nem akarjuk azonban az olvasót olyan algebrai jellegű definíciókkal terhelni, melyek a továbbiakban nem feltétlenül szükségesek.

Áttérünk a *lineáris kongruencia-rendszerek* (szimultán kongruenciák) vizsgálatára.

Lineáris kongruencia-rendszeren

$$\begin{aligned} a_1 x &\equiv b_1 \pmod{m_1}, \\ a_2 x &\equiv b_2 \pmod{m_2}, \\ &\vdots \\ a_k x &\equiv b_k \pmod{m_k} \end{aligned}$$

alakú kongruencia-rendszert értünk, ahol $k > 1$ természetes szám, $a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_k$ adott egész számok, $m_1, m_2, \ldots, m_k$ adott természetes számok, és azokat az x egész számokat keressük, melyek *egyidejűleg kielégítik valamennyi fenti kongruenciát.*

A fenti kongruencia-rendszer megoldhatóságának nyilván szükséges feltétele, hogy a kongruencia-rendszert alkotó

$$a_i x \equiv b_i \pmod{m_i} \quad (\text{ahol } i = 1, 2, \ldots, k),$$

lineáris kongruenciák mindegyike megoldható legyen. Ha e kongruenciák mind megoldhatók, akkor megoldva azokat,

$$x \equiv c_1 \pmod{m_1},$$
$$x \equiv c_2 \pmod{m_2},$$
$$\vdots$$
$$x \equiv c_k \pmod{m_k}$$

típusú kongruencia-rendszert nyerünk (ahol a modulusok nem feltétlenül azonosak az előbbi kongruenciák modulusaival, de mindenképpen osztói azoknak). Ezért a továbbiakban ilyen típusú kongruencia-rendszerek vizsgálatára szorítkozunk.

Igazolható, hogy abban a különösen fontos speciális esetben, amikor

(26) $(m_i, m_j) = 1 \quad (1 \leqq i < j \leqq k$ esetén),

ez utóbbi kongruencia-rendszer megoldható, és a kongruencia-rendszert kielégítő x egész számok egy modulo $m_1 m_2 \ldots m_k$ maradékosztály elemeivel azonosak. Ekkor az összes megoldás meghatározásához elegendő egy megoldást meghatározni. *Egy megoldás kiszámítása* viszont a következőképpen történhet:

Az első kongruenciát az

(27) $x = c_1 + m_1 x_1 \quad (x_1 = 0, \pm 1, \pm 2, \ldots)$

alakú egész számok és csak azok elégítik ki. E számok közül az olyanokat keressük, melyek kielégítik a második kongruenciát is. Így e kongruenciába helyettesítve:

$$c_1 + m_1 x_1 \equiv c_2 \pmod{m_2},$$

vagyis

(28) $m_1 x_1 \equiv c_2 - c_1 \pmod{m_2}$.

E lineáris kongruenciából kiszámítjuk x_1-et:

$$x_1 \equiv d \pmod{m_2},$$

vagyis x_1 szükségképpen

$$x_1 = d + m_2 x_2$$

alakú. (27)-be helyettesítve:

$$x = c_1 + m_1 x_1 = c_1 + m_1 d + m_1 m_2 x_2.$$

x-nek ki kell elégítenie a harmadik kongruenciát is, tehát e kongruenciába helyettesítünk. Az így x_2-re kapott lineáris kongruenciát megoldva, nyerjük x_2-nek

$$x_2 = e + m_3 x_3$$

alakú előállítását s í.t.

Az eljárást akkor fejezzük be, amikor az utolsó k-adik kongruenciába helyettesítve x-nek x_{k-1} által kifejezett alakját, x_{k-1}-re az

$$x \equiv s + m_{k-1} x_{k-1} \equiv c_k \pmod{m_k}$$

lineáris kongruenciát kapjuk. Ennek egy tetszőleges megoldását választhatjuk x_{k-1} gyanánt, ahonnan már x értéke is adódik.

Az ismertetett módszer abban az esetben is alkalmazható egy lineáris kongruencia-rendszer megoldására, ha a (26) feltétel nem teljesül. Például $k=2$, azaz két kongruenciából álló rendszer esetén (28)-ból látható, hogy $(m_1, m_2) | c_2 - c_1$ szükséges feltétele a megoldhatóságnak. Másrészt igazolható, hogy ez a feltétel elégséges is, és ha e feltétel teljesül, akkor a kongruencia-rendszert kielégítő x egész számok egy modulo $[m_1, m_2]$ maradékosztály elemeivel azonosak. Így ismét elég egyetlen megoldást kiszámítani, és ezt (27) és (28) alapján hajthatjuk végre. Az általános esetben (amikor (26) nem szükségképpen teljesül és $k>2$-t is megengedjük) hasonló, de valamivel komplikáltabb a megoldhatóság szükséges és elégséges feltétele; ezt itt nem részletezzük. Elégedjünk meg annyival, hogy az ismertetett módszer erre az esetre is átvihető.

Példák

10. Oldjuk meg a

$$21x \equiv 2 \pmod{34}$$

lineáris kongruenciát úgy, hogy lineáris diofantikus egyenletre vezetjük vissza!

Megoldás:

A vizsgált lineáris kongruencia ekvivalens a

(29) $21x-34y = 2$

lineáris diofantikus egyenlettel.

Határozzuk meg 34 és 21 legnagyobb közös osztóját a módosított (az abszolút legkisebb maradékokra épülő) euklideszi algoritmus segítségével:

$$34 = 2\cdot 21-8,$$

$$21 = 3\cdot 8-3,$$

$$8 = 3\cdot 3-1,$$

$$3 = 3\cdot 1,$$

tehát a legnagyobb közös osztó (az utolsó 0-tól különböző maradék) -1; természetesen tekinthetjük legnagyobb közös osztónak ennek negatívját, $+1$-et is. Innen következik, hogy a vizsgált kongruencia megoldható, hiszen most $(a, m)=1|b=2$.

Fejezzük ki ezután a legnagyobb közös osztót a két szám lineáris kombinációjaként! A fenti algoritmus egyes egyenlőségeiből rendre

$$8 = 2\cdot 21-34,$$

$$3 = 3\cdot 8-21 = 3\cdot(2\cdot 21-34)-21 = 6\cdot 21-3\cdot 34-21 =$$

$$= 5\cdot 21-3\cdot 34,$$

$$1 = 3\cdot 3-8 = 3\cdot(5\cdot 21-3\cdot 34)-(2\cdot 21-34) =$$

$$= 15\cdot 21-9\cdot 34-2\cdot 21+34 = 13\cdot 21-8\cdot 34,$$

tehát a kívánt előállítás:

$$13\cdot 21-8\cdot 34 = 1.$$

Mindkét oldalt 2-vel szorozva:

$$21\cdot(13\cdot 2)-34\cdot(8\cdot 2) = 2,$$

vagyis

$$21\cdot 26-34\cdot 16 = 2.$$

Innen látható, hogy $x_0=26$, $y_0=16$ megoldása a (29) lineáris diofantikus egyenletnek.

Így a vizsgált kongruencia egy megoldása $x_0=26$. Több lényegesen különböző megoldás nincs, hiszen $(a, m)=(21, 34)=1$. Az összes megoldás tehát:

$$x \equiv x_0 = 26 \pmod{34}.$$

11. Oldjuk meg a

$$45x \equiv 72 \pmod{84}$$

lineáris kongruenciát az Euler-tétel felhasználásával!

Megoldás:

$a=45$ kanonikus alakja $a=3^2\cdot 5$, $m=84$-é pedig $m=2^2\cdot 3\cdot 7$. Így $(a, m)=$ $=(45, 84)=(3^2\cdot 5, 2^2\cdot 3\cdot 7)=3$, ami osztója $b=72$-nek, tehát a kongruencia megoldható. A kongruenciát és a modulust is végigosztva $(a, m)=3$-mal, az eredetivel ekvivalens kongruenciát kapunk:

$$15x \equiv 24 \pmod{28}.$$

Itt már $(a, m)=(15, 28)=1$. Továbbá itt $(a, b)=(15, 24)=3$. Osszuk el tehát a kongruencia mindkét oldalát $(a, b)=3$-mal:

$$5x \equiv 8 \pmod{28}.$$

Az Euler-tételen alapuló (25) formula szerint ennek a kongruenciának az összes megoldásai

$$x \equiv 8\cdot 5^{\varphi(28)-1} \pmod{28}. \tag{30}$$

Itt a (10) formula szerint

$$\varphi(28) = \varphi(2^2\cdot 7) = 2^2\cdot 7\cdot\left(1-\frac{1}{2}\right)\left(1-\frac{1}{7}\right) = 2^2\cdot 7\cdot\frac{1}{2}\cdot\frac{6}{7} =$$
$$= 2\cdot 6 = 12,$$

tehát (30)-ból

$$x \equiv 8\cdot 5^{12-1} = 8\cdot 5^{11} = 8\cdot 5\cdot(5^2)^5 =$$
$$= 40\cdot 25^5 \equiv 12\cdot(-3)^5 = 12\cdot(-3)^3\cdot(-3)^2 =$$
$$= 12\cdot(-27)\cdot 9 \equiv 12\cdot 1\cdot 9 = 108 = 3\cdot 28+24 \equiv 24 \pmod{28}.$$

Így a vizsgált kongruenciának egy megoldása $x_0=24$. A (21) formula szerint tehát maximális számú, lényegesen különböző megoldást a következőképpen adhatunk meg:

$$24,\ 24+\frac{84}{(45, 84)} = 24+\frac{84}{3} = 52,\quad 24+2\cdot\frac{84}{(45, 84)} =$$
$$= 24+2\cdot 28 = 80.$$

A vizsgált lineáris kongruencia összes megoldása tehát

$$x \equiv 24 \pmod{84}.$$
$$x \equiv 52 \pmod{84}$$
$$x \equiv 80 \pmod{84}.$$

12. Oldjuk meg az alábbi lineáris kongruenciát:

$$2^9x \equiv 71 \pmod{283}.$$

Megoldás:

Ha m páratlan, akkor b és $b+m$ közül az egyik páros. Így, ha a jobb oldalon álló konstans nem páros, akkor m-et hozzáadva, páros számot kapunk. Ezután 2-vel osztjuk a kongruenciát, majd megismételjük az eljárást. Ezt addig folytatjuk, míg x együtthatója 1 nem lesz:

$$\begin{aligned}
2^9x &\equiv 71 \equiv 71+283 = 354 \pmod{283},\\
2^8x &\equiv 177 \equiv 177+283 = 460 \pmod{283},\\
2^7x &\equiv 230 \pmod{283},\\
2^6x &\equiv 115 \equiv 115+283 = 398 \pmod{283},\\
2^5x &\equiv 199 \equiv 199+283 = 482 \pmod{283},\\
2^4x &\equiv 241 \equiv 241+283 = 524 \pmod{283},\\
2^3x &\equiv 262 \pmod{283},\\
2^2x &\equiv 131 \equiv 131+283 = 414 \pmod{283},\\
2x &\equiv 207 \equiv 207+283 = 490 \pmod{283},
\end{aligned}$$

végül

$$x \equiv 245 \pmod{283}.$$

13. Bizonyítsuk be a multiplikatív inverz fogalmát felhasználva az ún. *Wilson-tételt:* ha p tetszőleges prímszám, akkor

$$(p-1)! \equiv -1 \pmod{p}.$$

Megoldás:

A bal oldalon álló $1\cdot2\cdot3\cdot\ldots\cdot(p-2)\cdot(p-1)$ szorzat tényezőit párosítsuk úgy, hogy egy-egy párba olyan a, a^* tényezők kerüljenek, melyekre

$$(31)\qquad a\cdot a^* \equiv 1 \pmod{p}$$

és

$$(32)\qquad a \not\equiv a^* \pmod{p}$$

teljesül, más szóval az egy-egy párba kerülő két szám egymás multiplikatív inverze legyen modulo p. Ha egy-egy ilyen tényezőpárt elhagyunk, akkor végeredményben egy 1-es szorzót hagyunk el (modulo p), tehát a vizsgált szorzat értéke modulo p nem változik. A multiplikatív inverz tulajdonságaiból és abból, hogy az $1, 2, \ldots, p-1$ számok redukált maradékrendszert alkotnak modulo p, következik, hogy ilyen módon végül is az $1\cdot2\cdot3\cdot\ldots\cdot a\cdot\ldots\cdot(p-1)$ szorzatból minden a tényezőt elhagyunk, kivéve azokat, melyekre

$$(33)\qquad a \equiv a^* \pmod{p}.$$

Ekkor (33) és (31) szerint

$$aa^* \equiv a\cdot a = a^2 \equiv 1 \pmod{p},$$

vagyis

$$a^2-1 \equiv 0 \pmod{p}.$$

Ezt a kongruenciát oszthatósági relációként felírva:

$$p|a^2-1 = (a-1)(a+1).$$

Ha egy p prímszám osztója egy szorzatnak, akkor szükségképpen osztója valamelyik tényezőjének is, tehát innen

$$a-1 \equiv 0 \pmod{p}$$

vagy

$$a+1 \equiv 0 \pmod{p}$$

következik, azaz

$$a \equiv 1 \pmod{p}$$

vagy

$$a \equiv -1 \equiv p-1 \pmod{p}.$$

Így az $1\cdot 2\cdot 3\cdot \ldots \cdot (p-1)$ szorzatból elhagyva a (31)-et és (32)-t kielégítő párok elemeit, csak az 1 és $p-1$ tényezők maradnak meg, tehát az említett szorzat e két tényező szorzatával kongruens modulo p:

$$(p-1)! = 1\cdot 2\cdot 3\cdot \ldots \cdot (p-1) \equiv 1\cdot (p-1) \equiv$$

$$\equiv 1\cdot(-1) = -1 \pmod{p},$$

és éppen ezt kellett igazolnunk.

14. Oldjuk meg a

$$3x \equiv 2 \pmod{5},$$

$$4x \equiv 1 \pmod{7},$$

$$5x \equiv 1 \pmod{8}$$

lineáris kongruencia-rendszert!

Megoldás:

Az első kongruencia mindkét oldalát 2-vel szorozva:

$$6x \equiv 4 \pmod{5},$$

vagyis

$$x \equiv 4 \pmod{5},$$

tehát x

$$x = 5t+4 \tag{34}$$

alakú, ahol t egész szám. A második kongruenciába helyettesítve:

$$4(5t+4) = 20t+16 \equiv 1 \pmod 7,$$

vagyis

$$6t \equiv -15 \equiv 6 \pmod 7,$$

ahonnan

$$t \equiv 1 \pmod 7.$$

Így t a következő alakban írható:

$$t = 7u+1.$$

(34)-be helyettesítve:

$$x = 5(7u+1)+4 = 35u+9. \tag{35}$$

x-nek ezt a kifejezését az utolsó kongruenciába helyettesítve:

$$5(35u+9) \equiv 5(3u+1) = 15u+5 \equiv 7u+5 \equiv 1 \pmod 8,$$

ahonnan

$$7u \equiv 4 \pmod 8,$$

vagyis

$$-u \equiv 4 \pmod 8.$$

Mindkét oldalt -1-gyel szorozva:

$$u \equiv -4 \equiv 4 \pmod 8.$$

u egy lehetséges értéke tehát $u=4$. (35)-be helyettesítve nyerjük a vizsgált kongruencia-rendszer egy megoldását:

$$x = 35u+9 = 35\cdot 4+9 = 149.$$

Mivel a modulusok (5, 7 és 8) páronként relatív prímek, a megoldások annak az $5\cdot 7\cdot 8=280$ modulusú maradékosztálynak az elemeivel azonosak, melynek egy reprezentánsa a fenti konkrét megoldás, 149. Az összes megoldás tehát:

$$x \equiv 149 \pmod{280}.$$

4. MAGASABBFOKÚ KONGRUENCIÁK

Magasabbfokú kongruencián

(36) $a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \equiv 0 \pmod{m}$

alakú kongruenciát értünk, ahol $a_0, a_1, \ldots, a_{n-1}, a_n$ adott egész számok, m adott természetes szám, és azokat az x egész számokat keressük, melyek ezt a kongruenciát kielégítik; az ilyen x egész számokat (36) *megoldásainak* nevezzük. Ha (36)-ban

$$a_0 \not\equiv 0 \pmod{m},$$

akkor a *kongruenciát* n-edfokúnak mondjuk. Az előző pontban tárgyalt lineáris kongruenciák nyilván az $n=1$ speciális esetnek felelnek meg.

Ha valamely x_1 egész szám kielégíti a (36) kongruenciát, akkor a kongruenciák (1. pontban említett) F) tulajdonsága szerint bármely olyan x_2 egész szám is kielégíti, melyre

$$x_2 \equiv x_1 \pmod{m}$$

teljesül. Így a (36) kongruencia megoldásai bizonyos modulo m maradékosztályok elemeivel azonosak.

(36) bizonyos x_1, x_2 megoldásait akkor mondjuk *lényegesen különbözőknek*, ha

$$x_1 \not\equiv x_2 \pmod{m}.$$

A megoldásokat tartalmazó maradékosztályok, vagyis a lényegesen különböző megoldások számát (36) *megoldásszámának* nevezzük. Két, (36) alakú kongruenciát akkor nevezünk *ekvivalensnek*, ha megoldásaik azonosak.

Magasabbfokú kongruenciák összes megoldásai (ellentétben a magasabbfokú egyenletek megoldásaival) mindenkor meghatározhatók egy *véges* algoritmus segítségével. Elegendő ugyanis egy modulo m teljes maradékrendszer elemeit behelyettesíteni (célszerű az *abszolút legkisebb* maradékok által alkotott teljes maradékrendszer elemeit helyettesítenünk). A teljes maradékrendszer azon elemei, melyek kielégítik a kongruenciát, nyilván maximális számú, lényegesen különböző megoldást adnak, és minden más megoldás e számok valamelyikével kongruens.

E próbálgatás jellegű megoldási módszer alkalmazása azonban meglehetősen sok számolással jár. Ezért célszerű olyan redukciós eljárásokat, megoldási módszereket keresnünk, melyekkel ez a számolás lerövidíthető.

Az egyik kínálkozó redukciós lépés az *együtthatókat* módosítja. (36)-ban az $a_0, a_1, \ldots, a_n$ együtthatók mindegyikét azok modulo m abszolút legkisebb maradékával helyettesíthetjük. (Azaz, mindegyik a_i együttható helyett egy vele modulo m kongruens számot írhatunk, mely abszolút értékben nem nagyobb $\frac{m}{2}$-nél). Így nyilván ekvivalens kongruenciát nyerünk, másrészt — mivel az együtthatók kisebbek, — a számolás egyszerűbbé válik.

A másik redukciós lépés a *modulusra* vonatkozik. Legyen ugyanis m kanonikus alakja

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$$

($m > 1$ feltehető), és tegyük fel, hogy az x egész szám kielégíti a (36) kongruenciát. Ekkor (36)-ból (az oszthatóság tranzitív tulajdonsága alapján) következik, hogy

$$(37) \quad a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n \equiv 0 \pmod{p_1^{\alpha_1}},$$

$$(38) \quad a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n \equiv 0 \pmod{p_2^{\alpha_2}},$$

$$\vdots$$

$$(39) \quad a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n \equiv 0 \pmod{p_r^{\alpha_r}};$$

másrészt, ha valamely x egész számra e kongruenciák mindegyike teljesül, akkor az oszthatóság *G)* tulajdonságára tekintettel (36) is fennáll. E kongruencia-rendszer tehát ekvivalens a (36) kongruenciával. Ha viszont az x_1 egész szám kielégíti a (37) kongruenciát, x_2 (38)-at, ..., x_r (39)-et, akkor az

$$x \equiv x_1 \pmod{p_1^{\alpha_1}},$$

$$x \equiv x_2 \pmod{p_2^{\alpha_2}},$$

$$\vdots$$

$$x \equiv x_r \pmod{p_r^{\alpha_r}}$$

lineáris kongruencia-rendszerrel definiált x egész számok nyilván kielégítik a (37), (38), ..., (39) által alkotott kongruencia-rendszert, tehát (36)-ot is. Másrészt a (37), (38), ..., (39) kongruenciák alkalmas $x_1, x_2, \ldots, x_r$ megoldásából kiindulva, az előbbiek szerint így (36)-nak minden x megoldásához eljuthatunk.

Végeredményben tehát (36) megoldásainak meghatározása visszavezethető a (37), (38), ..., (39) kongruenciák, vagyis az

$$(40)\quad f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \equiv 0 \pmod{p^\alpha}$$

típusú kongruenciák megoldásainak meghatározására, valamint ezt követően egy vagy több lineáris kongruencia-rendszer megoldásainak kiszámítására. (Ha a (37), (38), ..., (39) kongruenciák megoldásszáma rendre $t_1, t_2, \ldots, t_r$, akkor $t_1t_2\ldots t_r$ lineáris kongruencia-rendszert kell felírnunk és megoldanunk.) Így *összetett modulusú magasabbfokú kongruenciák megoldása visszavezethető prímhatvány modulusú kongruenciák megoldására*, ezért áttérünk ilyen, vagyis (40) alakú kongruenciák vizsgálatára.

Egy (40) típusú kongruencia megoldásait célszerű

$$(41)\quad x = x_0 + x_1p + x_2p^2 + \ldots + x_{\alpha-1}p^{\alpha-1}$$

alakban keresnünk. Itt először x_0 lehetséges értékeit határozzuk meg, a következőképpen:

Ha egy (41)-beli x-re (40) teljesül, akkor szükségképpen

$$(42)\quad f(x) \equiv 0 \pmod{p}$$

is fennáll. Azonban nyilván

$$(43)\quad f(x) = f(x_0 + p(x_1 + x_2p + \ldots + x_{\alpha-1}p^{\alpha-2})) \equiv f(x_0) \pmod{p}.$$

(42)-ből és (43)-ból következik, hogy

$$(44)\quad f(x_0) \equiv 0 \pmod{p},$$

tehát x_0 az

$$(45)\quad f(y) \equiv 0 \pmod{p}$$

kongruencia valamelyik megoldása. Így először ez utóbbi kongruenciát kell megoldanunk.

Ezután x_0-t futtatva (45) lényegesen különböző megoldásain, meghatározzuk az egyes x_0 értékekhez tartozó x_1 értékeket, a következőképpen:

Ha a (41) alatti x-re (40) teljesül, akkor szükségképpen

$$(46)\quad f(x) \equiv 0 \pmod{p^2}$$

is fennáll (feltéve, hogy $\alpha \geqq 2$). Azonban könnyen látható, hogy

$$(47)\quad f(x) = f\big(x_0 + x_1 p + p^2(x_2 + \ldots + x_{\alpha-1}p^{\alpha-2})\big) \equiv$$
$$\equiv f(x_0 + x_1 p) = f(x_0) + p x_1 g(x_0) \pmod{p^2},$$

ahol $g(x)$ alkalmas egész együtthatós polinom. (46)-ból és (47)-ből következik, hogy

$$f(x_0) + p x_1 g(x_0) \equiv 0 \pmod{p^2}.$$

(44) szerint a bal oldal első tagja osztható p-vel. Ekvivalens kongruenciát kapunk, ha a kongruencia mindkét oldalát és a modulust is osztjuk p-vel. Így

$$\frac{f(x_0)}{p} + x_1 g(x_0) = c_1 + d_1 x_1 \equiv 0 \pmod{p}$$

alakú kongruenciát nyerünk, ahol c_1, d_1 adott egész számok. x_1 tehát a

$$c_1 + d_1 x \equiv 0 \pmod{p}$$

lineáris kongruencia valamelyik megoldása, s így ezt a kongruenciát kell megoldanunk x_1 lehetséges értékeinek meghatározására.

Ezután tekintve az összes lehetséges x_0, x_1 párokat, x_2 megfelelő értékeit kell meghatároznunk. Az

$$f(x) = f\big(x_0 + x_1 p + x_2 p^2 + p^3(x_3 + \ldots + x_{\alpha-1}p^{\alpha-3})\big) \equiv$$
$$\equiv f(x_0 + x_1 p + x_2 p^2) = f(x_0 + x_1 p) + p^2 x_2 g(x_0 + x_1 p) \equiv 0$$
$$\pmod{p^3}$$

kongruenciából indulunk ki, melyet p^2-nel osztva, látható, hogy x_2 lehetséges értékeit egy

$$c_2+d_2x \equiv 0 \pmod{p}$$

alakú kongruencia megoldásai szolgáltatják s.í.t.

Végeredményben tehát a (40) *prímhatvány modulusú kongruencia megoldása visszavezethető a* (42) *prím modulusú kongruencia és lineáris kongruenciák megoldására.* Ezért e fejezetben a továbbiakban *prím modulusú kongruenciák vizsgálatára szorítkozunk.*

Ha egy prím modulusú kongruencia foka nagyobb a modulusnál, akkor *további redukció* lehetséges a *Fermat-tétel* (13) alakjából kiindulva. Legyen ugyanis a vizsgált kongruencia

$$(48) \quad a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n \equiv 0 \pmod{p},$$

ahol

$$a_0 \not\equiv 0 \pmod{p},$$

és $n \geqq p$. Osszuk el ekkor n-et p-vel:

$$n = kp+r,$$

ahol k pozitív egész szám és r olyan egész szám, melyre

$$0 \leqq r < p,$$

Ekkor (13) szerint tetszőleges x egész számra

$$x^n = x^{kp+r} = (x^p)^k \cdot x \equiv x^k \cdot x^r = x^{k+r} \pmod{p},$$

tehát (48)-ban az a_0x^n tag helyett a_0x^{k+r}-et írva, ekvivalens kongruenciát nyerünk. Másrészt

$$k+r < 2k+r \leqq kp+r = n,$$

tehát x^{k+r} kitevője kisebb, mint x^n-é. Így a mondott változtatást végrehajtva, alacsonyabb fokú kongruenciát nyerünk (vagy olyan kongruenciát, melynek mindkét oldalán az azonosan 0 polinom áll).

Ha a nyert alacsonyabb fokú kongruencia foka még mindig nem kisebb p-nél, akkor az ismertetett redukciós lépést megismételhetjük s í.t.

Így végeredményben bármely (48) alakú kongruencia *ekvivalens* egy olyan kongruenciával, melynek *foka legfeljebb* $p-1$, vagy pedig mindkét oldalon az azonosan 0 polinóm áll (ilyenkor nyilván bármely x egész szám megoldás).

Végül egy fontos tétel a *megoldásszámra* vonatkozóan (az ún. *fokszámtétel*): bármely n-edfokú prím modulusú kongruencia megoldásszáma legfeljebb n (l. az 52*. feladatot).

Megjegyezzük, hogy bár a fentiekben több redukciós eljárást ismertettünk, ezek nem teszik lehetővé a próbálgatás teljes kiküszöbölését (csupán egyszerűsítik azt). Bizonyos speciális kongruenciatípusok megoldására azonban kidolgozhatók olyan módszerek, melyekkel próbálgatás nélkül is célt érhetünk (e módszerek részben a magasabbfokú egyenletek elméletében szereplő módszerek analogonjai). Ilyen speciális kongruenciák például az ún. binom kongruenciák (melyekkel a következő pontban fogunk foglalkozni) és a másodfokú és másodfokúra redukálható kongruenciák (l. a 6. pontot, valamint a 100. és 101. feladatot); valamint a multiplikatív inverz fogalmára építve, kidolgozható a reciprok egyenletek elméletének analogonja. Javasoljuk, hogy az Olvasó ez utóbbit gyakorlatként dolgozza ki.

Példák

15. Oldjuk meg a

$$7x^3+4x+1 \equiv 0 \pmod{35}$$

kongruenciát!

Megoldás:

A vizsgált kongruencia a

$$7x^2+4x+1 \equiv 0 \pmod{5} \tag{49}$$

és

$$7x^3+4x+1 \equiv 0 \pmod{7} \tag{50}$$

kongruenciák megoldására redukálható.

(49)-cel nyilván ekvivalens az alábbi kongruencia:

$$f(x) = 2x^3-x+1 \equiv 0 \pmod{5}.$$

E kongruencia megoldásainak meghatározása céljából számítsuk ki $f(x)$ értékét $x=-2, -1, 0, 1, 2$ esetén:

$$f(-2) = 2\cdot(-2)^3-(-2)+1 = -16+2+1 = -13 \not\equiv 0 \pmod 5,$$

$$f(-1) = 2\cdot(-1)^3-(-1)+1 = -2+1+1 = 0 \equiv 0 \pmod 5,$$

$$f(0) = 2\cdot 0^3-0+1 = 1 \not\equiv 0 \pmod 5,$$

$$f(1) = 2\cdot 1^3-1+1 = 2 \not\equiv 0 \pmod 5$$

és

$$f(2) = 2\cdot 2^3-2+1 = 16-2+1 = 15 \equiv 0 \pmod 5.$$

Így

(51) $x \equiv -1 \pmod 5$

és

(52) $x \equiv 2 \pmod 5$

megoldásai (49)-nek; minthogy a $-2, -1, 0, 1, 2$ számok teljes maradékrendszert alkotnak modulo 5, több megoldás nincs.

(50) ekvivalens az alábbi kongruenciával:

$$-3x+1 \equiv 0 \pmod 7,$$

vagyis

$$3x \equiv 1 \pmod 7.$$

Helyettesítsük a jobb oldalon álló 1-et a vele modulo 7 kongruens -6-tal:

$$3x \equiv 1 = 7-6 \equiv -6 \pmod 7.$$

Mindkét oldalt 3-mal osztva:

(53) $x \equiv -2 \pmod 7.$

Így a vizsgált kongruencia összes megoldásainak meghatározása céljából az (51)-ből és (53)-ból, ill. az (52)-ből és (53)-ból álló lineáris kongruencia rendszert kell megoldanunk.

Ha x kielégíti (53)-at, akkor

(54) $x = -2+7t$

alakban írható. (51)-be helyettesítve:

$$-2+7t \equiv -1 \pmod 5,$$

vagyis

$$2t \equiv 1 \equiv 6 \pmod 5.$$

2-vel osztva:

$$t \equiv 3 \pmod 5.$$

Így t egy lehetséges értéke $t=3$, ahonnan (54)-be helyettesítve nyerjük, hogy

$$x = -2+7\cdot 3 = 19.$$

Az (51)-ből és (53)-ból álló kongruencia-rendszer egy megoldása tehát $x=19$. Mivel a modulusok, azaz 5 és 7 relatív prímek, a megoldások egy modulo $5\cdot 7=35$ maradékosztály elemei. Így az (51)-ből és (53)-ból álló rendszer összes megoldásai:

(55) $x \equiv 19 \pmod{35}$.

Továbbá (54)-ből (52)-be helyettesítve:

$$-2+7t \equiv 2 \pmod 5,$$

vagyis

$$2t \equiv 4 \pmod 5.$$

Innen

$$t \equiv 2 \pmod 5,$$

tehát (54) szerint az (52)-ből és (54)-ből álló kongruencia-rendszer egy megoldása

$$x = -2+7t = -2+7\cdot 2 = 12.$$

Így e rendszer összes megoldásai:

(56) $x \equiv 12 \pmod{35}$.

Végeredményben tehát (55) és (56) adja az eredeti feladat összes megoldásait.

16. Oldjuk meg az

$$f(x) = x^3-x^2-1 \equiv 0 \pmod{27}$$

kongruenciát!

Megoldás:

Minthogy $27=3^3$, x-et

(57) $x = t+3u+3^2v$

alakban keressük. t meghatározása céljából az

$$f(t) = t^3-t^2-1 \equiv 0 \pmod 3$$

kongruenciát kell megoldanunk. $t=-1, 0, +1$-et helyettesítve:

$$f(-1) = (-1)^3-(-1)^2-1 = -1-1-1 = -3 \equiv 0 \pmod 3,$$

$$f(0) = 0^3-0^2-1 = -1 \not\equiv 0 \pmod 3$$

és

$$f(1) = 1^3-1^2-1 = -1 \not\equiv 0 \pmod 3.$$

Így $t=-1$ egy lehetséges megoldás. (57)-be helyettesítve:

(58) $x = -1+3u+3^2v.$

u meghatározása céljából az

$$f(-1+3u) = (-1+3u)^3-(-1+3u)^2-1 \equiv 0 \pmod 9$$

kongruenciát kell megoldanunk, vagyis (a 9-cel osztható tagokat elhagyva):

$$(-1)-(1-6u)-1 = 6u-3 \equiv 0 \pmod 9.$$

3-mal osztva (beleértve a modulust is):

$$2u-1 \equiv 0 \pmod 3,$$

vagyis

$$2u \equiv 1 \equiv 4 \pmod 3.$$

Innen

$$u \equiv 2 \pmod 3,$$

így u-t választhatjuk $u=2$-nek. (58)-ba helyettesítve:

(59) $x = -1+3\cdot 2+3^2v = 5+9v.$

Végül v értékét az

$$f(x) = f(5+9v) = (5+9v)^3-(5+9v)^2-1 \equiv 0 \pmod{27}$$

kongruenciából határozhatjuk meg. A 27-tel osztható tagokat elhagyva:

$$125-(25+90v)-1 = 99-90v \equiv 0 \pmod{27}.$$

9-cel osztva (a modulust is):

$$11-10v \equiv 0 \pmod 3,$$

vagyis

$$10v \equiv 11 \pmod 3,$$

$$v \equiv 2 \pmod 3.$$

Így $v=2$ választható. (59)-be helyettesítve:

$$x = 5+9v = 5+9\cdot 2 = 23.$$

A vizsgált kongruenciának tehát

$$x \equiv 23 \pmod{27}$$

megoldása. Minthogy t, u és v értéke modulo 3 egyértelműen adódott, a kongruenciának több megoldása nincs.

17. Oldjuk meg a

$$46x^{20}-54x^{13}+34x^9-27x^5+17x \equiv 0 \pmod{7}$$

kongruenciát!

Megoldás:

Az együtthatókat modulo 7 redukálva:

$$-3x^{20}+2x^{13}-x^9+x^5+3x^2 \equiv 0 \pmod{7}. \tag{60}$$

A Fermat-tétel (13) alakját alkalmazva $p=7$ esetén:

$$x^7 \equiv x \pmod{7}.$$

Így (60)-ból:

$$-3x^{20}+2x^{13}-x^9+x^5+3x^2 =$$

$$= -3(x^7)^2\cdot x^6+2x^7\cdot x^6-x^7\cdot x^2+x^5+3x^2 \equiv$$

$$\equiv -3x^2\cdot x^6+2x\cdot x^6-x\cdot x^2+x^5+3x^2 = -3x\cdot x^7+2x^7-x^3+x^5+3x^2 \equiv$$

$$\equiv -3x\cdot x+2x-x^3+x^5+3x^2 = x^5-x^3+2x = x(x^4-x^2+2) \equiv 0 \pmod{7}.$$

Ez a kongruencia akkor és csak akkor teljesül, ha

$$x \equiv 0 \pmod{7} \tag{61}$$

vagy

$$f(x) = x^4-x^2+2 \equiv 0 \pmod{7}. \tag{62}$$

Ez utóbbi kongruencia megoldásait keresve, modulo 7 teljes maradékrendszer elemeit, így például a $-3, -2, -1, 0, 1, 2, 3$ számokat kell helyettesítenünk. Azonban $x=0$-ról (61) szerint tudjuk, hogy megoldás, továbbá a (62)-ben álló $f(x)$ polinom páros (vagyis $f(-x)=f(x)$), és így elég csak az $x=1, 2, 3$ értékeket helyettesíteni:

$$f(1) = f(-1) = 1^4-1^2+2 = 2 \not\equiv 0 \pmod{7},$$

$$f(2) = f(-2) = 2^4-2^2+2 = 16-4+2 = 14 \equiv 0 \pmod{7}.$$

és

$$f(3) = f(-3) = 3^4 - 3^2 + 2 = (3^2)^2 - 9 + 2 = 9^2 - 9 + 2 \equiv$$

$$\equiv 2^2 - 2 + 2 = 4 \not\equiv 0 \pmod 7,$$

tehát a vizsgált kongruencia megoldásai

$$x \equiv -2 \pmod 7,$$

$$x \equiv 2 \pmod 7,$$

valamint (61) szerint

$$x \equiv 0 \pmod 7.$$

5. BINOM KONGRUENCIÁK. PRIMITÍV GYÖKÖK

Binom kongruencián

(63) $ax^k \equiv b \pmod m$

alakú, magasabbfokú kongruenciát értünk, ahol a, b adott egész számok, k, m adott természetes számok. Az ilyen alakú kongruenciák az előző pontban tárgyalt módon visszavezethetők arra az esetre, amikor a modulus prímszám. Ha itt x^k helyére y-t írunk, y-ra lineáris kongruenciát nyerünk; e kongruenciából y a 3. pontban ismertetett módszerek valamelyikével kifejezhető. Így végeredményben a (63) típusú kongruenciák vizsgálata visszavezethető az

(64) $x^k \equiv a \pmod p$

alakú kongruenciákéra. Ezért e pontban csak ez utóbbi típusú kongruenciákkal fogunk foglalkozni.

Először az $a = 1$ speciális esettel, az

(65) $x^k \equiv 1 \pmod p$

alakú kongruenciákkal foglalkozunk. Itt a megoldhatóság nyilvánvaló, a kérdéses csupán a megoldásszám. Bizonyítható, hogy a (65) kongruencia megoldásszáma k és $p-1$ legnagyobb közös osztójával egyenlő.

Mielőtt az általánosabb (64) kongruencia vizsgálatára rátérnénk, be kell vezetnünk a rend, majd a primitív gyök fogalmát.

Legyen p tetszőleges prímszám, a pedig p-hez relatív prím egész szám. A legkisebb olyan k természetes számot, melyre

(66) $a^k \equiv 1 \pmod{p}$

teljesül, az a szám *rendjének* nevezzük *modulo* p, és $o_p(a)$-val, vagy — ha ez nem okoz félreértést — röviden $o(a)$-val jelöljük. ($(a, p)=1$ esetén (66)-ot kielégítő k természetes szám a Fermat-tétel szerint létezik, tehát a definíció nem üres. $p|a$ esetén viszont ilyen k természetes szám nyilván nem létezik; erre az esetre nem definiáljuk a rend fogalmát.)

A rend legfontosabb tulajdonságai:

A) A (66) kongruencia adott a esetén akkor és csak akkor teljesül valamely k természetes számra, ha $o(a)|k$. (L. a 61. feladatot.)

Innen a Fermat-tételre tekintettel következik, hogy

B) $(a, p)=1$ esetén $o(a)|p-1$.

C) $o(a), o(b)=1$ esetén $o(ab)=o(a)o(b)$.

D) $k|p-1$ esetén létezik olyan a egész szám, melynek rendje k.

A *D)* tulajdonságból következik ($k=p-1$-gyel alkalmazva azt), hogy létezik olyan g egész szám, melynek rendje $p-1$. Ha valamely g egész szám rendje $p-1$, akkor g-t *modulo* p *primitív gyöknek* mondjuk. Az a tény, hogy létezik modulo p primitív gyök, nagy segítséget nyújt binom kongruenciák megoldása során.

A definícióból könnyen levezethető (felhasználva a rend *A)* tulajdonságát), hogy

$$g^k \equiv g^l \pmod{p}$$

akkor és csak akkor teljesül valamely k, l nemnegatív egész számokra, ha

$$k \equiv l \pmod{p-1}.$$

Igazolható az is, hogy a primitív gyök fent adott definíciója ekvivalens az alábbival:

Ha valamely g egész számra a $g, g^2, g^3, \ldots, g^{p-1}$ számok redukált maradékrendszert alkotnak modulo p, akkor g-t modulo p primitív gyöknek mondjuk.

Ebből a definícióból viszont következik, hogy $(a, p) = 1$ esetén létezik olyan, egyértelműen meghatározott t egész szám, melyre

$$(67) \quad g^t \equiv a \pmod{p}$$

és

$$1 \leqq t \leqq p-1$$

teljesül. Ezt a t számot az a szám g *alapú indexének* nevezzük (modulo p), (és $\overset{g}{\mathrm{ind}}_p\, a$-val, vagy — ha ez nem okozhat félreértést — röviden $\overset{g}{\mathrm{ind}}\, a$-val,) vagy még rövidebben $\mathrm{ind}\, a$-val jelöljük. Ezt a jelölést alkalmazva, (67)-et a következő alakban írhatjuk:

$$g^{\overset{g}{\mathrm{ind}}_p a} \equiv a \pmod{p}.$$

Könnyen igazolhatók az index alábbi tulajdonságai:

A) Ha az a szám modulo p redukált maradékrendszeren fut végig, akkor $\overset{g}{\mathrm{ind}}_p\, a$ az $1, 2, \ldots, p-1$ értékeket veszi fel.

B) Ha továbbá a és b p-hez relatív prím egész számok, k tetszőleges természetes szám, akkor

$$(68) \quad \mathrm{ind}\, ab \equiv \mathrm{ind}\, a + \mathrm{ind}\, b \pmod{p-1}$$

és

$$(69) \quad \mathrm{ind}\, a^k \equiv k\, \mathrm{ind}\, a \pmod{p-1}.$$

Megjegyezzük, hogy a (67), (68) és (69) összefüggések szerint az indexszel való számolás szabályai sok szempontból emlékeztetnek a logaritmusfüggvény tulajdonságaira.

Ismerve egy a egész szám indexét (bármely g alap esetén), a rendje könnyen meghatározható, amennyiben

$$(70) \quad \mathrm{o}(a) = \frac{p-1}{(\mathrm{ind}\, a, p-1)}.$$

Innen levezethető a rend $D)$ tulajdonságának következő, élesebb alakja:

$k|p-1$ esetén az $o(a)=k$ és $1 \leqq a \leqq p-1$ feltételeket kielégítő a egész számok száma $\varphi(k)$. Speciálisan, $k=p-1$-et választva, nyerjük, hogy egy modulo p redukált maradékrendszernek $\varphi(p-1)$ olyan eleme van, amelyik primitív gyök modulo p.

Visszatérünk a (64) kongruenciára. Ha valamely a egész számra $(a, p)=1$ teljesül, és a (64) kongruencia megoldható, akkor a-t *k-adik hatványmaradéknak* mondjuk modulo p.

Valamely g primitív gyököt rögzítve, a (64) kongruencia a következő alakban írható:

$$g^{\overset{g}{\smile}\operatorname{ind} x^k} \equiv g^{\overset{g}{\smile}\operatorname{ind} a} \pmod{p}.$$

Ez viszont akkor és csak akkor teljesül, ha

$$\overset{g}{\smile}\operatorname{ind} x^k \equiv \overset{g}{\smile}\operatorname{ind} a \pmod{p-1},$$

vagyis

$$(71) \quad k \overset{g}{\smile}\operatorname{ind} x \equiv \overset{g}{\smile}\operatorname{ind} a \pmod{p-1}.$$

Ez lineáris kongruencia $\overset{g}{\smile}\operatorname{ind} x$-re nézve, mely akkor és csak akkor oldható meg, ha

$$(72) \quad (k, p-1) | \overset{g}{\smile}\operatorname{ind} a.$$

Így a (64) kongruencia $p \nmid a$ esetén akkor és csak akkor oldható meg, vagyis a akkor és csak akkor k-adik hatványmaradék modulo p, ha (72) teljesül. (71) megoldásszáma $(k, p-1)$, tehát ha (72) teljesül, akkor a (64) kongruencia megoldásszáma $(k, p-1)$.

Igazolható, hogy a (72) feltétel ekvivalens az alábbival:

$$(73) \quad a^{\frac{p-1}{(k,\, p-1)}} \equiv 1 \pmod{p}.$$

Így ez a feltétel is szükséges és elégséges feltétele annak, hogy az a szám k-adik hatványmaradék legyen modulo p.

Ez a módszer nem csupán a megoldhatóság és megoldásszám vizsgálatára, hanem egyúttal konkrét binom kongruenciák megoldására is alkalmas. Ha ugyanis adott egy p prímszám és egy g primitív gyök modulo p, akkor ezekhez könnyen elkészíthetünk egy ún. *indextáblázatot*, mely a modulo p redukált maradékrendszer egyes elemeinek g alapú indexét tünteti fel (sőt ilyen indextáblázatot készen találunk sok számelmélet tankönyvben). Ha már egyszer egy ilyen indextáblázat a rendelkezésünkre áll, akkor a fenti módszerrel bármely p modulusú binom kongruencia megoldása visszavezethető egy $p-1$ modulusú lineáris kongruencia megoldására. (L. a 19. és 20. példát.)

Példák

18. Határozzuk meg az 5 szám rendjét modulo 23.

Megoldás:

A 23 prímszám, tehát a rend *B)* tulajdonsága szerint $o_{23}(5)|23-1=22$. Így a rend 22 pozitív osztói, vagyis az 1, 2, 11, 22 számok közül kerül ki, tehát e számok közül kell a legkisebb olyan k számot meghatároznunk, melyre

$$5^k \equiv 1 \pmod{23}$$

teljesül.

Sorra $k=1, 2, 11$-et választva:

$$5^1 = 5 \not\equiv 1 \pmod{23},$$

$$5^2 = 25 \equiv 2 \not\equiv 1 \pmod{23},$$

$$5^{11} = (5^2)^5 \cdot 5 \equiv 2^5 \cdot 5 = 32 \cdot 5 \equiv 9 \cdot 5 = 45 \equiv 22 \not\equiv 1 \pmod{23}.$$

Tovább nem kell folytatnunk, hiszen már csak egy lehetőség van: $o_{23}(5)=22$ (az 5 szám tehát primitív gyök modulo 23).

19. Határozzuk meg a legkisebb olyan pozitív egész számot, amely primitív gyök modulo 17, és készítsünk ehhez indextáblázatot!

Megoldás:

A rend *B)* tulajdonsága szerint $(a, 17)=1$ esetén

$$o_{17}(a)|17-1 = 16 = 2^4.$$

Innen következik, hogy két eset lehetséges: vagy

$$o_{17}(a) = 16,$$

azaz a primitív gyök modulo 17; vagy pedig

$$o_{17}(a)|8,$$

és ekkor a nem primitív gyök modulo 17. Azonban ez utóbbi esetben a rend *A)* tulajdonsága szerint szükségképpen

(74) $a^8 \equiv 1 \pmod{17}$.

Az eddigiek szerint tehát $(a, 17)=1$ esetén a akkor és csak akkor primitív gyök modulo 17, ha (74) nem teljesül. Így a legkisebb olyan a pozitív egész számot kell meghatároznunk, melyre (74) nem teljesül (és amely relatív prím 17-hez). Számítsuk ki tehát sorra $a=2, 3, \ldots$ esetén a^8 legkisebb nemnegatív maradékát modulo 17:

$$2^8 = (2^4)^2 = 16^2 \equiv (-1)^2 = 1 \pmod{17},$$

$$3^8 = (3^2)^4 = 9^4 \equiv (-8)^4 = (8^2)^2 = 64^2 \equiv (-4)^2 = 16 \not\equiv 1 \pmod{17}$$

tehát a legkisebb primitív gyök (modulo 17) a 3.

Az indextáblázat elkészítése céljából számítsuk ki sorra $3^1, 3^2, \ldots, 3^{16}$ legkisebb nemnegatív maradékát (modulo 17):

$$3^1 \equiv 3 \pmod{17},$$

$$3^2 \equiv 9 \pmod{17},$$

$$3^3 = 27 \equiv 10 \pmod{17},$$

$$3^4 = 3 \cdot 3^3 \equiv 3 \cdot 10 = 30 \equiv 13 \pmod{17},$$

$$3^5 = 3 \cdot 3^4 \equiv 3 \cdot 13 = 39 \equiv 5 \pmod{17},$$

$$3^6 = 3 \cdot 3^5 \equiv 3 \cdot 5 = 15 \pmod{17},$$

$$3^7 = 3 \cdot 3^6 \equiv 3 \cdot 15 = 45 \equiv 11 \pmod{17},$$

$$3^8 = 3 \cdot 3^7 \equiv 3 \cdot 11 = 33 \equiv 16 \pmod{17},$$

$$3^9 = 3 \cdot 3^8 \equiv 3 \cdot 16 = 48 \equiv 14 \pmod{17},$$

$$3^{10} = 3 \cdot 3^9 \equiv 3 \cdot 14 = 42 \equiv 8 \pmod{17},$$

$$3^{11} = 3 \cdot 3^{10} \equiv 3 \cdot 8 = 24 \equiv 7 \pmod{17},$$

$$3^{12} = 3 \cdot 3^{11} \equiv 3 \cdot 7 = 21 \equiv 4 \pmod{17},$$

$$3^{13} = 3 \cdot 3^{12} \equiv 3 \cdot 4 = 12 \pmod{17},$$

$$3^{14} = 3 \cdot 3^{13} \equiv 3 \cdot 12 = 36 \equiv 2 \pmod{17},$$

$$3^{15} = 3 \cdot 3^{14} \equiv 3 \cdot 2 = 6 \pmod{17},$$

$$3^{16} = 3 \cdot 3^{15} \equiv 3 \cdot 6 = 18 \equiv 1 \pmod{17}.$$

Így az indextáblázat:

1. táblázat

$p=17$ $g=3$	Index	0	1	2	3	4	5	6	7	8	9
	0		3	9	10	13	5	15	11	16	14
	1	8	7	4	12	2	6	1			

(Ha például azt az a egész számot keressük, melyre

$$\overset{3}{\smile}\mathrm{ind}_{17} a = 13$$

és

$$1 \leqq a \leqq 16$$

teljesül, akkor a táblázat első oszlopában kikeressük a 13 első számjegyét, az 1-et, első sorában pedig 13 második számjegyét, a 3-at; a megfelelő sor, ill. oszlop kereszteződésénél álló szám, vagyis jelen esetben 12 adja meg a értékét.)

Célszerű a táblázatot az a szám értékei szerint átrendezve is elkészítenünk:

2. táblázat

$p=17$ $g=3$	Szám	0	1	2	3	4	5	6	7	8	9
	0		16	14	1	12	5	15	11	10	2
	1	3	7	13	4	9	6	8			

20. Az előző példa megoldása során készített indextáblázatokat felhasználva, oldjuk meg a

$$7x^{10} \equiv 12 \pmod{17}$$

kongruenciát!

Megoldás:

Mindkét oldalt a $g=3$ primitív gyök hatványaként felírva:

$$3^{\overset{3}{\smile}\mathrm{ind}\, 7x^{10}} \equiv 3^{\overset{3}{\smile}\mathrm{ind}\, 12} \pmod{17},$$

ami ekvivalens a

$$\overset{3}{\smile}\mathrm{ind}\, 7x^{10} \equiv \overset{3}{\smile}\mathrm{ind}\, 12 \pmod{16},$$

vagyis a

$$\overset{3}{\underset{\smile}{\text{ind}}}\, 7 + 10\, \overset{3}{\underset{\smile}{\text{ind}}}\, x \equiv \overset{3}{\underset{\smile}{\text{ind}}}\, 12 \pmod{16}$$

kongruenciával. A 2. táblázat szerint $\overset{3}{\underset{\smile}{\text{ind}}}\, 7 = 11$ és $\overset{3}{\underset{\smile}{\text{ind}}}\, 12 = 13$, tehát innen

$$11 + 10\, \overset{3}{\underset{\smile}{\text{ind}}}\, x \equiv 13 \pmod{16},$$

vagyis

$$(75) \qquad 10\, \overset{3}{\underset{\smile}{\text{ind}}}\, x \equiv 2 \pmod{16}.$$

Ez $\overset{3}{\underset{\smile}{\text{ind}}}\, x$-re lineáris kongruencia, mely megoldható, hiszen $(10, 16) = 2 | 2$. A kongruencia mindkét oldalát és a modulust is $(10, 16) = 2$-vel osztva, (75)-tel ekvivalens kongruenciát nyerünk:

$$5\, \overset{3}{\underset{\smile}{\text{ind}}}\, x \equiv 1 = 16 - 15 \equiv -15 \pmod{8},$$

ezt 5-tel osztva:

$$\overset{3}{\underset{\smile}{\text{ind}}}\, x \equiv -3 \equiv 5 \pmod{8}.$$

A (75) lineáris kongruencia összes, 1 és 16 közé eső megoldásai tehát

$$\overset{3}{\underset{\smile}{\text{ind}}}\, x = 5$$

és

$$\overset{3}{\underset{\smile}{\text{ind}}}\, x = 5 + 8 = 13.$$

Innen az 1. táblázat felhasználásával nyerjük, hogy a vizsgált kongruencia összes megoldásai:

$$x \equiv 5 \pmod{17}$$

és

$$x \equiv 12 \pmod{17}.$$

6. KVADRATIKUS MARADÉKOK

A (64) kongruenciának különösen fontos speciális esete a $k = 2$ speciális eset. Ha $(a, p) = 1$ és az

$$(76) \qquad x^2 \equiv a \pmod{p}$$

kongruencia megoldható, akkor a-t *kvadratikus maradéknak*, ha $(a, p)=1$ és (76) nem oldható meg, akkor a-t *kvadratikus nem-maradéknak* mondjuk modulo p.

Az előző pontban mondottakat (így konkrétan a (72) és (73) formulákat) specializálva erre az esetre, nyerjük, hogy $p>2$, $(a, p)=1$ esetén a akkor és csak akkor kvadratikus maradék modulo p, ha $\underset{g}{\text{ind}}\, a$ páros. Egy másik szükséges és elégséges feltétel az, hogy

$$(77) \quad a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

teljesüljön. Továbbá egy modulo p redukált maradékrendszer elemei között $\frac{p-1}{2}$ számú kvadratikus maradék van (vagyis egy redukált maradékrendszer elemeinek *fele* kvadratikus maradék).

Ha tehát $(a, p)=1$ és a kvadratikus nem-maradék modulo p, akkor

$$(78) \quad a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}.$$

A Fermat-tétel szerint

$$a^{p-1} \equiv 1 \pmod{p},$$

vagyis

$$a^{p-1}-1 = \left(a^{\frac{p-1}{2}}\right)^2 - 1 = \left(a^{\frac{p-1}{2}}-1\right)\left(a^{\frac{p-1}{2}}+1\right) \equiv 0 \pmod{p}.$$

Innen következik, hogy

$$(79) \quad a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

vagy

$$(80) \quad a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Minthogy (78) szerint (79) most nem állhat fenn, szükségképpen (80) teljesül.

$p>2$, $(a, p)=1$ esetén tehát a akkor és csak akkor kvadratikus nem-maradék modulo p, ha (80) teljesül. (Az előbbiek szerint egy másik szükséges és elégséges feltétel az, hogy $\operatorname{ind}_g a$ páratlan legyen.)

Azt a kritériumot, mely szerint $p>2$, $(a, p)=1$ esetén a aszerint kvadratikus maradék vagy nem-maradék, hogy (77) vagy (80) teljesül-e, *Euler-lemmának* nevezzük.

Minthogy az Euler-lemma konkrét számokra való alkalmazása meglehetősen sok számolással jár, célszerű olyan módszereket keresnünk, melyek révén kevesebb számolással is eldönthető, hogy egy adott a egész szám kvadratikus maradék-e vagy sem. Ehhez nyújt segítséget az ún. Legendre-szimbólum.

Legyen p tetszőleges prímszám, a pedig a p-hez relatív prím egész szám. Ekkor az $\left(\frac{a}{p}\right)$ *Legendre-szimbólum* értéke definíció szerint $+1$, ha a kvadratikus maradék, és -1, ha a kvadratikus nem-maradék modulo p. (Tehát $p|a$ esetén $\left(\frac{a}{p}\right)$-t nem definiáljuk!)

Könnyen igazolhatók a Legendre-szimbólum alábbi tulajdonságai:

A) Ha $(a, p)=(b, p)=1$ és

$$a \equiv b \pmod{p},$$

akkor

$$\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right).$$

B) $(a, p)=1$ esetén

$$\left(\frac{a^2}{p}\right)=+1,$$

speciálisan

$$\left(\frac{1}{p}\right)=+1.$$

C) $p > 2$, $(a, p) = 1$ esetén

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

(Ez a tulajdonság könnyen következik az Euler-lemmából.)

D) $(a, p) = (b, p) = 1$ esetén

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right),$$

vagyis a Legendre-szimbólum multiplikatív. (Az előző tulajdonság következménye.)

Ennek az összefüggésnek az a jelentősége, hogy ismételt alkalmazása révén valamely $\left(\frac{a}{p}\right)$ Legendre-szimbólum meghatározása visszavezethető $\left(\frac{q}{p}\right)$ — ahol *q prímszám* — alakú Legendre-szimbólumok meghatározására.

E) $p > 2$ esetén

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}},$$

tehát az

$$x^2 \equiv -1 \pmod{p}$$

kongruencia akkor és csak akkor oldható meg, ha $p = 2$ vagy p $4k+1$ alakú. (A *C)* tulajdonság következménye. — L. még a 23. példát.)

A fentieknél valamivel nehezebb az alábbi, *Gauss-lemma* néven ismert tulajdonság bizonyítása:

F) Legyen $p > 2$, $(a, p) = 1$. Jelöljük az $a, 2a, 3a, \ldots, \frac{p-1}{2}a$ számok legkisebb nemnegatív maradékai közül a $\frac{p}{2}$-nél nagyobbak számát m-mel. Ekkor

$$\left(\frac{a}{p}\right) = (-1)^m.$$

Az *F)* tulajdonságból levezethető, hogy
G) $p>2$ esetén

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

vagy másképpen:

$$\left(\frac{2}{p}\right) = \begin{cases} +1, & \text{ha } p\ 8k-1 \text{ vagy } 8k+1 \text{ alakú,} \\ -1, & \text{ha } p\ 8k-3 \text{ vagy } 8k+3 \text{ alakú.} \end{cases}$$

Ugyancsak a Gauss-lemmát felhasználva igazolható az ún. *reciprocitási tétel* (melynek azonban számos más bizonyítása is ismeretes):

H) Ha p és q 2-nél nagyobb, egymástól különböző prímszámok, akkor

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Másképpen megfogalmazva:

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), & \text{ha } p \text{ és } q \text{ közül legalább az egyik } 4k+1 \text{ alakú;} \\ -\left(\frac{q}{p}\right), & \text{ha mind } p, \text{ mind } q\ 4k-1 \text{ alakú.} \end{cases}$$

(Ez a tulajdonság a legmélyebb az itt felsoroltak közül.)

Az *A)*, *B)*, *D)*, *E)*, *G)* és *H)* tulajdonságok ismételt alkalmazásával bármely $\left(\frac{a}{p}\right)$ Legendre-szimbólum értéke viszonylag gyorsan meghatározható. (L. a 22. példát.)

Megjegyezzük, hogy az általános kvadratikus (másodfokú) kongruenciák teljes négyzetté kiegészítéssel visszavezethetők

$$x^2 \equiv a \pmod{p}$$

típusú kongruenciákra. Ez utóbbiak megoldhatóságának vizsgálata az ebben a pontban, megoldása pedig az előző pontban ismertetett módszerrel történhet.

Példák

21. Állapítsuk meg az Euler-lemma segítségével, hogy az

$$x^2 \equiv 3 \pmod{23}$$

kongruencia megoldható-e?

Megoldás:

$$3^{\frac{p-1}{2}} = 3^{\frac{23-1}{2}} = 3^{11} = (3^3)^3 \cdot 3^2 = 27^3 \cdot 9 \equiv 4^3 \cdot 9 =$$

$$= 64 \cdot 9 \equiv (-5) \cdot 9 = -45 \equiv 1 \pmod{23},$$

tehát az Euler-lemma szerint a 3 kvadratikus maradék modulo 23, vagyis a vizsgált kongruencia megoldható.

22. Állapítsuk meg, hogy az

$$x^2 \equiv 280 \pmod{401}$$

kongruencia megoldható-e?

Megoldás:

Könnyen ellenőrizhető, hogy 401 prímszám. Így a $\left(\frac{280}{401}\right)$ Legendre-szimbólum értékét kell meghatároznunk. Rendre a *D)*, *G)*, *B)* tulajdonságokat alkalmazva:

$$\left(\frac{280}{401}\right) = \left(\frac{2 \cdot 140}{401}\right) = \left(\frac{2 \cdot 2 \cdot 70}{401}\right) = \left(\frac{2 \cdot 2 \cdot 2 \cdot 5 \cdot 7}{401}\right) =$$

$$= \left(\frac{2}{401}\right)\left(\frac{2^2}{401}\right)\left(\frac{5}{401}\right)\left(\frac{7}{401}\right) = (+1) \cdot (+1) \cdot \left(\frac{5}{401}\right)\left(\frac{7}{401}\right) =$$

$$= \left(\frac{5}{401}\right)\left(\frac{7}{401}\right).$$

A kvadratikus reciprocitási tételt (*H)* tulajdonság) alkalmazva mindkét tényezőre:

$$\left(\frac{280}{401}\right) = \left(\frac{5}{401}\right)\left(\frac{7}{401}\right) =$$

$$= \left(\frac{401}{5}\right) \cdot (-1)^{\frac{401-1}{2} \cdot \frac{5-1}{2}} \cdot \left(\frac{401}{7}\right) \cdot (-1)^{\frac{401-1}{2} \cdot \frac{7-1}{2}} =$$

$$= \left(\frac{401}{5}\right) \cdot (-1)^{200 \cdot 2} \cdot \left(\frac{401}{7}\right) \cdot (-1)^{200 \cdot 3} = \left(\frac{401}{5}\right) \cdot \left(\frac{401}{7}\right).$$

Rendre az *A)*, *B)* majd *G)* tulajdonságokat alkalmazva:

$$\left(\frac{280}{401}\right) = \left(\frac{401}{5}\right)\left(\frac{401}{7}\right) = \left(\frac{80\cdot 5+1}{5}\right)\left(\frac{57\cdot 7+2}{7}\right) =$$

$$= \left(\frac{1}{5}\right)\left(\frac{2}{7}\right) = (+1)\cdot(+1) = +1,$$

tehát a 280 kvadratikus maradék modulo 401, és így a vizsgált kongruencia megoldható.

23. A Wilson-tételt (13. példa) felhasználva, igazoljuk, hogy ha p $4k+1$ alakú prímszám, akkor az

(81) $\quad x^2 \equiv -1 \pmod{p}$

kongruencia megoldásai

$$x \equiv \pm\left(\frac{p-1}{2}\right)! \pmod{p}.$$

Megoldás:

A fokszám-tétel szerint a kongruenciának legfeljebb két megoldása van. Másrészt, ha a $-\left(\frac{p-1}{2}\right)!$ és $+\left(\frac{p-1}{2}\right)!$ számok kielégítik a (81) kongruenciát, akkor ezek nyilván lényegesen különböző (inkongruens) megoldások; ezeken kívül tehát több (lényegesen különböző) megoldás nem létezik. Így elég igazolni, hogy e két szám kielégíti a (81) kongruenciát.

A Wilson-tétel szerint

(82) $\quad (p-1)! \equiv -1 \pmod{p}$

(tetszőleges p prímszámra). A bal oldal a következőképpen alakítható át:

(83) $$(p-1)! = 1\cdot 2\cdot\ldots\cdot\frac{p-1}{2}\cdot\left(\frac{p-1}{2}+1\right)\cdot\ldots\cdot(p-2)\cdot(p-1) =$$

$$= \left[1\cdot 2\cdot\ldots\cdot\frac{p-1}{2}\right]\cdot\left[\left(p-\frac{p-1}{2}\right)\cdot\ldots\cdot(p-2)\cdot(p-1)\right] \equiv$$

$$\equiv \left(\frac{p-1}{2}\right)!\left(-\frac{p-1}{2}\right)\cdot\ldots\cdot(-2)\cdot(-1) = \left(\frac{p-1}{2}\right)!(-1)^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! =$$

$$= (-1)^{\frac{p-1}{2}}\left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}.$$

(82)-ből és (83)-ból nyerjük, hogy

$$(-1)^{\frac{p-1}{2}}\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod{p}.$$

Mindkét oldalt megszorozva $(-1)^{\frac{p-1}{2}}$-vel:

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

Mivel p — feltevésünk szerint — $4k+1$ alakú, a jobb oldalon -1 kitevője $\frac{(4k+1)+1}{2}=2k+1$ alakú, vagyis páratlan. Így ez a kongruencia a következő alakban írható:

$$\left[\pm\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod{p},$$

ami azt jelenti, hogy $-\left(\frac{p-1}{2}\right)!$ és $+\left(\frac{p-1}{2}\right)!$ valóban kielégíti a (81) kongruenciát, és ezzel az állítást igazoltuk.

FELADATOK

1. Határozzuk meg a 17, -19, 24, -16, 31 számok

a. legkisebb nemnegatív,

b. abszolút legkisebb

maradékait modulo 11.

c. Állapítsuk meg, hogy a felsorolt számok közül melyek kongruensek egymással modulo 11?

2. Állapítsuk meg, hogy a -13, 21, 32, -9 számsorozat kiegészíthető-e teljes maradékrendszerré modulo 7? Ha a válasz igenlő, adjunk is meg egy ilyen teljes maradékrendszert!

3. Igazoljuk a kongruenciák *C)* tulajdonságát (a tranzitivitást)!

4. Igazoljuk a kongruenciák *G)* tulajdonságát!

5. Bizonyítsuk be, hogy ha egy p prímszámot 30-cal osztunk, akkor maradékul 1-et, vagy ismét prímszámot kapunk!

6. Oldjuk meg az 1. fejezet 20. feladatát kongruenciák felhasználásával!

7. Oldjuk meg az 1. fejezet 27. feladatát kongruenciák felhasználásával!

8. Oldjuk meg az 1. fejezet 30. feladatát kongruenciák felhasználásával!

9. Bizonyítsuk be, hogy ha m^2-m+1 és $2n^2+n-1$ oszthatók 3-mal, akkor $m-n$ is osztható 3-mal!

10. Állapítsuk meg, hogy $10^{10^{10}}$ milyen maradékot ad 101-gyel osztva?

11. Igazoljuk a 7-tel való oszthatóságra vonatkozó alábbi kritériumot:

A $b=a_n a_{n-1}\overset{10}{\smile}\ldots a_0$ természetes szám akkor és csak akkor osztható 7-tel, ha

$$7|(a_0+3a_1+2a_2)-(a_3+3a_4+2a_5)+\ldots=c.$$

12*. Legyen p 2-nél nagyobb prímszám. Milyen maradékot ad $\binom{2p}{p}$ p-vel osztva?

13. Legyenek a, b, c, d tetszőleges egész számok. Bizonyítsuk be, hogy az

$$(a-b)(a-c)(a-d)(b-c)(b-d)(c-d)$$

szorzat osztható 12-vel!

14. Bizonyítsuk be, hogy n számú egész szám közül mindig kiválaszthatók bizonyosak (legalább egy és esetleg mind; valamennyit legfeljebb egyszer vehetjük) úgy, hogy a kiválasztott számok összege osztható legyen n-nel!

15. Állapítsuk meg, hogy a 23, 17, -29 számsorozat kiegészíthető-e redukált maradékrendszerré modulo 10? Ha válasz igenlő, adjunk is meg egy ilyen redukált maradékrendszert!

16. Legyen p 2-nél nagyobb prímszám. Állapítsuk meg, hogy az $1\cdot 2, 2\cdot 3, 3\cdot 4, \ldots, (p-2)\cdot(p-1), (p-1)\cdot 1$ számok redukált maradékrendszert alkotnak-e modulo p?

17. Számítsuk ki $\varphi(450)$ értékét!

18. Oldjuk meg a

$$\varphi(3^x)=486$$

egyenletet!

19*. Bizonyítsuk be, hogy a $\varphi(n)$ számelméleti függvény multiplikatív (azaz ha m, n egymáshoz relatív prím természetes számok, akkor (8) teljesül)!

20. Az előző feladat állítását felhasználva, igazoljuk a $\varphi(n)$ függvény (10) alatti explicit alakját!

21. Tudjuk, hogy $\varphi(x)=840$ és $x=p^2q^2$, ahol p, q különböző prímszámok. Határozzuk meg x-et!

22. Legyen n tetszőleges természetes szám. Számítsuk ki az n-nél nem nagyobb, n-hez relatív prím természetes számok összegét!

23. Bizonyítsuk be, hogy ha m, n természetes számok, melyekre $m|n$, akkor $\varphi(m)|\varphi(n)$.

24. Bizonyítsuk be, hogy tetszőleges m, n természetes számokra

$$\varphi(mn) \geqq \varphi(m)\varphi(n).$$

25. Bizonyítsuk be, hogy ha m tetszőleges természetes szám, az $a_1, a_2, \ldots, a_{\varphi(m)}$ számok redukált maradékrendszert alkotnak modulo m és b az m-hez relatív prím egész szám, akkor a ba_1, $ba_2, \ldots, ba_{\varphi(m)}$ számok is redukált maradékrendszert alkotnak modulo m.

26. Az előző feladatot felhasználva, bizonyítsuk be az Euler-tételt!

27. Állapítsuk meg, hogy 247^{244} mennyi maradékot ad 23-mal osztva?

28. Bizonyítsuk be, hogy tetszőleges n természetes számra $42|n^7-n$.

29. Bizonyítsuk be, hogy ha az n egész szám nem osztható 11-gyel, akkor n^5-1 vagy n^5+1 osztható 11-gyel!

30. Bizonyítsuk be, hogy ha n tetszőleges egész szám, p tetszőleges prímszám, akkor $n^{p^p}-n$ osztható p-vel!

31. Határozzuk meg 403^{402} utolsó három számjegyét!

32. Bizonyítsuk be, hogy ha n a 10-hez relatív prím természetes szám, akkor létezik olyan többszöröse, melynek valamennyi számjegye 9-es!

33. Bizonyítsuk be, hogy ha n páratlan természetes szám, akkor $n|2^{n!}-1$.

34*. Bizonyítsuk be, hogy végtelen sok 10^n+3 (ahol n természetes szám) alakú összetett szám létezik!

35. Oldjuk meg a

$$26x \equiv 6 \pmod{68}$$

lineáris kongruenciát úgy, hogy lineáris diofantikus egyenletre vezetjük vissza!

36. Oldjuk meg a

$$19x \equiv 11 \pmod{24}$$

lineáris kongruenciát az Euler-tétel segítségével!

37. Állapítsuk meg, hogy az

a. $30x \equiv 39 \pmod{51}$,

b. $27x \equiv 33 \pmod{45}$,

c. $60x \equiv 30 \pmod{70}$

lineáris kongruenciák közül melyek oldhatók meg, és a megoldhatókat oldjuk is meg (tetszőleges módszerrel)!

38. Oldjuk meg a lehető legegyszerűbben az alábbi lineáris kongruenciákat:

a. $204x \equiv 139 \pmod{205}$,

b. $201x \equiv 118 \pmod{401}$,

c. $100x \equiv 123 \pmod{301}$.

39. Oldjuk meg a

$$3^8 x \equiv 23 \pmod{100}$$

lineáris kongruenciát!

40. Valamely x egész számról tudjuk, hogy x^{100} 10, x^{201} pedig 5 maradékot ad 67-tel osztva. Mennyi maradékot ad x 67-tel osztva?

41. Határozzuk meg 29^{3949} utolsó két számjegyét!

42. Legyen p 2-nél nagyobb prímszám. Bizonyítsuk be, hogy az

$$x^{p-2} \equiv a \pmod{p}$$

kongruencia minden a egész számra megoldható!

43. Oldjuk meg az

$$5x \equiv 3 \pmod 7,$$
$$3x \equiv 7 \pmod 8$$

lineáris kongruencia-rendszert!

44. Oldjuk meg a

$$7x \equiv 11 \pmod{12},$$
$$13x \equiv 17 \pmod{21}$$

lineáris kongruencia-rendszert!

45. Oldjuk meg az

$$x \equiv 3 \pmod 5,$$
$$x \equiv 1 \pmod 6,$$
$$x \equiv 2 \pmod 7$$

lineáris kongruencia-rendszert!

46. Bizonyítsuk be, hogy bármely x egész szám kielégíti az alábbi kongruenciák valamelyikét:

$$x \equiv 0 \pmod 2,$$
$$x \equiv 0 \pmod 3,$$
$$x \equiv 1 \pmod 4,$$
$$x \equiv 3 \pmod 8,$$
$$x \equiv 7 \pmod{12},$$
$$x \equiv 23 \pmod{24}.$$

(Az ilyen tulajdonságú kongruencia-rendszereket *lefedő kongruencia-rendszereknek* nevezzük.)

47. Egy négyjegyű természetes szám 72-vel osztva 46, 127-tel osztva 97 maradékot ad. Melyik ez a szám?

48. Bizonyítsuk be, hogy tetszőleges k természetes számhoz található k számú, egymást követő természetes szám, melyek egyike sem teljes hatvány (azaz egyikük sem természetes szám 1-nél nagyobb egész kitevőjű hatványa)!

49. Oldjuk meg az

$$f(x) = x^3 + x^2 + 2x - 2 \equiv 0 \pmod{20}$$

kongruenciát!

50. Oldjuk meg az

$$f(x) = x^3 - 2x^2 + 3x + 2 \equiv 0 \pmod{25}$$

kongruenciát!

51. Oldjuk meg a

$$33x^{18} - 22x^{16} + 21x^{11} + 17x^4 - 14 \equiv 0 \pmod{5}$$

kongruenciát!

52*. Bizonyítsuk be a magasabbfokú kongruenciák fokszámtételét (a fokszámra vonatkozó teljes indukcióval): bármely n-edfokú prím modulusú kongruencia megoldásszáma legfeljebb n (ahol n tetszőleges természetes szám).

53*. Bizonyítsuk be a Wilson-tételt (13. példa) az

$$(84) \quad f(x) = (x^{p-1} - 1) - (x-1)(x-2)\ldots[x-(p-1)] \equiv 0 \pmod{p}$$

kongruencia konstans tagját vizsgálva, és felhasználva az előző feladatban említett fokszámtételt!

54. Hány (lényegesen különböző) megoldása van az

$$x^{10} \equiv 1 \pmod{47}$$

kongruenciának? Oldjuk is meg ezt a kongruenciát!

55. Határozzuk meg a 4 szám rendjét modulo 47.

56. Tudjuk, hogy

$$21^{21} \equiv 1 \pmod{43},$$

$$21^{28} \equiv 1 \pmod{43}.$$

Határozzuk meg ennek alapján 21 rendjét modulo 43.

57. Legyen p tetszőleges prímszám, a egész szám, melyre $(a, p) = 1$, és legyen k természetes szám, melyre $k | o(a)$. Bizonyít-

suk be, hogy

$$o(a^k) = \frac{o(a)}{k}.$$

58. Igazoljuk a rend *A)* tulajdonságát!

59. Legyen p tetszőleges prímszám, a és a^* olyan egész számok, melyekre

$$(85) \quad aa^* \equiv 1 \pmod{p}$$

teljesül (azaz a^* multiplikatív inverze a-nak modulo p). Bizonyítsuk be, hogy ekkor

$$o_p(a) = o_p(a^*).$$

60. Legyen p 2-nél nagyobb prímszám, a pedig a p-hez relatív prím egész szám. Bizonyítsuk be, hogy ha $o_p(a)$ páratlan, akkor nem létezik olyan x nemnegatív egész szám, melyre

$$(86) \quad a^x + 1 \equiv 0 \pmod{p}.$$

61*. Legyen p 2-nél nagyobb prímszám, $a > 1$ természetes szám. Bizonyítsuk be, hogy $a^p - 1$ páratlan prímosztói vagy osztói $(a-1)$-nek is, vagy pedig $2pk+1$ (ahol k egész szám) alakúak!

62*. Legyen n tetszőleges természetes szám. Bizonyítsuk be, hogy $2^{2^n}+1$ prímosztói $2^{n+1}k+1$ alakúak! (Vö. az 1. fejezet 48. feladatával.)

63*. Bizonyítsuk be az előző feladatot felhasználva, hogy a $2^{2^5}+1$ Fermat-szám (l. az 1. fejezet 48. feladatát) összetett szám!

64. Állapítsuk meg, hogy melyek oldhatók meg az

a. $x^5 \equiv 9 \pmod{13}$,

b. $x^{10} \equiv 11 \pmod{13}$,

c. $x^9 \equiv 8 \pmod{13}$

kongruenciák közül? A megoldhatóknak hány (lényegesen különböző) megoldásuk van?

65. Legyen p 2-nél nagyobb prímszám. Az $1, 2, \ldots, p-1$ számok közül melyek p-edik hatványmaradékok modulo p?

66. Legyen p tetszőleges prímszám, k tetszőleges természetes szám. Bizonyítsuk be, hogy

a. ha az a, b egész számok k-adik hatványmaradékok modulo p, akkor a szorzatuk is az;

b. ha az a egész szám k-adik hatványmaradék modulo p, de a b egész szám nem az, akkor a szorzatuk sem az!

67. Legyen p tetszőleges prímszám, k páratlan természetes szám. Bizonyítsuk be, hogy ha a k-adik hatványmaradék modulo p, akkor $-a$ is az!

68. Legyen p tetszőleges prímszám, és legyenek a, a^* olyan egész számok, melyekre (85) teljesül (azaz legyen a^* multiplikatív inverze a-nak). Bizonyítsuk be, hogy ha valamely k természetes számra a k-adik hatványmaradék modulo p, akkor a^* is az!

69. Tudjuk, hogy

$$10^{24} \equiv -1 \pmod{17}.$$

Ennek alapján igazoljuk, hogy 10 primitív gyök modulo 17.

70. Milyen p prímszámokra primitív gyök a -1 modulo p?

71. Legyen p tetszőleges prímszám, a egész szám, k természetes szám. Bizonyítsuk be, hogy ha a^k primitív gyök modulo p, akkor a is az!

72. Legyen p tetszőleges prímszám, g primitív gyök modulo p. Bizonyítsuk be, hogy ha a g^* egész számra

$$gg^* \equiv 1 \pmod{p}$$

teljesül (vagyis g^* multiplikatív inverze g-nek), akkor g^* is primitív gyök modulo p.

73*. Legyen p $4k+1$ alakú prímszám, g primitív gyök modulo p. Bizonyítsuk be, hogy ekkor $-g$ is primitív gyök modulo p.

74*. Legyen p 2^n+1 alakú prímszám (ún. Fermat-prím; l. az 1. fejezet 48. feladatát), ahol n 2-nél nagyobb természetes szám. Bizonyítsuk be, hogy a 2 *nem* primitív gyök modulo p.

75*. Legyen p tetszőleges prímszám, k tetszőleges természetes szám. Mennyi maradékot ad p-vel osztva a $\sum_{i=1}^{p-1} i^k$ összeg?

76. Igazolható, hogy ha p 2-nél nagyobb prímszám, g primitív gyök modulo p, akkor

$$g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

(l. a 97. feladatot). Bizonyítsuk be a Wilson-tételt (13. példa), a primitív gyök fogalmát és ezt az összefüggést felhasználva!

77. A 19. példa megoldása során készített indextáblázatokat felhasználva, oldjuk meg az alábbi kongruenciákat:

a. $9x \equiv 14 \pmod{17}$,

b. $x^{11} \equiv 6 \pmod{17}$,

c. $11x^{10} \equiv 5 \pmod{17}$.

78. A 19. példa megoldása során készített indextáblázatokat felhasználva, oldjuk meg az alábbi kongruenciákat:

a. $5^x \equiv 12 \pmod{17}$,

b. $5 \cdot 6^x \equiv 7 \pmod{17}$.

79. Legyen $p>2$ prímszám, g primitív gyök modulo p. Bizonyítsuk be, hogy ha az a, a^* egész számokra (85) teljesül (vagyis a^* multiplikatív inverze a-nak), akkor

$$\underset{g}{\mathrm{ind}}_p\, a + \underset{g}{\mathrm{ind}}_p\, a^* \equiv 0 \pmod{p-1}.$$

80. Állapítsuk meg, hogy az 1, 2, ..., 12 redukált maradékrendszer mely elemei kvadratikus maradékok modulo 13?

81. Legyen p tetszőleges prímszám, a a p-hez relatív prím egész szám, k tetszőleges természetes szám. Bizonyítsuk be, hogy a és a^{2k+1} modulo p kvadratikus karaktere megegyezik (azaz: vagy mindkettő kvadratikus maradék, vagy egyikük sem)!

82. Legyen p tetszőleges prímszám, a, a^* egész számok, melyekre (85) teljesül. Bizonyítsuk be, hogy a és a^* modulo p kvadratikus karaktere megegyezik!

83. Legyen p 2-nél nagyobb prímszám, a a p-hez relatív prím, b tetszőleges egész szám. és $p|k$ esetén legyen a $\left(\frac{k}{p}\right)$ Legendre-

-szimbólum értéke definíció szerint 0. Számítsuk ki a $\sum_{x=0}^{p-1}\left(\frac{ax+c}{p}\right)$ összeg értéket!

84*. Az előző feladat jelöléseit használva, számítsuk ki a $\sum_{x=0}^{p-1}\left(\frac{x(x+k)}{p}\right)$ összeg értékét!

85. Állapítsuk meg az Euler-lemma segítségével, hogy megoldható-e az

$$x^2 \equiv 26 \pmod{29}$$

kongruencia?

86. Állapítsuk meg a Gauss-lemma segítségével, hogy megoldható-e az

$$x^2 \equiv 5 \pmod{19}$$

kongruencia?

87. Számítsuk ki (a kvadratikus reciprocitási tétel felhasználása nélkül) az alábbi Legendre-szimbólumok értékeit:

a. $\left(\frac{-4}{41}\right)$,

b. $\left(\frac{94}{103}\right)$,

c. $\left(\frac{101}{109}\right)$.

88. Legyen p 2-nél nagyobb prímszám. Számítsuk ki a $\left(\frac{\frac{p+1}{2}}{p}\right)$ Legendre-szimbólum értékét!

89. Számítsuk ki a kvadratikus reciprocitási tétel segítségével az alábbi Legendre-szimbólumok értékeit:

a. $\left(\frac{77}{103}\right)$,

b. $\left(\frac{131}{191}\right)$.

90*. Legyen p prímszám, a tetszőleges egész szám. Bizonyítsuk be, hogy az

$$x^2+ay^2 \equiv 0 \pmod{p}$$

kongruenciának akkor és csak akkor létezik nemtriviális — vagyis az

$$x \equiv y \equiv 0 \pmod{p}$$

megoldástól különböző — megoldása, ha a

$$z^2+a \equiv 0 \pmod{p}$$

kongruencia megoldható!

91. Bizonyítsuk be, hogy tetszőleges x egész számra x^2+1 páratlan prímosztói $4k+1$ alakúak!

92*. Bizonyítsuk be, hogy az

$$x^2+y^2 \equiv 0 \pmod{p}$$

(ahol p adott prímszám) kongruenciának akkor és csak akkor létezik nemtriviális (l. a 90. feladatot) megoldása, ha $p=2$ vagy p $4k+1$ alakú!

93*. Állapítsuk meg, hogy mely p primszámokra oldható meg az

$$x^2+2 \equiv 0 \pmod{p}$$

kongruencia?

94*. Állapítsuk meg, hogy mely p prímszámokra oldható meg az

$$x^2 \equiv 3 \pmod{p}$$

kongruencia?

95*. Bizonyítsuk be, hogy ha x tetszőleges egész szám, akkor $8x^2-1$ prímosztói $8k\pm 1$ alakúak!

96*. Bizonyítsuk be, hogy ha x tetszőleges egész szám, akkor $12x^2+1$ prímosztói $6k+1$ alakúak!

97. Bizonyítsuk be, hogy ha p 2-nél nagyobb prímszám, g primitív gyök modulo p, akkor

a. $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$,

b. g kvadratikus nem-maradék modulo p.

98. Legyen p 2-nél nagyobb prímszám. Bizonyítsuk be, hogy ha g_1 és g_2 primitív gyökök modulo p, akkor g_1g_2 *nem* primitív gyök modulo p.

99*. Legyen p $4q+1$ alakú prímszám, ahol q is prímszám. Bizonyítsuk be, hogy a 2 primitív gyök modulo p. (Megjegyezzük, nem ismeretes, hogy létezik-e végtelen sok olyan p prímszám, amelyre a 2 primitív gyök modulo p; ez természetesen azt jelenti, hogy az sem ismeretes, hogy létezik-e végtelen sok $4q+1$ alakú prímszám.)

100. Oldjuk meg az

$$x^2+3x-3 \equiv 0 \pmod{17}$$

kongruenciát!

101. A 19. példa megoldása során készített indextáblázatot felhasználva, oldjuk meg az

$$x^{10}-x^5-5 \equiv 0 \pmod{17}$$

kongruenciát!

A II. FEJEZETBEN KITŰZÖTT FELADATOK MEGOLDÁSAI

1. $$17 = 1\cdot 11+6 = 2\cdot 11-5,$$
$$-19 = (-2)\cdot 11+3,$$
$$24 = 2\cdot 11+2,$$
$$-16 = (-2)\cdot 11+6 = (-1)\cdot 11-5,$$
$$31 = 2\cdot 11+9 = 3\cdot 11-2.$$

Így

a. a legkisebb nemnegatív maradékok rendre 6, 3, 2, 6, 9;
b. az abszolút legkisebb maradékok rendre −5, 3, 2, −5, −2;
c. az *a.* és *b.* pont értelmében

$$17 \equiv -16 \pmod{11},$$

míg bármely más számpár elemei inkongruensek modulo 11.

2. A −13, 21, 32, −9 számok modulo 7 legkisebb nemnegatív maradékai rendre 1, 0, 4, 5. Ezek páronként különbözők, tehát a sorozat kiegészíthető teljes maradékrendszerré. Ezt megkaphatjuk például a legkisebb nemnegatív maradékok (vagyis a 0, 1, 2, 3, 4, 5, 6 számok) által alkotott teljes maradékrendszerből hiányzó számok, tehát 2, 3 és 6 hozzávétele révén. Egy kívánt tulajdonságú teljes maradékrendszer tehát: −13, 21, 32, −9, 2, 3, 6.

3. Az (1), ill. (2) kongruenciát oszthatósági relációként felírva:

(87) $m|a-b,$

ill.

(88) $m|b-c.$

Bizonyítanunk kell, hogy

$$m|a-c = (a-b)+(b-c);$$

ez azonban nyilván következik (87)-ből és (88)-ból.

4. (1)-et oszthatósági relációként felírva, (87)-et nyerjük; (87)-ből viszont következik, hogy létezik olyan c egész szám, melyre

$$a-b = mc,$$

vagyis

$$a - mc = b.$$

$(a, m)|b$, hiszen a bal oldal mindkét tagja és így a jobb oldal, b is osztható (a, m)-mel. Másrészt $(a, m)|m$, tehát

$$(89) \quad (a, m)|(b, m).$$

Minthogy a kongruenciareláció szimmetrikus, a és b szerepe felcserélhető; nyerjük hogy

$$(90) \quad (b, m)|(a, m).$$

(89)-ből és (90)-ből következik, hogy $(b, m) = (a, m)$, és ezt kellett igazolnunk.

5. Ha $p < 30$, akkor 30-cal osztva, a maradék maga p, tehát prímszám. Ha $p \geqq 30$, és p prímszám, akkor p nem lehet osztható 2-vel, 3-mal vagy 5-tel; ezért $(p, 30) = 1$. p tehát ekkor valamelyik modulo 30 redukált maradékosztályban helyezkedik el, és e maradékosztály legkisebb nemnegatív eleme szükségképpen azonos azzal a maradékkal, amelyet p 30-cal osztva ad. A modulo 30 redukált maradékosztályok legkisebb nemnegatív reprezentánsai azonban 1, 7, 11, 13, 17, 19, 23, 29. Ezek az 1-től eltekintve, mind prímszámok, és ezzel az állítást igazoltuk.

6. Azt kell bizonyítanunk, hogy ha n páratlan szám, akkor

$$n^2 \equiv 1 \pmod 8,$$

vagyis

$$(91) \quad f(n) = n^2 - 1 \equiv 0 \pmod 8.$$

Minthogy bármely páratlan szám modulo 8 abszolút legkisebb maradéka a $-3, -1, 1, 3$ számok közül kerül ki, bármely páratlan szám kongruens e számok valamelyikével; így a kongruenciák *F)* tulajdonsága szerint elég igazolni, hogy (91) $n = -3, -1, 1, 3$ esetén teljesül. Valóban,

$$f(\pm 1) = (\pm 1)^2 - 1 = 0 \equiv 0 \pmod 8$$

és

$$f(\pm 3) = (\pm 3)^2 - 1 = 8 \equiv 0 \pmod 8,$$

és ezzel az állítást igazoltuk.

7. Legyen $f(n) = n^2 + n + 4$. A kongruenciák *F)* tulajdonságára tekintettel elég igazolni, hogy $f(n)$ $n = 0, \pm 1, \pm 2, \pm 3, \pm 4$ esetén nem osztható 9-cel. Valóban, az $f(-4) = 16$, $f(-3) = 10$, $f(-2) = 6$, $f(-1) = 4$, $f(0) = 4$, $f(1) = 6$, $f(2) = 10$, $f(3) = 16$, $f(4) = 24$ számok egyike sem osztható 9-cel, és ezzel az állítást igazoltuk.

8. $333^{444}+444^{333} = (7\cdot 47+4)^{444}+(7\cdot 63+3)^{333} \equiv$

$\equiv 4^{444}+3^{333} = (4^3)^{148}+(3^3)^{111} = 64^{148}+27^{111} =$

$= (7\cdot 9+1)^{148}+(7\cdot 4-1)^{111} \equiv 1^{148}+(-1)^{111} = 1-1 = 0 \pmod 7.$

9. Legyen $f(m)=m^2-m+1$, $g(n)=2n^2+n-1$. Bizonyítanunk kell, hogy

(92) $f(m) \equiv 0 \pmod 3$,

(93) $g(n) \equiv 0 \pmod 3$

esetén szükségképpen

(94) $m \equiv n \pmod 3$.

$m=-1, 0, +1$-et (vagyis egy modulo 3 teljes maradékrendszer elemeit) helyettesítve:

$$f(-1) = (-1)^2-(-1)+1 = 3 \equiv 0 \pmod 3,$$

$$f(0) = 0^2-0+1 = 1 \not\equiv 0 \pmod 3,$$

$$f(+1) = 1^2-1+1 = 1 \not\equiv 0 \pmod 3.$$

Így — a kongruenciák *F)* tulajdonsága alapján — (92)-ből

(95) $m \equiv -1 \pmod 3$

következik.

Hasonlóan,

$$g(-1) = 2\cdot(-1)^2+(-1)-1 = 0 \equiv 0 \pmod 3,$$

$$g(0) = 2\cdot 0^2+0-1 = -1 \not\equiv 0 \pmod 3,$$

$$g(+1) = 2\cdot 1^2+1-1 = 2 \not\equiv 0 \pmod 3,$$

tehát (93)-ból

(96) $n \equiv -1 \pmod 3$

következik. (95)-ből és (96)-ból adódik (94).

10. $10^{10^{10}} = 10^{10\cdot 10^9} = (10^2)^{5\cdot 10^9} = 100^{5\cdot 10^9} \equiv$

$\equiv (-1)^{5\cdot 10^9} = ((-1)^2)^{5^2\cdot 10^8} = 1^{5^2\cdot 10^8} = 1 \pmod{101};$

a maradék tehát 1.

11. Tetszőleges k természetes számra

$$10^{6k} \equiv 3^{6k} = (3^3)^{2k} = 27^{2k} \equiv (-1)^{2k} = 1 \pmod 7,$$

tehát $l = 0, 1, 2, 3, 4, 5$ esetén

(97) $$10^{6k+l} = 10^{6k} \cdot 10^l \equiv 1 \cdot 10^l = 10^l \equiv 3^l \pmod 7.$$

Így

$$b = a_0 + 10a_1 + 10^2 a_2 + 10^3 a_3 + 10^4 a_4 + 10^5 a_5 + 10^6 a_6 + \ldots \equiv$$

$$\equiv a_0 + 3a_1 + 3^2 a_2 + 3^3 a_3 + 3^4 a_4 + 3^5 a_5 + a_6 + \ldots \equiv$$

$$\equiv (a_0 + 3a_1 + 3^2 a_2) + 3^3 (a_3 + 3a_4 + 3^2 a_5) + \ldots =$$

$$= (a_0 + 3a_1 + 9a_2) + 27 (a_3 + 3a_4 + 9a_5) + \ldots \equiv$$

$$\equiv (a_0 + 3a_1 + 2a_2) - (a_3 + 3a_4 + 2a_5) + \ldots \pmod 7,$$

ahol $a_0, a_1, a_2, \ldots$ együtthatói (97)-re tekintettel periodikusan váltakoznak, mégpedig egy periódus hossza 6, és ezt kellett igazolnunk.

12*. Legyen

$$\binom{2p}{p} = \frac{2p(2p-1)(2p-2)\cdot\ldots\cdot[2p-(p-1)]}{1\cdot 2\cdot 3\cdot\ldots\cdot(p-1)\cdot p} =$$

$$= \frac{2\cdot(2p-1)(2p-2)\cdot\ldots\cdot[2p-(p-1)]}{1\cdot 2\cdot 3\cdot\ldots\cdot(p-1)} \equiv x \pmod p.$$

Mindkét oldalt szorozva $1\cdot 2\cdot 3\cdot\ldots\cdot(p-1)$-gyel:

(98) $$2\cdot(2p-1)(2p-2)\cdot\ldots\cdot[2p-(p-1)] \equiv x\cdot 1\cdot 2\cdot 3\cdot\ldots\cdot(p-1) \pmod p.$$

A bal oldal a következőképpen alakítható át:

$$2\cdot(2p-1)(2p-2)\cdot\ldots\cdot[2p-(p-1)] \equiv 2(-1)(-2)\cdot\ldots\cdot[-(p-1)] =$$

$$= 2\cdot(-1)^{p-1}\cdot 1\cdot 2\cdot\ldots\cdot(p-1) = 2\cdot 1\cdot 2\cdot\ldots\cdot(p-1) \pmod p.$$

Így (98) a következőképpen írható:

$$2\cdot 1\cdot 2\cdot\ldots\cdot(p-1) \equiv x\cdot 1\cdot 2\cdot 3\cdot\ldots\cdot(p-1) \pmod p.$$

Mindkét oldalt osztva a modulushoz relatív prím $1\cdot 2\cdot 3\cdot\ldots\cdot(p-1)$ szorzattal:

$$2 \equiv x \pmod p.$$

A keresett maradék tehát 2.

13. Négy szám közt mindig van két olyan, amelyik ugyanabba a maradékosztályba esik modulo 3; ezek különbsége és így a vizsgált szorzat egyik tényezője, tehát maga a szorzat is osztható 3-mal. Ha továbbá az a, b, c, d számok közt van két olyan, amelyik ugyanabba a maradékosztályba esik modulo 4, akkor ezek különbsége osztható 4-gyel. Ha viszont

e négy szám páronként inkongruens modulo 4, akkor közülük kettő páros, kettő páratlan; mind az előbbiek, mind az utóbbiak különbsége páros, tehát a szorzatnak van két páros tényezője, és így ismét osztható 4-gyel. Végeredményben a szorzat osztható 3-mal is és 4-gyel is; minthogy $(3, 4)=1$, innen következik, hogy a szorzat osztható $3\cdot 4=12$-vel.

14. Legyenek az adott számok $a_1, a_2, \ldots, a_n$ és legyen $s_1=a_1$, $s_2=a_1+a_2, \ldots, s_n=a_1+a_2+\ldots+a_n$. Ha az $s_1, s_2, \ldots, s_n$ számok páronként inkongruensek modulo n, akkor szükségképpen teljes maradékrendszert alkotnak modulo n, tehát létezik olyan k, hogy

$$s_k = a_1+a_2+\ldots+a_k \equiv 0 \pmod{n},$$

és így az $a_1+a_2+\ldots+a_k$ összeg osztható n-nel. Ha viszont az $s_1, s_2, \ldots, s_n$ számok közt található két olyan, például s_i és s_j, amelyek ugyanabba a maradékosztályba esnek modulo n, akkor tekintsük ezek különbségét (feltehető, hogy $i<j$):

$$s_j-s_i = a_{i+1}+a_{i+2}+\ldots+a_j \equiv 0 \pmod{n}.$$

Ebben az esetben tehát az $a_{i+1}+a_{i+2}+\ldots+a_j$ összeg osztható n-nel.

15. A $23, 17, -29$ számok legkisebb nemnegatív maradékai rendre $3, 7$, ill. 1; ehhez a 9-et hozzávéve, redukált maradékrendszert kapunk modulo 10.

16. Nem, mert

$$1\cdot 2 \equiv (p-2)(p-1) \equiv 2 \pmod{p}.$$

17. 450 kanonikus alakja:

$$450 = 2\cdot 225 = 2\cdot 3\cdot 75 = 2\cdot 3\cdot 3\cdot 25 = 2\cdot 3^2\cdot 5^2.$$

Így

$$\varphi(450) = 2\cdot 3^2\cdot 5^2\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) =$$

$$= 2\cdot 3^2\cdot 5^2\cdot\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5} = 3\cdot 5\cdot 2\cdot 4 = 120.$$

18. A vizsgált egyenlet a következő alakban írható:

$$3^x\left(1-\frac{1}{3}\right) = 486 = 2\cdot 243,$$

vagyis

$$2\cdot 3^{x-1} = 2\cdot 3^5.$$

Innen

$$x-1 = 5,$$

$$x = 6.$$

19*. Legyenek az m-hez relatív prím, m-nél nem nagyobb természetes számok $a_1, a_2, \ldots, a_{\varphi(m)}$. Ekkor az mn-nél nem nagyobb, m-hez relatív prím természetes számok — mint ez könnyen ellenőrizhető — az alábbiak:

$$\begin{array}{llll} a_1, & a_2, & \ldots, & a_{\varphi(m)}, \\ m+a_1, & m+a_2, & \ldots, & m+a_{\varphi(m)}, \\ 2m+a_1, & 2m+a_2, & \ldots, & 2m+a_{\varphi(m)}, \\ & & \vdots & \\ (n-1)m+a_1, & (n-1)m+a_2, & \ldots, & (n-1)m+a_{\varphi(m)}. \end{array}$$

(Ennek igazolását az Olvasóra bízzuk.) Ha e számok közül kiválasztjuk azokat, amelyek m mellett n-hez is relatív prímek, a φ függvény definíciója szerint $\varphi(mn)$ számot nyerünk.

Másrészt az 1. pont *I)* tétele szerint — mivel $(m, n)=1$ — bármelyik oszlopot kiszemelve, az abban álló számok teljes maradékrendszert alkotnak modulo n. Egy modulo n teljes maradékrendszer elemei közt $\varphi(n)$ olyan szám van, amelyik relatív prím n-hez; így a fenti sémából kiválasztva azokat a számokat, amelyek m mellett n-hez is relatív prímek, $\varphi(m)$ oszlopból választunk ki egyenként $\varphi(n)$ számot, vagyis összesen $\varphi(m)\varphi(n)$ számot.

Ugyanazon számok számát kétféleképpen leszámlálva, egyszer $\varphi(mn)$-et, egyszer $\varphi(m)\varphi(n)$-et kaptunk; így szükségképpen

$$\varphi(mn) = \varphi(m)\varphi(n) \quad ((m, n) = 1 \text{ esetén}),$$

és ezt kellett igazolnunk.

20. Ha n kanonikus alakja a (9) alatti, akkor — felhasználva a $\varphi(n)$ függvény multiplikativitását —

$$(99) \qquad \varphi(n) = \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2} \ldots p_r^{\alpha_r}) =$$

$$= \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\varphi(p_3^{\alpha_3} \ldots p_r^{\alpha_r}) = \ldots = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \ldots \varphi(p_r^{\alpha_r}).$$

Így elég $\varphi(p^\alpha)$ értékét meghatároznunk, ahol p prímszám, α természetes szám. $\varphi(p^\alpha)$ értéke azonos az

$$(100) \quad 1, 2, \ldots, k, \ldots, p^\alpha$$

számok közül azoknak a számával, amelyekre $(k, p^\alpha)=1$ teljesül, vagyis amelyek nem oszthatók p-vel. A fenti számok közül a p-vel oszthatók:

$$p, 2p, \ldots, p^{\alpha-1} \cdot p.$$

Ezek száma nyilván $p^{\alpha-1}$, míg a (100)-belieké p^α; így

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right).$$

Ebből és (99)-ből adódik a (10) explicit képlet.

21. Ha $x=p^2q^2$, akkor

$$(101)\quad \varphi(x) = x\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right) = p^2q^2\cdot\frac{p-1}{p}\cdot\frac{q-1}{q} = pq(p-1)(q-1).$$

Feltehető, hogy $p<q$. Ekkor az itt álló $p, p-1, q-1$ tényezők mindegyike, következésképpen ezek prímosztói is kisebbek q-nál. Így q azonos $\varphi(x)$ legnagyobb prímosztójával. $\varphi(x)=840$ kanonikus alakja:

$$\varphi(x) = 840 = 2\cdot 240 = 2\cdot 2\cdot 210 = 2\cdot 2\cdot 2\cdot 105 = 2^3\cdot 3\cdot 35 =$$
$$= 2^3\cdot 3\cdot 5\cdot 7.$$

Az itt szereplő tényezők legnagyobbika 7, tehát $q=7$. Továbbá (101)-ből

$$p(p-1) = \frac{\varphi(x)}{q(q-1)} = \frac{2^3\cdot 3\cdot 5\cdot 7}{7\cdot 6} = 2^2\cdot 5.$$

A bal oldal legnagyobb prímosztója p, míg a jobb oldalé 5. Így $p=5$, tehát végeredményben

$$x = p^2q^2 = 5^2\cdot 7^2 = 25\cdot 49 = 1225.$$

22. A 6. példa II. megoldása során láttuk, hogy az n-nél nem nagyobb, n-hez relatív prím természetes számokból $n>2$ esetén párok alkothatók úgy, hogy egy párba $a, n-a$ alakú számok kerüljenek, és az összes ilyen párt képezve, a szóban forgó számok mindegyikét pontosan egyszer vegyük figyelembe. Így $n>2$ esetén a kérdéses összeg:

$$\sum_{\substack{(a,n)=1\\ a\leqq n}} a = \sum_{\substack{(a,n)=1\\ a<\frac{n}{2}}} [a+(n-a)] = \sum_{\substack{(a,n)=1\\ a<\frac{n}{2}}} n = n\sum_{\substack{(a,n)=1\\ a<\frac{n}{2}}} 1 = \frac{n\varphi(n)}{2}.$$

$n=1$ vagy 2 esetén pedig a kérdéses összeg értéke nyilván 1.

23. $m=1$ esetén az állítás nyilvánvaló. $m\geqq 2$ esetén legyen m kanonikus alakja

$$m = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r}.$$

Az $m|n$ feltételből következik, hogy a $p_1, p_2, \dots, p_r$ prímszámok mindegyike osztója n-nek is. Jelöljük n további prímosztóit $q_1, q_2, \dots, q_s$-sel, és legyen n kanonikus alakja

$$n = p_1^{\beta_1}\dots p_r^{\beta_r}q_1^{\gamma_1}\dots q_s^{\gamma_s}.$$

Vezessük be továbbá a következő jelölést:

$$n_1 = p_1^{\beta_1}\dots p_r^{\beta_r} \quad \text{és} \quad n_2 = q_1^{\gamma_1}\dots q_s^{\gamma_s}.$$

Ekkor nyilván

(102) $(m, n_2) = 1,$

és

(103) $(n_1, n_2) = 1.$

Az $m|n = n_1 n_2$ feltételből és (102)-ből a legnagyobb közös osztó *F)* tulajdonsága alapján következik, hogy $m|n_1$ is teljesül, vagyis létezik olyan a egész szám, melyre

$$n_1 = am.$$

(10) szerint

$$\varphi(m) = m\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_r}\right).$$

Mivel a $\varphi(n)$ függvény multiplikatív, (103) alapján

$$\varphi(n) = \varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2).$$

Innen ismét (10) alapján

$$\varphi(n) = \left[n_1\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_r}\right)\right]\varphi(n_2) =$$

$$= \left[am\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_r}\right)\right]\varphi(n_2) =$$

$$= \left[m\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_r}\right)\right]a\varphi(n_2) = \varphi(m)\cdot a\varphi(n_2),$$

tehát $\varphi(n)$ felírható $\varphi(m)$-nek és egy egész számnak a szorzataként, és így $\varphi(m)|\varphi(n)$.

24. Ha m vagy n valamelyike 1, nyilvánvaló az állítás; feltehető tehát, hogy $m \geqq 2$ és $n \geqq 2$.

Jelöljük m, n közös prímosztóit $p_1, p_2, \dots, p_s$-sel. Jelöljük továbbá m azon prímosztóit, melyek nem osztói n-nek, $q_1, q_2, \dots, q_u$-val, és n azon prímosztóit, melyek nem osztói m-nek, $r_1, r_2, \dots, r_v$-vel. (Természetesen előfordulhat, hogy a $p_1, p_2, \dots$; $q_1, q_2, \dots$; $r_1, r_2, \dots$ sorozatok valamelyike üres, vagyis például nem létezik közös prímosztó.)

Mivel m összes prímosztói $p_1, \dots, p_s, q_1, \dots, q_u$, (10) szerint

(104) $$\varphi(m) = m\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_s}\right)\left(1-\frac{1}{q_1}\right)\dots\left(1-\frac{1}{q_u}\right).$$

Hasonlóan,

$$(105)\quad \varphi(n) = n\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_s}\right)\left(1-\frac{1}{r_1}\right)\dots\left(1-\frac{1}{r_v}\right).$$

Végül, mivel mn összes prímosztói $p_1, \dots, p_s, q_1, \dots, q_u, r_1, \dots, r_v$, ismét (10) szerint

$$(106)\quad \varphi(mn) = mn\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_s}\right)\left(1-\frac{1}{q_1}\right)\dots$$

$$\dots\left(1-\frac{1}{q_u}\right)\left(1-\frac{1}{r_1}\right)\dots\left(1-\frac{1}{r_v}\right).$$

(104), (105) és (106) szerint a bizonyítandó

$$(107)\quad \varphi(mn) \geqq \varphi(m)\varphi(n)$$

egyenlőtlenség a következő alakban írható:

$$mn\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_s}\right)\left(1-\frac{1}{q_1}\right)\dots\left(1-\frac{1}{q_u}\right)\left(1-\frac{1}{r_1}\right)\dots\left(1-\frac{1}{r_r}\right) \geqq$$

$$\geqq \left[m\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_s}\right)\left(1-\frac{1}{q_1}\right)\dots\left(1-\frac{1}{q_u}\right)\right]\cdot$$

$$\cdot\left[n\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_s}\right)\left(1-\frac{1}{r_1}\right)\dots\left(1-\frac{1}{r_v}\right)\right].$$

Elvégezve a kínálkozó egyszerűsítéseket:

$$1 \geqq \left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_r}\right)$$

(ha m-nek és n-nek nincs közös prímosztója, akkor a jobb oldalon 1 áll). Minthogy a jobb oldalon álló tényezők mindegyike 1-nél kisebb, ez az egyenlőtlenség nyilván teljesül.

Az adott bizonyításból az is kiolvasható, hogy (107)-ben akkor és csak akkor áll egyenlőség, ha $(m, n) = 1$.

25. A $ba_1, ba_2, \dots, ba_{\varphi(m)}$ számok száma $\varphi(m)$, továbbá $(b, m) = (a_i, m) = 1$-ből (ahol $i = 1, 2, \dots, \varphi(m)$) a legnagyobb közös osztónak az I. fejezet 4. pontjában szereplő *E)* tulajdonsága szerint következik, hogy $(ba_i, m) = 1$ teljesül. Így a 2. pontban említett kritérium szerint elég azt belátni, hogy a $ba_1, ba_2, \dots, ba_{\varphi(m)}$ számok páronként inkongruensek modulo m. Tegyük fel indirekte, hogy létezik olyan i, j $(i \neq j)$, melyre

$$(108)\quad ba_i \equiv ba_j \pmod{m}.$$

Mivel $(b, m)=1$, a kongruenciák $H)$ tulajdonsága szerint innen következnék, hogy

$$a_i \equiv a_j \pmod{m}.$$

Azonban az $a_1, a_2, \ldots, a_{\varphi(m)}$ számok redukált maradékrendszert alkotnak modulo m, tehát szükségképpen páronként inkongruensek. Így a (108) indirekt feltevésből ellentmondásra jutottunk, és ezzel az állítást igazoltuk.

26. Legyen m tetszőleges természetes szám, a m-hez relatív prím egész szám,

(109) $b_1, b_2, \ldots, b_{\varphi(m)}$

redukált maradékrendszer modulo m. Az előző feladat szerint ($(a, m)=1$-re tekintettel) az

(110) $ab_1, ab_2, \ldots, ab_{\varphi(m)}$

számok is redukált maradékrendszert alkotnak modulo m, tehát a (109) alatti számok mindegyike kongruens a (110) alatti számok közül eggyel és csak eggyel (modulo m). Így e számok szorzatai is kongruensek:

$$(ab_1)\cdot(ab_2)\cdot\ldots\cdot(ab_{\varphi(m)}) \equiv b_1 b_2 \ldots b_{\varphi(m)} \pmod{m},$$

vagyis

$$a^{\varphi(m)} b_1 b_2 \ldots b_{\varphi(m)} \equiv b_1 b_2 \ldots b_{\varphi(m)} \pmod{m}.$$

A kongruencia mindkét oldalát osztva a modulushoz relatív prím $b_1 b_2 \ldots b_{\varphi(m)}$ szorzattal:

$$a^{\varphi(m)} \equiv 1 \pmod{m},$$

és ezt kellett igazolnunk.

27. $247^{244} = (10\cdot 23+17)^{244} \equiv 17^{244} \pmod{23}$.

Mivel $(17, 23)=1$, a Fermat-tétel szerint

$$17^{23-1} = 17^{22} \equiv 1 \pmod{23}.$$

Így

$$247^{244} \equiv 17^{244} = 17^{22\cdot 11+2} = (17^{22})^{11}\cdot 17^2 \equiv$$

$$\equiv 1^{11}\cdot(-6)^2 = 1\cdot 36 = 36 \equiv 13 \pmod{23}.$$

28. A Fermat-tétel (13) alakja szerint

$$n^7 \equiv n \pmod{7},$$

vagyis

(111) $7 \mid n^7 - n.$

Továbbá

$$n^7-n = n(n^6-1) = n(n^3-1)(n^3+1) =$$

$$= n(n-1)(n^2+n+1)(n+1)(n^2-n+1) =$$

$$= [(n-1)n(n+1)](n^2+n+1)(n^2-n+1).$$

Az I. fejezet 24. feladatának megoldása során mondottak szerint a szögletes zárójelben álló kifejezés (mely három egymást követő egész szám szorzata) osztható 6-tal, tehát

(112) $6|n^7-n.$

(111)-ből és (112)-ből $(7, 6)=1$ miatt következik az állítás.

29. A Fermat-tétel (13) alakja szerint

$$n^{11} \equiv n \pmod{11},$$

vagyis

$$11|n^{11}-n = n(n^{10}-1) = n(n^5-1)(n^5+1).$$

Mivel 11 prímszám, innen következik, hogy $11|n$, $11|n^5-1$ és $11|n^5+1$ közül legalább az egyik teljesül. Azonban feltettük, hogy $11\nmid n$; így kell, hogy a másik két oszthatósági reláció valamelyike teljesüljön.

30. Ismételten alkalmazva a Fermat-tétel (13) alakját:

$$n^{p^p}-n = (n^p)^{p^{p-1}}-n \equiv n^{p^{p-1}}-n = (n^p)^{p^{p-2}}-n \equiv$$

$$\equiv n^{p^{p-2}}-n \equiv \ldots \equiv n^p-n \equiv 0 \pmod{p}.$$

31. Azt kell megállapítanunk, hogy 403^{402} mennyi maradékot ad 1000-rel osztva. Mivel $(403, 1000)=1$, az Euler-tétel szerint

(113) $403^{\varphi(1000)} \equiv 1 \pmod{1000}.$

Itt

$$\varphi(1000) = \varphi(10^3) = \varphi(2^3\cdot 5^3) = 2^3\cdot 5^3\cdot\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{5}\right) =$$

$$= 2^3\cdot 5^3\cdot\frac{1}{2}\cdot\frac{4}{5} = 2^2\cdot 5^2\cdot 4 = 400.$$

Így (113)-ból

$$403^{400} \equiv 1 \pmod{1000},$$

tehát

$$403^{402} = 403^{400}\cdot 403^2 \equiv 403^2 = (4\cdot 10^2+3)^2 =$$

$$= 16\cdot 10^4+24\cdot 10^2+9 \equiv 4\cdot 10^2+9 = 409 \pmod{1000}.$$

A vizsgált szám tehát 409-re végződik.

32. Minthogy $(10, n)=1$, az Euler-tétel szerint

$$10^{\varphi(n)} \equiv 1 \pmod{n},$$

vagyis $10^{\varphi(n)}-1$ — melynek nyilván valamennyi számjegye 9-es — többszöröse n-nek.

33. Minthogy $(2, n)=1$, az Euler-tétel szerint

$$2^{\varphi(n)} \equiv 1 \pmod{n}.$$

Mivel nyilván $1 \leqq \varphi(n) \leqq n$, $\varphi(n)$ szerepel az $1 \cdot 2 \cdot \ldots \cdot n = n!$ szorzat tényezői közt, tehát $\varphi(n) | n!$, vagyis $\frac{n!}{\varphi(n)}$ egész szám. A kongruencia mindkét oldalát $\frac{n!}{\varphi(n)}$-edik hatványra emelve:

$$(2^{\varphi(n)})^{\frac{n!}{\varphi(n)}} = 2^{n!} \equiv 1 \pmod{n},$$

vagyis $n | 2^{n!}-1$.

34*. Válasszuk n-et $6k+4$ ($k=0, 1, 2, \ldots$) alakú számnak. Ekkor a Fermat-tétel alapján

$$10^{6k+4}+3 = (10^6)^k \cdot 10^4+3 \equiv 1^k \cdot 3^4+3 = 3(3^3+1) =$$

$$= 3 \cdot 28 \equiv 0 \pmod{7},$$

tehát $7 | 10^n+3$; másrészt nyilván $10^n+3>7$, tehát 10^n+3 valóban összetett szám.

35. 68 és 26 legnagyobb közös osztóját kell meghatároznunk:

$$68 = 3 \cdot 26-10,$$

$$26 = 3 \cdot 10-4,$$

$$10 = 2 \cdot 4+2,$$

$$4 = 2 \cdot 2,$$

így $(68, 26)=2$. Ezekből az egyenlőségekből rendre

$$10 = 3 \cdot 26-68,$$

$$4 = 3 \cdot 10-26 = 3(3 \cdot 26-68)-26 = 8 \cdot 26-3 \cdot 68,$$

$$2 = 10-2 \cdot 4 = (3 \cdot 26-68)-2 \cdot (8 \cdot 26-3 \cdot 68) = 5 \cdot 68-13 \cdot 26,$$

tehát

$$68 \cdot 5-26 \cdot 13 = 2.$$

$26x \equiv 6 \pmod{68}$

Mindkét oldalt 3-mal szorozva:

$$68\cdot 15-26\cdot 39 = 6,$$

tehát

$$26\cdot(-39) \equiv 6 \pmod{68},$$

és így

$$x \equiv -39 \equiv 29 \pmod{68}$$

megoldása a vizsgált kongruenciának. (21) szerint a másik megoldás:

$$x \equiv 29+\frac{68}{(26, 68)} = 29+\frac{68}{2} = 29+34 = 63 \pmod{68}.$$

36. Minthogy $(19, 24)=1$, az Euler-tételen alapuló (25) formula szerint a kongruencia megoldása:

(114) $x \equiv 11\cdot 19^{\varphi(24)-1} \pmod{24}$.

Itt

$$\varphi(24) = \varphi(2^3\cdot 3) = 2^3\cdot 3\cdot\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 2^3\cdot 3\cdot\frac{1}{2}\cdot\frac{2}{3} = 8.$$

(114)-be helyettesítve:

$$x \equiv 11\cdot 19^{8-1} \equiv 11\cdot(-5)^7 = -11\cdot(5^2)^3\cdot 5 =$$

$$= -11\cdot(25)^3\cdot 5 \equiv -11\cdot 1^3\cdot 5 = -55 \equiv 17 \pmod{24}.$$

37. *a.* $(30, 51)=3|39$, tehát a kongruencia megoldható. $(30, 51)=3$-mal osztva a kongruencia mindkét oldalát és a modulust is:

$$10x \equiv 13 \equiv 13+1\cdot 17 = 30 \pmod{17},$$

ahonnan $(10, 17)=1$-re tekintettel

$$x \equiv 3 \pmod{17}.$$

Így a megoldások:

$$x \equiv 3 \pmod{51},$$

$$x \equiv 3+\frac{51}{(30, 51)} = 3+\frac{51}{3} = 3+17 = 20 \pmod{51},$$

$$x \equiv 3+2\cdot\frac{51}{(30, 51)} = 3+2\cdot\frac{51}{3} = 3+34 = 37 \pmod{51}.$$

b. $(27, 45)=9\nmid 33$, tehát a kongruencia nem oldható meg.

c. $(60, 70)=10|30$, tehát a kongruencia megoldható. $(60, 70)=10$-zel osztva a kongruencia mindkét oldalát és a modulust is:

$$6x \equiv 3 \pmod 7.$$

Innen $(6, 7)=1$-re tekintettel

$$2x \equiv 1 \equiv 8 \pmod 7,$$

ahonnan

$$x \equiv 4 \pmod 7.$$

Az összes megoldások tehát az alábbiak:

$$x \equiv 4+\frac{70}{(60, 70)}k = 4+\frac{70}{10}k = 4+7k \pmod{70},$$

ahol $k=0, 1, 2, \ldots, 9$.

38. *a.* Minthogy

$$204 \equiv -1 \pmod{205},$$

a kongruencia a következő alakban írható:

$$-x \equiv 139 \pmod{205}.$$

Mindkét oldalt -1-gyel szorozva:

$$x \equiv -139 \equiv 66 \pmod{205},$$

b. Mindkét oldalt 2-vel szorozva:

$$402x \equiv x \equiv 236 \pmod{401}.$$

c. Mindkét oldalt 3-mal szorozva.

$$300x \equiv 369 \pmod{301},$$

vagyis

$$-x \equiv 68 \pmod{301}.$$

-1-gyel szorozva:

$$x \equiv -68 \equiv 233 \pmod{301}.$$

39. A kongruencia jobb oldalán álló számot b-vel, a modulust m-mel jelölve, $(m, 3)=1$ esetén a $b-m, b, b+m$ számok valamelyike osztható 3-mal; így b-t szükség esetén $b-m$-mel vagy $b+m$-mel helyettesítve, min-

denképpen elérhető, hogy egyszerűsíteni tudjunk 3-mal. Ezt a redukciós lépést ismételten alkalmazva:

$$3^8x \equiv 23 \equiv 23+100 = 123 \pmod{100},$$

$$3^7x \equiv 41 \equiv 41+100 = 141 \pmod{100},$$

$$3^6x \equiv 47 \equiv 47+100 = 147 \pmod{100},$$

$$3^5x \equiv 49 \equiv 49-100 = -51 \pmod{100},$$

$$3^4x \equiv -17 \equiv -17-100 = -117 \pmod{100},$$

$$3^3x \equiv -39 \pmod{100},$$

$$3^2x \equiv -13 \equiv -13+100 = 87 \pmod{100},$$

$$3x \equiv 29 \equiv 29+100 = 129 \pmod{100},$$

$$x \equiv 43 \pmod{100}.$$

40. $(x^{100})^2 \cdot x = x^{201}$,

tehát a feladat feltételei szerint

$$10^2 \cdot x \equiv 5 \pmod{67},$$

vagyis

$$100x \equiv 5 \pmod{67}.$$

$(5, 67)=1$-re tekintettel, oszthatunk 5-tel:

$$20x \equiv 1 \equiv 68 \pmod{67}.$$

4-gyel osztva:

$$5x \equiv 17 \equiv 17-67 = -50 \pmod{67},$$

ahonnan 5-tel osztva:

$$x \equiv -10 \equiv 57 \pmod{67},$$

tehát a keresett maradék 57.

41. Legyen $x=29^{39^{49}}$; ennek a számnak a modulo 100 legkisebb nemnegatív maradékát kell meghatároznunk. Minthogy $(29, 100)=1$, az Euler-tétel szerint

$$(115) \quad 29^{\varphi(100)} = 29^{40} \equiv 1 \pmod{100}.$$

(A 9. példa megoldása során már láttuk, hogy $\varphi(100)=40$.) Továbbá

$$39^{49} = (40-1)^{49} \equiv (-1)^{49} = -1 \pmod{40},$$

tehát 39^{49} $40k-1$ alakban írható. Így (115) alapján

$$29x = 29 \cdot 29^{39^{49}} = 29 \cdot 29^{40k-1} = 29^{40k} = (29^{40})^k \equiv 1^k = 1 \pmod{100},$$

tehát a

$$29x \equiv 1 \pmod{100}$$

lineáris kongruenciát kell megoldanunk. Mindkét oldalt 7-tel szorozva:

$$203x \equiv 7 \pmod{100}.$$

(A 7-es szorzóhoz úgy juthatunk el, hogy 29-nek olyan többszörösét keressük, amely „közel" esik 100 valamely többszöröséhez, másrészt 29 szorzója relatív prím 100-hoz.) Ez utóbbi kongruencia a következő alakban írható:

$$3x \equiv 7 \equiv 7-100 = -93 \pmod{100}.$$

ahonnan

$$x \equiv -31 \equiv 69 \pmod{100},$$

tehát a vizsgált szám 69-re végződik.

42. Ha $p|a$, akkor

$$x \equiv 0 \pmod{p}$$

megoldás. Ha viszont $(a, p)=1$, akkor az

$$ax \equiv 1 \pmod{p}$$

kongruencia megoldható. Legyen egy megoldás x_0:

(116) $ax_0 \equiv 1 \pmod{p}$.

Innen nyilván következik, hogy

(117) $(x_0, p) = 1$.

(116) mindkét oldalát x_0^{p-2}-nel szorozva:

(118) $ax_0^{p-1} \equiv x_0^{p-2} \pmod{p}$.

(117)-re tekintettel a Fermat-tétel szerint

$$x_0^{p-1} \equiv 1 \pmod{p}.$$

(118) tehát

$$a \equiv x_0^{p-2} \pmod{p}$$

alakban írható, és így x_0 megoldása a vizsgált kongruenciának.

JATE Móra Ferenc Kollégium
KÖNYVTÁRA

43. Az első kongruencia a következő alakban írható:

$$5x \equiv 3 \equiv 3+7 = 10 \pmod 7.$$

5-tel osztva:

$$x \equiv 2 \pmod 7,$$

tehát x a következő alakban írható:

(119) $x = 2+7t.$

A második kongruenciába helyettesítve:

$$3(2+7t) \equiv 7 \pmod 8,$$

ahonnan

$$21t \equiv 1 \pmod 8,$$

vagyis

$$-3t \equiv 9 \pmod 8.$$

-3-mal osztva:

$$t \equiv -3 \equiv 5 \pmod 8.$$

Így t-t választhatjuk $t=5$-nek; ezt (119)-be visszahelyettesítve, a kongruencia-rendszer egy megoldása

$$x = 2+7\cdot 5 = 37.$$

Az összes megoldás tehát

$$x \equiv 37 \pmod{56}.$$

44. Az első kongruencia a következő alakban írható:

$$7x \equiv 11+2\cdot 12 = 35 \pmod{12},$$

ahonnan 7-tel osztva:

$$x \equiv 5 \pmod{12}.$$

Az első kongruenciát tehát az

(120) $x = 5+12t$

alakú számok elégítik ki. A második kongruenciába helyettesítve:

$$13(5+12t) \equiv 17 \pmod{21},$$

ahonnan

$$156t \equiv -48 \pmod{21},$$

vagyis

$$9t \equiv -6 \pmod{21}.$$

Mindkét oldalt és a modulust is 3-mal osztva, ezzel ekvivalens kongruenciát kapunk:

$$3t \equiv -2 \equiv -9 \pmod{7},$$

ahonnan 3-mal osztva:

$$t \equiv -3 \equiv 4 \pmod{7}.$$

Ezt a kongruenciát a

$$t = 4+7u$$

alakú számok elégítik ki. Így (120)-ba helyettesítve, nyerjük, hogy a kongruencia-rendszer megoldásai:

$$x = 5+12t = 5+12(4+7u) = 53+84u \quad (\text{ahol } u=0, \pm 1, \pm 2, \ldots)$$

vagy kongruencia alakban:

$$x \equiv 53 \pmod{84}.$$

(A megoldások tehát egy maradékosztályt alkotnak modulo 84=[12, 21].)

45. Az első kongruencia megoldásai az

(121) $x = 3+5t$

alakú számok. A második kongruenciába helyettesítve:

$$3+5t \equiv 1 \pmod{6},$$

$$5t \equiv -2 \pmod{6},$$

$$-t \equiv -2 \pmod{6},$$

Mindkét oldalt -1-gyel szorozva:

$$t \equiv 2 \pmod{6}.$$

Más szóval, t a következő alakú:

$$t = 2+6u.$$

(121)-be helyettesítve:

(122) $x = 3+5t = 3+5(2+6u) = 13+30u.$

Végül a harmadik kongruenciába helyettesítve:

$$13+30u \equiv 2 \pmod 7,$$

$$30u \equiv -11 \pmod 7,$$

$$2u \equiv -4 \pmod 7.$$

Mindkét oldalt osztva 2-vel:

$$u \equiv -2 \equiv 5 \pmod 7.$$

Így u egy lehetséges értéke $u=5$. (122)-be helyettesítve nyerjük, hogy a kongruencia-rendszer egy megoldása:

$$x = 13+30u = 13+30\cdot 5 = 163.$$

Minthogy a modulusok, 5, 6 és 7 páronként relatív prímek, a megoldások egy maradékosztályt alkotnak modulo $5\cdot 6\cdot 7 = 210$:

$$x \equiv 163 \pmod{210}.$$

46. Ha $(x, 24)>1$, akkor x kielégíti az 1. vagy a 2. kongruenciát. Ha viszont $(x, 24)=1$, akkor x kongruens egy modulo 24 redukált maradékrendszer valamelyik elemével. Tekintsük azt a redukált maradékrendszert, amelyet a redukált maradékosztályok legkisebb nemnegatív elemei alkotnak:

1, 5, 7, 11, 13, 17, 19, 23.

Ha azonban x modulo 24 kongruens e számsorozat 1., 2., 3., 4., 5., 6., 7., ill. 8. elemével, akkor kielégíti rendre a 3., 3., 5., 4., 3., 3., 4., ill. 6. kongruenciát, és ezzel az állítást igazoltuk.

47. A keresett négyjegyű számot x-szel jelölve, a feltételek szerint

$$x \equiv 46 \pmod{72},$$

$$x \equiv 97 \pmod{127}.$$

Az első kongruencia szerint x a következő alakú:

(123) $x = 46+72t.$

A második kongruenciába helyettesítve:

$$46+72t \equiv 97 \pmod{127},$$

$$72t \equiv 51 \pmod{127}.$$

Mindkét oldalt osztva 3-mal:

$$24t \equiv 17 \equiv 17+127 = 144 \pmod{127}.$$

24-gyel osztva:

$$t \equiv 6 \pmod{127}.$$

Így t szükségképpen

$$t = 6+127u$$

alakú. (123)-ba helyettesítve:

$$x = 46+72t = 46+72(6+127u) = 478+9144u.$$

Ha itt $u<0$, negatív számot, ha $u=0$, háromjegyű számot, ha $u\geqq 2$, legalább ötjegyű számot kapunk eredményül. Így csak $u=1$ lehetséges, tehát az egyetlen megoldás:

$$x = 478+9144 = 9622.$$

48. Ha valamely n természetes számnak van olyan prímosztója, melynek kitevője n kanonikus alakjában 1, akkor — tekintettel az I. fejezet 17. példájára — n nem lehet teljes hatvány. Így elegendő megmutatni, hogy létezik k számú egymást követő természetes szám, melyek mindegyike ilyen tulajdonságú.

Legyenek $p_1, p_2, \ldots, p_k$ páronként különböző prímszámok. Ekkor az

$$\begin{aligned} x+1 &\equiv p_1 \pmod{p_1^2}, \\ x+2 &\equiv p_2 \pmod{p_2^2}, \\ &\vdots \\ x+k &\equiv p_k \pmod{p_k^2} \end{aligned}$$

kongruencia-rendszer megoldható, hiszen a modulusok páronként relatív prímek. Mivel a megoldások egy maradékosztályt alkotnak modulo $p_1^2p_2^2\ldots p_k^2$, található *pozitív* egész megoldás is. Jelöljünk egy pozitív megoldást x_0-val. Ekkor $x_0+1, x_0+2, \ldots, x_0+k$ egymást követő természetes számok. Továbbá, a j-edik ($j=1, 2, \ldots, k$) kongruencia szerint $p_j|x_0+j$, de $p_j^2 \nmid x_0+j$. Így p_j kitevője x_0+j kanonikus alakjában 1, és ezzel az állítást igazoltuk.

49. A vizsgált kongruencia visszavezethető az

$$(124) \quad f(x) = x^3+x^2+2x-2 \equiv 0 \pmod 4,$$

$$(125) \quad f(x) = x^3+x^2+2x-2 \equiv 0 \pmod 5$$

kongruenciák megoldására.

(124)-be helyettesítsük egy modulo 4 teljes maradékrendszer elemeit:

$$f(-1) = (-1)^3+(-1)^2+2\cdot(-1)-2 = -4 \equiv 0 \pmod 4,$$

$$f(0) = 0^3+0^2+2\cdot 0-2 = -2 \not\equiv 0 \pmod 4,$$

$$f(1) = 1^3+1^2+2\cdot 1-2 = 2 \not\equiv 0 \pmod 4,$$

$$f(2) = 2^3+2^2+2\cdot 2-2 \equiv -2 \not\equiv 0 \pmod 4.$$

Így (124) egyetlen megoldása:

(126) $x \equiv -1 \pmod 4$.

(125)-be helyettesítsük az $x = -2, -1, 0, 1, 2$ értékeket:

$$f(-2) = (-2)^3 + (-2)^2 + 2\cdot(-2) - 2 \equiv 2 + 4 - 4 - 2 = 0 \equiv 0 \pmod 5,$$

$$f(-1) = (-1)^3 + (-1)^2 + 2\cdot(-1) - 2 = -4 \not\equiv 0 \pmod 5,$$

$$f(0) = 0^3 + 0^2 + 2\cdot 0 - 2 = -2 \not\equiv 0 \pmod 5,$$

$$f(1) = 1^3 + 1^2 + 2\cdot 1 - 2 = 2 \not\equiv 0 \pmod 5,$$

$$f(2) = 2^3 + 2^2 + 2\cdot 2 - 2 \equiv 3 + 4 + 4 - 2 = 9 \not\equiv 0 \pmod 5.$$

Így (125) egyetlen megoldása:

(127) $x \equiv -2 \pmod 5$.

Végeredményben tehát a (126) és (127) által alkotott kongruencia-rendszert kell megoldanunk. A (126) kongruenciát kielégítő x egész számok

(128) $x = -1 + 4t$

alakban írhatók. (127)-be helyettesítve:

$$-1 + 4t \equiv -2 \pmod 5,$$

$$4t \equiv -1 \equiv 4 \pmod 5,$$

$$t \equiv 1 \pmod 5.$$

t tehát választható $t = 1$-nek. (128)-ba helyettesítve kapjuk, hogy a kongruencia-rendszer egy megoldása:

$$x = -1 + 4\cdot 1 = 3.$$

Az összes megoldás tehát:

$$x \equiv 3 \pmod{20}.$$

50. Oldjuk meg először az

(129) $f(x) = x^3 - 2x^2 + 3x + 2 \equiv 0 \pmod 5$

kongruenciát. Írjuk x helyébe a $-2, -1, 0, 1, 2$ értékeket:

$$f(-2) = (-2)^3-2(-2)^2+3(-2)+2 \equiv 2+2-1+2 = 5 \equiv 5 \pmod 5,$$

$$f(-1) = (-1)^3-2(-1)^2+3(-1)+2 = -1-2-3+2 = -4 \not\equiv 0 \pmod 5,$$

$$f(0) = 0^3-2\cdot 0^2+3\cdot 0+2 = 2 \not\equiv 0 \pmod 5,$$

$$f(1) = 1^3-2\cdot 1^2+3\cdot 1+2 = 1-2+3+2 = 4 \not\equiv 0 \pmod 5,$$

$$f(2) = 2^3-2\cdot 2^2+3\cdot 2+2 \equiv 3+2+1+2 = 8 \not\equiv 0 \pmod 5.$$

Így (129) egyetlen megoldása:

$$x \equiv -2 \pmod 5.$$

Az adott kongruencia megoldásai tehát

(130) $x = -2+5t$

alakúak. Behelyettesítve:

$$f(x) = f(-2+5t) = (-2+5t)^3-2(-2+5t)^2+3(-2+5t)+2 \equiv$$

$$\equiv -8+60t-8+40t-6+15t+2 = -20+115t \equiv 0 \pmod{25}.$$

5-tel osztva a kongruenciát is és a modulust is:

$$-4+23t \equiv 0 \pmod 5,$$

$$23t \equiv 4 \pmod 5,$$

$$3t \equiv 4 \equiv 4+5 = 9 \pmod 5.$$

3-mal osztva:

$$t \equiv 3 \pmod 5,$$

t tehát szükségképpen

$$t = 5u+3$$

alakú. (130)-ba helyettesítve.

$$x = -2+5t = -2+5\cdot(5u+3) = 13+25u.$$

Az összes megoldások tehát:

$$x \equiv 13 \pmod{25}.$$

51. Az együtthatókat modulo 5 abszolút legkisebb maradékukkal helyettesítve:

$$-2x^{18}-2x^{16}+x^{11}+2x^4+1 \equiv 0 \pmod 5.$$

A Fermat-tétel (13) alakja szerint

$$x^5 \equiv x \pmod 5.$$

Így a vizsgált kongruencia bal oldala a következőképpen alakítható át:

$$-2(x^5)^3\cdot x^3-2(x^5)^3\cdot x+(x^5)^2\cdot x+2x^4+1 \equiv$$

$$\equiv -2x^3\cdot x^3-2x^3\cdot x+x^2\cdot x+2x^4+1 = -2x^5\cdot x-2x^4+x^3+2x^4+1 \equiv$$

$$\equiv -2x\cdot x+x^3+1 = x^3-2x^2+1 \pmod 5.$$

Az alábbi kongruenciát kell tehát megoldanunk:

$$f(x) = x^3-2x^2+1 \equiv 0 \pmod 5.$$

A $-2, -1, 0, 1, 2,$ értékeket helyettesítve:

$$f(-2) = (-2)^3-2(-2)^2+1 \equiv 2+2+1 = 5 \equiv 0 \pmod 5,$$

$$f(-1) = (-1)^3-2(-1)^2+1 = -1-2+1 = -2 \not\equiv 0 \pmod 5,$$

$$f(0) = 0^3-2\cdot 0^2+1 = 1 \not\equiv 0 \pmod 5,$$

$$f(1) = 1^3-2\cdot 1^2+1 = 1-2+1 = 0 \equiv 0 \pmod 5,$$

$$f(2) = 2^3-2\cdot 2^2+1 \equiv 3-3+1 = 1 \not\equiv 0 \pmod 5.$$

A kongruenciának tehát két megoldása van:

$$x \equiv -2 \equiv 3 \pmod 5$$

és

$$x \equiv 1 \pmod 5.$$

52*. Az

$$a_0x+a_1 \equiv 0 \pmod p$$

lineáris kongruenciának $p \nmid a_0$ esetén pontosan egy megoldása van, tehát $n=1$ esetén az állítás teljesül.

Most tegyük fel, hogy az állítás teljesül valamely n természetes számra. Bizonyítanunk kell, hogy ebből következik, hogy az állítás n helyén $n+1$-gyel is igaz, vagyis tekintve valamely

$$(131)\quad f(x) = a_0x^{n+1}+a_1x^n+\ldots+a_nx+a_{n+1} \equiv 0 \pmod p$$

kongruenciát, ahol

(132) $a_0 \not\equiv 0 \pmod{p}$

teljesül, ennek megoldásszáma szükségképpen legfeljebb $n+1$.

Ha a (131) kongruencia megoldhatatlan, akkor az állítás nyilvánvalóan teljesül, hiszen a megoldásszám 0, ami kisebb, mint a fokszám, $n+1$. Így elég arra az esetre szorítkozni, amikor a (131) kongruencia megoldható. Legyen egy megoldás x_1, azaz tegyük fel, hogy

(133) $f(x_1) = a_0 x_1^{n+1} + a_1 x_1^n + \ldots + a_n x_1 + a_{n+1} \equiv 0 \pmod{p}$.

(131)-ből kivonva (133)-at, alkalmazva az I. fejezet (7) képletét, majd összevonva:

(134) $$f(x) - f(x_1) = a_0(x^{n+1} - x_1^{n+1}) + a_1(x^n - x_1^n) + \ldots + a_n(x - x_1) =$$
$$= (x - x_1)[a_0(x^n + x^{n-1}x_1 + \ldots + xx_1^{n-1} + x_1^n) + a_1(x^{n-1} +$$
$$+ \ldots + xx_1^{n-2} + x_1^{n-1}) + \ldots + a_n] = (x - x_1)(a_0 x^n + b_1 x^{n-1} +$$
$$+ \ldots + b_{n-1}x + b_n) = (x - x_1)g(x) \equiv 0 \pmod{p},$$

ahol $b_1, b_2, \ldots, b_n$ alkalmas egész számok, és

(135) $g(x) = a_0 x^n + b_1 x^{n-1} + \ldots + b_{n-1}x + b_n$.

(133) szerint

$$f(x_1) \equiv 0 \pmod{p},$$

tehát (134) bal oldalán a második tag helyettesíthető 0-val. Így (134) a következő alakban írható:

$$f(x) \equiv (x - x_1)g(x) \equiv 0 \pmod{p}.$$

Ha tehát x kielégíti a vizsgált (131) kongruenciát, akkor az

$$(x - x_1)g(x) \equiv 0 \pmod{p}$$

kongruenciát is. Minthogy p prímszám, ez a kongruencia akkor és csak akkor teljesül valamely x egész számra, ha

(136) $x - x_1 \equiv 0 \pmod{p}$

vagy

(137) $g(x) \equiv 0 \pmod{p}$.

A (136) kongruenciának pontosan egy megoldása van, míg a (137) kongruencia (132) és (135) szerint pontosan n-edfokú, tehát az indukciós feltevés szerint legfeljebb n megoldása van. Így a (136) és (137) kongruen-

ciáknak összesen legfeljebb $n+1$ megoldásuk van, tehát (131)-nek is legfeljebb ennyi megoldása van, és ezzel az állítást igazoltuk.

53*. Az $f(x)$ polinom első tagjában x^{p-1} együtthatója 1, a másodikban nyilván -1; így az összevonás után x^{p-1}-t tartalmazó tag nem fog szerepelni. Az összes többi tagban x kitevője legfeljebb $p-2$, tehát $f(x)$ legfeljebb $(p-2)$-edfokú vagy (modulo p) azonosan 0.

Másrészt $x=1, 2, \ldots, p-1$-et helyettesítve, $f(x)$ első tagja a Fermat-tétel szerint 0-val kongruens modulo p, a második tag pedig 0. Így e számok mindegyike, tehát $p-1$ páronként inkongruens szám kielégíti a (84) kongruenciát. Ebből a fokszámtétel (az előző feladat) szerint következik, hogy a (84) kongruencia legalább $(p-1)$-edfokú vagy pedig $f(x)$ azonosan 0 modulo p (azaz, minden együttható osztható p-vel). Az első eset az előbbiek szerint nem lehetséges, tehát a második eset áll fenn, vagyis minden együttható osztható p-vel. Így speciálisan a konstans tag is osztható p-vel:

$$-1-(-1)^{p-1}1\cdot 2\cdot\ldots\cdot(p-1) \equiv 0 \pmod{p},$$

vagyis

$$(-1)^p(p-1)! \equiv 1 \pmod{p}.$$

Mindkét oldalt szorozva $(-1)^p$-nel:

$$(-1)^{2p}(p-1)! \equiv (-1)^p \pmod{p},$$

vagyis

(138) $$(p-1)! \equiv (-1)^p \pmod{p}.$$

Ha $p>2$, akkor a jobb oldalon -1 áll; ha viszont $p=2$, akkor

$$(-1)^p = (-1)^2 = 1 \equiv -1 \pmod{2}.$$

(138) jobb oldalára mindkét esetben írhatunk -1-et, és ezzel a Wilson-tételt igazoltuk.

54. A megoldásszám $(10, 47-1)=(10, 46)=2(5, 23)=2$. E két megoldás nyilván

$$x \equiv -1 \pmod{47},$$

$$x \equiv 1 \pmod{47}.$$

55. A rend *B)* tulajdonsága szerint

$$o_{47}(4) | 47-1 = 46,$$

tehát $o_{47}(4)$ a 46 szám pozitív osztói, vagyis az 1, 2, 23, 46 számok közül kerül ki. Így e számok közül azt a legkisebb k-t kell kiválasztanunk, melyre

$$4^k \equiv 1 \pmod{47}$$

teljesül. Nyilván

$$4^1 \not\equiv 1 \pmod{47}$$

$$4^2 = 16 \not\equiv 1 \pmod{47}$$

és — felhasználva a Fermat-tételt —

$$4^{23} = (2^2)^{23} = 2^{46} \equiv 1 \pmod{47},$$

tehát $o_{47}(4)=23$.

56. A rend *A)* tulajdonsága szerint az adott kongruenciákból következik, hogy $o_{43}(21)|21$, illetve $o_{43}(21)|28$, tehát $o_{43}(21)|(21, 28)=7$ is teljesül. Így csak $o_{43}(21)=1$ vagy 7 lehetséges. Azonban nyilván

$$21^1 \not\equiv 1 \pmod{43},$$

tehát $o_{43}(21) = 7$.

57. $(a^k)^{\frac{o(a)}{k}} = a^{o(a)} \equiv 1 \pmod{p}$

($o(a)$ definíciójára tekintettel), ahonnan következik, hogy

$$(139) \quad o(a^k) \leqq \frac{o(a)}{k}.$$

Másrészt, ha valamely l nemnegatív egész számra

$$(140) \quad (a^k)^l = a^{kl} \equiv 1 \pmod{p},$$

akkor innen ismét $o(a)$ definíciójára tekintettel következik, hogy

$$kl \geqq o(a),$$

vagyis

$$l \geqq \frac{o(a)}{k}.$$

Minthogy ez bármely (140)-et kielégítő l-re teljesül, szükségképpen

$$(141) \quad o(a^k) \geqq \frac{o(a)}{k}.$$

(139)-ből és (141)-ből következik a bizonyítandó állítás.

58. Tegyük fel, hogy valamely k természetes számra $o(a)|k$ teljesül, vagyis létezik olyan b természetes szám, hogy $k=b\cdot o(a)$. Ekkor $o(a)$ definíciója alapján

$$a^k = a^{b\cdot o(a)} = (a^{o(a)})^b \equiv 1^b = 1 \pmod{p}.$$

Másrészt, tegyük fel, hogy valamely k természetes számra

(142) $a^k \equiv 1 \pmod{p}$.

k-t $o(a)$-val osztva, legyen a hányados q, a maradék r:

$$k = q \cdot o(a) + r,$$

ahol q, r nemnegatív egész számok és

(143) $0 \leqq r < o(a)$.

Ekkor $o(a)$ definícióját alkalmazva

$$a^k = a^{q \cdot o(a) + r} = (a^{o(a)})^q \cdot a^r \equiv 1^q \cdot a^r = a^r \pmod{p}.$$

(142)-vel egybevetve, nyerjük, hogy

$$a^r \equiv 1 \pmod{p}.$$

Innen ismét $o(a)$ definíciója alapján következik, hogy $r=0$ vagy pedig $r \geqq o(a)$. Ez utóbbi eset (143) szerint nem lehetséges, tehát szükségképpen $r=0$, vagyis $o(a)|k$, és ezt kellett igazolnunk.

59. (85)-öt $o(a)$-adik hatványra emelve és felhasználva $o(a)$ definícióját:

$$1 \equiv (aa^*)^{o(a)} = a^{o(a)} \cdot (a^*)^{o(a)} \equiv 1 \cdot (a^*)^{o(a)} = (a^*)^{o(a)} \pmod{p}.$$

Innen a rend definíciója értelmében következik, hogy

(144) $o(a^*) \leqq o(a)$.

Ugyanúgy igazolható, hogy

(145) $o(a) \leqq o(a^*)$

is teljesül (hivatkozhatunk a multiplikatív inverz *D)* tulajdonságára is). (144) és (145) adja a bizonyítandó összefüggést.

60. Tegyük fel indirekte, hogy valamely x nemnegatív egész számra (86) teljesül, vagyis

(146) $a^x \equiv -1 \pmod{p}$.

Mindkét oldalt négyzetre emelve:

$$a^{2x} \equiv 1 \pmod{p}.$$

Innen a rend *A)* tulajdonsága szerint következik, hogy $o(a)|2x$. Minthogy feltevésünk szerint $(o(a), 2)=1$, innen nyerjük, hogy $o(a)|x$. Ekkor azonban ismét a rend *A)* tulajdonságából következik, hogy

(147) $a^x \equiv 1 \pmod{p}$.

(146)-ból és (147)-ből adódik, hogy

$$-1 \equiv 1 \pmod{p},$$

$$0 \equiv 2 \pmod{p},$$

ami $p>2$ miatt lehetetlen. Így az indirekt feltevésből ellentmondásra jutottunk.

61*. Tegyük fel, hogy q páratlan prímosztója a^p-1-nek, vagyis

$$a^p \equiv 1 \pmod{q}.$$

Innen, a rend *A)* tulajdonsága szerint következik, hogy $o(a)|p$, tehát $o(a)=1$ vagy

(148) $o(a) = p.$

Az előbbi esetben

$$a^1 \equiv 1 \pmod{q},$$

tehát

(149) $q|a-1.$

Ha viszont (148) teljesül, akkor a rend *B)* tulajdonsága szerint szükségképpen

$$o(a) = p|q-1,$$

tehát létezik olyan l nemnegatív egész szám, hogy

$$q-1 = pl,$$

vagyis

(150) $q = pl+1.$

Minthogy itt q páratlan, pl-nek és így ($p>2$-re tekintettel) l-nek is párosnak kell lennie, tehát $l\,2k$ alakú. (150)-be helyettesítve:

(151) $q = 2pk+1.$

Végeredményben vagy (149) teljesül, vagy pedig q (151) alakú, és ezt kellett igazolnunk.

62*. Tegyük fel, hogy $p|2^{2^n}+1$, vagyis

(152) $2^{2^n} \equiv -1 \pmod{p}.$

Mindkét oldalt négyzetre emelve:

$$2^{2\cdot 2^n} \equiv 2^{2^{n+1}} \equiv 1 \pmod{p}.$$

Innen a rend *A)* tulajdonsága szerint következik, hogy

(153) $o(2)|2^{n+1}$.

Ha

(154) $o(2) < 2^{n+1}$,

akkor (153)-ból adódik, hogy $o(2)|2^n$. Innen viszont ismét a rend *A)* tulajdonsága szerint következik, hogy

$$2^{2^n} \equiv 1 \pmod{p}.$$

Ez ellentmond (152)-nek (hiszen nyilván $p>2$), tehát (154) nem lehetséges, és így (153)-ból nyerjük, hogy

$$o(2) = 2^{n+1}.$$

Innen a rend *B)* tulajdonsága szerint következik, hogy

$$o(2) = 2^{n+1}|p-1,$$

tehát létezik olyan k nemnegatív egész szám, hogy

$$p-1 = 2^{n+1}k,$$

vagyis

$$p = 2^{n+1}k+1.$$

63*. Az előző feladat szerint $2^{2^5}+1$ prímosztói

$$p = 2^6k+1 = 64k+1$$

alakúak. Itt $k=1, 2, 3, \ldots$-at választva, nyerjük, hogy a lehetséges prímosztók a 65, 129, 193, 257, 321, 385, 449, 513, 577, 641, ... számok közül kerülnek ki. Ezek közt azonban vannak összetett számok is: $65=5\cdot 13$, $129=3\cdot 43$, $321=3\cdot 107$, $385=5\cdot 77$, $513=3\cdot 171$ s í. t. Az összetett számokat elhagyva, a lehetséges prímosztók: 193, 257, 449, 577, 641, ... Sorban ellenőriznünk kell, hogy ezek prímosztói-e $2^{2^5}+1$-nek (mindaddig, amíg egy osztót nem találunk).

Némi számolással látható, hogy a 193, 257, 449, 577 prímszámok egyike sem osztója $2^{2^5}+1$-nek. (E számolás hasonló az alábbihoz; a részleteket az Olvasóra bízzuk.) Áttérve a következő prímszámra, 641-re, azt kell ellenőriznünk, hogy

(155) $2^{2^5}+1 \equiv 0 \pmod{641}$

teljesül-e. A bal oldal első tagja:

$$2^{2^5} = 2^{32} = (2^9)^3 \cdot 2^5 = 512^3 \cdot 32 \equiv (-129)^3 \cdot 32 =$$

$$= -3^3 \cdot 43^3 \cdot 32 = -(27 \cdot 32) \cdot 43^2 \cdot 43 = -864 \cdot 1849 \cdot 43 \equiv$$

$$\equiv -223 \cdot (-74) \cdot 43 = (223 \cdot 2) \cdot 37 \cdot 43 = 446 \cdot 1591 \equiv -195 \cdot 309 =$$

$$= -195 \cdot 3 \cdot 103 = -585 \cdot 103 \equiv 56 \cdot 103 = 8 \cdot 7 \cdot 103 = 8 \cdot 721 \equiv$$

$$\equiv 8 \cdot 80 = 640 \equiv -1 \pmod{641},$$

ahonnan látható, hogy (155) teljesül. Így $641 | 2^{2^5}+1$, másrészt

$$2^{2^5}+1 = 2^{32}+1 = (2^4)^8+1 > 10^8 > 641,$$

tehát $2^{2^5}+1$ valóban összetett szám.

64.

a. $9^{\frac{12}{(5,12)}} = 9^{\frac{12}{1}} = 9^{12} \equiv 1 \pmod{13}$.

(tekintettel a Fermat-tételre), tehát a kongruencia megoldható. A megoldásszám: $(5, 12)=1$.

b. $11^{\frac{12}{(10,12)}} = 11^{\frac{12}{2}} = 11^6 \equiv (-2)^6 = 64 \equiv -1 \pmod{13}$,

tehát a kongruencia megoldhatatlan.

c. $8^{\frac{12}{(9,12)}} = 8^{\frac{12}{3}} = 8^4 \equiv (-5)^4 = (5^2)^2 = 25^2 \equiv (-1)^2 = 1 \pmod{13}$,

tehát a kongruencia megoldható. A megoldásszám: $(9, 12)=3$.

65. Az a egész szám akkor és csak akkor p-edik hatványmaradék modulo p, ha

$$a^{\frac{p-1}{(p,p-1)}} = a^{\frac{p-1}{1}} = a^{p-1} \equiv 1 \pmod{p}$$

(nyilván $(p, p-1)=1$). Ez utóbbi kongruencia azonban a Fermat-tétel szerint $a=1, 2, \ldots, p-1$ esetén teljesül, tehát e számok mindegyike p-edik hatványmaradék modulo p.

66. *a.* Ha mind a, mind b k-adik hatványmaradék modulo p, akkor

(156) $a^{\frac{p-1}{(k,p-1)}} \equiv 1 \pmod{p}$,

(157) $b^{\frac{p-1}{(k,p-1)}} \equiv 1 \pmod{p}$.

E két kongruenciát összeszorozva:

$$(158)\quad (ab)^{\frac{p-1}{(k,p-1)}} \equiv 1 \pmod{p},$$

ami azt jelenti, hogy ab is k-adik hatványmaradék modulo p.

b. Ha a és ab is k-adik hatványmaradék modulo p, vagyis (156) és (158) is teljesül, akkor (156)-ra tekintettel (158) bal oldala:

$$(159)\quad (ab)^{\frac{p-1}{(k,p-1)}} = a^{\frac{p-1}{(k,p-1)}} b^{\frac{p-1}{(k,p-1)}} \equiv 1 \cdot b^{\frac{p-1}{(k,p-1)}} = b^{\frac{p-1}{(k,p-1)}} \pmod{p}.$$

(156)-ból és (159)-ből következik (157), tehát b is k-adik hatványmaradék modulo p. Innen következik az állítás.

67. Minthogy a k-adik hatványmaradék modulo p, szükségképpen $(a,p)=1$ és létezik olyan x_0 egész szám, melyre

$$x_0^k \equiv a \pmod{p}.$$

Innen következik, hogy $(-a,p)=1$ is teljesül, továbbá, mivel k páratlan,

$$(-x_0)^k = -x \equiv -a \pmod{p}.$$

Így $-x_0$ megoldása az

$$x^k \equiv -a \pmod{p}$$

kongruenciának, tehát $-a$ is k-adik hatványmaradék modulo p.

68. Ha a k-adik hatványmaradék modulo p, és $(a,p)=1$, akkor létezik olyan x_0 egész szám, melyre

$$x_0^k \equiv a \pmod{p}.$$

Innen következik, hogy $(x_0,p)=1$ is teljesül, tehát létezik olyan x_0^* egész szám, melyre

$$(161)\quad x_0 x_0^* \equiv 1 \pmod{p}.$$

Ekkor (160)-ból és (161)-ből

$$a(x_0^*)^k \equiv x_0^k (x_0^*)^k = (x_0 x_0^*)^k \equiv 1^k = 1 \pmod{p}.$$

Innen a^* definíciója és a multiplikatív inverz *A)* tulajdonsága alapján következik, hogy

$$(x_0^*)^k \equiv a^* \pmod{p},$$

ami azt jelenti, hogy a^* is k-adik hatványmaradék modulo p.

69. A rend *B)* tulajdonsága szerint

$$(162)\quad o_{17}(10) \mid 17-1 = 16.$$

Ha indirekte feltesszük, hogy 10 nem primitív gyök modulo 17, vagyis

(163) $o_{17}(10) < 16$,

akkor (162)-ből következik, hogy

$$o_{17}(10) | 8.$$

Innen viszont a rend *A)* tulajdonsága alapján,

$$10^8 \equiv 1 \pmod{17}.$$

Köbre emelve:

$$10^{24} \equiv 1 \pmod{17},$$

ami ellentmond az adott kongruenciának. A (163) indirekt feltevésből tehát ellentmondásra jutottunk, és ezzel az állítást igazoltuk.

70. Minthogy

$$(-1)^2 = 1 \equiv 1 \pmod{p},$$

szükségképpen $o_p(-1) \leqq 2$. Másrészt, ha -1 primitív gyök modulo p, akkor $o_p(-1) = p-1$. E két feltétel egyidejűleg csak akkor teljesülhet, a $p=2$ vagy 3; könnyen ellenőrizhető, hogy -1 mindkét esetben primitív gyök modulo p.

71. Azt kell igazolnunk, hogy ha

(164) $o(a^k) = p-1$,

akkor

(165) $o(a) = p-1$.

Mindenekelőtt megjegyezzük, hogy ha a^k primitív gyök modulo p, akkor nyilván $(a^k, p) = 1$, és így $(a, p) = 1$, tehát $o(a)$ létezik. Továbbá bármely, az $(a, p) = 1$ feltételt kielégítő a egész számra $o(a) \leqq p-1$ (tekintettel a Fermat-tételre), tehát (165) igazolásához elegendő megmutatni, hogy

$$o(a) \geqq p-1.$$

Azonban

$$(a^k)^{o(a)} = (a^{o(a)})^k \equiv 1^k \equiv 1 \pmod{p-1},$$

ahonnan a rend definíciója értelmében — (164) alapján — következik, hogy

$$o(a) \geqq o(a^k) = p-1,$$

és ezzel az állítást maradéktalanul igazoltuk.

72. Az 59. feladatból $a=g$ helyettesítéssel nyerjük, hogy

$$(p-1=)\mathrm{o}_p(g)=\mathrm{o}_p(g^*),$$

tehát g^* is primitív gyök modulo p.

73*. Először igazolni fogjuk, hogy $\mathrm{o}(-g)$ páros. Tegyük fel ugyanis indirekte, hogy $\mathrm{o}(-g)$ páratlan. A rend *B)* tulajdonsága szerint $\mathrm{o}(-g)|p-1=4k$. Minthogy $\mathrm{o}(-g)$ páratlan, $(\mathrm{o}(-g),4)=1$, tehát innen $\mathrm{o}(-g)|k$. Így a rend *A)* tulajdonsága szerint

$$(-g)^k \equiv 1 \pmod{p}.$$

Mindkét oldalt négyzetre emelve:

$$(-g)^{2k}=(-1)^{2k}g^{2k} \equiv 1 \pmod{p},$$

vagyis

$$g^{2k} \equiv 1 \pmod{p}.$$

Innen következnék, hogy

$$\mathrm{o}(g) \leqq 2k=\frac{p-1}{2}<p-1,$$

ami ellentmond annak a feltételnek, hogy g primitív gyök modulo p. Így az indirekt feltevésből ellentmondásra jutottunk, tehát $\mathrm{o}(-g)$ valóban páros. Ekkor azonban

$$(166)\quad (-g)^{\mathrm{o}(-g)}=(-1)^{\mathrm{o}(-g)}g^{\mathrm{o}(-g)}=g^{\mathrm{o}(-g)},$$

másrészt a rend definíciója szerint

$$(167)\quad (-g)^{\mathrm{o}(-g)} \equiv 1 \pmod{p}.$$

(166)-ot és (167)-et egybevetve, nyerjük, hogy

$$g^{\mathrm{o}(-g)} \equiv 1 \pmod{p},$$

tehát

$$(168)\quad \mathrm{o}(-g) \geqq \mathrm{o}(g)=p-1.$$

Másrészt a Fermat-tétel alapján bármely p-hez relatív prím egész szám rendje legfeljebb $p-1$, tehát

$$(169)\quad \mathrm{o}(-g) \leqq p-1.$$

(168)-ból és (169)-ből következik, hogy $\mathrm{o}(-g)=p-1$, tehát $-g$ primitív gyök modulo p.

74*. Nyilván

$$p-1 \equiv -1 \pmod{p},$$

vagyis

$$2^n \equiv -1 \pmod{p}.$$

Mindkét oldalt négyzetre emelve:

$$2^{2n} \equiv 1 \pmod{p}.$$

Innen következik, hogy

(170) $o(2) \leqq 2n.$

Azt kell igazolnunk, hogy

$$o(2) < p-1 = 2^n.$$

(170)-re tekintettel elég igazolni, hogy

$$2n < 2^n,$$

ha $n>2$. Ez n-re vonatkozó teljes indukcióval könnyen igazolható; a részleteket az Olvasóra bízzuk.

75*. Ha $p-1|k$, akkor a Fermat-tétel szerint a vizsgált összeg valamennyi tagja 1-gyel kongruens modulo p, tehát a keresett maradék nyilván $p-1$.

Ha viszont $p-1 \nmid k$, akkor tetszőleges g primitív gyököt tekintve, szükségképpen

(171) $g^k \not\equiv 1 \pmod{p}.$

A primitív gyök második definíciója szerint az $1, 2, \ldots, p-1$ számok — sorrendtől eltekintve — kongruensek a $g, g^2, \ldots, g^{p-1}$ számokkal, tehát

$$\sum_{i=1}^{p-1} i^k \equiv \sum_{i=1}^{p-1} (g^i)^k = \sum_{i=1}^{p-1} (g^k)^i \pmod{p}.$$

Itt g^k hányadosú mértani sor áll. (171)-ből következik, hogy $g^k \neq 1$, tehát alkalmazható a mértani sor összegképlete:

(172) $$\sum_{i=1}^{p-1} i^k \equiv g^k \frac{(g^k)^{p-1}-1}{g^k-1} \pmod{p}.$$

A Fermat-tétel szerint

$$(g^k)^{p-1}-1 = (g^{p-1})^k-1 \equiv 1^k-1 = 0 \pmod{p}.$$

(171) szerint $(g^k-1, p)=1$, tehát oszthatunk g^k-1-gyel:

$$\frac{(g^k)^{p-1}-1}{g^k-1} \equiv 0 \pmod{p}.$$

Így (172)-ből

$$\sum_{i=1}^{p-1} i^k \equiv g^k \cdot 0 \equiv 0 \pmod{p},$$

tehát a keresett maradék ebben az esetben 0.

76. Legyen g tetszőleges primitív gyök modulo p. Ekkor az $1, 2, \ldots, p-1$ számok — sorrendtől eltekintve — kongruensek a $g, g^2, \ldots, g^{p-1}$ számokkal, tehát a 97. feladat alapján $p>2$ esetén

$$(p-1)! = 1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv g^1 \cdot g^2 \cdot \ldots \cdot g^{p-1} =$$

$$= g^{p\frac{p-1}{2}} = \left(g^{\frac{p-1}{2}}\right)^p \equiv (-1)^p = -1 \pmod{p}.$$

$p=2$ esetén pedig nyilván

$$(p-1)! = 1 \cdot 2 \equiv -1 \pmod{3}.$$

77. *a.* Mindkét oldalt felírva a 3 primitív gyök hatványaként:

$$3^{\overset{3}{\smile}\mathrm{ind}_{17} 9x} \equiv 3^{\overset{3}{\smile}\mathrm{ind}_{17} 14} \pmod{17}.$$

Ez a kongruencia a primitív gyökökről mondottak szerint akkor és csak akkor teljesül, ha

$$\overset{3}{\smile}\mathrm{ind}_{17} 9x \equiv \overset{3}{\smile}\mathrm{ind}_{17} 14 \pmod{16},$$

vagyis

$$\overset{3}{\smile}\mathrm{ind}_{17} 9 + \overset{3}{\smile}\mathrm{ind}_{17} x \equiv \overset{3}{\smile}\mathrm{ind}_{17} 14 \pmod{16}.$$

A 2. táblázatból kikeresve ind 9 és ind 14 értékét:

$$2 + \overset{3}{\smile}\mathrm{ind}_{17} x \equiv 9 \pmod{16},$$

$$\overset{3}{\smile}\mathrm{ind}_{17} x \equiv 7 \pmod{16}.$$

Innen az 1. táblázatot felhasználva, nyerjük, hogy

$$x \equiv 11 \pmod{17}.$$

b. Mindkét oldalt 3 hatványaként írva:

$$3^{\overset{3}{\smile}\mathrm{ind}_{17} x^{11}} \equiv 3^{\overset{3}{\smile}\mathrm{ind}_{17} 6} \pmod{17}.$$

Innen

$$11\,\overset{3}{\underset{\smile}{\mathrm{ind}}}_{17}x \equiv \overset{3}{\underset{\smile}{\mathrm{ind}}}_{17}6 \pmod{16},$$

vagyis a 2. táblázatot felhasználva:

$$-5\,\overset{3}{\underset{\smile}{\mathrm{ind}}}_{17}x \equiv 15 \pmod{16}.$$

Mindkét oldalt -5-tel osztva:

$$\overset{3}{\underset{\smile}{\mathrm{ind}}}_{17}x \equiv -3 \equiv 13 \pmod{16}.$$

Innen az 1. táblázat alapján:

$$x \equiv 12 \pmod{17}.$$

c. Mindkét oldalt 3 hatványaként írva:

$$3^{\overset{3}{\underset{\smile}{\mathrm{ind}}}_{17}11x^{10}} \equiv 3^{\overset{3}{\underset{\smile}{\mathrm{ind}}}_{17}5} \pmod{17}.$$

Innen

$$\overset{3}{\underset{\smile}{\mathrm{ind}}}_{17}11 + 10\,\overset{3}{\underset{\smile}{\mathrm{ind}}}_{17}x \equiv \overset{3}{\underset{\smile}{\mathrm{ind}}}_{17}5 \pmod{16},$$

vagyis a 2. táblázat alapján:

$$7 + 10\,\overset{3}{\underset{\smile}{\mathrm{ind}}}_{17}x \equiv 5 \pmod{16},$$

$$10\,\overset{3}{\underset{\smile}{\mathrm{ind}}}_{17}x \equiv -2 \pmod{16}.$$

Mindkét oldalt és a modulust is osztva 2-vel:

$$5\,\overset{3}{\underset{\smile}{\mathrm{ind}}}_{17}x \equiv -1 \equiv -1 + 2\cdot 8 = 15 \pmod{8}.$$

5-tel osztva:

$$\overset{3}{\underset{\smile}{\mathrm{ind}}}_{17}x \equiv 3 \pmod{8},$$

tehát (21) szerint az összes megoldások modulo 16:

$$\overset{3}{\underset{\smile}{\mathrm{ind}}}_{17}x \equiv 3 \pmod{16},$$

$$\overset{3}{\underset{\smile}{\mathrm{ind}}}_{17}x \equiv 11 \pmod{16}.$$

Az 1. táblázat segítségével visszakeresve, megkapjuk az eredeti kongruencia összes megoldásait:

$$x \equiv 10 \pmod{17},$$

$$x \equiv 7 \pmod{17}.$$

78. *a.* Mindkét oldalt 3 hatványaként írva:

$$3^{\overset{3}{\smile}\mathrm{ind}_{17} 5^x} \equiv 3^{\overset{3}{\smile}\mathrm{ind}_{17} 12} \pmod{17}.$$

Innen

$$x \overset{3}{\smile}\mathrm{ind}_{17} 5 \equiv \overset{3}{\smile}\mathrm{ind}_{17} 12 \pmod{16},$$

vagyis a 2. táblázatot felhasználva:

$$5x \equiv 13 \equiv 13+2\cdot 16 = 45 \pmod{16}.$$

ahonnan 5-tel osztva:

(173) $x \equiv 9 \pmod{16}.$

Továbbá x-nek nyilván ki kell elégítenie az

(174) $x \geqq 0$

feltételt is; a vizsgált kongruencia összes megoldásai a (173)-at és (174)-et kielégítő egész számok.

b. Mindkét oldalt 3 hatványaként írva:

$$3^{\overset{3}{\smile}\mathrm{ind}_{17} 5\cdot 6^x} \equiv 3^{\overset{3}{\smile}\mathrm{ind}_{17} 7} \pmod{17}.$$

Innen

$$\overset{3}{\smile}\mathrm{ind}_{17} 5 + x \overset{3}{\smile}\mathrm{ind}_{17} 6 \equiv \overset{3}{\smile}\mathrm{ind}_{17} 7 \pmod{16},$$

vagyis a 2. táblázatot felhasználva:

$$5+15x \equiv 11 \pmod{16},$$

$$15x \equiv -x \equiv 6 \pmod{16}.$$

Mindkét oldalt -1-gyel szorozva:

(175) $x \equiv -6 \equiv 10 \pmod{16}.$

A vizsgált kongruencia megoldásai a (175)-öt kielégítő *pozitív* egész számok.

79. Felírva (85) mindkét oldalát g hatványaként:

$$g^{\overset{g}{\mathrm{ind}}_p aa^*} \equiv g^0 \pmod{p}.$$

Innen

$$\overset{g}{\mathrm{ind}}_p aa^* \equiv 0 \pmod{p-1},$$

vagyis

$$\overset{g}{\mathrm{ind}}_p a + \overset{g}{\mathrm{ind}}_p a^* \equiv 0 \pmod{p-1}.$$

80. Az 1, 2, ..., 12 számok közül azok a kvadratikus maradékok modulo 13, melyek kongruensek a $(\pm 1)^2$, $(\pm 2)^2$, ..., $(\pm 6)^2$ számok valamelyikével. Így e számok legkisebb nemnegatív maradékait kell meghatároznunk:

$$(\pm 1)^2 = 1 \equiv 1 \pmod{13},$$

$$(\pm 2)^2 = 4 \equiv 4 \pmod{13},$$

$$(\pm 3)^2 = 9 \equiv 9 \pmod{13},$$

$$(\pm 4)^2 = 16 \equiv 3 \pmod{13},$$

$$(\pm 5)^2 = 25 \equiv 12 \pmod{13},$$

$$(\pm 6)^2 = 36 \equiv 10 \pmod{13}.$$

A kvadratikus maradékok tehát 1, 3, 4, 9, 10, 12.

81. A Legendre-szimbólum *B)* és *D)* tulajdonságát felhasználva:

$$\left(\frac{a^{2k+1}}{p}\right) = \left(\frac{(a^2)^k \cdot a}{p}\right) = \left(\frac{a^2}{p}\right)^k \cdot \left(\frac{a}{p}\right) = 1^k \cdot \left(\frac{a}{p}\right) = \left(\frac{a}{p}\right),$$

ahonnan következik az állítás.

82. (85)-ből következik, hogy $(a, p) = (a^*, p) = 1$, tehát az $\left(\frac{a}{p}\right)$ és $\left(\frac{a^*}{p}\right)$ Legendre-szimbólumok léteznek. (85)-ből a Legendre-szimbólum *A)* tulajdonsága alapján nyerjük, hogy

$$\left(\frac{aa^*}{p}\right) = \left(\frac{1}{p}\right).$$

Innen a Legendre-szimbólum *B)*, ill. *D)* tulajdonsága alapján következik hogy

$$\left(\frac{a}{p}\right)\left(\frac{a^*}{p}\right) = 1.$$

Mindkét oldalt $\left(\frac{a^*}{p}\right)$-vel szorozva:

$$\left(\frac{a}{p}\right)\left(\frac{a^*}{p}\right)^2 = \left(\frac{a^*}{p}\right).$$

A bal oldal második tényezője nyilván 1, hiszen az $\left(\frac{a^*}{p}\right)$ Legendre-szimbólum értéke akár -1, akár $+1$, négyzete $+1$-gyel egyenlő. Így innen

$$\left(\frac{a}{p}\right) = \left(\frac{a^*}{p}\right)$$

következik, és éppen ezt kellett igazolnunk.

83. Az 1. pont *I)* tételéből $(a, p)=1$-re tekintettel következik, hogy az $ax+b$ számok — ahol $x=0, 1, \ldots, p-1$ — teljes maradékrendszert alkotnak modulo p. Így a Legendre-szimbólum *A)* tulajdonsága alapján

$$\sum_{x=0}^{p-1}\left(\frac{ax+b}{p}\right) = \sum_{k=0}^{p-1}\left(\frac{k}{p}\right) = \left(\frac{0}{p}\right)+\sum_{k=1}^{p-1}\left(\frac{k}{p}\right) = \sum_{k=1}^{p-1}\left(\frac{k}{p}\right).$$

Azonban egy modulo p redukált maradékrendszer elemeinek fele kvadratikus maradék, fele kvadratikus nem-maradék modulo p. Így ez utóbbi összeg tagjainak fele -1, fele $+1$, tehát az összeg értéke 0.

84*. Ha $p|k$, akkor a Legendre-szimbólum *A)* és *B)* tulajdonsága szerint

$$\sum_{x=0}^{p-1}\left(\frac{x(x+k)}{p}\right) = \sum_{x=0}^{p-1}\left(\frac{x^2}{p}\right) = \left(\frac{0}{p}\right)+\sum_{x=1}^{p-1}\left(\frac{x^2}{p}\right) = \sum_{x=1}^{p-1} 1 = p-1.$$

Ha viszont $(p, k)=1$, akkor induljunk ki abból, hogy $(x, p)=1$ esetén létezik olyan x^* egész szám, melyre

$$xx^* \equiv 1 \pmod{p}.$$

Ekkor a Legendre-szimbólum *A)*, *B)* és *D)* tulajdonságait felhasználva:

$$(176)\quad \sum_{x=0}^{p-1}\left(\frac{x(x+k)}{p}\right) = \left(\frac{0}{p}\right)+\sum_{x=1}^{p-1}\left(\frac{x(x+k)}{p}\right) =$$

$$= \sum_{x=1}^{p-1}\left(\frac{(x^*)^2}{p}\right)\left(\frac{x(x+k)}{p}\right) = \sum_{x=1}^{p-1}\left(\frac{xx^*(xx^*+kx^*)}{p}\right) =$$

$$= \sum_{x=1}^{p-1}\left(\frac{1\cdot(1+kx^*)}{p}\right) = \sum_{x=1}^{p-1}\left(\frac{kx^*+1}{p}\right).$$

(A végzett átalakítás során felhasználtuk, hogy — mint könnyen ellenőrizhető — $\left(\frac{k}{p}\right)$-t $p|k$ esetén a mondott módon definiálva, az *A)* és *D)* tulajdonságok kiterjeszthetők arra az esetre is, amikor $p|a$ vagy $p|b$ teljesül.) Minthogy most $(k, p)=1$, és a multiplikatív inverz *E)* tulajdonsága szerint az $x=1, 2, \ldots, p-1$ számokkal együtt a megfelelő x^* számok is redukált maradékrendszert alkotnak, szükségképpen a kx^* számok is redukált maradékrendszert alkotnak. Így a kx^*+1 számok — sorrendtől eltekintve — kongruensek a $2, 3, \ldots, p$ számokkal modulo p, tehát (176)-ból az előző feladat alapján

$$\sum_{x=0}^{p-1}\left(\frac{x(x+k)}{p}\right)=\sum_{x=1}^{p-1}\left(\frac{kx^*+1}{p}\right)=\sum_{x=2}^{p}\left(\frac{x}{p}\right)=$$

$$=\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)-\left(\frac{1}{p}\right)+\left(\frac{p}{p}\right)=0-1+0=-1.$$

A vizsgált összeg értéke tehát $p|k$ esetén $p-1$, $p\nmid k$ esetén -1.

85. $26^{\frac{29-1}{2}}=26^{14}\equiv(-3)^{14}=3^{14}=(3^3)^4\cdot 3^2=$

$$=27^4\cdot 9\equiv(-2)^4\cdot 9=16\cdot 9=4\cdot 36\equiv 4\cdot 7=28\equiv -1 \pmod{29},$$

tehát a kongruencia megoldhatatlan.

86. Az $5, 2\cdot 5, 3\cdot 5, \ldots, \frac{19-1}{2}\cdot 5=9\cdot 5$ számok legkisebb nemnegatív maradékát kell meghatároznunk:

$5\equiv 5 \pmod{19}$,

$2\cdot 5=10\equiv 10 \pmod{19}$,

$3\cdot 5=15\equiv 15 \pmod{19}$,

$4\cdot 5=20\equiv 1 \pmod{19}$,

$5\cdot 5=25\equiv 6 \pmod{19}$,

$6\cdot 5=30\equiv 11 \pmod{19}$,

$7\cdot 5=35\equiv 16 \pmod{19}$,

$8\cdot 5=40\equiv 2 \pmod{19}$,

$9\cdot 5=45\equiv 7 \pmod{19}$.

Ezek közül a $\frac{19}{2}$-nél nagyobbak: 10, 11, 15, 16. Így $m=4$, tehát

$$\left(\frac{5}{19}\right) = (-1)^4 = +1,$$

vagyis a kongruencia megoldható.

87. *a.* A Legendre-szimbólum *B)*, *D)* és *E)* tulajdonságait felhasználva:

$$\left(\frac{-4}{41}\right) = \left(\frac{-1}{41}\right)\left(\frac{4}{41}\right) = \left(\frac{-1}{41}\right)\left(\frac{2^2}{41}\right) = (+1)\cdot(+1) = +1.$$

b. Az *A)*, *B)*, *D)*, *E)* tulajdonságok alapján:

$$\left(\frac{94}{103}\right) = \left(\frac{-9}{103}\right) = \left(\frac{-1}{103}\right)\left(\frac{9}{103}\right) = \left(\frac{-1}{103}\right)\left(\frac{3^2}{103}\right) = (-1)\cdot(+1) = -1.$$

c. Az *A)*, *B)*, *D)*, *E)*, *G)* tulajdonságok alapján:

$$\left(\frac{101}{109}\right) = \left(\frac{-8}{109}\right) = \left(\frac{-2}{109}\right)\left(\frac{4}{109}\right) = \left(\frac{-1}{109}\right)\left(\frac{2}{109}\right)\left(\frac{2^2}{109}\right) =$$

$$= (+1)\cdot(-1)\cdot(+1) = -1.$$

88. A Legendre-szimbólum *A)*, *B)* és *D)* tulajdonságait felhasználva:

$$\left(\frac{\frac{p+1}{2}}{p}\right) = \left(\frac{2^2}{p}\right)\left(\frac{\frac{p+1}{2}}{p}\right) = \left(\frac{2^2\cdot\frac{p+1}{2}}{p}\right) = \left(\frac{2p+2}{p}\right) = \left(\frac{2}{p}\right).$$

Így a *G)* tulajdonság szerint

$$\left(\frac{\frac{p+1}{2}}{p}\right) = \left(\frac{2}{p}\right) = \begin{cases} +1, \text{ ha } p \ 8k-1 \text{ vagy } 8k+1 \text{ alakú,} \\ -1, \text{ ha } p \ 8k-3 \text{ vagy } 8k+3 \text{ alakú.} \end{cases}$$

89.

a. $$\left(\frac{77}{103}\right) = \left(\frac{7}{103}\right)\left(\frac{11}{103}\right) =$$

$$= \left(\frac{103}{7}\right)(-1)^{\frac{103-1}{2}\cdot\frac{7-1}{2}}\left(\frac{103}{11}\right)(-1)^{\frac{103-1}{2}\cdot\frac{11-1}{2}} =$$

$$= \left(\frac{5}{7}\right)(-1)^{51\cdot 3}\left(\frac{4}{11}\right)(-1)^{51\cdot 5} = \left(\frac{-2}{7}\right)(-1)\left(\frac{2^2}{11}\right)(-1) =$$

$$= \left(\frac{-1}{7}\right)\left(\frac{2}{7}\right) = (-1)\cdot(+1) = -1.$$

$$b.\quad \left(\frac{131}{191}\right) = \left(\frac{191}{131}\right)(-1)^{\frac{191-1}{2}\cdot\frac{131-1}{2}} = \left(\frac{60}{131}\right)(-1)^{95\cdot 65} =$$

$$= \left(\frac{2^2}{131}\right)\left(\frac{3}{131}\right)\left(\frac{5}{131}\right)(-1) =$$

$$= \left(\frac{131}{3}\right)(-1)^{\frac{3-1}{2}\cdot\frac{131-1}{2}}\left(\frac{131}{5}\right)(-1)^{\frac{5-1}{2}\cdot\frac{131-1}{2}}(-1) =$$

$$= \left(\frac{-1}{3}\right)(-1)^{1\cdot 65}\left(\frac{1}{5}\right)(-1)^{2\cdot 65}(-1) = (-1)(-1)(+1)(+1)(-1) =$$

$$= -1.$$

90. Tegyük fel, hogy az

(177) $x^2 + ay^2 \equiv 0 \pmod{p}$

kongruenciának létezik nemtriviális megoldása, vagyis léteznek olyan x_0, y_0 egész számok, melyekre

(178) $x_0^2 + ay_0^2 \equiv 0 \pmod{p}$

és

$$x_0 \not\equiv 0 \pmod{p}$$

vagy

(179) $y_0 \not\equiv 0 \pmod{p}$

teljesül. Ekkor (179) mindenképpen fennáll, hiszen

$$y_0 \equiv 0 \pmod{p}$$

esetén (178)-ból

$$x_0 \equiv 0 \pmod{p}$$

is következne, vagyis x_0, y_0 triviális megoldás lenne. (179)-ből viszont következik, hogy létezik olyan y_0^* egész szám, melyre

$$y_0 y_0^* \equiv 1 \pmod{p}$$

teljesül. (178) mindkét oldalát megszorozva $(y_0^*)^2$-nel:

$$(x_0 y_0^*)^2 + a(y_0 y_0^*)^2 \equiv 0 \pmod{p},$$

vagyis

$$(x_0 y_0^*)^2 + a \equiv 0 \pmod{p}.$$

Így $z = x_0 y_0^*$ megoldása a

(180) $z^2 + a \equiv 0 \pmod{p}$

kongruenciának.

Másrészt, ha (180) megoldható, vagyis valamely z_0 egész számra (180) teljesül, akkor $x = z_0$, $y = 1$ nyilván megoldása (177)-nek, tehát (177) is megoldható.

91. Ha p páratlan prímosztója x^2+1-nek, akkor

$$x^2 + 1 \equiv 0 \pmod{p},$$

vagyis

$$x^2 \equiv -1 \pmod{p}.$$

Ez páratlan p-re az *E)* tulajdonság szerint valóban csak akkor teljesülhet, ha p $4k+1$ alakú.

92. A 90. feladat szerint a vizsgált kongruenciának akkor és csak akkor létezik nemtriviális megoldása, ha a

$$z^2 + 1 \equiv 0 \pmod{p}$$

vagyis

$$z^2 \equiv -1 \pmod{p}$$

kongruencia megoldható. Ez utóbbi kongruencia viszont a Legendre-szimbólum *E)* tulajdonsága szerint akkor és csak akkor oldható meg, ha $p=2$ vagy p $4k+1$ alakú.

93*. A kongruencia mindkét oldalából 2-t kivonva:

$$x^2 \equiv -2 \pmod{p}.$$

Ha $p=2$, akkor ez a kongruencia nyilván megoldható. Ha viszont $p>2$, akkor a $\left(\frac{-2}{p}\right)$ Legendre-szimbólum értékét kell meghatároznunk. Azonban a Legendre-szimbólum *D)* tulajdonsága szerint

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right).$$

Így az *E)* és *G)* tulajdonságokat felhasználva, nyerjük, hogy

a. ha p $8k-3$ alakú, akkor

$$\left(\frac{-2}{p}\right) = (+1)\cdot(-1) = -1;$$

b. ha p $8k-1$ alakú, akkor

$$\left(\frac{-2}{p}\right) = (-1)\cdot(+1) = -1;$$

c. ha p $8k+1$ alakú, akkor

$$\left(\frac{-2}{p}\right) = (+1)\cdot(+1) = +1;$$

d. ha p $8k+3$ alakú, akkor

$$\left(\frac{-2}{p}\right) = (-1)\cdot(-1) = +1.$$

Végeredményben tehát a vizsgált kongruencia akkor és csak akkor oldható meg, ha $p=2$ vagy pedig p $8k+1$ vagy $8k+3$ alakú.

94*. Ha $p=2$, akkor $x=1$, ha $p=3$, akkor $x=0$ megoldása a vizsgált kongruenciának. Így a továbbiakban a $p>3$ esetre szorítkozhatunk.

A $\left(\frac{3}{p}\right)$ Legendre-szimbólum értékét kell meghatároznunk. Minthogy $p>3$, alkalmazhatjuk a kvadratikus reciprocitási tételt:

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)\cdot(-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}} = \left(\frac{p}{3}\right)\cdot(-1)^{\frac{p-1}{2}}.$$

Mivel $p>3$, szükségképpen $(p, 12)=1$, tehát p $12k-5$, $12k-1$, $12k+1$ vagy $12k+5$ alakú.

a. Ha p $12k-5$ alakú, akkor

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)\cdot(-1)^{\frac{p-1}{2}} = \left(\frac{1}{3}\right)\cdot(-1)^{6k-3} = (+1)\cdot(-1) = -1.$$

b. Ha p $12k-1$ alakú, akkor

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)\cdot(-1)^{\frac{p-1}{2}} = \left(\frac{-1}{3}\right)\cdot(-1)^{6k-1} = (-1)\cdot(-1) = +1.$$

c. Ha p $12k+1$ alakú, akkor

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)\cdot(-1)^{\frac{p-1}{2}} = \left(\frac{1}{3}\right)\cdot(-1)^{6k} = (+1)\cdot(+1) = +1.$$

d. Ha p $12k+5$ alakú, akkor

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)\cdot(-1)^{\frac{p-1}{2}} = \left(\frac{-1}{3}\right)\cdot(-1)^{6k+2} = (-1)\cdot(+1) = -1.$$

Végeredményben tehát a vizsgált kongruencia akkor és csak akkor oldható meg, ha $p=2$ vagy 3, vagy pedig p $12k-1$ vagy $12k+1$ alakú.

95*. Tegyük fel, hogy $p|8x^2-1$, vagyis

$$8x^2 \equiv 1 \pmod{p};$$

ekkor nyilván $p>2$. Mindkét oldalt 2-vel szorozva:

$$(4x)^2 \equiv 2 \pmod{p}.$$

Így 2 kvadratikus maradék modulo p, ahonnan ($p>2$-re tekintettel) a Legendre-szimbólum *G)* tulajdonsága alapján következik az állítás.

96*. Tegyük fel, hogy $p|12x^2+1$, vagyis

$$(181) \quad 12x^2 \equiv -1 \pmod{p};$$

ekkor nyilván $p>3$. Mindkét oldalt 3-mal szorozva:

$$(6x)^2 \equiv -3 \pmod{p}.$$

Azt kell megállapítanunk, hogy

$$\left(\frac{-3}{p}\right) = +1$$

mely p prímszámokra teljesül. A kvadratikus reciprocitási tételt és a Legendre-szimbólum *E)* tulajdonságát alkalmazva ($p>2$-re tekintettel):

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)(-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}} =$$

$$= (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}} = \left(\frac{p}{3}\right)(-1)^{2\cdot\frac{p-1}{2}} = \left(\frac{p}{3}\right).$$

Minthogy $p>3$, szükségképpen $(p, 6)=1$, tehát p $6k-1$ vagy $6k+1$ alakú.

a. Ha p $6k-1$ alakú, akkor

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{-1}{3}\right) = -1.$$

b. Ha p $6k+1$ alakú, akkor

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = +1.$$

Így (182)-ből következik, hogy p $6k+1$ alakú, és ezt kellett igazolnunk.

97. *a.* Minthogy g primitív gyök modulo p, szükségképpen $(g, p)=1$, tehát az Euler-lemma szerint ($p>2$-re tekintettel)

$$(182) \quad g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

vagy

$$g^{\frac{p-1}{2}} \equiv +1 \pmod{p}.$$

Ez utóbbiból azonban $o(g) \leqq \frac{p-1}{2}$ következnék, ellentétben a primitív gyök definíciójával. Így szükségképpen (182) teljesül, és ezt kellett igazolnunk.

b. (182)-ből az Euler-lemma szerint következik, hogy g kvadratikus nem-maradék modulo p.

98. Ha g_1, g_2 primitív gyökök modulo p, akkor ($p > 2$-re tekintettel) az előző feladat *b.* részéből következik, hogy

$$\left(\frac{g_1}{p}\right) = \left(\frac{g_2}{p}\right) = -1.$$

Így a Legendre-szimbólum multiplikativitására (*D)* tulajdonságára) tekintettel

$$\left(\frac{g_1 g_2}{p}\right) = \left(\frac{g_1}{p}\right)\left(\frac{g_2}{p}\right) = (-1)(-1) = +1,$$

ahonnan viszont ismét az előző feladat alapján következik, hogy $g_1 g_2$ *nem* primitív gyök modulo p.

99*. Tegyük fel indirekte, hogy

(183) $o_p(2) < p-1 = 4q.$

A rend *B)* tulajdonságából következik, hogy

(184) $o_p(2) | p-1 = 4q.$

Mivel q prímszám, (183) és (184) egyidejűleg csak úgy teljesülhetnek, ha

(185) $o_p(2) | 4$

vagy

(186) $o_p(2) | 2q.$

(185)-ből a rend *A)* tulajdonsága alapján következnék, hogy

$$2^4 \equiv 1 \pmod{p},$$

vagyis

$$2^4 - 1 = 15 \equiv 0 \pmod{p}.$$

15-nek azonban nincs $4q+1$ alakú prímosztója (a 3 és 5 prímosztók egyike sem ilyen alakú), tehát ez az eset nem lehetséges.

(186)-ból ismét a rend *A)* tulajdonsága alapján következnék, hogy

$$2^{2q} = 2^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

tehát 2 kvadratikus maradék lenne modulo p. Azonban, ha q prímszám és $p=4q+1$ is prímszám, akkor q szükségképpen páratlan szám, tehát p

$$p = 4q+1 = 4(2k-1)+1 = 8k-3$$

alakú. Így a Legendre-szimbólum *G)* tulajdonságából következik, hogy 2 kvadratikus nem-maradék modulo p. A (183) indirekt feltevésből tehát ellentmondásra jutottunk, és ezzel az állítást igazoltuk.

100. A kongruencia a következő alakban írható:

$$x^2+3x-3 \equiv x^2-14x-3 = (x-7)^2-52 \equiv (x-7)^2-1 \equiv 0 \pmod{17},$$

vagyis

$$(x-7)^2 \equiv 1 \pmod{17}.$$

E kongruenciának nyilván két lényegesen különböző megoldása van $x-7$-re, nevezetesen -1 és $+1$. Így innen nyerjük, hogy az adott kongruencia összes megoldásai:

$$x \equiv -1+7 = 6 \pmod{17},$$

$$x \equiv +1+7 = 8 \pmod{17}.$$

101. A kongruencia a következő alakban írható:

$$x^{10}-x^5-5 \equiv x^{10}+16x^5-5 = (x^5+8)^2-69 \equiv 0 \pmod{17},$$

$$(x^5+8)^2 \equiv 69 \equiv 1 \pmod{17}.$$

Innen

$$x^5+8 \equiv \pm 1 \pmod{17},$$

tehát

(187) $x^5 \equiv -1-8 \equiv 8 \pmod{17}$

vagy

(188) $x^5 \equiv +1-8 \equiv 10 \pmod{17}$.

(187) a következő alakban írható:

$$3^{\overset{3}{\smile}\mathrm{ind}_{17}x^5} \equiv 3^{\overset{3}{\smile}\mathrm{ind}_{17}8} \pmod{17},$$

ahonnan a 2. táblázat alapján:

$$5\,\overset{3}{\smile}\mathrm{ind}_{17}x \equiv \overset{3}{\smile}\mathrm{ind}_{17}8 = 10 \pmod{16}.$$

Mindkét oldalt 5-tel osztva (mely relatív prím a moduloshoz, 16-hoz):

$$\overset{3}{\smile}\mathrm{ind}_{17} x \equiv 2 \pmod{16}.$$

Visszakeresve az 1. táblázat segítségével:

(189) $x \equiv 9 \pmod{17}$.

(188) a következő alakban írható:

$$3^{\overset{3}{\smile}\mathrm{ind}_{17} x^5} \equiv 3^{\overset{3}{\smile}\mathrm{ind}_{17} 10} \pmod{17}.$$

Innen a 2. táblázatot felhasználva:

$$5\,\overset{3}{\smile}\mathrm{ind}_{17} x \equiv \overset{3}{\smile}\mathrm{ind}_{17} 10 = 3 \equiv 35 \pmod{16}.$$

Mindkét oldalt 5-tel osztva:

$$\overset{3}{\smile}\mathrm{ind}_{17} x \equiv 7 \pmod{16}.$$

Visszakeresve az 1. táblázat segítségével:

(190) $x \equiv 11 \pmod{17}$.

A vizsgált kongruencia megoldásai tehát a (189) és (190) alattiak.

III. SZÁMELMÉLETI FÜGGVÉNYEK

1. A $\sigma(n)$ FÜGGVÉNY. A PRÍMOSZTÓK SZÁMA

Már az előző két fejezetben találkoztunk két fontos számelméleti függvénnyel, nevezetesen a $d(n)$, illetve a $\varphi(n)$ függvénnyel. Ebben a pontban néhány további konkrét számelméleti függvényt fogunk tárgyalni.

Az n természetes szám pozitív osztóinak az összegét $\sigma(n)$-nel jelöljük. Igazolható, hogy *a* $\sigma(n)$ *számelméleti függvény multiplikatív* (erre a kérdésre a következő pontban még visszatérünk).

Mint a II. fejezet 2. pontjában (a $\varphi(n)$ függvénnyel kapcsolatban) már láttuk, egy $f(n)$ multiplikatív számelméleti függvény explicit alakjának meghatározása visszavezethető az $f(p^\alpha)$ értékek meghatározására. Ezért először $\sigma(p^\alpha)$-t (ahol p prímszám, α természetes szám) fogjuk kiszámítani. A p^α szám pozitív osztói $1, p, p^2, \ldots, p^\alpha$, tehát

$$(1) \qquad \sigma(p^\alpha) = 1+p+p^2+\ldots+p^\alpha = \frac{p^{\alpha+1}-1}{p-1}.$$

Így, ha az $n>1$ természetes szám kanonikus alakja

$$(2) \qquad n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r},$$

akkor $\sigma(n)$ multiplikativitására tekintettel

$$(3) \qquad \sigma(n) = \sigma(p_1^{\alpha_1})\sigma(p_2^{\alpha_2}) \ldots \sigma(p_r^{\alpha_r}) =$$

$$= \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}-1}{p_2-1} \cdot \ldots \cdot \frac{p_r^{\alpha_r+1}-1}{p_r-1}$$

(és nyilván $\sigma(1)=1$).

A $\sigma(n)$ számelméleti függvényhez kapcsolódik a *tökéletes szám* fogalma. Az n természetes számot akkor nevezzük töké-

letes számnak, ha

$$(4) \quad \frac{\sigma(n)}{n} = 2.$$

(A tökéletes szám fogalmát az teszi érdekessé, hogy ez a fogalom már Euklidesz műveiben is szerepel, másrészt néhány, a tökéletes számokkal kapcsolatos egyszerű kérdés azóta is eldöntetlen.) Ha $\frac{\sigma(n)}{n}<2$, akkor *hiányos*, ha $\frac{\sigma(n)}{n}>2$, akkor *bővelkedő* számnak mondjuk n-et.

Bizonyítható, hogy egy páros szám akkor és csak akkor tökéletes szám, ha $2^{p-1}(2^p-1)$ alakú, ahol p prímszám, és 2^p-1 is prímszám (ún. Mersenne-féle prímszám; l. az I. fejezet 61. feladatát). Minthogy nem tudjuk, hogy létezik-e végtelen sok 2^p-1 alakú prímszám, szükségképpen azt sem tudjuk, hogy létezik-e végtelen sok páros tökéletes szám? Nem ismeretes továbbá az sem, hogy létezik-e egyáltalán páratlan tökéletes szám?

Az alábbiakban további két számelméleti függvényt definiálunk, melyekkel gyakran találkozunk.

Legyen az $n>1$ természetes szám kanonikus alakja a (2) alatti. Az n szám *különböző prímosztóinak számát* $\nu(n)$-nel, *összes prímosztóinak számát* $\varkappa(n)$-nel jelöljük, tehát

$$\nu(n) = r$$

és

$$\varkappa(n) = \alpha_1+\alpha_2+\ldots+\alpha_r,$$

továbbá legyen $\nu(1)=\varkappa(1)=1$. (Megjegyezzük, hogy e két függvényre számos más jelölés is használatos.)

Könnyen látható, hogy a $\nu(n)$ és a $\varkappa(n)$ számelméleti függvények egyike sem multiplikatív, de van egy másik hasonló jellegű tulajdonságuk: *additivak*.

Ha egy $f(n)$ számelméleti függvény olyan, hogy bármely, az

$$(5) \quad (a, b) = 1$$

feltételt kielégítő a, b természetes számokra

$$(6) \quad f(ab) = f(a)+f(b)$$

teljesül, akkor $f(n)$-et *additív számelméleti függvénynek* nevezzük. Ha a (6) összefüggés bármely a, b számpárra teljesül (nem csupán az (5)-öt kielégítőkre), akkor $f(n)$-et *totálisan additív számelméleti függvénynek* mondjuk. Így például az $f(n)=\log n$ számelméleti függvény totálisan additív. Könnyen ellenőrizhető, hogy *a* $\nu(n)$ *számelméleti függvény additív* (de nem totálisan additív), míg *a* $\varkappa(n)$ *függvény totálisan additív.*

Néhány általános megjegyzés multiplikatív, ill. additív számelméleti függvényekre vonatkozóan:

Az azonosan 0 számelméleti függvény egyidejűleg multiplikatív és additív.

Ha $f(n)$ additív számelméleti függvény, akkor $g(n)=e^{f(n)}$ multiplikatív számelméleti függvény. Másrészt, ha a $g(n)$ multiplikatív számelméleti függvény csak pozitív értékeket vesz fel, akkor $f(n)=\log g(n)$ additív számelméleti függvény. Így az additív számelméleti függvények vizsgálata visszavezethető a multiplikatív számelméleti függvényekére (és ez részben megfordítva is igaz).

Ha $f(n)$ nem azonosan 0 multiplikatív, $g(n)$ additív számelméleti függvény, akkor szükségképpen $f(n)=1$ és $g(n)=0$ (l. a 3. példát).

Ha $f(n)$ multiplikatív, $g(n)$ totálisan multiplikatív, $h(n)$ additív, $k(n)$ totálisan additív számelméleti függvény, és az 1-nél nagyobb n természetes szám kanonikus alakja a (2) alatti, akkor

$$(7)\qquad f(n)=f(p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r})=f(p_1^{\alpha_1})f(p_2^{\alpha_2})\dots f(p_r^{\alpha_r}),$$

$$(8)\qquad g(n)=g(p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r})=[g(p_1)]^{\alpha_1}[g(p_2)]^{\alpha_2}\dots[g(p_r)]^{\alpha_r},$$

$$(9)\qquad h(n)=h(p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r})=h(p_1^{\alpha_1})+h(p_2^{\alpha_2})+\dots+h(p_r^{\alpha_r}),$$

$$(10)\qquad k(n)=k(p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r})=\alpha_1k(p_1)+\alpha_2k(p_2)+\dots+\alpha_rk(p_r).$$

Így multiplikatív vagy additív számelméleti függvényt elegendő prímszámhatvány helyeken, totálisan multiplikatív vagy totálisan additív számelméleti függvényt prímszám helyeken megadni; ezáltal a függvényt egyértelműen definiáljuk.

Ha $f(n)$, $g(n)$ multiplikatív, $h(n)$, $k(n)$ additív számelméleti függvények, akkor az $r(n)=f(n)g(n)$ számelméleti függvény szintén multiplikatív, az $s(n)=h(n)+k(n)$ függvény additív.

Példák

1. Oldjuk meg a

$$\sigma(p^x) = 2801$$

egyenletet p-re és x-re, ahol p prímszám, x természetes szám.

Megoldás:

$$\sigma(p^x) = 1+p+p^2+\ldots+p^x = 2801,$$

ahonnan

(11) $$p+p^2+\ldots+p^x = p(1+p+\ldots+p^{x-1}) = 2800.$$

Innen látható, hogy

(12) $$p|2800, \quad \text{de} \quad p^2 \nmid 2800.$$

Másrészt 2800 kanonikus alakja:

$$2800 = 28\cdot 100 = 2^2\cdot 7\cdot 2^2\cdot 5^2 = 2^4\cdot 5^3\cdot 7.$$

Így nyilván az egyetlen olyan p prímszám, melyre (12) teljesül, $p=7$. (11)-be helyettesítve:

$$7(1+7+\ldots+7^{x-1}) = 2800.$$

Mindkét oldalt 7-tel osztva:

$$1+7+\ldots+7^{x-1} = 400,$$

$$\frac{7^x-1}{7-1} = 400.$$

Innen

$$7^x = (7-1)\cdot 400+1 = 6\cdot 400+1 = 2401 = 7\cdot 343 =$$

$$= 7\cdot 7\cdot 49 = 7\cdot 7\cdot 7\cdot 7 = 7^4,$$

tehát végeredményben $p=7$ és $x=4$.

2. Számítsuk ki

a. $\nu(6!)$,

b. $\varkappa(6!)$

értékét!

Megoldás:

6! kanonikus alakja:

$$6! = 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6 = 2\cdot 3\cdot 2^2\cdot 5\cdot 2\cdot 3 = 2^4\cdot 3^2\cdot 5.$$

Így

a. $\nu(6!) = 3$,

b. $\varkappa(6!) = 4+2+1 = 7$.

3. Bizonyítsuk be, hogy ha $f(n)$ nem azonosan 0 multiplikatív számelméleti függvény, akkor

(13) $f(1) = 1$.

Megoldás:
Minthogy $f(n)$ multiplikatív,

(14) $(a, b) = 1$

esetén

(15) $f(ab) = f(a)f(b)$.

Továbbá feltevésünk szerint létezik olyan c természetes szám, melyre

(16) $f(c) \neq 0$.

$a=1, b=c$-t választva, (14) nyilván teljesül, tehát (15) is fennáll:

$$f(1 \cdot c) = f(1)f(c),$$

vagyis

$$f(c) = f(1)f(c).$$

(16)-ra tekintettel oszthatunk $f(c)$-vel, és ekkor éppen a bizonyítandó állítást nyerjük.

2. ÖSSZEGEZÉSI FÜGGVÉNY. A MÖBIUS-FÜGGVÉNY

Legyen $f(n)$ tetszőleges számelméleti függvény. A

(17) $g(n) = \sum_{d|n} f(d) \quad (n = 1, 2, \ldots)$

számelméleti függvényt az $f(n)$ függvény *összegzési függvényének* nevezzük.

Itt a jobb oldalon álló összegzés úgy értendő, hogy tekintjük n valamennyi d pozitív osztóját, minden egyes ilyen d-re kiszámítjuk $f(d)$ értékét, és a kapott $f(d)$ értékeket összeadjuk. Így például $f(n)=\varphi(n)$ és $n=10$ esetén

$$\sum_{d|10} \varphi(d) = \varphi(1)+\varphi(2)+\varphi(5)+\varphi(10) = 1+1+4+4 = 10.$$

A $d(n)$ függvény nyilván az $f(n)=1$, a $\sigma(n)$ függvény az $f(n)=n$ függvény összegzési függvénye:

$$(18)\quad d(n) = \sum_{d|n} 1,$$

$$(19)\quad \sigma(n) = \sum_{d|n} d.$$

A számelmélet alaptételéből könnyen levezethető, hogy ha az a, b, d természetes számokra

$$(20)\quad (a, b) = 1$$

és

$$(21)\quad d|ab,$$

akkor léteznek olyan *egyértelműen meghatározott* d_1, d_2 természetes számok, melyekre

$$(22)\quad d_1|a, \quad d_2|b$$

és

$$(23)\quad d = d_1 d_2$$

teljesül; másrészt, ha a d_1, d_2 természetes számokra (22) igaz, és d-t (23)-mal definiáljuk, akkor (21) nyilván teljesül. Ezt a segédtételt felhasználva könnyen látható, hogy *multiplikatív számelméleti függvény összegzési függvénye is multiplikatív.*

Ennek igazolása céljából először is megjegyezzük, hogy (20)-ból és (22)-ből következik, hogy $(d_1, d_2)=1$. Így a fenti segédtételt felhasználva, $f(n)$ multiplikativitásából következik, hogy $(m, n)=1$ esetén

$$g(m)g(n) = \left(\sum_{d_1|m} f(d_1)\right)\left(\sum_{d_2|n} f(d_2)\right) =$$

$$= \sum_{d_1|m} \sum_{d_2|n} f(d_1)f(d_2) = \sum_{d_1|m} \sum_{d_2|n} f(d_1 d_2) = \sum_{d|mn} f(d) = g(mn),$$

tehát a $g(n)$ függvény is multiplikatív.

Minthogy a (18), ill. (19) formula szerint $d(n)$ az $f(n)=1$, $\sigma(n)$ az $f(n)=n$ *multiplikatív* számelméleti függvény összegzési függvénye, az előbbi tétel szerint mind $d(n)$, mind $\sigma(n)$ multi-

plikatív (mint erre az I. fejezet 6. pontjában, ill. az előző pontban már utaltunk).

Az említett tételből az is következik, hogy valamely $f(n)$ multiplikatív számelméleti függvény $g(n)$ összegzési függvényét elegendő prímszámhatvány helyeken meghatározni; innen, a multiplikativitásra tekintettel, (7) alapján már adódik a függvényérték tetszőleges n-re. (Ezt az elvet követtük $d(n)$, ill. $\sigma(n)$ kiszámítása során is.)

Felmerül a kérdés, hogy (17)-ben a $g(n)$ összegzési függvényt ismerve, hogyan lehet az $f(n)$ függvényre visszakövetkeztetni? E probléma megválaszolásához szükségünk lesz a *Möbius-függvény* definíciójára.

Legyen n tetszőleges természetes szám. A

$$\mu(n) = \begin{cases} 1, \text{ ha } n = 1, \\ (-1)^r, \text{ ha } n = p_1 p_2 \dots p_r, \text{ ahol } i \neq j \text{ esetén } p_i \neq p_j, \\ 0, \text{ ha létezik olyan } p \text{ prím, melyre } p^2 | n \end{cases}$$

utasítással definiált számelméleti függvényt Möbius-függvénynek nevezzük. (Tehát $\mu(n) \neq 0$ akkor és csak akkor teljesül, ha n *négyzetmentes szám*; ezzel kapcsolatban l. az I. fejezet 68. feladatát.) Könnyen ellenőrizhető, hogy a $\mu(n)$ függvény multiplikatív.

Igazolható továbbá, hogy a Möbius-függvény összegzési függvénye:

$$(24) \quad \sum_{d|n} \mu(d) = \begin{cases} 1, & \text{ha } n = 1 \\ 0, & \text{ha } n > 1 \end{cases}$$

(l. a 6. példát).

Most már válaszolni tudunk a (17) formulával kapcsolatban felvetett kérdésre.

Legyen $g(n)$ tetszőleges számelméleti függvény. Az

$$(25) \quad f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right)$$

függvényt a $g(n)$ függvény *Möbius-transzformáltjának* nevez-

zük. (Ha d az n szám pozitív osztóin fut végig, akkor nyilván $\frac{n}{d}$ is, csupán fordított sorrendben; ezért a (25)-ben szereplő két összeg nyilván azonos). (24)-et felhasználva, igazolható, hogy (17)-ben a $g(n)$ összegzési függvényt megadva, (17) *egyértelműen definiálja $f(n)$-et*, nevezetesen *$f(n)$ a $g(n)$ függvény Möbius-transzformáltjával azonos.* Így valamely $f(n)$ számelméleti függvény $g(n)$ összegzési függvényének ismeretében (25) révén számítható ki; ebben a vonatkozásban (25)-öt *Möbius-féle inverziós* (megfordítási) *formulának* nevezzük. Igazolható továbbá, hogy *multiplikatív függvény Möbius-transzformáltja is multiplikatív*, tehát végeredményben (17)-ben $g(n)$ akkor és csak akkor multiplikatív, ha $f(n)$ is az.

Példák

4. Számítsuk ki az Euler-féle $\varphi(n)$ függvény összegzési függvényét!

Megoldás:
Minthogy a $\varphi(n)$ függvény multiplikatív, annak

$$g(n) = \sum_{d|n} \varphi(d)$$

összegzési függvénye is multiplikatív. Így elég $g(p^\alpha)$-t (ahol p prímszám, α természetes szám) meghatározni. Azonban $g(n)$ definíciójára és $\varphi(n)$ explicit alakjára tekintettel:

$$g(p^\alpha) = \sum_{d|p^\alpha} \varphi(p^\alpha) = \sum_{k=0}^{\alpha} \varphi(p^k) =$$

$$= \varphi(1)+\varphi(p)+\varphi(p^2)+\ldots+\varphi(p^{\alpha-1})+\varphi(p^\alpha) =$$

$$= 1+(p-1)+(p^2-p)+\ldots+(p^{\alpha-1}-p^{\alpha-2})+(p^\alpha-p^{\alpha-1}) = p^\alpha.$$

Így ha $n>1$ esetén n kanonikus alakja a (2) alatti, akkor

$$g(n) = g(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r}) = g(p_1^{\alpha_1})g(p_2^{\alpha_2})\ldots g(p_r^{\alpha_r}) =$$

$$= p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r} = n,$$

tehát az összegzési függvény $n>1$ esetén $g(n)=n$:

$$n = \sum_{d|n} \varphi(d),$$

és ez az egyenlőség nyilván $n=1$ esetén is teljesül.

5. Határozzuk meg $\mu(30)$ értékét!

Megoldás:

$$\mu(30) = \mu(2\cdot 3\cdot 5) = (-1)^3 = -1.$$

6. Igazoljuk a (24) összefüggést!

Megoldás:
Minthogy a $\mu(n)$ függvény multiplikatív, annak

$$g(n) = \sum_{d|n} \mu(d)$$

összegzési függvénye is az. Így elég $g(p^\alpha)$-t meghatározni:

$$g(p^\alpha) = \sum_{d|p^\alpha} \mu(d) = \sum_{k=0}^{\alpha} \mu(p^k) =$$

$$= \mu(1)+\mu(p)+\mu(p^2)+\ldots+\mu(p^\alpha) = 1+(-1)+0+\ldots+0 = 0.$$

Így ha $n>1$, és n kanonikus alakja a (2) alatti, akkor

$$g(n) = g(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r}) = g(p_1^{\alpha_1})g(p_2^{\alpha_2})\ldots g(p_r^{\alpha_r}) =$$

$$= 0\cdot 0\cdot\ldots\cdot 0 = 0,$$

továbbá nyilván

$$g(1) = \mu(1) = 1.$$

Ezzel (24)-et igazoltuk.

7. Határozzuk meg a $g(n)=n$ függvény $f(n)$ Möbius-transzformáltját!

Megoldás:
Legegyszerűbben azáltal érhetünk célt, hogy hivatkozunk a 4. példára. A 4. példa szerint ugyanis a $g(n)=n$ függvény az

$$f(n) = \varphi(n) \tag{26}$$

függvény összegzési függvénye. Így szükségképpen az előbbinek, $g(n)$-nek a Möbius-transzformáltja az utóbbi, tehát a $\varphi(n)$ függvény.

Érdemes azonban a Möbius-transzformáltat a (25) formula révén is kiszámítani:

$$f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d)\frac{n}{d} = n\sum_{d|n}\frac{\mu(d)}{d}.$$

Ezt az eredményt (26)-tal egybevetve, nyerjük a $\varphi(n)$ függvény egy gyakran használt előállítását (melyre még mi is fogunk hivatkozni):

$$\varphi(n) = n\sum_{d|n}\frac{\mu(d)}{d}. \tag{27}$$

3. SZÁMELMÉLETI FÜGGVÉNYEK ÉRTÉKEINEK ELOSZLÁSA. SZÁMELMÉLETI FÜGGVÉNYEK KÖZÉPÉRTÉKEI

Gyakran találkozunk a számelméletben azzal a problémával, hogy mit lehet egy konkrét számelméleti függvény vagy bizonyos tulajdonságokkal jellemzett számelméleti függvények értékeinek eloszlásáról mondani? A legegyszerűbb ilyen típusú kérdés az, hogy milyen nagyok, ill. milyen kicsik lehetnek egy $f(n)$ számelméleti függvény értékei n függvényében? (Az ilyen jellegű eredményeknek sok alkalmazásuk van például az ún. kombinatorikus számelméletben.)

Például a $\varphi(n)$ függvényre $n>1$ esetén nyilván

$$\varphi(n) \leqq n-1,$$

és ez a $\varphi(n)$-re adott felső korlát általában nem javítható, hiszen ha n prímszám, akkor itt egyenlőség áll. Így a $\varphi(n)$ függvénnyel kapcsolatban csupán az a kérdéses, hogy $\varphi(n)$ milyen „kicsi" lehet? A 24.* feladat kapcsán igazolni fogjuk, hogy $n>1$ esetén

$$\varphi(n) > \frac{n}{4 \log n}.$$

Felmerül az a kérdés, hogy ez az alsó becslés mennyiben javítható? A IV. fejezet 25. feladatában még foglalkozni fogunk ezzel a problémával.

Hasonló probléma vethető fel a $d(n), \sigma(n), \nu(n), \varkappa(n)$ függvényekkel kapcsolatban is.

Könnyen látható, hogy mind a négy esetben csupán az a kérdéses, hogy a szóban forgó számelméleti függvény milyen nagy értékeket vehet fel? A $\varkappa(n)$ függvény esetében könnyen megadható a válasz (l. a 8. példát). A másik három függvény esetében viszont fel kell használnunk a prímszámelmélet bizonyos eredményeit; ezért e kérdésekre szintén a következő fejezetben fogunk visszatérni.

Mint az említett számelméleti függvények alaposabb vizsgálata is mutatja, egy $f(n)$ számelméleti függvény értékei általában igen erősen ingadoznak. Bizonyos esetekben az ebből

eredő nehézségek kiküszöbölhetők, ha tudjuk, hogy $f(n)$ „középértéke" viszonylag szabályosan viselkedik, vagy $f(n)$ ingadozása „kevés" kivételes n-et elhagyva, viszonylag szűk határok közé szorítható. Először az előbbi típusú eredményekkel fogunk foglalkozni.

Egy $f(n)$ számelméleti függvény

$$(28) \quad \frac{\sum_{i \leqq x} f(i)}{x}$$

középértékének vizsgálata nyilván ekvivalens a

$$(29) \quad \sum_{i \leqq x} f(i)$$

összeg vizsgálatával. Célunk általában *aszimptotikus formulát* vagy röviden *aszimptotikát* találni erre az összegre. Ezen a következőt értjük:

Ha a $g(x)$ és $h(x)$ — például $x \geqq 0$ esetén definiált — függvényekre teljesül, hogy x-szel tartva a végtelenhez, a $\frac{g(x)}{h(x)}$ hányados 1-hez tart, vagyis

$$\lim_{x \to +\infty} \frac{g(x)}{h(x)} = 1,$$

akkor azt mondjuk, hogy $g(x)$ aszimptotikusan egyenlő $h(x)$-szel. Így a (29) összegre vonatkozó aszimptotikus formulán olyan $g(x)$ függvény megadását értjük, mely aszimptotikusan egyenlő ezzel az összeggel.

A konkrét számelméleti függvények középértékeire vonatkozó tételek közül talán a $d(n)$-re vonatkozó a legfontosabb. A 9. példa kapcsán igazolni fogjuk, hogy

$$(30) \quad \sum_{i \leqq x} d(i) \sim x \log x.$$

A bal oldalon álló összegre az itteninél pontosabb közelítő formula is megadható, és fontos és távolról sem lezárt kérdés e formula hibatagjának (vagyis a vizsgált összeg és az azt közelítő kifejezés különbségének) vizsgálata. Ez az ún. *Dirichlet-féle osztó-probléma.*

A 33. feladat kapcsán a $\sigma(n)$ és $\varphi(n)$ függvényre is megfogunk adni olyan összefüggéseket, melyekből levezethető egy aszimptotikus formula e függvények középértékére. *Additív* számelméleti függvények (így $\nu(n)$ és $\varkappa(n)$) középértékei a 29. és 30. feladatokban szereplő összefüggések segítségével vizsgálhatók.

Mint említettük, bizonyos alkalmazásokban nem annyira a szóban forgó számelméleti függvény középértékére van szükségünk, mint inkább arra, hogy a függvényértékek leggyakrabban (a legtöbb n-re) milyen határok közé esnek? (A két kérdés nem ugyanaz, mint azt például a $d(n)$ függvény mutatja; a $d(1), d(2), \ldots, d(n)$ számok középértéke ugyanis (30) szerint $\log n$, másrészt az alábbi tételt felhasználva igazolható, hogy a legtöbb, $1 \leqq j \leqq n$ feltételt kielégítő j számra $d(j)$ értéke $(\log n)^{\log 2}$ „közelébe" esik.) A legfontosabb ilyen jellegű eredmény az ún. *Hardy—Ramanujan-tétel*, melynek igen sok alkalmazása van:

Tetszőlegesen kicsi ε pozitív számhoz találhatók olyan ω és n_0 számok, hogy $n > n_0$ esetén az $1, 2, \ldots, n$ számok közül legfeljebb εn számot elhagyva, a megmaradó j számokra

$$|\nu(j) - \log\log n| < \omega \sqrt{\log\log n}$$

teljesül. (Tehát a $\nu(j)$ értékek leggyakrabban a középérték — l. a IV. fejezet 24. feladatát —, vagyis $\log\log n$ közelébe esnek.) Ez az állítás igaz marad akkor is, ha itt $\nu(n)$-et $\varkappa(n)$-nel helyettesítjük.

E tételhez kapcsolódva a számelmélet egy új területe alakult ki, melynek tárgyát *valószínűségszámítási módszerek számelméleti alkalmazásai* képezik.

Végül még egy kérdéskört említünk (mely eredetileg az információelmélet axiomatizálásával kapcsolatosan alakult ki). Nevezetesen a probléma az, hogy mennyiben lehet egy multiplikatív vagy additív számelméleti függvényt (vagy azok egy csoportját), így mindenekelőtt az $f(n) = c \log n$ (c állandó) függvényt bizonyos egyszerű analitikus tulajdonságokkal egyértelműen karakterizálni? Ezzel kapcsolatban *Erdős Pál tételét* említjük:

Ha $f(n)$ totálisan additív monoton (növekvő vagy csökkenő) számelméleti függvény, akkor szükségképpen

$$f(n) = c \log n$$

alakú (ahol c állandó).

Példák

8. Bizonyítsuk be, hogy

a. létezik végtelen sok olyan n természetes szám, melyre

$$\varkappa(n) = \frac{\log n}{\log 2}; \tag{31}$$

b. tetszőleges n természetes számra

$$\varkappa(n) \leqq \frac{\log n}{\log 2}. \tag{32}$$

Megoldás:

a. Legyen

$$n = 2^k. \tag{33}$$

Ekkor

$$\varkappa(n) = k, \tag{34}$$

másrészt (33) mindkét oldalának logaritmusát véve:

$$\log n = \log 2^k = k \log 2.$$

log 2-vel osztva, (34)-re tekintettel adódik (31).

b. $n=1$ esetén mindkét oldalon 0 áll, tehát igaz az állítás. $n>2$ esetén pedig legyen n kanonikus alakja a (2) alatti. Ekkor nyilván

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} \geqq 2^{\alpha_1} \cdot 2^{\alpha_2} \cdot \dots \cdot 2^{\alpha_r} = 2^{\alpha_1+\alpha_2+\dots+\alpha_r} = 2^{\varkappa(n)}.$$

Mivel a $\log x$ függvény monoton növő, innen következik, hogy

$$\log n \geqq \log 2^{\varkappa(n)} = \varkappa(n) \log 2.$$

log 2-vel osztva, adódik (32).

9. Az analízisből ismeretes, hogy tetszőleges n természetes számra fennáll az

$$\left| \sum_{i=1}^{n} \frac{1}{i} - \log n \right| < 1 \tag{35}$$

egyenlőtlenség.

E segédtételt felhasználva igazoljuk, hogy tetszőleges n természetes számra

$$(36) \qquad \left|\sum_{i=1}^{n} d(i) - n\log n\right| < 2n.$$

Megoldás:

$$\sum_{i=1}^{n} d(i) = \sum_{i=1}^{n} \sum_{k|i} 1.$$

Itt tehát először i-t rögzítjük (úgy, hogy $1 \leqq i \leqq n$ legyen), majd pedig k-t futtatjuk i (pozitív) osztóin, és minden ilyen osztónak megfelel egy 1-es tag.

Most cseréljük fel az összegzés sorrendjét, vagyis rögzítsük először k-t. k értéke nyilván az 1, 2, ..., n számok közül kerül ki. Továbbá k-t rögzítve, azon i számoknak felel meg egy-egy 1-es tag, melyekre $k|i$ és $i \leqq n$ teljesül. Ezek az i számok $i = kj$ alakúak, ahol $1 \leqq j \leqq \frac{n}{k}$. Így

$$(37) \qquad \sum_{i=1}^{n} d(i) = \sum_{k=1}^{n} \sum_{\substack{k|i \\ i \leqq n}} 1 = \sum_{k=1}^{n} \sum_{j=1}^{\left[\frac{n}{k}\right]} 1 = \sum_{k=1}^{n} \left[\frac{n}{k}\right].$$

Innen $\sum_{k=1}^{n} \frac{n}{k}$-t kivonva és az

$$(38) \qquad |a+b| \leqq |a| + |b|$$

egyenlőtlenséget felhasználva, nyerjük, hogy

$$(39) \qquad \left|\sum_{i=1}^{n} d(i) - \sum_{k=1}^{n} \frac{n}{k}\right| = \left|\sum_{k=1}^{n} \left[\frac{n}{k}\right] - \sum_{k=1}^{n} \frac{n}{k}\right| =$$

$$= \left|\sum_{k=1}^{n} \left(\left[\frac{n}{k}\right] - \frac{n}{k}\right)\right| \leqq \sum_{k=1}^{n} \left|\left[\frac{n}{k}\right] - \frac{n}{k}\right| < \sum_{k=1}^{n} 1 = n.$$

Másrészt (35) alapján

$$(40) \qquad \left|\sum_{k=1}^{n} \frac{n}{k} - n\log n\right| = \left|n \sum_{k=1}^{n} \frac{1}{k} - n\log n\right| =$$

$$= n\left|\sum_{k=1}^{n} \frac{1}{k} - \log n\right| < n.$$

(39)-ből és (40)-ből ismét a (38) egyenlőtlenség alapján következik, hogy

$$\left|\sum_{i=1}^{n} d(i)-n\log n\right| = \left|\left(\sum_{i=1}^{n} d(i)-\sum_{k=1}^{n}\frac{n}{k}\right)+\left(\sum_{k=1}^{n}\frac{n}{k}-n\log n\right)\right| \leqq$$

$$\leqq \left|\sum_{i=1}^{n} d(i)-\sum_{k=1}^{n}\frac{n}{k}\right|+\left|\sum_{k=1}^{n}\frac{n}{k}-n\log n\right| < n+n = 2n,$$

és ezzel igazoltuk (36)-ot.

Megjegyezzük, hogy a komplementer osztók fogalmát (l. az I. fejezet 5. pontját), valamint a (35) segédtétel egy élesebb alakját felhasználva, a $\sum_{i=1}^{n} d(i)$ összegre itt adott becslés lényegesen javíthat, amennyiben igazolható, hogy tetszőleges n természetes számra

$$\left|\sum_{i=1}^{n} d(i)-(n\log n+(2C-1)n)\right| < A\sqrt{n},$$

ahol C az ún. Euler—Mascheroni-állandó, A pedig alkalmas explicit konstans. A Dirichlet-féle osztóproblémának az a lényege, hogy a jobb oldalon álló $A\sqrt{n}$ mennyiség mennyire csökkenthető?

10*. *a.* Legyen $f(n)$ tetszőleges számelméleti függvény, és jelöljük összegzési függvényét $g(n)$-nel. Legyen továbbá $h(n)$ totálisan multiplikatív számelméleti függvény. Bizonyítsuk be, hogy tetszőleges n természetes számra

$$\sum_{i=1}^{n} h(i)g(i) = \sum_{j=1}^{n} h(j)f(j)\sum_{k=1}^{\left[\frac{n}{j}\right]} h(k). \tag{41}$$

b. Mit ad az *a.* állítás $h(n)=1$, speciálisan $h(n)=f(n)=1$ esetén, valamint $h(n)=n$ esetén?

Megoldás:

a. $$\sum_{i=1}^{n} h(i)g(i) = \sum_{i=1}^{n} h(i)\sum_{d|i} f(d) = \sum_{i=1}^{n}\sum_{d|i} h(i)f(d).$$

Az i-re, ill. d-re vonatkozó összegzés sorrendjét felcserélve (ugyanúgy, mint az előző feladat megoldása során) nyerjük, hogy

$$\sum_{i=1}^{n} h(i)g(i) = \sum_{d=1}^{n}\sum_{\substack{d|i\\ i\leqq n}} h(i)f(d) =$$

$$= \sum_{d=1}^{n}\sum_{k=1}^{\left[\frac{n}{d}\right]} h(kd)f(d) = \sum_{d=1}^{n}\sum_{k=1}^{\left[\frac{n}{d}\right]} h(k)h(d)f(d) =$$

$$= \sum_{d=1}^{n} h(d)f(d)\sum_{k=1}^{\left[\frac{n}{d}\right]} h(k).$$

d helyett j-t írva, (41)-et nyerjük.

b. $h(n)=1$-et helyettesítve:

$$\sum_{i=1}^{n} g(i) = \sum_{j=1}^{n} f(j) \sum_{k=1}^{\left[\frac{n}{j}\right]} 1,$$

vagyis

$$(42) \qquad \sum_{i=1}^{n} g(i) = \sum_{j=1}^{n} f(j) \left[\frac{n}{j}\right].$$

Ha továbbá $f(n)=1$, akkor

$$g(n) = \sum_{d|n} f(d) = \sum_{d|n} 1 = d(n),$$

tehát (42)-ből az előző feladat megoldása során felhasznált (37) összefüggést nyerjük.

Végül (41)-ben $h(n)=n$-et helyettesítve, nyerjük, hogy

$$\sum_{i=1}^{n} ig(i) = \sum_{j=1}^{n} jf(j) \sum_{k=1}^{\left[\frac{n}{j}\right]} k,$$

vagyis

$$(43) \qquad \sum_{i=1}^{n} ig(i) = \sum_{j=1}^{n} jf(j) \left(\frac{\left[\frac{n}{j}\right]+1}{2}\right).$$

FELADATOK

1. Számítsuk ki $\sigma(84)$ értékét!

2. Állapítsuk meg, hogy $\sigma(n)$ értéke mely n természetes számokra páratlan?

3. Oldjuk meg a

$$\sigma(x) = x+3$$

(x természetes szám) egyenletet!

4. Igazoljuk, hogy tetszőleges p prímszámra és α természetes számra

$$(44) \qquad \frac{\sigma(p^\alpha)}{p^\alpha} < \frac{1}{1-\frac{1}{p}}.$$

5. Bizonyítsuk be, hogy tetszőleges n természetes számra

(45) $\sigma(n)\varphi(n) \leqq n^2$.

6. Bizonyítsuk be, hogy tetszőleges p prímszámra és α természetes számra

(46) $$\frac{\sigma(p^\alpha)}{p^\alpha} \geqq 1+\frac{1}{p}.$$

7*. Bizonyítsuk be, hogy tetszőleges n természetes számra

(47) $$\frac{1}{2}n^2 < \sigma(n)\varphi(n).$$

8. Állapítsuk meg, hogy prímszám lehet-e tökéletes szám?

9. Számítsuk ki

a. $\nu(300)$,

b. $\varkappa(300)$

értékét!

10. Bizonyítsuk be, hogy tetszőleges n természetes számra

(48) $2^{\nu(n)} \leqq d(n)$.

11. Bizonyítsuk be, hogy tetszőleges n természetes számra

(49) $d(n) \leqq 2^{\varkappa(n)}$.

12*. Bizonyítsuk be, hogy tetszőleges n természetes számra

$$\varphi(n) \geqq \frac{n}{\nu(n)+1}.$$

13. Állapítsuk meg, hogy létezik-e olyan $f(n)$ additív számelméleti függvény, amely az $f(1)=0$ értéket kivéve, csak páratlan egész értékeket vesz fel?

14. Igazoljuk, hogy a

$$\lambda(n) = (-1)^{\varkappa(n)}$$

függvény (az ún. *Liouville-függvény*) totálisan multiplikatív!

15. Írjuk fel az

a. $\nu(n)$,

b. $\varkappa(n)$

függvényt összegzési függvény alakjában!

16. Számítsuk ki a 14. feladatban definiált $\lambda(n)$ számelméleti függvény összegzési függvényét!

17. A $\Lambda(n)$ függvényt (az ún. *Mangoldt-szimbólumot*) a következőképpen definiáljuk: legyen

$$\Lambda(n) = \begin{cases} \log p, \text{ ha } n = p^\alpha \text{ (ahol } p \text{ primszám, } \alpha \\ \qquad\qquad\qquad\qquad \text{ természetes szám)} \\ 0, \text{ ha } n \text{ nem } p^\alpha \text{ alakú (vagyis } \nu(n) \neq 1). \end{cases}$$

Számítsuk ki a $\Lambda(n)$ függvény összegzési függvényét!

18. Számítsuk ki

a. $\mu(70)$,

b. $\mu(300)$

értékét!

19. Oldjuk meg a

$$\mu(x^2) + \mu(x) = 2$$

egyenletet!

20. Bizonyítsuk be, hogy tetszőleges n természetes számra

$$(50) \quad \sum_{d^2 | n} \mu(d) = \mu^2(n).$$

21. Bizonyítsuk be, hogy tetszőleges n természetes számra

$$\sum_{d | n} \mu(d) \log d = -\Lambda(n)$$

(ahol $\Lambda(n)$ a 17. feladatban definiált függvény).

22*. (35)-öt felhasználva bizonyítsuk be, hogy ha n 1-nél nagyobb természetes szám, akkor

$$(51) \quad \sigma(n) < 2n \log n.$$

23*. Bizonyítsuk be, hogy ha m tart a végtelenhez, akkor $\frac{\sigma(m!)}{m!}$ is végtelenhez tart!

24*. Bizonyítsuk be, hogy ha n 1-nél nagyobb természetes szám, akkor

$$\varphi(n) > \frac{n}{4 \log n}.$$

25*. Bizonyítsuk be, hogy ha m tart a végtelenhez, akkor $\frac{\varphi(m!)}{m!}$ 0-hoz tart!

26. Bizonyítsuk be, hogy tetszőleges n természetes számra

$$\sum_{i=1}^{n} \mu(i) \left[\frac{n}{i}\right] = 1. \tag{52}$$

27. Bizonyítsuk be, hogy tetszőleges n természetes számra

$$\left|\sum_{i=1}^{n} \frac{\mu(i)}{i}\right| \leqq 2.$$

28*. Bizonyítsuk be, hogy tetszőleges n természetes számra

a. $$\sum_{i=1}^{n} \sigma(i) = \sum_{j=1}^{n} j \left[\frac{n}{j}\right],$$

b. $$\sum_{i=1}^{n} \frac{\varphi(i)}{i} = \sum_{j=1}^{n} \frac{\mu(j)}{j} \left[\frac{n}{j}\right],$$

c. $$\sum_{i=1}^{n} \frac{\sigma(i)}{i} = \sum_{j=1}^{n} \frac{1}{j} \left[\frac{n}{j}\right],$$

d. $$\sum_{i=1}^{n} \lambda(i) \left[\frac{n}{i}\right] = [\sqrt{n}]$$

(ahol $\lambda(n)$ a 14. feladatban definiált függvény),

e. $$\sum_{i=1}^{n} \mu^2(i) = \sum_{j=1}^{[\sqrt{n}]} \mu(j) \left[\frac{n}{j^2}\right].$$

29*. Legyen $h(n)$ olyan additív számelméleti függvény, hogy tetszőleges p prímszámra

$$(53)\quad h(p) = h(p^2) = h(p^3) = \dots$$

teljesül. Bizonyítsuk be, hogy ekkor

$$(54)\quad \sum_{i=1}^{n} h(i) = \sum_{p \leqq n} h(p) \left[\frac{n}{p}\right].$$

A $\sum_{p \leqq n} f(p)$ jelölés úgy értendő, hogy miden, a $p \leqq n$ feltételt kielégítő p prímszámra kiszámítjuk $f(p)$-t, és az így nyert számokat összeadjuk. Így például

$$\sum_{p \leqq 8} \sigma(p) = \sigma(2)+\sigma(3)+\sigma(5)+\sigma(7) = 3+4+6+8 = 21.$$

30*. Legyen $k(n)$ tetszőleges, totálisan additív számelméleti függvény. Bizonyítsuk be, hogy tetszőleges n természetes számra

$$(55)\quad \sum_{i=1}^{n} k(i) = \sum_{p^\alpha \leqq n} k(p) \left[\frac{n}{p^\alpha}\right].$$

31*. Bizonyítsuk be, hogy tetszőleges n természetes számra

a.

$$(56)\quad \sum_{i=1}^{n} \nu(i) = \sum_{p \leqq n} \left[\frac{n}{p}\right],$$

b.

$$(57)\quad \sum_{i=1}^{n} \varkappa(i) = \sum_{p^\alpha \leqq n} \left[\frac{n}{p^\alpha}\right].$$

32*. Bizonyítsuk be a *Legendre-formulát:* ha n 1-nél nagyobb természetes szám, akkor $n!$ kanonikus alakja:

$$n! = \prod_{p \leqq n} p^{\gamma_p},$$

ahol

$$\gamma_p = \sum_{\alpha=1}^{+\infty} \left[\frac{n}{p^\alpha}\right].$$

Itt a jobb oldalon álló összeg nyilván csak formálisan végtelen; a $p^{\alpha} > n$ feltételt kielégítő α-knak megfelelő tagok ugyanis 0-val azonosak.

33*. Bizonyítsuk be, hogy tetszőleges n természetes számra

a.

$$(58) \quad \sum_{i=1}^{n} \sigma(i) = \sum_{j=1}^{n} \binom{\left[\frac{n}{j}\right]+1}{2},$$

b.

$$(59) \quad \sum_{i=1}^{n} \varphi(i) = \sum_{j=1}^{n} \mu(j) \binom{\left[\frac{n}{j}\right]+1}{2}.$$

A III. FEJEZETBEN KITŰZÖTT FELADATOK MEGOLDÁSAI

1. $\sigma(84) = \sigma(2^2 \cdot 3 \cdot 7) = \frac{2^3-1}{2-1} \cdot \frac{3^2-1}{3-1} \cdot \frac{7^2-1}{7-1} =$

$= \frac{7}{1} \cdot \frac{8}{2} \cdot \frac{48}{6} = 7 \cdot 4 \cdot 8 = 224.$

2. $\sigma(1)$ nyilván páratlan. $n-1$ esetén legyen n kanonikus alakja a (2) alatti; ekkor

$$\sigma(n) = \sigma(p_1^{\alpha_1})\sigma(p_2^{\alpha_2}) \dots \sigma(p_r^{\alpha_r}). \tag{60}$$

$\sigma(n)$ nyilván akkor és csak akkor páratlan, ha itt a $\sigma(p_i^{\alpha_i})$ tényezők mindegyike páratlan szám. Azonban

$$\sigma(2^\alpha) = 1+2+2^2+\dots+2^\alpha = 1+2(1+2+\dots+2^{\alpha-1})$$

(ahol α természetes szám) nyilván páratlan szám bármely α-ra. Ha viszont p páratlan prímszám, akkor

$$\sigma(p^\alpha) = 1+p+p^2+\dots+p^\alpha$$

$\alpha+1$ számú páratlan szám összege, tehát akkor és csak akkor páratlan, ha $\alpha+1$ páratlan, vagyis α páros. Így a (60) jobb oldalán álló tényezők mindegyike akkor és csak akkor páratlan, ha n kanonikus alakjában valamennyi páratlan prímtényező kitevője páros. Ez a feltétel viszont az I. fejezet 16. példájára tekintettel átfogalmazható úgy, hogy $\sigma(n)$ akkor és csak akkor páratlan, ha n négyzetszám vagy négyzetszám kétszerese.

3. $\sigma(x)$ definíciója szerint

$$\sigma(x) = \sum_{d|x} d = 1 + \sum_{\substack{d|x \\ 1<d<x}} d + x.$$

Ezt az egyenlőséget kivonva az adott egyenletből, azt nyerjük, hogy

$$\sum_{\substack{d|x \\ 1<d<x}} d = 2. \tag{61}$$

Azonban a 2 szám nyilván csak egyféleképpen írható fel 1-nél nagyobb természetes számok összegeként; nevezetesen olyan összegként, melynek egyetlen tagja $d=2$. Így szükségképpen $2|x$, ahonnan az is következik, hogy $\frac{x}{2}\Big|x$. $x>4$ esetén azonban nyilván $2<\frac{x}{2}<x$, tehát az $\frac{x}{2}$ szám a (61) bal oldalán álló összegnek $d=2$-től különböző tagja lenne. Így csak $x\leqq 4$ lehetséges, továbbá az előbbiek szerint $2|x$ és $2<x$; az egyetlen megoldás tehát $x=4$ (mely valóban kielégíti az adott egyenletet).

4. $$\frac{\sigma(p^\alpha)}{p^\alpha}=\frac{1}{p^\alpha}\cdot\frac{p^{\alpha+1}-1}{p-1}=\frac{p^{\alpha+1}-1}{p^{\alpha+1}-p^\alpha}=\frac{1-\frac{1}{p^{\alpha+1}}}{1-\frac{1}{p}}<\frac{1}{1-\frac{1}{p}}.$$

5. $n=1$ esetén (45) nyilván teljesül (ekkor mindkét oldalon 1 áll). $n>1$ esetén viszont legyen n kanonikus alakja a (2) alatti. Ekkor (44)-et felhasználva:

$$\sigma(n)\varphi(n)=\sigma(p_1^{\alpha_1}\dots p_r^{\alpha_r})\varphi(p_1^{\alpha_1}\dots p_r^{\alpha_r})=$$

$$=\sigma(p_1^{\alpha_1})\dots\sigma(p_r^{\alpha_r})\varphi(p_1^{\alpha_1})\dots\varphi(p_r^{\alpha_r})=$$

$$=[\sigma(p_1^{\alpha_1})\varphi(p_1^{\alpha_1})]\dots[\sigma(p_r^{\alpha_r})\varphi(p_r^{\alpha_r})]=$$

$$=\left[\sigma(p_1^{\alpha_1})\cdot p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right)\right]\dots\left[\sigma(p_r^{\alpha_r})\cdot p_r^{\alpha_r}\left(1-\frac{1}{p_r}\right)\right]<$$

$$<\left[\frac{p_1^{\alpha_1}}{\left(1-\frac{1}{p_1}\right)}\cdot p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right)\right]\dots\left[\frac{p_r^{\alpha_r}}{\left(1-\frac{1}{p_r}\right)}\cdot p_r^{\alpha_r}\left(1-\frac{1}{p_r}\right)\right]=$$

$$=p_1^{2\alpha_1}\dots p_r^{2\alpha_r}=(p_1^{\alpha_1}\dots p_r^{\alpha_r})^2=n^2.$$

6. $$\sigma(p^\alpha)=1+p+p^2+\dots+p^\alpha\geqq p^{\alpha-1}+p^\alpha.$$

p^α-val osztva, adódik az állítás.

7. (46)-ot felhasználva:

$$\sigma(p^\alpha)\varphi(p^\alpha)\geqq p^\alpha\left(1+\frac{1}{p}\right)\cdot p^\alpha\left(1-\frac{1}{p}\right)=p^{2\alpha}\left(1-\frac{1}{p^2}\right)$$

(ahol p tetszőleges prímszám, α természetes szám). Így, ha $n>1$ esetén n kanonikus alakja a (2) alatti, akkor

$$= \sigma(n)\varphi(n) = \sigma(p_1^{\alpha_1} \dots p_r^{\alpha_r})\varphi(p_1^{\alpha_1} \dots p_r^{\alpha_r}) =$$

$$= [\sigma(p_1^{\alpha_1})\varphi(p_1^{\alpha_1})] \dots [\sigma(p_r^{\alpha_r})\varphi(p_r^{\alpha_r})] \geqq$$

$$\geqq \left[p_1^{2\alpha_1}\left(1-\frac{1}{p_1^2}\right)\right] \dots \left[p_r^{2\alpha_r}\left(1-\frac{1}{p_r^2}\right)\right] =$$

$$= (p_1^{\alpha_1} \dots p_r^{\alpha_r})^2 \left(1-\frac{1}{p_1^2}\right) \dots \left(1-\frac{1}{p_r^2}\right) =$$

$$= n^2 \prod_{p|n} \left(1-\frac{1}{p^2}\right) \geqq n^2 \prod_{p\leqq n} \left(1-\frac{1}{p^2}\right).$$

Elég tehát igazolni, hogy

$$\prod_{p\leqq n} \left(1-\frac{1}{p^2}\right) \geqq \frac{1}{2}. \tag{62}$$

A bal oldal a következőképpen becsülhető:

$$\prod_{p\leqq n} \left(1-\frac{1}{p^2}\right) \geqq \prod_{2\leqq i\leqq n} \left(1-\frac{1}{i^2}\right) = \prod_{2\leqq i\leqq n} \frac{i^2-1}{i^2} =$$

$$= \prod_{2\leqq i\leqq \alpha} \frac{(i-1)(i+1)}{i^2} =$$

$$= \frac{1\cdot 3}{2^2}\cdot\frac{2\cdot 4}{3^2}\cdot\frac{3\cdot 5}{4^2}\cdot\frac{4\cdot 6}{5^2}\cdot\dots\cdot\frac{(n-3)(n-1)}{(n-2)^2}\cdot\frac{(n-2)n}{(n-1)^2}\cdot\frac{(n-1)(n+1)}{n^2} =$$

$$= \frac{1}{2}\cdot\frac{n+1}{n} > \frac{1}{2}.$$

Ezzel (62)-t és így (47)-et is igazoltuk.

8. Ha p prímszám, akkor

$$\sigma(p) = p+1. \tag{63}$$

Másrészt, ha p tökéletes szám lenne, akkor

$$\sigma(p) = 2p \tag{64}$$

teljesülne. (63)-ból és (64)-ből azonban az következnék, hogy

$$p+1 = 2p,$$

$$p = 1,$$

ami lehetetlen (az 1 nem prímszám).

9.

a. $\nu(300) = \nu(2^2 \cdot 3 \cdot 5^2) = 3.$

b. $\varkappa(300) = \varkappa(2^2 \cdot 3 \cdot 5^2) = 2+1+2 = 5.$

10. $n=1$ esetén (48) mindkét oldalán 1 áll, tehát (48) teljesül. Ha viszont $n>1$, és n kanonikus alakja a (2) alatti, akkor

$$d(n) = d(p_1^{\alpha_1} \dots p_r^{\alpha_r}) = (\alpha_1+1) \dots (\alpha_r+1) >$$

$$> 2 \cdot \dots \cdot 2 = 2^r = 2^{\nu(n)}.$$

11. $n=1$ esetén (45) nyilván teljesül. Ha $n>1$, és n kanonikus alakja a (2) alatti, akkor ismét

(65) $d(n) = (\alpha_1+1) \dots (\alpha_r+1).$

Teljes indukcióval könnyen igazolható (a részleteket az olvasóra bízzuk), hogy tetszőleges α természetes számra

$$\alpha+1 \leqq 2^\alpha.$$

Így (65)-ből

$$d(n) \leqq 2^{\alpha_1} \cdot \dots \cdot 2^{\alpha_r} = 2^{\alpha_1+\dots+\alpha_r} = 2^{\varkappa(n)}.$$

12*. $n=1$ esetén nyilvánvaló az állítás. $n>1$ esetén legyen n kanonikus alakja a (2) alatti, és tegyük fel, hogy ott $p_1<p_2<\dots<p_r$. Ekkor nyilván $p_i \geqq i+1$ (ahol $i=1, 2, \dots, r$), tehát

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_r}\right) \geqq$$

$$\geqq n \cdot \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\dots\left(1-\frac{1}{r+1}\right) =$$

$$n \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{3}{4} \cdot \dots \frac{r-1}{r} \cdot \frac{r}{r+1} = \frac{n}{r+1} = \frac{n}{\nu(n)+1}.$$

13. Legyenek p, q különböző prímszámok. Ekkor $f(p), f(q)$ és $f(pq)$ nem lehetnek egyidejűleg páratlan egész számok, hiszen

$$f(pq) = f(p)+f(q).$$

Így a kívánt tulajdonságú $f(n)$ számelméleti függvény nem létezik.

14. Minthogy a $\varkappa(n)$ függvény totálisan additív, tetszőleges m, n természetes számokra

$$\lambda(mn) = (-1)^{\varkappa(mn)} = (-1)^{\varkappa(m)+\varkappa(n)} = (-1)^{\varkappa(m)}(-1)^{\varkappa(n)} =$$
$$= \lambda(m)\lambda(n).$$

15.

a. Nyilván

$$\nu(n) = \sum_{d|n} f(d),$$

ahol

$$f(n) = \begin{cases} 1, & \text{ha } n \text{ prímszám,} \\ 0, & \text{ha } n \text{ nem prímszám.} \end{cases}$$

b. $\varkappa(n) = \sum_{d|n} f(d),$

ahol

$$f(n) = \begin{cases} 1, & \text{ha } n \text{ prímszámhatvány } (p^\alpha \text{ alakú),} \\ 0, & \text{ha } n \text{ nem prímszámhatvány.} \end{cases}$$

16. Minthogy a 14. feladat szerint $\lambda(n)$ multiplikatív, szükségképpen $g(n)$ összegzési függvénye is az. Elég tehát $g(p^\alpha)$-t kiszámítani:

$$g(p^\alpha) = \sum_{d|p^\alpha} \lambda(d) = \lambda(1)+\lambda(p)+\lambda(p^2)+\ldots+\lambda(p^\alpha) =$$
$$= 1+(-1)+(-1)^2+\ldots+(-1)^\alpha = \begin{cases} 0, & \text{ha } \alpha \text{ páratlan,} \\ 1, & \text{ha } \alpha \text{ páros.} \end{cases}$$

Így ha $n(>1)$ kanonikus alakja a (2) alatti, akkor

$$g(n) = g(p_1^{\alpha_1}) \ldots g(p_r^{\alpha_r}) =$$
$$= \begin{cases} 0, & \text{ha } \alpha_1, \ldots, \alpha_r \text{ között van páratlan szám,} \\ 1, & \text{ha } \alpha_1, \ldots, \alpha_r \text{ mindegyike páros.} \end{cases}$$

Más szóval (tekintettel az I. fejezet 13. példájára):

$$g(n) = \begin{cases} 0, & \text{ha } n \text{ nem négyzetszám,} \\ 1, & \text{ha } n \text{ négyzetszám} \end{cases}$$

(utóbbiba beleértve $n=1$-et is).

17. Legyen $n>1$ esetén n kanonikus alakja a (2) alatti. Ekkor

$$\sum_{d|n} \Lambda(d) = \sum_{p^\alpha|n} \Lambda(p^\alpha) = \sum_{i=1}^{r} \sum_{j=1}^{\alpha_i} \Lambda(p_i^j) =$$

$$= \sum_{i=1}^{r} \sum_{j=1}^{\alpha_i} \log p_i = \sum_{i=1}^{r} \alpha_i \log p_i = \sum_{i=1}^{r} \log p_i^{\alpha_i} =$$

$$= \log p_1^{\alpha_1} \dots p_r^{\alpha_r} = \log n$$

(és az összegzési függvény értéke $n=1$-re $\log 1=0$).

18.

a. $\mu(70) = \mu(2\cdot 5\cdot 7) = (-1)^3 = -1.$

b. $\mu(300) = \mu(2^2\cdot 3\cdot 5^2) = 0.$

19. Ha $x>1$, akkor nyilván $\mu(x^2)=0$, tehát

$$\mu(x^2)+\mu(x) \leqq 0+1 = 1 < 2.$$

Így csak $x=1$ lehet megoldás, ami viszont valóban kielégíti az adott egyenletet.

20. Írjuk n-et $n=p_1p_2\dots p_rk^2$ alakban, ahol $p_1, p_2, \dots, p_r$ páronként különböző prímszámok, k természetes szám (vö. az I. fejezet 65. feladatával). Ekkor a (24) formula szerint

$$\sum_{d^2|n} \mu(d) = \sum_{d|k} \mu(d) = \begin{cases} 1, & \text{ha } k = 1, \\ 0, & \text{ha } k > 1. \end{cases} \tag{66}$$

Másrészt a Möbius-függvény definíciója szerint

$$\mu^2(n) = \begin{cases} 1, & \text{ha } n \text{ négyzetmentes szám, vagyis } k = 1, \\ 0, & \text{ha } n \text{ nem négyzetmentes szám, vagyis } k > 1. \end{cases} \tag{67}$$

(66)-ot és (67)-et egybevetve, adódik (50).

21. A 17. feladat szerint az $f(n)=\Lambda(n)$ függvény összegzési függvénye a $g(n)=\log n$ függvény. Így a (25) inverziós formula szerint

$$\Lambda(n) = \sum_{d|n} \mu(d) \log \frac{n}{d} = \sum_{d|n} \mu(d)(\log n - \log d) =$$

$$= \sum_{d|n} \mu(d) \log n - \sum_{d|n} \mu(d) \log d =$$

$$= \log n \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log d.$$

A (24) formulára (és $\log 1=0$-ra) tekintettel a $\log n \sum_{d|n} \mu(d)$ tag bármely n-re 0. Így innen

$$\Lambda(n) = -\sum_{d|n} \mu(d) \log d.$$

-1-gyel szorozva, adódik az állítás.

22*. A (35) segédtétel alapján igazolható, hogy $n \geqq 2$ esetén

$$\sum_{d=1}^{n} \frac{1}{d} < 2 \log n.$$

Így

$$\sigma(n) = \sum_{d|n} d = \sum_{d|n} \frac{n}{d} = n \sum_{d|n} \frac{1}{d} \leqq n \sum_{d=1}^{n} \frac{1}{d} <$$

$$< n \cdot 2 \log n = 2n \log n.$$

23*. $$\frac{\sigma(m!)}{m!} = \frac{1}{m!} \sum_{d|m!} d = \frac{1}{m!} \sum_{d|m!} \frac{m!}{d} =$$

$$= \frac{1}{m!} \cdot m! \sum_{d|m!} \frac{1}{d} = \sum_{d|m!} \frac{1}{d} \geqq \sum_{d=1}^{m} \frac{1}{d}.$$

A (35) segédtétel szerint ez utóbbi összeg végtelenhez tart, ha m-mel tartunk a végtelenhez, ahonnan következik az állítás.

24*. (47)-et és (51)-et felhasználva:

$$\varphi(n) > \frac{n^2}{2\sigma(n)} > \frac{n^2}{2 \cdot 2n \log n} = \frac{n}{4 \log n}.$$

(Megjegyezzük, hogy az állított egyenlőtlenség igazolható a 12*. feladat és (32) alapján is, felhasználva a $\nu(n) \leqq \varkappa(n)$ egyenlőtlenséget.)

25*. (45)-ből nyerjük, hogy

$$\frac{\varphi(m!)}{m!} \leqq \frac{m!}{\sigma(m!)}.$$

Innen a 23*. feladat alapján következik az állítás.

26. A (42) formulában válasszunk $f(n)=\mu(n)$-et. A (24) formulára tekintettel nyerjük, hogy ($g(n)=\sum_{d|n} \mu(d)$-t írva)

$$\sum_{j=1}^{n} \mu(j) \left[\frac{n}{j}\right] = \sum_{i=1}^{n} g(i) = g(1)+g(2)+\ldots+g(n) =$$

$$= 1+0+\ldots+0 = 1.$$

27. (52) alapján (felhasználva a (38) egyenlőtlenséget):

$$\left|\sum_{i=1}^{n} \frac{\mu(i)}{i}\right| = \left|\frac{1}{n} \sum_{i=1}^{n} \mu(i) \frac{n}{i}\right| =$$

$$= \left|\frac{1}{n} \sum_{i=1}^{n} \left(\mu(i) \frac{n}{i} - \mu(i) \left[\frac{n}{i}\right]\right) + \frac{1}{n} \sum_{i=1}^{n} \mu(i) \left[\frac{n}{i}\right]\right| =$$

$$= \left|\frac{1}{n} \sum_{i=1}^{n} \mu(i) \left(\frac{n}{i} - \left[\frac{n}{i}\right]\right) + \frac{1}{n}\right| \leqq$$

$$\leqq \frac{1}{n} \sum_{i=1}^{n} |\mu(i)| \left|\frac{n}{i} - \left[\frac{n}{i}\right]\right| + \frac{1}{n} \leqq$$

$$\leqq \frac{1}{n} \sum_{i=1}^{n} 1 + \frac{1}{n} = \frac{1}{n} \cdot n + \frac{1}{n} = 1 + \frac{1}{n} \leqq 2.$$

28*. Legyen

a. $f(n) = n,\ g(n) = \sigma(n)$;

b. $f(n) = \dfrac{\mu(n)}{n},\quad g(n) = \dfrac{\varphi(n)}{n}$;

c. $f(n) = \dfrac{1}{n},\quad g(n) = \dfrac{\sigma(n)}{n}$;

d. $f(n) = \lambda(n),\ g(n) = \begin{cases} 0, & \text{ha } n \text{ nem négyzetszám,} \\ 1, & \text{ha } n \text{ négyzetszám;} \end{cases}$

e. $f(n) = \begin{cases} 0, & \text{ha } n \text{ nem négyzetszám,} \\ \mu(\sqrt{n}), & \text{ha } n \text{ négyzetszám,} \end{cases} \qquad g(n) = \mu^2(n).$

Ekkor

(68) $$g(n) = \sum_{d|n} f(d)$$

valamennyi esetben teljesül, mégpedig az *a.*, *b.*, *d.*, *e.* feladatoknál rendre (19), (27), a 16. feladat, ill. (50) szerint. A *c.* feladatnál pedig ez következik a

(69) $$\frac{\sigma(n)}{n} = \frac{1}{n} \sum_{d|n} d = \frac{1}{n} \sum_{d|n} \frac{n}{d} = \sum_{d|n} \frac{1}{d}$$

összefüggésből.

Így valamennyi esetben alkalmazható a (42) formula, mely éppen az *a...e* összefüggéseket adja.

29*. Legyen

$$f(n) = \begin{cases} h(n), & \text{ha } n \text{ prímszám,} \\ 0, & \text{ha } n \text{ nem prímszám,} \end{cases}$$

és legyen $g(n)=h(n)$. Ha $n>1$ és n kanonikus alakja a (2) alatti, akkor $h(n)$ additivitására és (53)-ra tekintettel

$$g(n) = h(n) = h(p_1^{\alpha_1} \dots p_r^{\alpha_r}) = h(p_1^{\alpha_1}(+\dots+h)p_r^{\alpha_r}) =$$

$$= h(p_1)+\dots+h(p_r) = \sum_{p|n} h(p) = \sum_{d|n} f(d)$$

(és a nyert összefüggés nyilván $n=1$ esetén is teljesül), tehát a (42) összefüggés alkalmazható. (42) bal oldala nyilván azonos (54) bal oldalával, míg (42) jobb oldala:

$$\sum_{j=1}^{n} f(j)\left[\frac{n}{j}\right] = \sum_{p\leqq n} f(p)\left[\frac{n}{p}\right] = \sum_{p\leqq n} h(p)\left[\frac{n}{p}\right],$$

tehát (54) jobb oldalát nyerjük.

30*. Legyen

$$f(n) = \begin{cases} k(p), & \text{ha } n = p^{\alpha}, \\ 0, & \text{ha } n \text{ nem prímszámhatvány,} \end{cases}$$

és legyen $g(n)=k(n)$. Ha $n>1$ és n kanonikus alakja a (2) alatti, akkor

$$g(n) = k(n) = k(p_1^{\alpha_1} \dots p_r^{\alpha_r}) = \alpha_1 k(p_1)+\dots+\alpha_r k(p_r) =$$

$$= (f(p_1)+f(p_1^2)+\dots+f(p_1^{\alpha_1}))+\dots+(f(p_r)+f(p_r^2)+\dots+f(p_r^{\alpha_r})) =$$

$$= \sum_{d|n} f(d)$$

(és ez az egyenlőség $n=1$-re is teljesül). Így (42) alkalmazható. (42) bal oldala azonos (55) bal oldalával, míg jobb oldala egyezik (55)-ével:

$$\sum_{j=1}^{n} f(j)\left[\frac{n}{j}\right] = \sum_{p^{\alpha}\leqq n} f(p^{\alpha})\left[\frac{n}{p^{\alpha}}\right] = \sum_{p^{\alpha}\leqq n} k(p)\left[\frac{n}{p^{\alpha}}\right].$$

31*. A 29. feladatban $h(n)=\nu(n)$-et, ill. a 30. feladatban $k(n)=\varkappa(n)$-et választva, adódik (56), ill. (57).

32*. Mint megjegyeztük, a $k(n)=\log n$ függvény totálisan additív, és így (55) alkalmazható. A bal oldal:

$$\sum_{i=1}^{n} k(i) = \sum_{i=1}^{n} \log i = \log n!.$$

(55) jobb oldala:

$$\sum_{p^\alpha \leqq n} k(p) \left[\frac{n}{p^\alpha}\right] = \sum_{p^\alpha \leqq n} (\log p) \cdot \left[\frac{n}{p^\alpha}\right] =$$

$$= \sum_{p \leqq n} (\log p) \cdot \sum_{\alpha=1}^{+\infty} \left[\frac{n}{p^\alpha}\right] = \sum_{p \leqq n} (\log p) \cdot \gamma_p =$$

$$= \sum_{p \leqq n} \log p^{\gamma_p} = \log \prod_{p \leqq n} p^{\gamma_p}.$$

Így (55)-ből azt nyerjük, hogy

$$\log n! = \log \prod_{p \leqq n} p^{\gamma_p},$$

ahonnan következik a bizonyítandó egyenlőség (minthogy $\log x = \log y$ esetén szükségképpen $x = y$).

33*. Legyen

$$a. \quad f(n) = \frac{1}{n}, \quad g(n) = \frac{\sigma(n)}{n},$$

$$b. \quad f(n) = \frac{\mu(n)}{n}, \quad g(n) = \frac{\varphi(n)}{n}.$$

Ekkor (69), ill. (27) szerint (68) teljesül, tehát (43) alkalmazható. (43)-ba helyettesítve $f(n)$ és $g(n)$ fenti értékeit, nyilván (58), ill. (59) adódik.

IV. A PRÍMSZÁMELMÉLET ELEMEI

1. A PRÍMSZÁMOK SZÁMA. KÖVETKEZMÉNYEK

Előrebocsátjuk, hogy ebben a fejezetben sok olyan abszolút állandóval fogunk találkozni, melyek explicit értékét nem ismerjük, vagy pedig ez az explicit érték nem játszik különösebb szerepet. Mint a számelméletben szokásos, ezeket az állandókat $c_1, c_2, \ldots$-vel fogjuk jelölni.

Az I. fejezet 63. feladatának kapcsán már igazoltuk, hogy *végtelen sok prímszám létezik.* Az alábbiakban ismertetjük e tételnek *Euklidesztől* származó bizonyítását, minthogy e bizonyítás gondolatmenetét a továbbiakban még többször fogjuk alkalmazni.

Tegyük fel indirekte, hogy csak véges sok prímszám létezik; legyenek ezek $p_1, p_2, \ldots, p_k$. Tekintsük az $n=p_1p_2\ldots p_k+1$ számot. Ez a szám nem osztható a $p_1, p_2, \ldots, p_k$ prímek egyikével sem, hiszen ezekkel osztva 1 maradékot ad. Másrészt az n szám nyilván 1-nél nagyobb, hiszen a $p_1p_2\ldots p_k$ szorzat 0-nál nagyobb (mivel létezik legalább egy prímszám, például 2). Minthogy $n>1$, létezik olyan p prímszám, melyre $p|n$ teljesül. Ekkor az előbbiek szerint a p prímszám különbözik $p_1, p_2, \ldots, p_k$ mindegyikétől, ami ellentmond az indirekt feltevésnek, mely szerint $p_1, p_2, \ldots, p_k$-n kívül nem létezik több prímszám. Ezzel az állítást igazoltuk.

Felmerül a kérdés — mely egyike a számelmélet legfontosabb problémáinak —, hogy mit lehet valamely x számnál nem nagyobb prímszámok számáról mondani? *Az x-nél nem nagyobb prímszámok számát $\pi(x)$-szel jelöljük.*

$\pi(x)$ értéke természetesen bármely konkrét x számra meghatározható, némi számolással. Az I. fejezet 5. pontjában ismertetett *eratoszthenészi szita* segítségével ez a számolás egyszerűsíthető. Az ott mondottak szerint az $1, 2, \ldots, [x]$ számok közül elhagyva a $\sqrt{x}$-nél nem nagyobb prímszámok többszöröseit, a megmaradó számok éppen a $\sqrt{x}$ és x közé eső prímszámok,

valamint az 1 szám, tehát számuk $\pi(x)-\pi(\sqrt{x})+1$. Másrészt e számokat az ún. *logikai szita formula* segítségével is leszámlálhatjuk. Az így nyert eredményt az előbbivel egybevetve, a következő formulát kapjuk:

$$(1) \qquad \pi(x)-\pi(\sqrt{x})+1 = [x]+ \\ + \sum_{j=1}^{k}(-1)^j \sum_{1\leq i_1<i_2<\ldots<i_j\leq k} \left[\frac{x}{p_{i_1}p_{i_2}\cdots p_{i_j}}\right].$$

(L. az 1. példát).

A Möbius-függvény segítségével a jobb oldal egyszerűbb alakban írható:

$$(2) \qquad \pi(x)-\pi(\sqrt{x})+1 = \sum_{d|p_1p_2\ldots p_k} \mu(d)\left[\frac{x}{d}\right].$$

Ha a $\sqrt{x}$-nél nem nagyobb prímszámokat már meghatároztuk (ez jóval kevesebb számolással jár, mint az x-nél nem nagyobb prímszámok meghatározása), akkor innen $\pi(x)$ kiszámítható.

Megjegyezzük, hogy az (1) összefüggés alkalmazása meglehetősen sok számolással jár. Másrészt ez az összefüggés (ebben a formában) nem alkalmas arra, hogy abból *végtelenhez tartó* x *mellett* $\pi(x)$ nagyságára tudjunk következtetni. Ezért indokolt olyan formulák, módszerek keresése, melyek ugyan nem adják meg $\pi(x)$ pontos értékét, viszont alkalmasak $\pi(x)$ *nagyságának* alsó, ill. felső *becslésére.*

Példaként megemlítjük az eratoszthenészi szitának két olyan egyszerű módosítását, melyek segítségével viszonylag pontos *felső* becslés nyerhető $\pi(x)$ nagyságára. Az első észrevétel az, hogy ha rögzítünk valamely, az $1\leq y\leq\sqrt{x}$ feltételt kielégítő y számot, és az 1, 2, ..., $[x]$ számok közül nem az összes, az $1<p\leq\sqrt{x}$ feltételt kielégítő p prímszámok többszöröseit, hanem csupán az $1<p\leq y$ feltételt kielégítő p prímszámok többszöröseit „szitáljuk ki", akkor a megmaradó számok között nyilván valamennyi, $\sqrt{x}$ és x közé eső prímszám szerepel (és általában bizonyos további számok is). Így a megmaradó számok száma (1) bal oldalát felülről becsüli.

A másik észrevétel — mely a

$$\sum_{i=0}^{j}(-1)^i\binom{n}{i} = (-1)^j\binom{n-1}{j} \quad (0\leq j\leq n)$$

összefüggésre támaszkodva igazolható — az, hogy az (1) jobb oldalán álló $\sum_{j=1}^{k}$ összegzést a $\sum_{j=1}^{2l}$ (ahol $0 \leqq 2l \leqq k$) típusú összegzéssel pótolva (vagyis pozitív előjelű tagok után és negatív előjelű tagok előtt megállva), (1) bal oldalára *felső* becslést nyerünk. (Ha viszont ott $\sum_{j=1}^{2l+1}$ típusú összegzést végzünk, akkor (1) bal oldalára *alsó* becslést kapunk.)

Lényegében e két észrevétel képezi az ún. *Brun-szita* alapgondolatát, mely tehát $\pi(x)$ felső becslésére alkalmas. E módszer részletes ismertetése túlhaladja könyvünk kereteit. A Brun-szita és más hasonló szitamódszerek igazi jelentősége azonban abban áll, hogy azok jóval általánosabb problémák vizsgálatára is felhasználhatók. Igen fontosak az *additív prímszámelmélethez* kapcsolódó alkalmazásaik. Ezekre az alkalmazásokra a következő pontban még visszatérünk.

$\pi(x)$ becslésére alkalmasabbak az $n!$ kanonikus alakjára, az ún. *Legendre-formulára* épülő módszerek. E formula szerint valamely 1-nél nagyobb n természetes számot megadva, $n!$ kanonikus alakja:

$$n! = \prod_{p \leqq n} p^{\gamma_p},$$

ahol

$$\gamma_p = \sum_{\alpha=1}^{+\infty} \left[\frac{n}{p^\alpha}\right].$$

(L. a III. fejezet 32. feladatát.)

$\pi(x)$ felső becslése céljából abból indulhatunk ki, hogy tetszőleges n természetes számra

$$\prod_{\frac{n}{2} < p \leqq n} p \,\Big|\, \binom{n}{\left[\frac{n}{2}\right]}; \tag{3}$$

ez közvetlenül, a Legendre-formula felhasználása nélkül is igazolható (l. a 3. példát). Ennek alapján felülről becsülhetjük a $\pi(n) - \pi\left(\frac{n}{2}\right)$ különbséget. Az így nyert egyenlőtlenséget ismételten alkalmazva, $x \geqq 2$ esetén $\pi(x)$-re az alábbi felső becslést

kapjuk:

$$(4) \qquad \pi(x) < c_1 \frac{x}{\log x} \quad (x \geqq 2),$$

ahol c_1 alkalmas pozitív állandó. (L. a 4. példát.)

Másfelől viszont (4) bizonyításához hasonló segédeszközökkel, de valamivel több fáradsággal, a Legendre-formulára erősebben építve (például az 5. példa állításából kiindulva) igazolható, hogy létezik olyan c_2 pozitív állandó, amelyre $x \geqq 2$ esetén

$$(5) \qquad c_2 \frac{x}{\log x} < \pi(x) \quad (x \leqq 2).$$

Az $x<2$ esetet azért célszerű mind (4)-nél, mind (5)-nél kizárni, mert $0<x<1$ esetén $\frac{x}{\log x}$ negatív, míg ha $x>1$, de x „közel" van 1-hez, akkor $\frac{x}{\log x}$ „nagy" pozitív szám.

Hasonló módszerekkel igazolható az ún. *Csebisev-tétel* is: ha n 1-nél nagyobb természetes szám, akkor létezik olyan p prímszám, melyre $n<p<2n$ teljesül.

Ez a tétel egyébként nyilván következik — legalábbis elég nagy n-re — abból, ha (4)-et és (5)-öt olyan c_1, c_2 pozitív állandókkal igazoljuk, melyekre $c_2<2c_1$ teljesül.

(4)-ből és (5)-ből elemi analízisbeli segédeszközök felhasználásával könnyen levezethetők az alábbi fontos egyenlőtlenségek:

Jelöljük az n-edik prímszámot p_n-nel (tehát $p_1=2, p_2=3, p_3=5, \ldots$). Ekkor léteznek olyan c_3, c_4 pozitív állandók, hogy

$$(6) \qquad p_n > c_3 n \log n \quad (n = 1, 2, \ldots)$$

(l. a 16. feladatot), és $n \geqq 2$ esetén

$$(7) \qquad p_n < c_4 n \log n \quad (n = 2, 3, \ldots).$$

Továbbá léteznek olyan c_5, c_6 pozitív állandók, hogy $x \geqq 2$ esetén

$$(8) \qquad c_5^x < \prod_{p \leqq x} p < c_6^x \quad (x \geqq 2).$$

Ennek az egyenlőtlenségnek egy következményére hivatkozni fogunk a 25*. feladat kapcsán. Jelöljük ugyanis az i-edik prímszámot ismét p_i-vel, és legyen

$$P_n = \prod_{i=1}^{n} p_i \quad (n = 1, 2, \ldots).$$

Ekkor nyilván

$$P_n = \prod_{i=1}^{n} p_i = \prod_{p \leqq p_n} p,$$

tehát P_n olyan típusú szorzatnak tekinthető, mint amilyenek a (8) egyenlőtlenségben szerepelnek.

Ennek alapján (8)-ból levezethető, hogy léteznek olyan c_7, c_8 állandók, hogy tetszőleges, 1-nél nagyobb n természetes számra

$$(9) \qquad c_7 \frac{\log P_n}{\log \log P_n} < n < c_8 \frac{\log P_n}{\log \log P_n} \quad (n = 2, 3, \ldots).$$

A fentiekhez részben hasonló módszerrel, még mindig viszonylag elemi úton igazolható a következő formula is:

$$(10) \qquad \sum_{p \leqq x} \frac{1}{p} \sim \log \log x.$$

(A $\sim$ jel, ill. az aszimptotika fogalmának definícióját l. a III. fejezet 3. pontjában.) Sőt, némi fáradsággal igazolható e formula alábbi élesebb alakja is: léteznek olyan c_9, c_{10} állandók, hogy $x \geqq 2$ esetén

$$(11) \qquad \left| \sum_{p \leqq x} \frac{1}{p} - (\log \log x + c_9) \right| < \frac{c_{10}}{\log x}.$$

A (10) bal oldalán álló összeg becslése összefügg a $\prod_{p \leqq n} \left(1 - \frac{1}{p}\right)$ szorzatéval.

Az analízis elemeiből ugyanis ismeretes, hogy $x \to 0$ esetén e^{-x} igen jól közelíthető $(1-x)$-szel, pontosabban például $|x| < \frac{1}{2}$ esetén a két kifejezés különbségének abszolút értéke kisebb, mint $\frac{1}{4} x^2$. Ebből következik, hogy

$p \to +\infty$ esetén $e^{-\frac{1}{p}}$ jól közelíti $\left(1-\frac{1}{p}\right)$-t, tehát a $\prod_{p \leqq x}\left(1-\frac{1}{p}\right)$ szorzat becslése ekvivalens a $\prod_{p \leqq x} e^{-\frac{1}{p}} = e^{-\sum_{p \leqq x} \frac{1}{p}}$ kifejezésével, vagyis végső soron a $\sum_{p \leqq x} \frac{1}{p}$ összegével.

Ezen az úton (11)-ből le lehet vezetni az ún. *Mertens-formulát:* létezik olyan c_{11} pozitív állandó, hogy

$$(12) \quad \prod_{p \leqq n}\left(1-\frac{1}{p}\right) \sim \frac{c_{11}}{\log n}.$$

Továbbá igazolható, hogy itt $c_{11}=e^{-\gamma}$, ahol $\gamma(\approx 0{,}5772...)$ az ún. *Euler-féle állandó*, amely például a $\sum_{i=1}^{n} \frac{1}{i} - \log n$ különbség határértékeként definiálható.

Ismételten hangsúlyozzuk, hogy az eddig ismertetett formulák viszonylag egyszerűen, (4) bizonyításához hasonló elemi módszerekkel (valamint elemi analízisbeli segédeszközök felhasználásával) igazolhatók. E formuláknál jóval mélyebb a számelméletben centrális szerepet játszó ún. *prímszámtétel*, mely a (4), (5) formulák élesítése:

$$(13) \quad \pi(x) \sim \frac{x}{\log x}.$$

Ezt az összefüggést már korábban sejtették, de csupán 1896-ban bizonyították be (egymástól függetlenül Hadamard és de la Vallée Poussin) nehéz komplex függvénytani segédeszközök felhasználásával. Ezekre a segédeszközökre még utalni fogunk az utolsó fejezetben. A prímszámtételre elemi bizonyítást csupán 1948-ban sikerült adni (A. Selbergnek és Erdős Pálnak), azonban a ma ismert legegyszerűbb elemi bizonyítás is igen komplikált. Fontos kérdés a *prímszámtétel maradéktagjának* vizsgálata, vagyis a $\left|\pi(x)-\frac{x}{\log x}\right|$, pontosabban $\left|\pi(x)-\int_2^x \frac{du}{\log u}\right|$ kifejezés felső becslése; ebben az irányban csupán meglehetősen gyenge részeredmények ismeretesek.

A prímszámtételből levezethető a (6)–(8) összefüggések alábbi élesebb alakja:

$$p_n \sim n \log n$$

és

$$\log \prod_{p \leqq x} p \sim x.$$

Példák

1. Igazoljuk az (1) összefüggést!

Megoldás:

Mint említettük, az 1, 2, ..., $[x]$ számok közül elhagyva a $\sqrt{x}$-nél nagyobb prímszámok többszöröseit, a megmaradó számok száma (1) bal oldalával azonos. Elegendő tehát azt igazolni, hogy az említett számokat másféleképpen leszámlálva, (1) jobb oldala adódik.

Ez a leszámlálás a logikai szita formula segítségével végezhető. E formula legáltalánosabb alakjának megfogalmazása és bebizonyítása azonban túlhaladná e könyv kereteit. Ezért itt beérjük azzal, hogy a vizsgált speciális esetben alkalmazzuk az említett általános formula bizonyításának gondolatmenetét.

Jelöljük a $\sqrt{x}$-nél nem nagyobb prímszámokat $p_1, p_2, \ldots, p_k$-val (tehát $k=\pi(\sqrt{x})$). Az 1, 2, ..., $[x]$ számok közül (melyek száma $[x]$) el kell hagynunk a p_1-gyel oszthatókat $\left(\text{melyek száma nyilván } \left[\frac{x}{p_1}\right]\right)$, ..., végül a p_k-val oszthatókat $\left(\text{melyek száma } \left[\frac{x}{p_k}\right]\right)$. Így a következő formulát nyernénk:

$$(14) \qquad x-\left[\frac{x}{p_1}\right]-\ldots-\left[\frac{x}{p_k}\right] = x-\sum_{i=1}^{k}\left[\frac{x}{p_i}\right].$$

Tekintsünk azonban egy olyan számot, mely osztható például p_1-gyel és p_2-vel, de $p_3, \ldots, p_k$ egyikével sem. Egy ilyen számot 0-szor kell számlálnunk, hiszen nem prímszám. Azonban e számot a (14) összeg három tagjánál vettük figyelembe, nevezetesen az első három tagnál (és egyetlen más tagnál sem). Így e szám adaléka a (14) összeghez $1-1-1=-1$. Hogy valóban 0-t kapjunk, minden ilyen számot még $+1$ „súllyal" figyelembe kell vennünk, vagyis e számok számát, $\left[\frac{x}{p_1 p_2}\right]$-t hozzá kell adni a (14) összeghez. Természetesen ugyanez vonatkozik p_1, p_2 helyett bármely más p_{i_1}, p_{i_2} $(1 \leqq i_1 < i_2 \leqq k)$ párra is. Így a (14) formulát a következőképpen kell

korrigálnunk:

$$(15)\quad [x]-\left[\frac{x}{p_1}\right]-\ldots-\left[\frac{x}{p_k}\right]-\left[\frac{x}{p_1p_2}\right]-\left[\frac{x}{p_1p_3}\right]-\ldots-\left[\frac{x}{p_{k-1}p_k}\right]=$$

$$=[x]-\sum_{i=1}^{k}\left[\frac{x}{p_i}\right]+\sum_{1\leq i_1<i_2\leq k}\left[\frac{x}{p_{i_1}p_{i_2}}\right].$$

Ekkor már azokat a számokat, melyek $p_1, p_2, \ldots, p_k$ közül legfeljebb kettővel oszthatók, a helyes multiplicitással számoljuk (1-szer, ha e prímek egyikével sem oszthatók, és 0-szor ellenkező esetben).

Továbbra is problémát okoznak azonban azok a számok, melyek e prímek közül legalább 3-mal oszthatók. Ha például egy szám osztható p_1, p_2, p_3-mal, de $p_4, \ldots, p_k$ egyikével sem, akkor azt az $[x]$, $-\left[\frac{x}{p_1}\right]$, $-\left[\frac{x}{p_2}\right]$, $-\left[\frac{x}{p_3}\right]$, $\left[\frac{x}{p_1p_2}\right]$, $\left[\frac{x}{p_1p_3}\right]$, $\left[\frac{x}{p_2p_3}\right]$ tagoknál vettük figyelembe, tehát eddig $1-1-1-1+1+1+1=1$-szer számoltuk, holott 0-szor kellene számolnunk. Ezt korrigálandó, a (15) összegből ki kell vonnunk az $\left[\frac{x}{p_{i_1}p_{i_2}p_{i_3}}\right]$ (ahol $1\leq i_1<i_2<i_3\leq k$) típusú tagok összegét s í. t. Így végeredményben valóban az (1) jobb oldalán álló összeget kapjuk.

Megjegyezzük, hogy a fenti, kissé vázlatos bizonyítást a

$$\sum_{j=1}^{n}(-1)^j\binom{n}{j}=0$$

összefüggés segítségével lehetne pontosabban megfogalmazni.

2. A (2) formulát felhasználva, számítsuk ki $\pi(120)$ értékét!

Megoldás:

Minthogy

$$10<\sqrt{120}<11,$$

a $\sqrt{120}$-nál kisebb prímszámok: 2, 3, 5 és 7. Így

$$\pi(\sqrt{120})=4.$$

Továbbá (2)-ből ($x=120$-at és $p_1=2, p_2=3, p_3=5, p_4=7$-et helyettesítve):

$$\pi(120) = \pi(\sqrt{120}) - 1 + \sum_{d \mid 2\cdot 3\cdot 5\cdot 7} \mu(d) \left[\frac{120}{d}\right] =$$

$$= 4 - 1 + \left([120] - \left[\frac{120}{2}\right] - \left[\frac{120}{3}\right] - \left[\frac{120}{5}\right] - \left[\frac{120}{7}\right] + \right.$$

$$+ \left[\frac{120}{2\cdot 3}\right] + \left[\frac{120}{2\cdot 5}\right] + \left[\frac{120}{2\cdot 7}\right] + \left[\frac{120}{3\cdot 5}\right] + \left[\frac{120}{3\cdot 7}\right] + \left[\frac{120}{5\cdot 7}\right] -$$

$$\left. - \left[\frac{120}{2\cdot 3\cdot 5}\right] - \left[\frac{120}{2\cdot 3\cdot 7}\right] - \left[\frac{120}{2\cdot 5\cdot 7}\right] - \left[\frac{120}{3\cdot 5\cdot 7}\right] + \left[\frac{120}{2\cdot 3\cdot 5\cdot 7}\right]\right) =$$

$$= 3 + (120 - 60 - 40 - 24 - 17 + 20 + 12 + 8 + 8 + 5 + 3 - 4 - 2 - 1 -$$

$$- 1 + 0) = 3 + 27 = 30.$$

3. Bizonyítsuk be, hogy (3) tetszőleges n természetes számra teljesül!

Megoldás:

Azt kell bizonyítanunk, hogy

$$\frac{n}{2} < p \leqq n \tag{16}$$

esetén

$$p \mid \binom{n}{\left[\frac{n}{2}\right]} = \frac{n!}{\left(\left[\frac{n}{2}\right]!\right)^2}$$

(ahol p prímszám), vagy másképpen

$$p \left(\left[\frac{n}{2}\right]!\right)^2 \Big| n!. \tag{17}$$

Minthogy

$$\binom{n}{\left[\frac{n}{2}\right]} = \frac{n!}{\left(\left[\frac{n}{2}\right]!\right)^2} \tag{18}$$

egész szám, szükségképpen

$$\left(\left[\frac{n}{2}\right]!\right)^2 \Big| n!. \tag{19}$$

Továbbá (16)-ra ($p \leqq n$-re) tekintettel az $n! = 1 \cdot 2 \cdot \ldots \cdot n$ szorzat tényezői közt szerepel p, tehát nyilván

(20) $p | n!$.

Végül ugyancsak (16)-ból $\left(p > \frac{n}{2}\text{-ből}\right)$ következik, hogy az $\left[\frac{n}{2}\right]! = 1 \cdot 2 \cdot \ldots \cdot \left[\frac{n}{2}\right]$ szorzat valamennyi tényezője kisebb p-nél; így — mivel p prímszám — szükségképpen

$$(21) \qquad \left(p, \left(\left[\frac{n}{2}\right]!\right)^2\right) = 1.$$

(19)-ből, (20)-ból és (21)-ből az I. fejezet 4. pontjának *G)* állítására tekintettel következik (17).

4. (3)-ból kiindulva, igazoljuk, hogy létezik olyan c_1 pozitív állandó, melyre (4) teljesül!

Megoldás:

A binomiális tételre tekintettel

$$(22) \qquad \binom{n}{\left[\frac{n}{2}\right]} < \sum_{i=0}^{n} \binom{n}{i} = (1+1)^n = 2^n.$$

(3)-ból és (22)-ből következik, hogy

$$2^n > \prod_{\frac{n}{2} < p \leqq n} p.$$

Mivel a logaritmus függvény monoton növő, innen $n \geqq 4$ esetén nyerjük, hogy

$$n \log 2 > \log \prod_{\frac{n}{2} < p \leqq n} p = \sum_{\frac{n}{2} < p \leqq n} \log p >$$

$$> \sum_{\frac{n}{2} < p \leqq n} \log \frac{n}{2} = \log \frac{n}{2} \sum_{\frac{n}{2} < p \leqq n} 1 = \log \frac{n}{2} \left(\pi(n) - \pi\left(\frac{n}{2}\right)\right) >$$

$$> \log \sqrt{n} \left(\pi(n) - \pi\left(\frac{n}{2}\right)\right) = \frac{\log n}{2} \left(\pi(n) - \pi\left(\frac{n}{2}\right)\right),$$

ahonnan

$$(23) \qquad \pi(n) - \pi\left(\frac{n}{2}\right) < 2 \log 2 \frac{n}{\log n} \quad (n \geqq 4).$$

Legyen most x tetszőleges valós szám, melyre $x \geqq 2$. Definiáljuk a k természetes számot a

(24). $2^{k-1} < x \leqq 2^k$

egyenlőtlenséggel. Ekkor (23)-ban $n = 2^2, 2^3, \ldots, 2^k$-t helyettesítve, és az így nyert egyenlőtlenségeket, valamint a

$$\pi(2) - \pi(1) = 1$$

egyenlőséget összeadva, a bal oldalon a következőt kapjuk:

$$\pi(2^k) - \pi(1) = \pi(2^k) \geqq \pi(x).$$

A jobb oldalak összeadása révén nyert

$$1 + 2 \log 2 \sum_{j=1}^{k} \frac{2^j}{\log 2^j}$$

összegre vonatkozóan pedig elemi analízis segítségével könnyen igazolható, hogy az ($x \geqq 2$-re tekintettel) kisebb, mint

$$3 \cdot 2 \log 2 \cdot \frac{2^k}{\log 2^k} < 3 \cdot 2 \log 2 \cdot 2 \frac{x}{\log x} = 12 \log 2 \frac{x}{\log x}.$$

(A részletek kidolgozását az Olvasóra bízzuk.) Így (4) teljesül $c_1 = 12 \log 2$ választással.

5. Bizonyítsuk be, hogy ha n tetszőleges természetes szám, k természetes szám és a p prímszámra

(25) $$n^{\frac{1}{k+1}} < p$$

eljesül, akkor

(26) $$p^{k+1} \nmid \binom{n}{\left[\frac{n}{2}\right]}.$$

Megoldás:

(18)-ra tekintettel p kitevője $\binom{n}{\left[\frac{n}{2}\right]}$ kanonikus alakjában a Legendre-formula felhasználásával határozható meg. A Legendre-formula szerint p kitevője $n!$ kanonikus alakjában

$$\gamma_p = \sum_{\alpha=1}^{+\infty} \left[\frac{n}{p^\alpha}\right].$$

Azonban (25)-re tekintettel $\alpha \geqq k+1$ esetén $p^\alpha > n$, tehát ekkor $\left[\frac{n}{p^\alpha}\right]=0$, és így

$$\gamma_p = \sum_{\alpha=1}^{k} \left[\frac{n}{p^\alpha}\right].$$

Továbbá ugyancsak a Legendre-formula szerint p kitevője $\left[\frac{n}{2}\right]!$ kanonikus alakjában

$$\delta_p = \sum_{\alpha=1}^{+\infty} \left[\frac{\left[\frac{n}{2}\right]}{p^\alpha}\right] = \sum_{\alpha=1}^{+\infty} \left[\frac{n}{2p^\alpha}\right]$$

(tekintettel az I. fejezet 2. feladatára). (25) szerint $\alpha \geqq k+1$ esetén $2p^\alpha > n$, tehát $\left[\frac{n}{2p^\alpha}\right]=0$, így

$$\delta_p = \sum_{\alpha=1}^{k} \left[\frac{n}{2p^\alpha}\right].$$

Végeredményben p kitevője

$$\binom{n}{\left[\frac{n}{2}\right]} = \frac{n!}{\left(\left[\frac{n}{2}\right]!\right)^2}$$

kanonikus alakjában

$$\gamma_p - 2\delta_p = \sum_{\alpha=1}^{k} \left[\frac{n}{p^\alpha}\right] - 2\sum_{\alpha=1}^{k} \left[\frac{n}{2p^\alpha}\right] =$$

$$= \sum_{\alpha=1}^{k} \left(\left[\frac{n}{p^\alpha}\right] - \left[\frac{n}{2p^\alpha}\right] - \left[\frac{n}{2p^\alpha}\right]\right).$$

Az I. fejezet (2) képlete szerint itt valamennyi tag legfeljebb 1, tehát

$$\gamma_p - 2\delta_p \leqq \sum_{\alpha=1}^{k} 1 = k,$$

és ezzel (26)-ot igazoltuk.

2. ADDITÍV PRÍMSZÁMELMÉLET. PRÍMDIFFERENCIÁK

Jelöljük ismét az n-edik prímszámot p_n-nel (tehát $p_1=2$, $p_2=3$, $p_3=5$, ...), és legyen

(27) $d_n = p_{n+1} - p_n \quad (n = 1, 2, \ldots).$

Igazolható, hogy *az egymást követő prímszámok közt tetszőlegesen nagy hézagok vannak*, vagyis d_n tetszőlegesen nagy értékeket vehet fel.

Legyen ugyanis K tetszőlegesen nagy természetes szám. Állítjuk, hogy az

$$\begin{aligned} A &= (K+1)!+2, \\ A+1 &= (K+1)!+3, \\ &\vdots \\ A+K-1 &= (K+1)!+(K+1) \end{aligned}$$

számok összetett számok. Valóban, e számok mindegyike nagyobb, mint $(K+1)!>K+1$, másrészt e számok nyilván rendre oszthatók 2-vel, 3-mal, ..., ill. $(K+1)$-gyel; innen következik, hogy összetett számok. Az A, $A+1$, ..., $A+K-1$ egymást követő összetett számokat közrefogó prímszámok különbsége nyilván nagyobb K-nál, és ezzel az állítást igazoltuk.

A prímszámtételből könnyen következik az a jóval élesebb állítás is, hogy tetszőlegesen kicsi ε pozitív számot megadva, *végtelen sok* n-re

$$d_n > (1-\varepsilon)\log n.$$

Ennél valamivel több is ismeretes. Nem tudjuk azonban például azt, hogy létezik-e olyan ε pozitív szám, hogy

$$d_n > n^{\varepsilon}$$

végtelen sokszor teljesül?

Ismeretes továbbá, hogy létezik olyan 1-nél kisebb c_{12} állandó, hogy minden n természetes számra

$$d_n < n^{c_{12}}$$

(ez csak nehéz analitikus segédeszközök felhasználásával igazolható); nevezetesen ismeretes, hogy itt például $c_{12}=\frac{38}{61}$ írható. Nem tudjuk azonban, hogy teljesül-e ez az egyenlőtlenség például $c_{12}=\frac{1}{2}$-del, vagy kissé átfogalmazva, két egymást követő négyzetszám közé esik-e mindig prímszám?

Eddig a „nagy" prímdifferenciákkal foglalkoztunk; most áttérünk a „kis" prímdifferenciák vizsgálatára.

Ha $d_n = 2$, akkor p_n-et és p_{n+1}-et *ikerprímszámoknak* mondjuk. Igen régi és máig bizonyítatlan sejtés, hogy végtelen sok ikerprímszám létezik; ez az ún. *ikerprímsejtés.*

Ha valamely x-re az *x-nél nem nagyobb ikerprímszámokat* akarjuk meghatározni, akkor eljárhatunk az eratoszthenészi szitához hasonló módon. Ha ugyanis

$$(28) \qquad \sqrt{x} < n-2 < n \leqq x,$$

akkor az $n-2$ és n számok nyilván akkor és csak akkor ikerprímek, ha bármely, az

$$(29) \qquad 1 < p \leqq x$$

feltételt kielégítő p prímszámra $p \nmid n-2$ és $p \nmid n$, vagyis

$$(30) \qquad n \not\equiv 2 \pmod{p}$$

és

$$(31) \qquad n \not\equiv 0 \pmod{p}.$$

Ezen az alapon a $\sqrt{x}$ és x közé eső ikerprímek számára felírható egy (2)-höz hasonló formula. Ez a formula azonban nem alkalmas arra, hogy segítségével az ikerprímek számát végtelenhez tartó x mellett vizsgáljuk (ugyanúgy, mint ahogy (2) sem alkalmas $\pi(x)$ becslésére). Ezen az előző pontban említett Brun-szita vagy egy másik (még mindig viszonylag elemi) szitamódszer, az ún. *Selberg-szita* révén segíthetünk. Mindkét szitamódszer segítségével igazolható a következő:

Az x-nél nem nagyobb ikerprímek száma az összes x-nél nem nagyobb prímszámok számához, azaz $\pi(x)$-hez viszonyítva „kicsi", pontosabban kisebb, mint

$$c_{13} \frac{x}{\log^2 x} \left(< c_{14} \frac{\pi(x)}{\log x} \right),$$

ahol c_{13} alkalmas állandó.

A Brun-szita és főképpen a Selberg-szita jóval általánosabb problémák tárgyalására is alkalmazható, mint $\pi(x)$ vagy az ikerprímek számának (felső) becslése. Az ikerprímekkel kapcsolatos alkalmazás ugyanis a fentiek szerint úgy fogalmazható, hogy azon n számok számára keresünk felső becslést, melyek kielégítik (28)-at, valamint a (30) és (31) kongruencia feltételeket, vagyis amelyek bármely (29)-et kielégítő p-re kihagynak két adott „tilos" maradékosztályt modulo p. Mármost az említett szitamódszerek alkalmazhatók abban az esetben is, ha a (30) és (31) alatti két

„tilos" maradékosztály helyett bármely két más „tilos" maradékosztályt írunk elő.

Sőt, e módszerek alkalmazhatók akkor is, ha a (29)-et kielégítő p prímek mindegyikére $f(p)$ számú „tilos" maradékosztályt írunk elő, ahol $f(p)$ korlátos vagy pedig az $f(y)$ függvény y függvényében „lassan" tart a végtelenhez — például valamely $c>0$-ra $f(y)>cy$, vagyis minden p-re a modulo p maradékosztályok pozitív százaléka „tilos" —, akkor egy másik szitamódszerhez, az ún. Rényi—Linnik-féle „*nagy szitához*" kell folyamodnunk.

A Brun- vagy Selberg-szität ebben az általánosabb formában alkalmazva, *felülről* becsülhető az általánosabb

(32) $p-q=d$ (ahol $q<p\leqq n$)

ill.

(33) $p+q=n$

egyenletek megoldásszáma, ahol d, n adott páros természetes számok. (Ha (32)-ben $d=2$-t írunk, akkor speciális esetként az ikerprímek számára nyerhetünk felső becslést.) Igazolható, hogy (32) megoldásszáma kisebb, mint

$$(34)\quad c_{15}\prod_{p|d}\left(1-\frac{1}{p}\right)^{-1}\frac{n}{\log^2 n}\quad\left(=A_d\frac{n}{\log^2 n}\right),$$

(33)-é pedig kisebb, mint

$$(35)\quad c_{16}\prod_{p|n}\left(1-\frac{1}{p}\right)^{-1}\frac{n}{\log^2 n},$$

ahol c_{15}, c_{16} abszolút állandók, A_d pedig csak d-től függő (n-től független) állandó. (E becsléseket Schnirelman igazolta először e század 30-as éveiben.)

Megjegyezzük, hogy az itt szereplő $\prod_{p|n}\left(1-\frac{1}{p}\right)^{-1}$ faktor a „legtöbb" n-re korlátos.

Ismételten hangsúlyozzuk, hogy a szitamódszerek valamenynyi említett esetben csupán *felső* becslést adnak bizonyos számok (adott korlát alatti prímek, ikerprímek s í. t.) számára.

Kidolgozható ugyan — elsősorban a Selberg-szitának — egy alsó becslésre szolgáló változata is, ez azonban nem elég hatékony például az ikerprímsejtés igazolásához.

(33) megoldásszámának vizsgálata kapcsolódik a számelmélet egyik legfontosabb problémájához, az ún. *Goldbach-sejtéshez*. Goldbach ui. — a XVIII. sz. közepén — sejtette, hogy bármely 4-nél nagyobb páros szám felírható két, bármely 7-nél nagyobb páratlan szám pedig három páratlan prímszám összegeként. Megjegyezzük, hogy ha a sejtés páros számokra vonatkozó része igaz, akkor ebből következik a páratlan számokra vonatkozó állítás is (l. a 7. példát); így az előbbi nyilván mélyebb az utóbbinál.

A Goldbach-sejtés irányában az első lényeges eredményeket Hardynak és Littlewoodnak sikerült elérnie, komplex függvénytani segédeszközök felhasználásával. A következő fontos részeredmény Schnirelmantól származik, aki a (33) megoldásszámára adott (35) felső becslésből kiindulva, elemi úton igazolta, hogy létezik olyan k szám, hogy bármely 1-nél nagyobb természetes szám felírható legfeljebb k prímszám összegeként.

Végül I. M. Vinogradov 1937-ben lényegében bebizonyította — a Hardy—Littlewood-módszerre építve, analitikus segédeszközök (exponenciális összegek) segítségével — a Goldbach-sejtés *páratlan* számokra vonatkozó részét. Továbbá Vinogradov módszerét felhasználva, többen egymástól függetlenül igazolták, hogy „majdnem minden" páros szám felírható két prímszám összegeként (azaz: azon páros számok száma, melyek x-nél nem nagyobbak és *nem* írhatók fel két prímszám összegeként, x-szel osztva 0-hoz tart, ha x tart a végtelenhez). A Goldbach-sejtés páros számokra vonatkozó része azonban eredeti formájában még nincs bebizonyítva.

Példák

6. Határozzuk meg az összes olyan p, q, r prímszámhármasokat, melyekre $(0<)p<q<r$ teljesül, és mind p, q, mind q, r ikerprímek!

Megoldás:

Ha p, q ikerprímek (és $q>p$), akkor

$$q = p+2.$$

Ha továbbá q, r is ikerprímek (és $r>q$), akkor

$$r = q+2 = (p+2)+2 = p+4.$$

A feladat feltételei szerint tehát $p, p+2$ és $p+4$ is prímszámok.

A $p, p+1, p+2$ számok — három egymást követő szám — valamelyike osztható 3-mal. Továbbá $p+4=(p+1)+3$ nyilván akkor és csak akkor osztható 3-mal, ha $p+1$ is osztható 3-mal; így szükségképpen a $p, p+2$,

$p+4$ számok valamelyike is osztható 3-mal. Az egyetlen 3-mal osztható (pozitív) prímszám azonban a 3, tehát szükségképpen

$$(36) \qquad p = 3,$$

vagy

$$p+2 = 3$$

$$p+4 = 3$$

teljesül. Utóbbi kettőből $p=1$, ill. $p=-1$ következnék, azonban 1 és -1 nem prímszámok. (36)-ból viszont az egyetlen olyan prímszámhármast nyerjük, mely kielégíti a feladat követelményeit: $p=3$, $q=5$, $r=7$.

7. Bizonyítsuk be, hogy ha a Goldbach-sejtés páros számokra vonatkozó része igaz, akkor szükségképpen a páratlan számokra vonatkozó része is igaz; azaz, ha minden 4-nél nagyobb páros szám felírható két páratlan prímszám összegeként, akkor szükségképpen minden 7-nél nagyobb páratlan szám felírható három páratlan prímszám összegeként!

Megoldás:

Legyen n 7-nél nagyobb páratlan szám. Ekkor $n-3$ páros szám, mely 4-nél nagyobb, tehát ha a Goldbach-sejtés páros számokra vonatkozó része igaz, akkor $n-3$ felírható két páratlan prímszám összegeként:

$$n-3 = p+q.$$

Átrendezve:

$$p+q+3 = n,$$

tehát n felírható három páratlan prímszám összegeként, és ezt kellett igazolnunk.

3. DIRICHLET TÉTELE

Ebben a pontban a *prímszámoknak a számtani sorozatokban való eloszlásával* fogunk foglalkozni.

Legyen a adott természetes szám, b adott egész szám, és tekintsük az

$$(37) \quad a+b,\ 2a+b,\ \ldots,\ ak+b,\ \ldots$$

végtelen számtani sorozatot. Nyilván e számtani sorozat valamennyi eleme osztható (a, b)-vel. Így e számtani sorozat $(a, b)>1$ esetén csak akkor tartalmazhat prímszámot, ha (a, b) prímszám, és ebben az esetben is legfeljebb kettőt, ti. $-(a, b)$-t és $+(a, b)$-t.

Másrészt L. Dirichlet 1837-ben nehéz analitikus segédeszközök felhasználásával igazolta azt az igen mély tételt, mely szerint $(a, b)=1$ *esetén a* (37) *számtani sorozat végtelen sok prímszámot tartalmaz.*

A 8. és 9. példák, valamint a 34—38. feladatok kapcsán igazolni fogjuk Dirichlet tételének néhány speciális esetét. Megjegyezzük, hogy Dirichlet tételére az általános esetben máig sem ismeretes elemi bizonyítás. Az említett példák és feladatok kapcsán vázolt módszerek csupán annak a speciális esetnek a vizsgálatára alkalmasak, amikor a (37) számtani sorozatban $b=\pm 1$ vagy valamivel általánosabban

$$b \equiv \pm 1 \pmod{a}.$$

1947-ben J. Linnik bebizonyította a Dirichlet-tétel következő élesítését: Létezik olyan c_{17} állandó, hogy tetszőleges a természetes számot megadva

$$(38) \qquad (a, b) = 1 \quad \text{és} \quad 1 \leqq b < a$$

esetén a (37) számtani sorozat tartalmaz olyan p prímszámot, melyre $p<a^{c_{17}}$ teljesül. (Vagyis (38) esetén a (37) számtani sorozat által tartalmazott legkisebb prímszám szükségképpen viszonylag „kicsi".) Linnik tételének bizonyítása egyike a legnehezebb matematikai bizonyításoknak, melyet valaha is publikáltak.

Példák

8. Bizonyítsuk be, hogy végtelen sok $4k-1$ alakú (pozitív) prímszám létezik!

Megoldás:

A végtelen sok prímszám létezésének bizonyítása során alkalmazott euklideszi gondolatmenetet követve, tegyük fel indirekte, hogy csak véges sok $4k-1$ alakú prímszám létezik; legyenek ezek $p_1, p_2, \ldots, p_r$. Képezzük az $n=4p_1p_2\ldots p_r-1$ számot. Minthogy nyilván $n>1$, a számelmélet alaptétele szerint n felírható $n=q_1q_2\ldots q_s$ alakban, ahol $q_1, q_2, \ldots, q_s$ prímszámok.

$q_1, q_2, \ldots, q_s$ osztói n-nek, másrészt n nem osztható $p_1, p_2, \ldots, p_r$ egyikével sem (hiszen n $p_1, \ldots, p_r$-rel osztva, rendre $p_1-1, \ldots, p_r-1$ maradékot ad); így a $q_1, q_2, \ldots, q_s$ prímek különböznek a $p_1, p_2, \ldots, p_r$ prímektől, tehát nem lehetnek $4k-1$ alakúak. Továbbá $q_1, q_2, \ldots, q_s$ különböznek 2-től, hiszen n páratlan. Végeredményben tehát $q_1, q_2, \ldots, q_s$ nem

lehetnek $4k-1$ alakúak, és különböznek 2-től; így szükségképpen $4k+1$ alakúak. Azonban a $4k+1$ alakú számok szorzata is $4k+1$ alakú:

$$(4a+1)(4b+1) = 16ab+4a+4b+1 = 4(4ab+a+b)+1 = 4c+1.$$

Így $q_1 \cdot q_2 \cdot \ldots \cdot q_s = n$ is $4k+1$ alakú szám.

Másrészt, mint n definíciójából látszik, n nyilván $4k-1$ alakú. Egy egész szám azonban nem lehet egyidejűleg $4k+1$ és $4k-1$ alakú; az indirekt feltevésből tehát ellentmondásra jutottunk, és ezzel az állítást igazoltuk.

9. A II. fejezet 91. feladatát felhasználva, bizonyítsuk be, hogy végtelen sok $4k+1$ alakú (pozitív) prímszám létezik!

Megoldás:

Tegyük fel indirekte, hogy csak véges sok $4k+1$ alakú prímszám létezik; legyenek ezek $p_1, p_2, \ldots, p_r$. Képezzük az

$$n = 4p_1^2 p_2^2 \ldots p_r^2 + 1 = (2p_1 p_2 \ldots p_r)^2 + 1 = x^2 + 1$$

számot. Nyilván $n > 1$, tehát n felírható $n = q_1 q_2 \ldots q_s$ alakban, ahol $q_1, q_2, \ldots, q_s$ prímszámok. Ekkor n osztható $q_1, q_2, \ldots, q_s$-sel, másrészt nyilván nem osztható $p_1, p_2, \ldots, p_r$-rel. Így a $q_1, q_2, \ldots, q_r$ prímszámok különböznek a $p_1, p_2, \ldots, p_s$ prímszámoktól.

Továbbá n páratlan szám, tehát $q_1, q_2, \ldots, q_s$ különböznek 2-től. Így a $q_1, q_2, \ldots, q_s$ prímszámok páratlan prímosztói $n = x^2+1$-nek, következésképpen a II. fejezet 91. feladata szerint $4k+1$ alakúak.

Végeredményben tehát $q_1, q_2, \ldots, q_s$ $4k+1$ alakú prímszámok, melyek különböznek $p_1, p_2, \ldots, p_r$-től, ami ellentmond az indirekt feltevésnek, és ezzel az állítást igazoltuk.

(Megjegyezzük, hogy a 8. példa megoldásának gondolatmenete most azért nem alkalmazható, mert $4k+1$ alakú egész számnak — mint ezt például a $21 = 3 \cdot 7$ szám mutatja — nem feltétlenül van $4k+1$ alakú prímosztója.)

10. Bizonyítsuk be, hogy tetszőleges m természetes számot megadva, létezik olyan p prímszám, melyet 10-es számrendszerben felírva, számjegyei közt legalább m számú 0 szerepel!

Megoldás:

A $10^{m+1}k+1$ (ahol $k = 1, 2, \ldots$) alakú számok utolsó számjegye 1, ezt megelőzően pedig (legalább) m számú 0 áll, tehát e számok számjegyei közt legalább m számú 0 szerepel.

Másrészt $(10^{m+1}, 1) = 1$, tehát Dirichlet tétele szerint végtelen sok $10^{m+1}k+1$ alakú prímszám létezik, és ezzel az állítást igazoltuk.

(Megjegyezzük, hogy a feladat állítása Dirichlet tételének felhasználása nélkül, (10)-ből kiindulva is igazolható; l. a 12* feladatot.)

FELADATOK

1. Bizonyítsuk be, hogy ha n 2-nél nagyobb természetes szám, akkor az $n, n+1, n+2, n+3$ számok közt van legalább egy olyan, melynek legalább két különböző prímosztója van!

2. Jelöljük az n-edik prímszámot p_n-nel. Adjunk új bizonyítást a

$$p_n < 2^{2^n}$$

(l. I. fejezet (22)) formulára anélkül, hogy hivatkoznánk a Fermat-számokra!

3. Bizonyítsuk be $\varphi(n)$ explicit alakjából kiindulva, hogy végtelen sok prímszám létezik!

4. Bizonyítsuk be, hogy nem létezik olyan $f(x)$ legalább elsőfokú egész együtthatós polinom, hogy $f(n)$ minden n egész számra prímszám!

5. Legyen $f(x)$ tetszőleges egész együtthatós polinom, p tetszőleges prímszám. Ha található olyan n egész szám, hogy $p|f(n)$, akkor azt mondjuk, hogy p prímosztója az $f(x)$ polinomnak. Bizonyítsuk be, hogy minden legalább elsőfokú egész együtthatós polinomnak végtelen sok prímosztója van!

6. Mennyi $\pi(20)$ értéke?

7. Hány 1975-nél nem nagyobb és 140-hez relatív prím természetes szám létezik?

8. Hány olyan 2000-nél nem nagyobb n természetes szám létezik, melyre $(n, 252)>1$ teljesül?

9. Állapítsuk meg, hogy 1975! hány 0-ra végződik?

10. Osztható-e $\binom{1000}{500}$ 7-tel?

11. Legyenek $a_1, a_2, \ldots, a_k, n$ természetes számok, melyekre

$$a_1+a_2+\ldots+a_k \leqq n. \tag{39}$$

Bizonyítsuk be kombinatorikai segédeszközök felhasználása nélkül, hogy $A=\dfrac{n!}{a_1!a_2!\ldots a_k!}$ egész szám!

12*. Igazoljuk a 10. példa állítását Dirichlet tételének felhasználása nélkül, (5)-ből kiindulva!

13. Bizonyítsuk be, hogy létezik végtelen sok olyan prímszám, melyet tízes számrendszerben felírva, az első számjegye 1-es!

14. Bizonyítsuk be, hogy ha n 1-nél nagyobb természetes szám, akkor $n!$ nem lehet teljes hatvány (természetes szám 1-nél nagyobb egész kitevős hatványa)!

15. Legyen n tetszőleges természetes szám. Bizonyítsuk be, hogy n és $n+1$ közül legalább az egyik felírható csupa különböző prímszám összegeként!

16. Igazoljuk, hogy (4)-ből következik (6) (alkalmas c_3 pozitív állandóval)!

17. Bizonyítsuk be, hogy léteznek olyan c_{18}, c_{19} pozitív állandók, hogy tetszőleges, 1-nél nagyobb n természetes számra

$$e^{c_{18}n} < [1, 2, \dots, n] < e^{c_{19}n}.$$

18*. Bizonyítsuk be, hogy léteznek olyan c_{20}, c_{21} pozitív állandók, hogy végtelen sok m, n természetes számra

a.

$$(40) \quad \nu(m) > c^{20} \frac{\log m}{\log\log m},$$

b.

$$(41) \quad d(n) > e^{c_{21}\frac{\log n}{\log\log n}}.$$

19*. Bizonyítsuk be, hogy ha $a_1, a_2, \dots, a_k, \dots$ egymástól különböző természetes számok (lehet e sorozat akár véges, akár végtelen), és egyikük sem osztható 3-nál nagyobb prímszámmal, akkor

$$\sum_k \frac{1}{a_k} \leqq 3.$$

20*. Bizonyítsuk be, hogy tetszőleges 1-nél nagyobb n természetes számra

$$(42) \quad \prod_{p \leqq n} \frac{1}{1-\frac{1}{p}} \geqq \sum_{i=1}^{n} \frac{1}{i}.$$

21*. (42)-ből kiindulva, igazoljuk, hogy végtelen sok prímszám létezik!

22*. Az analízisből ismeretes, hogy teszőleges n természetes számra

$$(43) \quad \sum_{i=1}^{n} \frac{1}{i} > \log n,$$

továbbá $|x| \leqq \frac{1}{2}$ esetén

$$(44) \quad 1-x > e^{-x-x^2}.$$

Ezt a két segédtételt felhasználva, (42) alapján igazoljuk, hogy létezik olyan c_{22} pozitív állandó, hogy tetszőleges, 1-nél nagyobb n természetes számra

$$(45) \quad \sum_{p \leqq n} \frac{1}{p} > \log \log n + c_{22}.$$

23*. Jelöljük az i-edik prímszámot p_i-vel. Bizonyítsuk be, hogy tetszőlegesen kicsi ε pozitív számhoz található végtelen sok olyan i természetes szám, melyre

$$p_{i+1} < (1+\varepsilon)p_i.$$

24*. Bizonyítsuk be, hogy léteznek olyan c_{23}, c_{24} pozitív állandók, hogy tetszőleges, 1-nél nagyobb n természetes számra

a. $$\left| \sum_{i=1}^{n} \nu(i) - n \log \log n \right| < c_{23} n,$$

b. $$\left| \sum_{i=1}^{n} \varkappa(i) - n \log \log n \right| < c_{24} n.$$

25*. Bizonyítsuk be, hogy léteznek olyan c_{25}, c_{26} pozitív állandók, hogy végtelen sok k, l természetes számra

a.

$$(46) \quad \varphi(k) < c_{25} \frac{k}{\log \log k},$$

b.

(47) $\sigma(l) > c_{26} l \log\log l.$

Megjegyezzük, hogy még mindig elemi úton, de valamivel nehezebben igazolható lenne, hogy a (40), (41), (46), (47) becslések $\nu(n)$, $d(n)$, $\sigma(n)$ „nagy", $\varphi(n)$ „kis" értékeire „közel" a lehető legjobbak. Pontosabban, igazolható lenne, hogy az említett egyelőtlenségekben szereplő $c_{20}, c_{21}, c_{25}, c_{26}$ állandókat más alkalmas állandókkal helyettesítve, bármely 2-nél nagyobb m, n, k, l természetes számokra ellenkező irányú egyenlőtlenség teljesül.

26. Bizonyítsuk be, hogy ha n 2-nél nagyobb természetes szám, akkor 2^n-1 és 2^n+1 nem lehetnek ikerprímszámok!

27. Bizonyítsuk be, hogy végtelen sok olyan prímszám létezik, mely nem tagja egyetlen ikerprímszámpárnak sem!

28. Bizonyítsuk be, hogy akkor és csak akkor létezik végtelen sok ikerprímszámpár, ha létezik végtelen sok olyan egész szám, amelyik nem állítható elő u, v természetes számokkal a $6uv+u+v$, $6uv+u-v$, $6uv-u+v$, $6uv-u-v$ alakok egyikében sem!

29. Bizonyítsuk be, hogy minden 11-nél nagyobb természetes szám felírható két összetett szám összegeként!

30. Bizonyítsuk be, hogy létezik végtelen sok páratlan természetes szám, mely nem írható fel 3-nál kevesebb prímszám összegeként!

31. Tegyük fel, hogy igaz a páros számokra vonatkozó Goldbach-sejtés a következő módosított formában: minden 6-nál nagyobb páros szám felírható két különböző prímszám összegeként. Bizonyítsuk be, hogy ekkor a

$$\sigma(x)-x = n$$

egyenlet páratlan n-re akkor és csak akkor megoldhatatlan, ha $n=5$.

32*. Bizonyítsuk be, hogy létezik végtelen sok természetes szám, mely nem írható fel n^2+p alakban (n természetes szám, p prímszám)!

33. Bizonyítsuk be, hogy tetszőleges k természetes számhoz található olyan k tagú (különböző számokból álló) számtani sorozat, melynek elemei páronként relatív prímek!

34. Bizonyítsuk be, hogy végtelen sok $6k-1$ alakú prímszám létezik!

35. Bizonyítsuk be a II. fejezet 96*. feladatát felhasználva, hogy végtelen sok $6k+1$ alakú prímszám létezik!

36. Bizonyítsuk be a II. fejezet 95*. feladatát felhasználva, hogy végtelen sok $8k-1$ alakú prímszám létezik!

37*. Legyen p 2-nél nagyobb prímszám. Bizonyítsuk be a II. fejezet 61*. feladatát felhasználva, hogy végtelen sok $pk+1$ alakú prímszám létezik!

38. Legyen α tetszőleges természetes szám. Bizonyítsuk be a II. fejezet 62*. feladatát felhasználva, hogy végtelen sok $2^{\alpha}k+1$ alakú prímszám létezik!

39. Legyenek a, n tetszőleges természetes számok, b az a-hoz relatív prím egész szám. Bizonyítsuk be, hogy az $ak+b$ $(k=0, 1, 2, \ldots)$ számtani sorozatnak végtelen sok olyan eleme van, amely n különböző prímszám szorzata!

40. Bizonyítsuk be, hogy tetszőleges k természetes számhoz található olyan prímszám, amely számjegyeinek összege k-nál nagyobb!

41. Bizonyítsuk be, hogy tetszőleges a természetes számhoz található végtelen sok olyan n természetes szám, amelyre $d(n^a)$ prímszám!

42. Bizonyítsuk be, hogy tetszőleges a természetes számhoz található végtelen sok olyan n természetes szám, melyre $a|\sigma(n)$ teljesül!

43. Bizonyítsuk be, hogy tetszőleges a páratlan egész számhoz található végtelen sok olyan páratlan n természetes szám, melyre $(a, \varphi(n))=1$.

44. Bizonyítsuk be, hogy tetszőleges k természetes számot megadva, található végtelen sok olyan p prímszám, hogy a $p-k, \ldots, p-2, p-1, p+1, p+2, \ldots, p+k$ számok mindegyike összetett szám (azaz, léteznek ún. „izolált" prímek)!

45*. Bizonyítsuk be, hogy tetszőleges k természetes számot megadva, található végtelen sok olyan p prímszám, hogy az $1, 2, \ldots, k$ számok mindegyike kvadratikus maradék modulo p.

Jelöljük tetszőleges p primszámra a legkisebb olyan természetes számot, mely kvadratikus nem-maradék modulo p—röviden: a modulo p legkisebb kvadratikus nem-maradékot — $q(p)$-vel, a modulo p legkisebb primitív

gyököt $g(p)$-vel. E jelöléseket használva, a feladat állítása a következőképpen fogalmazható át: bizonyítandó, hogy $q(p)$ tetszőlegesen nagy értékeket vehet fel, azaz

$$\limsup_{p \to +\infty} q(p) = +\infty. \tag{48}$$

Mivel a II. fejezetben mondottak szerint kvadratikus maradék nem lehet primitív gyök modulo p, szükségképpen

$$q(p) \leqq g(p).$$

Így (48)-ból az is következik, hogy

$$\limsup_{p \to +\infty} g(p) = +\infty.$$

Megjegyezzük, hogy $q(p)$, ill. $g(p)$ nagyságrendjének vizsgálata fontos és sokak által vizsgált probléma. D. Burgess bizonyította 1957-ben, hogy tetszőlegesen kicsi ε pozitív számot megadva, $p > p_0(\varepsilon)$ esetén

$$q(p) < p^{\frac{1}{4\sqrt{e}}+\varepsilon};$$

hasonló becslés igaz $g(p)$-re is. Nem ismeretes azonban például az, hogy létezik-e olyan c pozitív állandó, hogy végtelen sok p prímszámra

$$q(p) > p^c?$$

Valószínűnek látszik, hogy ilyen c nem létezik.

A IV. FEJEZETBEN KITŰZÖTT FELADATOK MEGOLDÁSAI

1. A négy szám közt van két (egymást követő) páros szám; ezek egyike $4k+2=2(2k+1)$ alakú. Ez utóbbi szám nyilván a kívánt tulajdonságú.

2. n-re vonatkozó teljes indukcióval bizonyítunk. $n=1$ esetén az állítás igaz:

$$p_1 = 2 < 2^{2^1} = 4.$$

Most tegyük fel, hogy $n=1, 2, \ldots, k$ esetén teljesül az állítás; bizonyítanunk kell, hogy ebből következik, hogy

$$p_{k+1} < 2^{2^{k+1}}. \tag{49}$$

Képezzük az $m=p_1p_2\ldots p_k+1$ számot. Ez 1-nél nagyobb, tehát a számelmélet alaptétele szerint felírható prímszámok szorzataként. m prímosztóinak mindegyike különbözik $p_1, p_2, \ldots, p_k$-tól, hiszen m nem osztható $p_1, p_2, \ldots, p_k$-val. Így létezik legalább egy, m-nél nem nagyobb, $p_1, p_2, \ldots, \ldots, p_k$-tól különböző prímszám, tehát

$$p_{k+1} \leqq m. \tag{50}$$

Másrészt az indukciós feltevésre tekintettel

$$\begin{aligned} m &= p_1p_2\ldots p_k+1 < 2^{2^1}\cdot 2^{2^2}\cdot\ldots\cdot 2^{2^k}+1 = \\ &= 2^{2^1+2^2+\ldots+2^k}+1 = 2^{2^{k+1}-2}+1 = \frac{1}{4}\cdot 2^{2^{k+1}}+\frac{1}{4}\cdot 2^{2^1} < \\ &< \frac{1}{4}\cdot 2^{2^{k+1}}+\frac{1}{4}\cdot 2^{2^{k+1}} = \frac{1}{2}\cdot 2^{2^{k+1}} < 2^{2^{k+1}}. \end{aligned} \tag{51}$$

(50)-ből és (51)-ből adódik (49), és ezzel az állítást igazoltuk.

3. Tegyük fel indirekte, hogy csak véges sok prímszám létezik; legyenek ezek $p_1=2, p_2=3, \ldots, p_k$. A számelmélet alaptétele szerint bármely 1-nél nagyobb n természetes szám felírható prímszámok szorzataként. Indirekt feltevésünk szerint n prímosztói $p_1, p_2, \ldots, p_k$ közül kerülnek ki, tehát szükségképpen

$$(n, p_1p_2\ldots p_k) > 1$$

(bármely, 1-nél nagyobb n természetes számra). Így csak egyetlen olyan n természetes szám létezik, melyre $(n, p_1p_2 \dots p_k)=1$ és $1 \leqq n \leqq p_1p_2 \dots p_k$ teljesül, nevezetesen $n=1$. Ebből következik, hogy

(52) $\varphi(p_1p_2 \dots p_k) = 1.$

Másrészt a $\varphi(n)$-re vonatkozó explicit képlet szerint

$$\varphi(p_1p_2 \dots p_k) = \varphi(p_1)\varphi(p_2) \dots \varphi(p_k) =$$

$$= (p_1-1)(p_2-1) \dots (p_k-1) = (2-1)(3-1) \dots (p_k-1) =$$

$$= 2 \cdot (p_3-1) \dots (p_k-1) > 2 \cdot 1 \cdot \dots \cdot 1 = 2,$$

ami ellentmond (52)-nek, és ezzel az állítást igazoltuk.

4. Legyen $f(x)$ m-edfokú egész együtthatós polinom, ahol $m \geqq 1$. Feltehető, hogy létezik olyan n_0 egész szám, hogy $f(n_0)=p$ prímszám (ellenkező esetben nincs mit bizonyítanunk). A kongruenciák $F)$ tulajdonása szerint

(53) $n \equiv n_0 \pmod{p}$

esetén szükségképpen

$$f(n) \equiv f(n_0) \equiv 0 \pmod{p}$$

is fennáll, tehát $f(n)$ is osztható p-vel.

Mint az algebrából ismeretes, az

(54) $f(x) = 0,$

(55) $f(x)-p = 0,$

ill.

(56) $f(x)+p = 0$

egyenleteknek külön-külön legfeljebb m, összesen legfeljebb $3m$ (valós) megoldásuk van. Így ha az (53)-at kielégítő végtelen sok n egész szám közül elhagyjuk azokat, melyek (54)-nek, (55)-nek vagy (56)-nak gyökei (tehát legfeljebb $3m$ számot), még mindig végtelen sok n egész szám marad. Ezekre az n-ekre a fentiek szerint egyrészt $p|f(n)$, másrészt $f(n)$ különbözik 0-tól, $-p$-től és $+p$-től; így ezekre az n-ekre $f(n)$ nyilván összetett szám, és ezzel az állítást igazoltuk.

5. Legyen

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$$

legalább elsőfokú egész együtthatós polinom.

Ha $a_n=0$, akkor nyilván bármely p prímszámra $p|f(p)$, tehát a polinomnak minden p prímszám prímosztója.

Legyen most $a_n \neq 0$, és tegyük fel, hogy az állítással ellentétben $f(x)$-nek csak véges sok prímosztója van; legyenek ezek $p_1, p_2, \ldots, p_r$. Legyen továbbá

$$g(y) = \frac{f(a_n y)}{a_n} = a_0 a_n^{n-1} y^n + a_1 a_n^{n-2} y^{n-1} + \ldots + a_{n-1} y + 1.$$

Minthogy $a_n \neq 0$, $f(x)$ és $g(y)$ fokszáma megegyezik, tehát $g(y)$ is legalább elsőfokú. Így — mint az analízisből ismeretes — található olyan y_0 szám, hogy $y > y_0$ esetén $|g(y)| > 1$. Ebből következik, hogy létezik olyan k természetes szám, hogy $|g(kp_1p_2 \ldots p_r)| > 1$. Mivel $g(y)$ is egész együtthatós polinom, $|g(kp_1p_2 \ldots p_r)|$ egész szám. Így $|g(kp_1p_2 \ldots p_r)|$ 1-nél nagyobb egész szám, tehát (a számelmélet alaptételére tekintettel) létezik olyan p prímszám, melyre $p | g(kp_1p_2 \ldots p_r)$ teljesül. Ekkor

$$p | a_n g(kp_1p_2 \ldots p_r) = f(a_n kp_1p_2 \ldots p_r),$$

tehát p prímosztója az $f(x)$ polinomnak. Továbbá abból, hogy

$$p_1p_2 \ldots p_r | g(kp_1p_2 \ldots p_r) - 1 \quad \text{és} \quad p | g(kp_1p_2 \ldots p_r),$$

következik, hogy p különbözik $p_1, p_2, \ldots, p_r$ mindegyikétől, és így az indirekt feltevésből ellentmondásra jutottunk.

6. A 20-nál kisebb prímszámok: 2, 3, 5, 7, 11, 13, 17 és 19. Ezek száma 8, tehát $\pi(20) = 8$.

7. Minthogy 140 kanonikus alakja $140 = 2^2 \cdot 5 \cdot 7$, $(n, 140) > 1$ akkor és csak akkor teljesül, ha n osztható 2-vel, 5-tel vagy 7-tel. Így az 1975-nél nem nagyobb természetes számok közül azokat kell „kiszitálnunk", melyek oszthatók 2-vel, 5-tel vagy 7-tel. A megmaradó számok számára (1)-hez hasonló formula írható fel:

$$1975 - \left[\frac{1975}{2}\right] - \left[\frac{1975}{5}\right] - \left[\frac{1975}{7}\right] + \left[\frac{1975}{2 \cdot 5}\right] + \left[\frac{1975}{2 \cdot 7}\right] + \left[\frac{1975}{5 \cdot 7}\right] -$$

$$- \left[\frac{1975}{2 \cdot 5 \cdot 7}\right] = 1975 - 987 - 395 - 282 + 197 + 141 + 56 - 28 = 677.$$

8. 252 kanonikus alakja: $252 = 2^2 \cdot 3^2 \cdot 7$. $(n, 252) > 1$ tehát akkor és csak akkor teljesül, ha n osztható 2-vel, 3-mal vagy 7-tel. A 2000-nél nem nagyobb, az $(n, 252) > 1$ feltételt kielégítő számokhoz tehát eljuthatunk úgy, hogy az 1, 2, ..., 2000 számok (vagyis 2000 szám) közül elhagyjuk azokat, melyek relatív prímek 252-höz, tehát nem oszthatók sem 2-vel, sem 3-mal, sem 7-tel. Ez utóbbi számok számát viszont az előző feladat megoldása során követett módszerrel határozhatjuk meg. Végeredményben tehát a 2000-nél nem nagyobb, az $(n, 252) > 1$ feltételt kielégítő n szá-

mok száma:

$$2000-\left(2000-\left[\frac{2000}{2}\right]-\left[\frac{2000}{3}\right]-\left[\frac{2000}{7}\right]+\left[\frac{2000}{2\cdot 3}\right]+\left[\frac{2000}{2\cdot 7}\right]+\right.$$

$$\left.+\left[\frac{2000}{3\cdot 7}\right]-\left[\frac{2000}{2\cdot 3\cdot 7}\right]\right)=2000-(2000-1000-666-285+333+$$

$$+142+95-47)=1000+666+285-333-142-95+47=1428.$$

9. Egy szám nyilván annyi 0-ra végződik, 10-nek ahányadik hatványával osztható. Így ha 1975! k számú 0-ra végződik, akkor $10^k|1975!$, de $10^{k+1}\nmid 1975!$. Ezt a k számot 1975! kanonikus alakjának ismeretében határozhatjuk meg. Legyen ugyanis 1975! kanonikus alakja

$$1975!=2^\alpha 3^\beta 5^\gamma 7^\delta \ldots .$$

Ekkor k nyilván α és γ közül a kisebbikkel azonos.

A Legendre-formula szerint

$$\alpha=\sum_{k=1}^{+\infty}\left[\frac{1975}{2^k}\right]$$

és

$$\gamma=\sum_{k=1}^{+\infty}\left[\frac{1975}{5^k}\right].$$

Minthogy az előbbi összeg k-adik tagja legalább akkora, mint az utóbbié, nyilván $\alpha\geqq\gamma$. Így elég γ-t kiszámítani:

$$k=\gamma=\left[\frac{1975}{5}\right]+\left[\frac{1975}{25}\right]+\left[\frac{1975}{125}\right]+\left[\frac{1975}{625}\right]=$$

$$=395+79+15+3=492.$$

1975! tehát 492 darab 0-ra végződik.

10. $$\binom{1000}{500}=\frac{1000!}{(500!)^2}.$$

A Legendre-formula szerint 7 kitevője a számláló kanonikus alakjában

$$\left[\frac{1000}{7}\right]+\left[\frac{1000}{49}\right]+\left[\frac{1000}{343}\right]=142+20+2=164,$$

míg a nevezőében

$$2\left(\left[\frac{500}{7}\right]+\left[\frac{500}{49}\right]+\left[\frac{500}{343}\right]\right)=2(71+10+1)=2\cdot 82=164.$$

7 kitevője $\binom{1000}{500}$ kanonikus alakjában az említett kitevők különbsége:

$$164-164=0,$$

tehát a vizsgált szám nem osztható 7-tel.

11. A Legendre-formula szerint az A racionális szám kanonikus alakjában csak az n-nél nem nagyobb p prímszámok szerepelhetnek. Ezek kitevője:

$$\sum_{\alpha=1}^{+\infty}\left[\frac{n}{p^\alpha}\right]-\sum_{\alpha=1}^{+\infty}\left[\frac{a_1}{p^\alpha}\right]-\sum_{\alpha=1}^{+\infty}\left[\frac{a_2}{p^\alpha}\right]-\ldots-\sum_{\alpha=1}^{+\infty}\left[\frac{a_k}{p^\alpha}\right]=$$

$$=\sum_{p^\alpha\leqq n}\left(\left[\frac{n}{p^\alpha}\right]-\left[\frac{a_1}{p^\alpha}\right]-\left[\frac{a_2}{p^\alpha}\right]-\ldots-\left[\frac{a_k}{p_\alpha}\right]\right).$$

Az I. fejezet 3. feladata szerint itt valamennyi tag nemnegatív, tehát összegük, vagyis p kitevője is nemnegatív. Így az A racionális szám kanonikus alakjában szereplő valamennyi kitevő nemnegatív egész szám, tehát A szükségképpen egész szám.

12. Legyen $x=10^{mk}$, ahol k tetszőleges természetes szám. Felülről fogjuk becsülni azoknak az x-nél nem nagyobb számoknak a számát, melyek számjegyei közt m-nél kevesebb 0 van.

Tekintsünk egy olyan n természetes számot, melyre $1\leqq n\leqq x$ teljesül, és melynek számjegyei közt m-nél kevesebb 0 szerepel (ekkor nyilván $n<x$ is teljesül). Írjuk fel ezt a számot 10-es számrendszerben:

$$n=a_1a_2\overset{10}{\smile}\ldots a_{mk}=a_1 10^{mk-1}+a_2 10^{mk-2}+\ldots+a_{mk-1}10+a_{mk}$$

(ahol most $a_1=a_2=\ldots=0$-t is megengedünk). Írjuk át ezt a számot 10^m alakú számrendszerre:

$$n=b_1b_2\overset{10^m}{\smile}\ldots b_k=b_1(10^m)^{k-1}+b_2(10^m)^{k-2}+\ldots+b_{k-1}10^m+b_k,$$

ahol

$$0\leqq b_i\leqq 10^m-1\quad(i=1,2,\ldots,k). \tag{57}$$

Ekkor nyilván

$$b_1=a_1a_2\overset{10}{\smile}\ldots a_m=a_1 10^{m-1}+a_2 10^{m-2}+\ldots+a_m,$$

$$b_2=a_{m+1}a_{m+2}\overset{10}{\smile}\ldots a_{2m}=a_{m+1}10^{m-1}+a_{m+2}10^{m-2}+\ldots+a_{2m},$$

$$\vdots$$

$$b_k=a_{mk-m+1}a_{mk-m+2}\overset{10}{\smile}\ldots a_{mk}=a_{mk-m+1}10^{m-1}+a_{mk-m+2}10^{m-2}+$$

$$+\ldots+a_{mk}.$$

Minthogy az $a_1, a_2, \ldots, a_{mk}$ számjegyek közt feltevésünk szerint m-nél kevesebb 0 van, szükségképpen $b_1, b_2, \ldots, b_k$ mindegyike különbözik 0-tól. Így az (57) feltétel az

$$1 \leqq b_i \leqq 10^m - 1 \quad (i = 1, 2, \ldots, k)$$

feltétellel pótolható. Az egyes b_i-k tehát csak $10^m - 1$-féleképpen választhatók, és így egy $b_1, b_2, \ldots, b_k$ szám-k-as, vagyis egy mondott tulajdonságú n szám $(10^m - 1)^k$-féleképpen választható. Az x-nél nem nagyobb, m-nél kevesebb 0 számjeggyel rendelkező n számok száma tehát legfeljebb

$$(10^m - 1)^k = \left(\frac{10^m - 1}{10^m}\right)^k \cdot 10^{mk} = \left(1 - \frac{1}{10^m}\right)^k x.$$

Nyilván elég azt igazolni, hogy az x-nél nem nagyobb prímszámok száma, vagyis $\pi(x)$ ennél a számnál nagyobb:

$$(58) \qquad \pi(x) > \left(1 - \frac{1}{10^m}\right)^k x.$$

Azonban (5) szerint

$$\pi(x) > c_2 \frac{x}{\log x} = c_2 \frac{x}{\log 10^{mk}} = c_2 \frac{x}{mk \log 10}.$$

(58) helyett tehát elég bizonyítanunk, hogy

$$c_2 \frac{x}{mk \log 10} > \left(1 - \frac{1}{10^m}\right)^k x,$$

vagyis

$$\left(\frac{1}{1 - \frac{1}{10^m}}\right)^k > \frac{m \log 10}{c_2} k.$$

Ez az egyenlőtlenség azonban — rögzített m mellett — minden elég nagy k természetes számra teljesül (az exponenciális függvény „gyorsabban" tart a végtelenhez, mint a hatványfüggvény).

13. Tetszőleges k természetes számot megadva, Csebisev tétele szerint létezik olyan p prímszám, melyre $10^k < p < 2 \cdot 10^k$; másrészt egy ilyen p prímszám első számjegye nyilván 1-es.

14. Csebisev tétele szerint $n \geqq 4$ esetén létezik olyan p prímszám, melyre

$$\left[\frac{n}{2}\right] < p < 2\left[\frac{n}{2}\right] \leqq n$$

teljesül. Egy ilyen p prímszám kitevője $n!$ kanonikus alakjában nyilván 1, tehát az I. fejezet 16. példája szerint $n!$ nem lehet teljes hatvány. ($n=2, 3$ esetén nyilvánvaló az állítás.)

15. Az állítást n-re vonatkozó teljes indukcióval fogjuk igazolni.

$n=1$ esetén nyilván igaz az állítás.

Most tegyük fel, hogy $1 \leqq n \leqq k-1$ (ahol $k=2, 3, \ldots$) esetén igaz az állítás, vagyis $1 \leqq n \leqq k-1$ esetén n és $n+1$ közül legalább az egyik felírható csupa különböző prímszám összegeként. Azt kell igazolnunk, hogy ebből következik, hogy k és $k+1$ közül legalább az egyik felírható csupa különböző prímszám összegeként.

Csebisev tétele szerint $k \geqq 3$ esetén létezik olyan p prímszám, melyre

$$(59) \qquad \frac{k+1}{2} < p \leqq k+1$$

teljesül (és ilyen p akkor is létezik, ha $k=2$ nevezetesen ekkor $p=3$ választható). Ha $(k+1)-p=0$ vagy 1, akkor készen vagyunk, hiszen ekkor $k+1$, ill. k prímszám, tehát felírható csupa különböző prímszám (egyetlen tagból álló) összegeként. Feltehető tehát, hogy $(k+1)-p \geqq 2$. Ekkor $1 \leqq k-p \leqq \leqq k-2$, tehát az indukciós feltevés szerint $k-p$ és $k-p+1$ közül legalább az egyik felírható csupa különböző prímszám összegeként:

$$(60) \qquad k-p = p_1+p_2+\ldots+p_l$$

vagy

$$(61) \qquad k-p+1 = p_1+p_2+\ldots+p_l,$$

ahol $p_1, p_2, \ldots, p_l$ páronként különböző prímszámok. Innen (59)-re tekintettel következik, hogy $i=1, 2, \ldots, l$ esetén

$$p_i \leqq k+1-p < k+1-\frac{k+1}{2} = \frac{k+1}{2} < p,$$

tehát p különbözik a $p_1, p_2, \ldots, p_l$ prímek mindegyikétől. Így (60)-ból, ill. (61)-ből következik, hogy k vagy $k+1$ felírható csupa különböző prímszám (nevezetesen $p_1, p_2, \ldots, p_l, p$) összegeként.

16. Tetszőleges n természetes számra $\pi(p_n)=n$ és $p_n > n$. Így (4)-be $x=p_n$-et ($n=1, 2, \ldots$) helyettesítve (ekkor $x \geqq 2$ nyilván teljesül):

$$\pi(p_n) = n < c_1 \frac{p_n}{\log p_n},$$

ahonnan

$$p_n > \frac{1}{c_1} n \log p_n > \frac{1}{c_1} n \log n,$$

tehát (6) $c_3 = \dfrac{1}{c_1}$ választással teljesül.

(Megjegyezzük, hogy (7) szintén levezethető viszonylag elemi úton (5)-ből, a bizonyítás azonban valamivel komplikáltabb.)

17. Definiáljuk valamely n-nél nem nagyobb p prímszámra az α_p természetes számot a

$$p^{\alpha_p} \leqq n p^{\alpha_p+1}$$

egyenlőtlenséggel. Ekkor $[1, 2, \ldots, n]$ kanonikus alakja nyilván

$$[1, 2, \ldots, n] = \prod_{p \leqq n} p^{\alpha_p}.$$

Így (8)-at felhasználva:

$$(62) \qquad [1, 2, \ldots, n] = \prod_{p \leqq n} p^{\alpha_p} \geqq \prod_{p \leqq n} p > c_5^n = e^{n \log c_5}.$$

Másrészt (4)-re tekintettel $n \geqq 2$ esetén

$$(63) \qquad [1, 2, \ldots, n] = \prod_{p \leqq n} p^{\alpha_p} \leqq \prod_{p \leqq n} n = n^{\pi(n)} =$$

$$= e^{\log n \cdot \pi(n)} < e^{\log n \cdot c_1 \frac{n}{\log n}} = e^{c_1 n}.$$

(62), ill. (63) szerint $c_{18} = \log c_5$, $c_{19} = c_1$ választással teljesül a bizonyítandó egyenlőtlenség.

18*. Legyen t tetszőleges, 1-nél nagyobb természetes szám, és válasszuk m-et, ill. n-et

$$m = n = P_t = \prod_{i=1}^{t} p_i$$

alakú számnak. Ekkor (9) szerint

$$\nu(m) = \nu(P_t) = t > c_7 \frac{\log P_t}{\log \log P_t} = c_7 \frac{\log m}{\log \log m}$$

és

$$d(n) = d(P_t) = 2^t = e^{t \log 2} > e^{c_7 \log 2 \frac{\log P_n}{\log \log P_n}} =$$

$$= e^{c_{21} \frac{\log n}{\log \log n}}$$

(ahol $c_{21} = c_7 \log 2$).

19*. A $\sum \frac{1}{a_k}$ összeget nyilván növeljük (vagy legalábbis nem csökkentjük), ha az összegezést kiterjesztjük az összes olyan természetes számra, mely nem osztható 3-nál nagyobb prímszámmal, vagyis amely $2^i 3^j$ alakú

(ahol $i=0, 1, 2, \ldots$; $j=0, 1, 2, \ldots$). Így

$$\sum_k \frac{1}{a_k} \leqq \sum_{i=0}^{+\infty} \sum_{j=0}^{+\infty} \frac{1}{2^i 3^j}.$$

Ezt a (pozitív tagokból álló) végtelen sort felfoghatjuk két (ugyancsak pozitív tagú) végtelen sor szorzataként, majd alkalmazhatjuk a végtelen mértani sor összegképletét:

$$\sum_k \frac{1}{a_k} \leqq \left(\sum_{i=0}^{+\infty} \frac{1}{2^i}\right)\left(\sum_{j=0}^{+\infty} \frac{1}{3^j}\right) = \frac{1}{1-\frac{1}{2}} \cdot \frac{1}{1-\frac{1}{3}} = 2 \cdot \frac{3}{2} = 2.$$

20*. Jelöljük az n-nél nem nagyobb prímszámokat $p_1, p_2, \ldots, p_k$-val. Ekkor a végtelen mértani sor összegképletét alkalmazva (és figyelembe véve, hogy a szereplő végtelen sorok pozitív tagúak):

$$\prod_{p \leqq n} \frac{1}{1-\frac{1}{p}} = \frac{1}{1-\frac{1}{p_1}} \cdot \frac{1}{1-\frac{1}{p_2}} \cdot \ldots \cdot \frac{1}{1-\frac{1}{p_k}} =$$

$$= \left(1+\frac{1}{p_1}+\frac{1}{p_1^2}+\ldots+\frac{1}{p_1^{i_1}}+\ldots\right)\left(1+\frac{1}{p_2}+\frac{1}{p_2^2}+\ldots+\frac{1}{p_2^{i_2}}+\ldots\right)\ldots$$

$$\ldots\left(1+\frac{1}{p_k}+\frac{1}{p_k^2}+\ldots+\frac{1}{p_k^{i_k}}+\ldots\right) =$$

$$= \sum_{0 \leqq i_1,\, 0 \leqq i_2,\, \ldots,\, 0 \leqq i_k} \frac{1}{p_1^{i_1} p_2^{i_2} \ldots p_k^{i_k}}.$$

A számelmélet alaptételéből következik, hogy az $1, 2, \ldots, n$ számok mindegyike felírható a $p_1, p_2, \ldots, p_k$ prímek hatványainak szorzataként, vagyis $p_1^{i_1} p_2^{i_2} \ldots p_k^{i_k}$ $(0 \leqq i_1, 0 \leqq i_2, \ldots, 0 \leqq i_k)$ alakban. Így a kapott végtelen sor tagjai közt szükségképpen szerepel $1, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{n}$. Ezeken kívül szerepelnek bizonyos további pozitív tagok nevezetesen bizonyos n-nél nagyobb számok (a $p_1, p_2, \ldots, p_k$ prímek hatványainak szorzataként felírható szá-

mok) reciprokai. Csökkentünk, ha ez utóbbi pozitív tagokat elhagyjuk:

$$\prod_{p\leqq n}\frac{1}{1-\frac{1}{p}}=\sum_{0\leqq i_1,\,0\leqq i_2,\,\ldots,\,0\leqq i_k}\frac{1}{p_1^{i_1}p_2^{i_2}\ldots p_k^{i_k}}>$$

$$>1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{n},$$

és ezzel az állítást igazoltuk.

21*. Tegyük fel indirekte, hogy csak véges sok prímszám létezik, és legyenek ezek $p_1, p_2, \ldots, p_k$, ahol $p_1<p_2<\ldots<p_k$. Ekkor $n\geqq p_k$ esetén

$$\prod_{p\leqq n}\frac{1}{1-\frac{1}{p}}=\prod_{i=1}^{k}\frac{1}{1-\frac{1}{p_i}},$$

ami n-től független állandó.

Ugyanakkor mint az analízis elemeiből ismeretes, a (42) jobb oldalán álló összeg (az ún. *harmonikus sor* részletösszege) végtelenhez tart, ha n tart a végtelenhez. Így (42) elég nagy n-re nem teljesülhet, tehát az indirekt feltevésből ellentmondásra jutottunk.

22*. (44) szerint tetszőleges p prímre

$$\frac{1}{1-\frac{1}{p}}<\frac{1}{e^{-\frac{1}{p}-\frac{1}{p^2}}}=e^{\frac{1}{p}+\frac{1}{p^2}}.$$

Így (42) és (43) alapján

$$\log n<\sum_{i=1}^{n}\frac{1}{i}<\prod_{p\leqq n}\frac{1}{1-\frac{1}{p}}<\prod_{p\leqq n}e^{\frac{1}{p}+\frac{1}{p^2}}=$$

$$=e^{\sum\limits_{p\leqq n}\left(\frac{1}{p}+\frac{1}{p^2}\right)}.$$

Mivel a logaritmus függvény monoton, innen következik, hogy

$$\log\log n<\sum_{p\leqq n}\left(\frac{1}{p}+\frac{1}{p^2}\right)=\sum_{p\leqq n}\frac{1}{p}+\sum_{p\leqq n}\frac{1}{p^2}\leqq \tag{64}$$

$$\leqq\sum_{p\leqq n}\frac{1}{p}+\sum_{k=2}^{n}\frac{1}{k^2}.$$

JATE Méra Ferenc Kollégium
KÖNYVTÁRA

Azonban

$$\sum_{k=2}^{n} \frac{1}{k^2} < \sum_{k=2}^{n} \frac{1}{(k-1)k} = \sum_{k=2}^{n} \left(\frac{1}{k-1} - \frac{1}{k}\right) =$$

$$= \left(\frac{1}{1} - \frac{1}{2}\right) + \left(\frac{1}{2} - \frac{1}{3}\right) + \left(\frac{1}{3} - \frac{1}{4}\right) + \ldots + \left(\frac{1}{n-2} - \frac{1}{n-1}\right) +$$

$$+ \left(\frac{1}{n-1} - \frac{1}{n}\right) = 1 - \frac{1}{n} < 1,$$

tehát (64)-ből

$$\sum_{p \leqq n} \frac{1}{p} > \log\log n - \sum_{k=2}^{n} \frac{1}{k^2} > \log\log n - 1.$$

(Megjegyezzük, hogy

$$\sum_{p \leqq n} \frac{1}{p} < \log\log n + c_{27}$$

bizonyítása — bár még mindig elemi úton történhet — lényegesen nehezebb.)

23*. Tegyük fel indirekte, hogy valamely $\varepsilon > 0$ számhoz található olyan i_0 szám, hogy $i \geqq i_0$ esetén

$$p_{i+1} > (1+\varepsilon) p_i \quad (i \geqq i_0).$$

Innen indukcióval nyilvánvalóan következik, hogy tetszőleges k természetes számra

$$p_{i_0+k} > (1+\varepsilon)^k p_{i_0}.$$

Így tetszőleges m természetes számra (a végtelen mértani sor összegképletét alkalmazva)

$$\sum_{i=1}^{i_0+m} \frac{1}{p_i} = \sum_{i=1}^{i_0-1} \frac{1}{p_i} + \sum_{k=0}^{m} \frac{1}{p_{i_0}+k} <$$

$$< \sum_{i=1}^{i_0-1} \frac{1}{p_i} + \sum_{k=0}^{m} \frac{1}{(1+\varepsilon)^k p_{i_0}} < \sum_{i=1}^{i_0-1} \frac{1}{p_i} + \sum_{k=0}^{+\infty} \frac{1}{(1+\varepsilon)^k p_{i_0}} =$$

$$= \sum_{i=1}^{i_0-1} \frac{1}{p_i} + \frac{1}{p_{i_0}} \cdot \frac{1}{1 - \frac{1}{1+\varepsilon}} = \sum_{i=1}^{i_0-1} \frac{1}{p_i} + \frac{1}{p_{i_0}} \left(\frac{1}{\varepsilon} + 1\right).$$

Ebből következnék, hogy n-nel tartva a végtelenhez, a $\sum_{p \leqq n} \frac{1}{p}$ összeg korlátos maradna, ami ellentmond (45)-nek.

24*. *a.* A III. fejezet 31. *a.* feladatából az

$$(65)\qquad |a+b| \leqq |a|+|b|$$

egyenlőtlenség alapján következik, hogy

$$(66)\qquad \left|\sum_{i=1}^{n} \nu(i) - n \sum_{p\leqq n} \frac{1}{p}\right| = \left|\sum_{p\leqq n}\left[\frac{n}{p}\right] - \sum_{p\leqq n}\frac{n}{p}\right| =$$

$$= \left|\sum_{p=n}\left(\left[\frac{n}{p}\right]-\frac{n}{p}\right)\right| \leqq \sum_{p\leqq n}\left|\left[\frac{n}{p}\right]-\frac{n}{p}\right| \leqq \sum_{p\leqq n} 1 = \pi(n) < n.$$

Másrészt (11)-ből következik, hogy létezik olyan c_{28} állandó, hogy $n\geqq 2$ esetén

$$(67)\qquad \left|n \sum_{p\leqq n}\frac{1}{p} - n\log\log n\right| = n\left|\sum_{p\leqq n}\frac{1}{p} - \log\log n\right| < c_{28}n.$$

(66)-ból és (67)-ből (65) alapján következik, hogy $n\geqq 2$ esetén

$$\left|\sum_{i=1}^{n} \nu(i) - n\log\log n\right| =$$

$$= \left|\left(\sum_{i=1}^{n}\nu(i) - n\sum_{p\leqq n}\frac{1}{p}\right) + \left(n\sum_{p\leqq n}\frac{1}{p} - n\log\log n\right)\right| \leqq$$

$$\leqq \left|\sum_{i=1}^{n}\nu(i) - n\sum_{p\leqq n}\frac{1}{p}\right| + \left|n\sum_{p\leqq n}\frac{1}{p} - n\log\log n\right| <$$

$$< n + c_{28}n = (1+c_{28})n,$$

tehát a bizonyítandó állítás teljesül $c_{23}=1+c_{28}$ választással.

b. (65)-re tekintettel (a végtelen mértani sor összegképletét alkalmazva):

$$\left|\sum_{p^\alpha\leqq n}\frac{1}{p^\alpha} - \sum_{p\leqq n}\frac{1}{p}\right| = \sum_{\substack{p^\alpha\leqq n\\ \alpha\geqq 2}}\frac{1}{p^\alpha} < \sum_{p\leqq n}\sum_{\alpha=2}^{+\infty}\frac{1}{p^\alpha} =$$

$$= \sum_{p\leqq n}\frac{1}{p^2}\sum_{i=0}^{+\infty}\frac{1}{p_i} = \sum_{p\leqq n}\frac{1}{p^2}\cdot\frac{1}{1-\frac{1}{p}} = \sum_{p\leqq n}\frac{1}{p(p-1)} \leqq$$

$$\leqq \sum_{k=2}^{n}\frac{1}{k(k-1)} = \sum_{k=2}^{n}\left(\frac{1}{k-1}-\frac{1}{k}\right) = 1-\frac{1}{n} < 1.$$

Ezt az összefüggést és (67)-et felhasználva, a III .fejezet 31. *b.* feladatából kiindulva ugyanúgy okoskodhatunk, mint az *a.* állítás bizonyítása során.

25*. Legyen t tetszőleges, 1-nél nagyobb természetes szám, és válasszuk k-t, ill. l-et

$$k = l = P_t = \prod_{i=1}^{t} p_i$$

alakú számnak (ahol p_i az i-edik prímszámot jelöli).

(12)-ből következik, hogy létezik olyan c_{29} állandó, hogy $n \geqq 2$ esetén

$$\prod_{p \leqq n} \left(1 - \frac{1}{p}\right) < \frac{c_{29}}{\log n} \quad (n \geqq 2). \tag{68}$$

Felhasználva (68)-at és (9)-et, nyerjük, hogy létezik olyan k_0 szám, hogy $k > k_0$ esetén

$$\varphi(k) = \varphi(P_t) = P_t \prod_{i=1}^{t} \left(1 - \frac{1}{p_i}\right) = k \prod_{p \leqq p_t} \left(1 - \frac{1}{p}\right) <$$

$$< k \frac{c_{29}}{\log p_t} < \frac{c_{29} k}{\log t} < \frac{c_{29} k}{\log\left(c_7 \dfrac{\log P_t}{\log\log P_t}\right)} =$$

$$= \frac{c_{29} k}{\log\log k - \log\log\log k + \log c_7} >$$

$$> \frac{c_{29} k}{\log\log k - \dfrac{1}{2}\log\log k} = \frac{2 c_{29} k}{\log\log k},$$

tehát (46) teljesül $c_{25} = 2c_{29}$-cel.

Továbbá a III. fejezet (47) képletét és (46)-ot felhasználva:

$$\sigma(l) > \frac{1}{2}\frac{l^2}{\varphi(l)} = \frac{1}{2}\frac{k^2}{\varphi(k)} > \frac{1}{2} \cdot \frac{k^2}{c_{25}\dfrac{k}{\log\log k}} =$$

$$= \frac{1}{2c_{25}} k \log\log k = \frac{1}{2c_{25}} l \log\log l,$$

tehát (47) teljesül $c_{26} = \dfrac{1}{2c_{25}}$-tel.

26. Ha $2^n - 1$ prímszám, akkor az I. fejezet 58. feladata szerint n is prímszám, ha pedig $2^n + 1$ prímszám, akkor az I. fejezet 59. feladata szerint n 2^k alakú. $n > 2$ esetén azonban n nem lehet egyidejűleg prímszám és 2^k alakú.

27. Mivel $(15,7)=1$, Dirichlet tétele szerint végtelen sok $15k+7$ alakú prímszám létezik. Az ilyen alakú prímszámok azonban $k>1$ esetén nem tagjai ikerprímszámpárnak, hiszen $(15k+7)-2=15k+5$ osztható 5-tel és $k>1$ miatt 5-nél nagyobb, tehát összetett szám, hasonlóan $(15k+7)+2=$ $=15k+9$ osztható 3-mal és $k>1$ miatt 3-nál nagyobb, tehát szintén összetett szám.

28. A 2-től és 3-tól különböző prímszámok nyilván $6k-1$ vagy $6k+1$ alakúak. Így egy (a 3, 5 pártól különböző) ikerprímszámpár kisebbik tagja szükségképpen $6k-1$, a nagyobbik $6k+1$ alakú (ugyanazon k-val).

$6k-1$ (ahol $k\geqq 1$) akkor és csak akkor prímszám, ha nem írható fel $6k-1=ab$ alakban, ahol a, b 1-nél nagyobb természetes számok. Ha ilyen a, b létezik, akkor itt szükségképpen a és b is relatív prímek 6-hoz, tehát $6u+1$ vagy $6v-1$ alakú számok. Továbbá nem lehet mindkettő $6u+1$ vagy mindkettő $6v-1$ alakú, mert akkor szorzatuk $ab=6k+1$ lenne. Így szükségképpen a, b egyike, mondjuk a $6u+1$ alakú, a másik $6v-1$ alakú. Továbbá $a=6u+1>1$ és $b=6v-1>1$ akkor és csak akkor teljesül, ha u, v *pozitív* egész számok. Végeredményben tehát $6k-1$ akkor és csak akkor prímszám, ha nem léteznek olyan u, v természetes számok, melyekre

$$6k-1 = (6u+1)(6v-1) = 36uv-6u+6v-1 = 6(6uv-u+v)-1,$$

vagyis

$$k = 6uv-u+v. \tag{69}$$

Hasonlóan látható, hogy $6k+1$ akkor és csak akkor prímszám, ha nem léteznek olyan u, v természetes számok, melyekre

$$6k+1 = (6u+1)(6v+1) = 36uv+6u+6v+1 = 6(6uv+u+v)+1,$$

vagyis

$$k = 6uv+u+v, \tag{70}$$

ill. melyekre

$$6k+1 = (6u-1)(6v-1) = 36uv-6u-6v+1 = 6(6uv-u-v)+1,$$

vagyis

$$k = 6uv-u-v. \tag{71}$$

(69)-ben u-t és v-t felcserélve, a

$$k = 6uv+u-v \tag{72}$$

alakot nyerjük; k tehát nyilván akkor és csak akkor írható fel a (72) alakban, ha felírható a (69) alakban is.

Végeredményben igazoltuk, hogy $6k-1$ és $6k+1$ akkor és csak akkor ikerprímszámok, ha k nem írható fel a (69), (70), (71), (72) alakok egyikében sem, és ezzel a feladat állítását igazoltuk.

29. Ha n páros, akkor $n=4+(n-4)$, ha n páratlan, akkor $n=9+(n-9)$ a kívánt típusú előállítás; $n>11$-re tekintettel ugyanis ekkor $n-4$, ill. $n-9$ 2-nél nagyobb páros szám, tehát összetett szám.

30. Ilyenek például a $30k+27$ alakú számok (ahol $k=0, 1, 2, \ldots$). Ezek ugyanis nem prímszámok (vagyis nem írhatók fel prímszámoknak egyetlen tagból álló összegeként), hiszen oszthatók 3-mal és 3-nál nagyobbak. Ha viszont egy ilyen alakú számot felírunk két természetes szám összegeként, akkor szükségképpen ezek egyike páros szám, a másik páratlan szám. Ha a páros tag prímszám, akkor csak 2 lehet; ekkor azonban a másik tag, $(30k+27)-2=30k+25$ osztható 5-tel és 5-nél nagyobb, tehát összetett szám. Így egy ilyen alakú szám nem írható fel két prímszám összegeként sem.

31. $n=1, 3, 7$ esetén rendre $x=2, 4, 8$ megoldás. $n>7$ esetén pedig feltevésünk szerint léteznek olyan p, q egymástól különböző prímszámok, melyekre $p+q=n-1$. Ekkor $x=pq$ megoldása a vizsgált egyenletnek:

$$\sigma(pq)-pq = (p+1)(q+1)-pq = p+q+1 = n.$$

32. Állítjuk, hogy a $(3k+2)^2$ alakú számok (ahol $k=1, 2, \ldots$) nem írhatók fel n^2+p alakban. Tegyük fel ugyanis indirekte, hogy valamely n természetes számra és p prímszámra

$$(3k+2)^2 = n^2+p,$$

vagyis

$$p = (3k+2)^2-n^2 = (3k+2-n)(3k+2+n).$$

Valamely p prímszámot felírva két természetes szám szorzataként (minthogy a második tényező pozitív, az elsőnek is pozitívnak kell lennie), szükségképpen a kisebbik tényező 1, a nagyobbik p:

$$3k+2-n = 1, \tag{73}$$

$$3k+2+n = p. \tag{74}$$

(73)-ból

$$n = 3k+1.$$

(74)-be helyettesítve:

$$p = (3k+2)+n = (3k+2)+(3k+1) = 6k+3 = 3(2k+1).$$

A p prímszám tehát felírható lenne két, 1-nél nagyobb természetes szám szorzataként, vagyis az indirekt feltevésből ellentmondásra jutottunk.

33. Tekintsük a $k!+1, 2\cdot k!+1, \ldots, k\cdot k!+1$ számtani sorozatot. Állítjuk, hogy e sorozat elemei páronként relatív prímek. Tegyük fel indirekte, hogy a sorozat két elemének, mondjuk $i\cdot k!+1$-nek és $j\cdot k!+1$-nek (ahol $1\leqq i<j\leqq k$) a legnagyobb közös osztója nagyobb 1-nél. Ekkor létezik

olyan p prímszám, mely osztója e két elemnek. Egy ilyen p prímre szükségképpen

$$p|(j\cdot k!+1)-(i\cdot k!+1) = (j-i)k!$$

Innen nyilván következik, hogy $p \leqq k$. Másrészt $ik!+1$ egy k-nál nem nagyobb prímszámmal osztva, nyilván 1 maradékot ad, tehát $i\cdot k!+1$ prímosztói k-nál nagyobbak. Így $p|i\cdot k!+1$-ből $p>k$ következik, tehát az indirekt feltevésből ellentmondásra jutottunk.

34. Tegyük fel indirekte, hogy csak véges sok $6k-1$ alakú prímszám létezik; legyenek ezek $p_1, p_2, \ldots, p_r$. Képezzük az

$$(75) \qquad n = 6p_1p_2 \ldots p_r - 1$$

számot. Minthogy n 1-nél nagyobb ($p_1=5$ $6k-1$ alakú prímszám, tehát $n \geqq 6\cdot 5-1=29$), a számelmélet alaptétele szerint felírható prímszámok szorzataként: $n=q_1q_2\ldots q_s$. Az n szám nyilván nem osztható a 2, 3, p_1, $p_2, \ldots, p_r$ prímek egyikével sem, így — tekintettel az indirekt feltevésre — $q_1, q_2, \ldots, q_s$ mindegyike $6k+1$ alakú. Azonban $6k+1$ alakú számok szorzata is ilyen alakú:

$$(6k+1)(61+1) = 6(6kl+k+l)+1.$$

Így szükségképpen a $q_1, q_2, \ldots, q_s$ prímek szorzata, n is $6k+1$ alakú. Azonban (75) szerint n nyilván $6k-1$ alakú, tehát az indirekt feltevésből ellentmondásra jutottunk.

35. Tegyük fel indirekte, hogy csak véges sok $6k+1$ alakú prímszám létezik; legyenek ezek $p_1, p_2, \ldots, p_r$. Képezzük az

$$n = 12(p_1p_2 \ldots p_r)^2+1$$

számot. Ez 1-nél nagyobb szám ($p_1=7$ $6k+1$ alakú prímszám), tehát felírható prímszámok szorzataként: $n=q_1q_2\ldots q_s$. A II. fejezet 96*. feladata szerint a $q_1, q_2, \ldots, q_s$ prímek $6k+1$ alakúak. Másrészt n nyilván nem osztható a $p_1, p_2, \ldots, p_r$ prímszámok egyikével sem, tehát a $q_1, q_2, \ldots, q_s$ prímosztók $p_1, p_2, \ldots, p_r$-től különböző $6k+1$ alakú prímszámok. Így az indirekt feltevésből ellentmondásra jutottunk.

36. Tegyük fel indirekte, hogy csak véges sok $8k-1$ alakú prímszám létezik; legyenek ezek $p_1, p_2, \ldots, p_r$. Képezzük az

$$(76) \qquad n = 8(p_1p_2 \ldots p_r)^2-1$$

számot. Minthogy $n>1$, n felírható prímszámok szorzataként: $n=q_1q_2\ldots q_s$. A II. fejezet 95*. feladata szerint a $q_1, q_2, \ldots, q_s$ prímek $8k\pm1$ alakúak. Mivel n nem osztható $p_1, p_2, \ldots, p_r$ egyikével sem, a $q_1, q_2, \ldots, q_s$ prímek különböznek a $p_1, p_2, \ldots, p_r$ prímektől, tehát indirekt feltevésünk szerint csak $8k+1$ alakúak lehetnek. Azonban $8k+1$ alakú számok szorzata is $8k+1$ alakú:

$$(8k+1)(8l+1) = 8(8kl+k+l)+1.$$

Így $q_1, q_2, \ldots, q_s$ szorzata, n is $8k+1$ alakú, ami ellentmond (76)-nak.

37*. Legyen

$$f(x) = \frac{x^p - 1}{x - 1}.$$

Tegyük fel indirekte, hogy csak véges sok $pk+1$ alakú prímszám létezik; legyenek ezek $p_1, p_2, \ldots, p_r$. Képezzük az

$$n = f(pp_1p_2 \ldots p_r) = \frac{(pp_1p_2 \ldots p_r)^p - 1}{pp_1p_2 \ldots p_r - 1} = 1 + pp_1p_2 \ldots p_r +$$

$$+ (pp_1p_2 \ldots p_r)^2 + \ldots + (pp_1p_2 \ldots p_r)^{p-1}$$

számot. Nyilván

$$n \geqq 1 + pp_1p_2 \ldots p_r \geqq 1 + p > 1,$$

tehát n felírható prímszámok szorzataként: $n = q_1q_2 \ldots q_s$. Minthogy n nem osztható $p, p_1, p_2, \ldots, p_r$ egyikével sem (ugyanis n-et e prímekkel osztva, 1 maradékot kapunk), a $q_1, q_2, \ldots, q_s$ prímosztók szükségképpen különböznek a $p, p_1, p_2, \ldots, p_r$ prímektől. Legyen továbbá $a = pp_1p_2 \ldots p_r$. Ekkor

$$n = \frac{a^p - 1}{a - 1}.$$

Innen látható, hogy az n szám $q_1, q_2, \ldots, q_s$ prímosztói $a^p - 1$ prímosztói közül kerülnek ki. Így a II. fejezet 61*. feladata szerint a $q_1, q_2, \ldots, q_s$ prímek vagy $pk+1$ alakúak, vagy pedig osztói $a-1$-nek, azaz

$$(77) \qquad a - 1 \equiv 0 \pmod{q_i}$$

teljesül. Ez utóbbi eset azonban nem lehetséges (egyetlen i-re sem). A $q_1, q_2, \ldots, q_s$ prímek definíciója szerint ugyanis

$$(78) \qquad n = \frac{a^p - 1}{a - 1} \equiv 0 \pmod{q_i} \quad (i = 1, 2, \ldots, s).$$

Másrészt (77)-ből következnék, hogy

$$(79) \qquad \frac{a^p - 1}{a - 1} = 1 + a + a^2 + \ldots + a^{p-1} \equiv 1 + 1 + 1 + \ldots + 1 = p \pmod{q_i}.$$

(78)-at és (79)-et egybevetve, nyerjük, hogy

$$p \equiv 0 \pmod{q_i}.$$

Minthogy p, q_i prímszámok, innen $p = q_i$ következnék; azonban láttuk, hogy a q_i prímek mindegyike különbözik p-től. Így a (77) eset nem fordulhat elő, tehát a $q_1, q_2, \ldots, q_s$ prímek mindegyikének $pk+1$ alakúnak

kellene lennie. Végeredményben a $q_1, q_2, \ldots, q_s$ tényezőknek olyan $pk+1$ alakú prímszámoknak kellene lenniük, melyek különböznek $p_1, p_2, \ldots, p_r$-től, ami ellentmond indirekt feltevésünknek.

38. Elég megmutatni, hogy rögzítve bizonyos $p_1, p_2, \ldots, p_r$ (ahol $r \geqq 0$) $2^\alpha k+1$ alakú prímszámokat, található legalább egy további ilyen alakú prímszám. Ehhez viszonyt elég megmutatni, hogy *tetszőleges* β természetes számhoz található $2^\beta l+1$ alakú p prímszám (ahol l természetes szám). Ha ugyanis β-t olyan nagynak választjuk, hogy 2^β nagyobb legyen, mint $p_1, p_2, \ldots, p_r$ mindegyike ($r=0$ esetén — vagyis amikor legalább egy $2^\alpha k+1$ alakú prímszám létezését akarjuk igazolni — $\beta=\alpha$ választható), akkor $p=2^\beta l+1>2^\beta$, tehát p nagyobb $p_1, p_2, \ldots, p_r$ mindegyikénél (és így különbözik ezektől), másrészt nyilván $\beta \geqq \alpha$, tehát $p=2^\beta l+1=$ $=2^\alpha(2^{\beta-\alpha}l)+1$ szintén $2^\alpha k+1$ alakú.

Azonban a II. fejezet 62*. feladata szerint a $2^{2^\beta}+1$ szám (mely 1-nél nagyobb) minden prímosztója $2^{\beta+1}k+1=2^\beta(2k)+1=2^\beta l+1$ alakú, tehát e szám bármely prímosztója választható p gyanánt.

39. n-re vonatkozó teljes indukcióval fogunk bizonyítani. $n=1$ esetén az állítás Dirichlet tétele szerint igaz. Tegyük fel most, hogy az állítás valamely n természetes számra igaz; ekkor tehát létezik olyan k_0 természetes szám, hogy ak_0+b $q_1q_2\ldots q_n$ alakban írható, ahol $q_1, q_2, \ldots, q_n$ különböző prímszámok. Dirichlet tételéből következik, hogy létezik olyan l természetes szám, melyre $al+1=q$ prímszám, amely $q_1, q_2, \ldots, q_n$ mindegyikénél nagyobb (sőt végtelen sok ilyen l létezik). Legyen egy ilyen l-re

$$k = (ak_0+a)l+k_0.$$

Ekkor

$$ak+b = a((ak_0+b)l+k_0)+b = (ak_0+b)(al+1) = q_1q_2\ldots q_nq,$$

és ezzel az állítást igazoltuk.

40. 10^k és 10^k-1 — mivel szomszédos számok — relatív prímek. Így Dirichlet tétele szerint végtelen sok $10^kl+(10^k-1)$ alakú prímszám létezik. Az ilyen alakú számok utolsó k számjegye azonban 9-es, tehát számjegyeik összege legalább $k\cdot 9>k$.

41. Válasszuk n-et $n=2^k$ alakú számnak, ahol $k=1, 2, \ldots$. Ekkor

$$d(n^a) = d(2^{ak}) = ak+1.$$

Minthogy $(a, 1)=1$, Dirichlet tétele szerint végtelen sok ilyen alakú prímszám létezik.

42. Minthogy $(a, -1)=1$, Dirichlet tétele szerint végtelen sok olyan p prímszám létezik, mely $p=ak-1$ alakú. Ha n ilyen alakú prímszám, akkor

$$\sigma(n) = \sigma(p) = p+1 = (ak-1)+1 = ak$$

osztható a-val.

43. Mivel a páratlan, $(a, 2)=1$. Így Dirichlet tétele szerint létezik végtelen sok olyan p prímszám, mely $p=ak+2$ alakú. Ha n ilyen alakú prím-

szám, akkor

$$\varphi(n) = \varphi(p) = p-1 = ak+1.$$

Ha egy ilyen n-re d közös osztója a-nak és $\varphi(n)$-nek, akkor d osztója e két szám lineáris kombinációinak is:

$$d|\varphi(n)-k\cdot a = (ak+1)-ak = 1.$$

Így csak $d=\pm 1$ lehetséges, tehát $(a, \varphi(n))=1$.

44. Legyen q tetszőleges prímszám, melyre

(80) $\quad q \geqq k+2.$

Legyen

$$a = 2\cdot 3\cdot \ldots \cdot (q-2)(q-1)(q+1)(q+2)\ldots(2q-2).$$

Ekkor nyilván $(a, q)=1$, tehát Dirichlet tétele szerint létezik végtelen sok $p=al+q$ alakú prímszám, ahol l természetes szám. Állítjuk, hogy egy ilyen alakú prímszám a kívánt tulajdonságú, vagyis $1\leqq i\leqq k$, $1\leqq j\leqq k$ esetén a $p-i$, $p+j$ számok összetettek.

Valóban, $1\leqq i\leqq k$ esetén

$$p-i = (al+q)-i =$$

$$= 2\cdot 3\cdot \ldots \cdot (q-i)\cdot \ldots \cdot (q-1)(q+1)\ldots(2q-2)l+(q-i) =$$

$$=(q-i)(2\cdot 3\cdot \ldots \cdot (q-i-l)(q-i+l)\ldots(q-1)(q+1)\ldots(2q-2)l+1),$$

tehát $q-i$ osztója $p-i$-nek. Továbbá (80)-ra tekintettel

$$q-i \geqq q-k \geqq 2$$

és

$$q-i < (al+q)-i = p-i,$$

tehát $q-i$ 1-nél nagyobb és $(p-i)$-nél kisebb osztója $(p-i)$-nek, tehát $p-i$ összetett szám.

Hasonlóan látható, hogy $1\leqq j\leqq k$ esetén $q+j$ 1-nél nagyobb és $(p+j)$-nél kisebb osztója $(p+j)$-nek, tehát $p+j$ is összetett szám.

45*. Jelöljük az i-edik prímszámot p_i-vel (tehát $p_1=2, p_2=3, \ldots$), és definiáljuk r-ret a

$$p_r \leqq k < p_{r+1}$$

egyenlőtlenséggel. Tekintsük az

$$x \equiv 1 \pmod 8,$$

$$x \equiv 1 \pmod{p_2},$$

$$\vdots$$

$$x \equiv 1 \pmod{p_r}$$

lineáris kongruencia-rendszert. Minthogy a modulusok páronként relatív prímek, ennek a kongruencia-rendszernek az összes megoldásai

$$x \equiv 1 \pmod{8p_2 \dots p_r},$$

vagyis

$$(81) \qquad x = 8p_2 \dots p_r l + 1$$

alakúak. Mivel $(8p_2 \dots p_r, 1) = 1$, Dirichlet tétele szerint végtelen sok ilyen alakú p prímszám létezik.

Legyen most a tetszőleges természetes szám, melyre $1 \leqq a \leqq k$, és írjuk a-t

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

alakban, ahol $\alpha_1, \alpha_2, \dots, \alpha_r$ nemnegatív egész számok. (Mivel $a \leqq k$, a prímosztói nyilván a $p_1, p_2, \dots, p_k$ prímek közül kerülnek ki, tehát a felírható ilyen alakban.) Ekkor az $\left(\frac{a}{p}\right)$ Legendre-szimbólum értéke (ahol p egy (81) alakú, vagyis a fenti kongruencia-rendszert kielégítő prímszám) a következőképpen számítható ki:

$$(82) \qquad \left(\frac{a}{p}\right) = \left(\frac{p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}}{p}\right) = \left(\frac{p_1}{p}\right)^{\alpha_1} \left(\frac{p_2}{p}\right)^{\alpha_2} \dots \left(\frac{p_r}{p}\right)^{\alpha_r}.$$

A p prím $8t+1$ alakú, tehát

$$\left(\frac{p_1}{p}\right) = \left(\frac{2}{p}\right) = +1,$$

továbbá a kvadratikus reciprocitási tételt felhasználva, $2 \leqq i \leqq r$ esetén

$$\left(\frac{p_i}{p}\right) = (-1)^{\frac{p_i - 1}{2} \cdot \frac{p-1}{2}} \left(\frac{p}{p_i}\right) = \left(\frac{1}{p_i}\right) = 1$$

(hiszen $\frac{p-1}{2} = \frac{(8t+1)-1}{2} = 4t$ páros szám). Így a (82)-ben szereplő valamennyi tényező értéke $+1$, tehát, ha p a mondott alakú prímszám, akkor minden, az $1 \leqq a \leqq k$ feltételt kielégítő a természetes számra

$$\left(\frac{a}{p}\right) = +1.$$

V. DIOFANTIKUS EGYENLETEK

1. A DIOFANTIKUS EGYENLETEKRŐL ÁLTALÁBAN

Diofantikus egyenleten olyan egyenletet értünk, melynek *egész* (bizonyos esetekben *pozitív egész*, néha *racionális*) megoldásait keressük. Ebben a fejezetben csak olyan

$$(1) \quad f(x_1, x_2, \ldots, x_k) = 0$$

alakú — vagy ilyen alakra hozható — diofantikus egyenletekkel fogunk foglalkozni, melyekben az $f(x_1, x_2, \ldots, x_k)$ függvény *egész együtthatós* (k változós) *polinom*.

Természetesen például

$$f(x_1, \ldots, x_k) = g(x_1, \ldots, x_k)$$

alakú egyenletek — ahol mindkét oldalon egész együtthatós polinomok állnak — a fenti alakra hozhatók. Egész együtthatós racionális törtfüggvényeket tartalmazó egyenletek szintén a fenti alakra hozhatók.

Az I. fejezetben már foglalkoztunk a *lineáris diofantikus egyenletekkel;* ezért itt csak *magasabb fokú* (valamely ismeretlennek 1-nél nagyobb kitevőjű hatványát vagy két ismeretlen szorzatát tartalmazó) diofantikus egyenletekkel fogunk foglalkozni.

Egy diofantikus egyenlet vizsgálata során optimális célunk természetesen az *összes megoldás* meghatározása. Bizonyos esetekben azonban be kell érnünk a *megoldásszám* meghatározásával, vagy éppen annak megállapításával, hogy létezik-e *végtelen sok* megoldás vagy sem? Gyakran előfordul, hogy az (1) diofantikus egyenletet bizonyos $x_1 = a_1, \ldots, x_n = a_n$ szám-n-esek — rendszerint azok, melyek egy vagy több eleme 0 — nyilvánvalóan kielégítik. Ilyenkor ezeket a megoldásokat *triviális meg-*

oldásoknak nevezzük, és csupán a többi megoldásnak, az ún. *nemtriviális megoldásoknak* a meghatározása jelent problémát.

Legyen az (1) diofantikus egyenlet bal oldalán álló $f(x_1, \ldots, x_k)$ polinom egyes tagjaiban a változók kitevőinek összege állandó (tehát egy tagot $ax_1^{i_1}x_2^{i_2}\ldots x_k^{i_k}$-val jelölve, az $i_1+i_2+\ldots+i_k$ összeg legyen minden tagban ugyanannyi). Ekkor mind az $f(x_1, \ldots, x_k)$ polinomot, mind az (1) egyenletet *homogénnak* mondjuk. Könnyen látható, hogy ha az (1) egyenlet homogén, és $x_1=a_1, \ldots, x_k=a_k$ megoldása az egyenletnek, akkor $x_1=$ $=t\frac{a_1}{(a_1, \ldots, a_k)}, \ldots, x_k=t\frac{a_k}{(a_1, \ldots, a_k)}$ (ahol t tetszőleges egész szám) is megoldása (1)-nek. Így homogén diofantikus egyenletek összes megoldásainak meghatározása nyilván az $(x_1, x_2, \ldots, \ldots, x_n)=1$ feltételt kielégítő megoldások — az ún. *alapmegoldások* vagy *primitív megoldások* — meghatározására redukálható.

Egy-egy konkrét diofantikus egyenlet vizsgálata rendszerint valamilyen „ad hoc" módszerrel történik; olykor még formálisan csaknem azonos diofantikus egyenletek megoldásához is igen különböző eszközök lehetnek szükségesek (sőt a nyert eredmények is merőben különbözhetnek). Ezért a diofantikus egyenletek tárgyalása során célszerű az egyenlettípusok szerinti csoportosítás helyett inkább azt a néhány megoldó *módszert* ismertetnünk, mely a diofantikus egyenletek viszonylag szélesebb csoportjára alkalmazható. E pont hátralevő részében, valamint a 2—5. pontokban ilyen módszereket fogunk ismertetni, mégpedig a 2—5. pontokban — a könnyebb összehasonlíthatóság végett — ugyanazon diofantikus egyenlet, nevezetesen az

$$x^2+y^2=n$$

(ahol n adott természetes szám) diofantikus egyenlet kapcsán. A 6. és 7. pontban azonban külön is ki fogunk térni két különösen fontos diofantikus problémára, nevezetesen a Waring-problémára, ill. a Fermat-sejtésre; e két problémakör kapcsán egyúttal az első öt pontban ismertetett módszerek újabb alkalmazásaival is fogunk találkozni.

Valamely konkrét diofantikus egyenlet megoldásához — vagy legalábbis részeredmények eléréséhez — szerencsés esetben nagy segítséget nyújthat egy alkalmasan választott *azonosság* (vagy azonos átalakítás, például szorzattá alakítás). (L. az 1. példát.)

Az alábbiakban vázolunk egy gyakran alkalmazható elemi módszert, amely diofantikus egyenletek *megoldhatatlanságának* igazolására alkalmas. Tegyük fel, hogy az (1) diofantikus egyenlet megoldható; legyen egy megoldása $x_1=a_1, \ldots, x_k=a_k$. Ekkor

$$f(a_1, a_2, \ldots, a_k) = 0,$$

ahonnan következik, hogy bármely m természetes számra

$$f(a_1, a_2, \ldots, a_k) \equiv 0 \pmod{m}.$$

Ez azt jelenti, hogy ha az (1) diofantikus egyenlet megoldható, akkor szükségképpen az

$$(2) \qquad f(x_1, x_2, \ldots, x_k) \equiv 0 \pmod{m}$$

kongruencia is megoldható (bármely m természetes számra), nevezetesen egy megoldás $x_1=a_1, \ldots, x_k=a_k$. Tehát, *ha található olyan m természetes szám, melyre a* (2) *kongruencia megoldhatatlan, akkor az* (1) *diofantikus egyenlet is megoldhatatlan.* Ha egy diofantikus egyenlet megoldhatatlanságát ezen az úton akarjuk igazolni, akkor célszerű egy ilyen tulajdonságú m számot a prímszámok, ill. a prímszámhatványok körében keresnünk. (L. a 2. példát.)

Hangsúlyozzuk, hogy olyan m szám létezése, melyre (2) megoldhatatlan, csupán *elégséges*, de *nem szükséges* feltétele a megoldhatatlanságnak! Más szóval, előfordulhat, hogy a (2) kongruencia minden m természetes számra megoldható, de az (1) diofantikus egyenlet mégis megoldhatalan (vö. a 3. példával).

Példák

1. Állapítsuk meg, hogy az

$$(3) \qquad x^2-y^2 = n$$

diofantikus egyenlet mely n természetes számokra oldható meg!

Megoldás:

(3) bal oldalát szorzattá alakítva:

$$(x-y)(x+y) = n.$$

Innen látható, hogy

$$(4) \qquad x-y = d_1,$$

$$(5) \qquad x+y = d_2$$

osztói, mégpedig komplementer osztói n-nek, azaz

$$(6) \qquad d_1 d_2 = n.$$

Így (3) minden x, y megoldásához hozzárendelhető n-nek egy d_1, d_2 komplementer osztópárja (mégpedik (4) és (5) által). Továbbá (4)-et és (5)-öt összeadva, majd 2-vel osztva, nyerjük, hogy

$$(7) \qquad x = \frac{d_1+d_2}{2}.$$

Hasonlóan, (5)-ből kivonva (4)-et, majd 2-vel osztva:

$$(8) \qquad y = \frac{d_2-d_1}{2}.$$

(7) és (8) bal oldalán egész szám áll, tehát a jobb oldalon is egész számnak kell állnia, vagyis d_1+d_2-nek és d_2-d_1-nek is páros számnak kell lennie. E két szám viszont nyilván akkor és csak akkor páros, ha d_1 és d_2 azonos paritásúak.

A fenti okoskodást visszafelé követve, látható, hogy ha n felírható valamely d_1, d_2 azonos paritású egész számok szorzataként, akkor a (7) és (8) által definiált x, y egész számok egy megoldását adják a (3) diofantikus egyenletnek.

Így a vizsgált diofantikus egyenlet akkor és csak akkor oldható meg, ha n felírható két azonos paritású egész szám szorzataként. Ha n páratlan, akkor $n=1\cdot n$, ha n osztható 4-gyel, vagyis $n=4k$, akkor $n=2\cdot 2k$ egy ilyen felbontás, tehát ekkor (3) megoldható. Ha viszont n páros, de nem osztható 4-gyel, vagyis $n=4k+2$, akkor n-et bárhogyan felírva a (6) alakban, ott nyilván d_1 és d_2 közül az egyik szükségképpen páros, a másik páratlan; ekkor tehát (3) nem oldható meg. A vizsgált diofantikus egyenlet tehát akkor és csak akkor oldható meg, ha n nem $4k+2$ alakú.

Továbbá az adott megoldásból az is kiolvasható, hogy ha az n szám

$$n = 2^\alpha m$$

alakban írható, ahol α nemnegatív egész szám, m páratlan szám, akkor a (3) egyenlet $f(n)$ megoldásszáma (megengedve *negatív* egész megoldásokat is) a következőképpen számítható ki:

$$f(n) = \begin{cases} 2d(m), & \text{ha } \alpha = 0, \\ 0, & \text{ha } \alpha = 1, \\ 2(\alpha-1)d(m), & \text{ha } \alpha < 1. \end{cases}$$

2. Bizonyítsuk be, hogy az

$$x^3+y^3+z^3 = 9xyz+4$$

diofantikus egyenlet megoldhatatlan!

Megoldás:

Elegendő megmutatni, hogy az

$$x^3+y^3+z^3 \equiv 9xyz+4 \pmod 9,$$

vagyis az

$$x^3+y^3+z^3 \equiv 4 \pmod 9 \tag{9}$$

kongruencia megoldhatatlan. Vizsgáljuk meg, hogy ha u egész szám, akkor u^3 milyen maradékot adhat modulo 9? E célból elegendő u-t a modulo 9 abszolút legkisebb maradékrendszer elemein futtatni:

$$0^3 = 0 \equiv 0 \pmod 9,$$

$$(\pm 1)^3 = \pm 1 \equiv \pm 1 \pmod 9,$$

$$(\pm 2)^3 = \pm 8 \equiv \mp 1 \pmod 9,$$

$$(\pm 3)^3 = \pm 27 \equiv 0 \pmod 9,$$

$$(\pm 4)^3 = \pm 64 \equiv \pm 1 \pmod 9.$$

Egész szám harmadik hatványa tehát 9-cel osztva csak $-1, 0$, vagy $+1$ maradékot adhat. Így a (9) kongruencia bal oldalának mindhárom tagja $-1, 0$ vagy $+1$ maradékot ad 9-cel osztva. Ha mindhárom tag e számok legkisebbikével, -1-gyel kongruens modulo 9, akkor összegük -3-mal kongruens; ha viszont mindegyikük $+1$ maradékot ad 9-cel osztva, akkor összegük $+3$-mal kongruens. Így (9) bal oldala (bármely x, y, z-re) valamely -3 és $+3$ közé eső számmal, vagyis a $-3, -2, -1, 0, 1, 2, 3$ számok valamelyikével kongruens modulo 9. Azonban e számok mindegyike inkongruens a jobb oldalon álló számmal, 4-gyel, s így a (9) kongruencia valóban megoldhatatlan.

3. Igazoljuk, hogy az

$$(10) \quad f(x, y, z) = (x^2+1)(y^2+2)(z^2-2) = 0$$

diofantikus egyenlet megoldhatatlan, noha az

$$(11) \quad f(x, y, z) \equiv 0 \pmod{p}$$

kongruencia bármely p prímszámra megoldható!

Megoldás:

Ha $x=x_0$, $y=y_0$, $z=z_0$ megoldása a (10) egyenletnek, akkor szükségképpen az

$$f(x_0, y_0, z_0) = (x_0^2+1)(y_0^2+2)(z_0^2-2)$$

szorzat valamelyik tényezője 0. Az első két tényező azonban nyilván pozitív (bármely valós x_0, y_0-ra), tehát innen

$$z_0^2-2 = 0,$$

$$z_0 = \pm\sqrt{2}$$

következnék. $\sqrt{2}$ azonban nem egész szám, tehát a (10) egyenletnek valóban nincs egész megoldása.

Másrészt a (11) kongruencia nyilván akkor és csak akkor oldható meg, ha az

$$x^2 \equiv -1 \pmod{p},$$

$$y^2 \equiv -2 \pmod{p},$$

$$z^2 \equiv 2 \pmod{p}$$

kongruenciák valamelyike megoldható. Ha $p=2$, akkor mindhárom kongruencia megoldható, ti. $x=1$, $y=0$, $z=0$ megoldás. Ha viszont $p>2$, akkor az egyes kongruenciák akkor és csak akkor oldhatók meg, ha a $\left(\frac{-1}{p}\right)$, $\left(\frac{-2}{p}\right)$, ill. $\left(\frac{2}{p}\right)$ Legendre-szimbólum értéke $+1$. Így elég azt igazolnunk, hogy e Legendre-szimbólumok valamelyikének értéke $+1$. Számítsuk ki e Legendre-szimbólumok szorzatát (felhasználva a Legendre-szimbólum *B)* és *D)* tulajdonságait):

$$\left(\frac{-1}{p}\right)\left(\frac{-2}{p}\right)\left(\frac{2}{p}\right) = \left(\frac{(-1)(-2)(2)}{p}\right) = \left(\frac{4}{p}\right) = \left(\frac{2^2}{p}\right) = +1.$$

Innen következik, hogy legalább egy tényező értéke $+1$, és ezzel az állítást igazoltuk.

2. AZ $x^2+y^2=n$ DIOFANTIKUS EGYENLET MEGOLDHATÓSÁGÁNAK SZÜKSÉGES ÉS ELÉGSÉGES FELTÉTELE. A „DESCENTE INFINIE" MÓDSZER

A 2—5. pontban — különböző módszerek illusztrációjaként — azt fogjuk vizsgálni, hogy az

(12) $x^2+y^2=n$

diofantikus egyenlet mely n természetes számokra oldható meg? Igazolható, hogy a megoldhatóság szükséges és elégséges feltétele az alábbi:

A (12) *diofantikus egyenlet* $n>1$ *esetén akkor és csak akkor oldható meg, ha n kanonikus alakjában valamennyi* $4k-1$ *alakú prímszám kitevője páros szám* (továbbá $n=1$ esetén az egyenlet nyilván megoldható).

Viszonylag könnyen bizonyítható, hogy e feltétel *szükséges* feltétele a megoldhatóságnak; az *elégségesség* bizonyítása lényegesen nehezebb. A szükségesség igazolható például a II. fejezet 92*. feladatát, vagyis a kvadratikus maradékok elméletét felhasználva (l. a 4. példát). Egy másik, még elemibb bizonyítás adható az ún. „*descente infinie*" („végtelen leszállás") módszer segítségével.

A — teljes indukcióval rokon — descente infinie módszer lényege a következő:

Feltesszük, hogy bizonyos állítás igaz valamely n természetes számra, majd igazoljuk, hogy az állítás igaz valamely n-nél kisebb n_1 természetes számra is. Ha bármely n természetes számhoz található ilyen n_1 természetes szám, akkor ezáltal természetes számok szigorúan csökkenő végtelen sorozatát nyerjük: $n>n_1>\ldots$. Természetes számoknak ilyen sorozata azonban nem lehet végtelen, következésképpen az eredeti állítás semmilyen n természetes számra sem teljesülhet, vagyis igazoltuk, hogy annak ellenkezője teljesül bármely n-re. Így például valamely (1) alakú diofantikus egyenlet megoldhatatlansága a következőképpen igazolható ezzel a módszerrel:

Feltesszük, hogy az állítással ellentétben (1) megoldható, és definiálunk egy $g(x_1, \ldots, x_k)$ függvényt, mely (1) $x_1=a_1, \ldots,$

$\ldots, x_k = a_k$ megoldásaihoz valamely $g(a_1, \ldots, a_k)$ természetes számot rendel (például $g(x_1, \ldots, x_k) = x_1^2 + \ldots + x_k^2$). Ha (1) bármely $a_1, \ldots, a_k$ megoldásához található olyan $b_1, \ldots, b_k$ megoldás, hogy

$$(13) \quad (0 <)\ g(b_1, \ldots, b_k) < g(a_1, \ldots, a_k),$$

akkor az előbbiek szerint innen következik az egyenlet megoldhatatlansága.

A gyakorlatban sokszor úgy fogalmazzuk a bizonyítást, hogy olyan $a_1, \ldots, a_k$ megoldásból indulunk ki, melyre $g(a_1, \ldots, a_k)$ *minimális*. Ezután igazoljuk, hogy található olyan $b_1, \ldots, b_k$ megoldás, melyre (13) teljesül; ez azonban ellentmond $a_1, \ldots, a_k$ minimumtulajdonságának, és így abból az indirekt feltevésből, hogy (1) megoldható, ellentmondásra jutottunk.

A (12) megoldhatóságára adott feltétel szükségességének az a bizonyítása, mely a descente infinie módszerre épül, elemibb ugyan a 4. példában közöltnél, viszont jóval terjedelmesebb; ezért itt nem részletezzük azt. (Ez a bizonyítás megtalálható például Erdős Pál—Surányi János „Válogatott fejezetek a számelméletből" c. könyvében.) Alkalmazni fogjuk azonban a descente infinie módszer egy másik változatát az elégségesség igazolására (mint említettük, a (12) megoldhatóságára vonatkozó tételnek ez a nehezebb fele).

Az elégségesség vizsgálatára áttérve, először is megjegyezzük, hogy itt igen fontos szerepet játszik az

$$(14) \quad (a^2 + b^2)(x^2 + y^2) = (ax + by)^2 + (ay - bx)^2$$

azonosság. Ebből az azonosságból ugyanis nyilvánvalóan következik, hogy ha két természetes szám külön-külön felírható két négyzetszám összegeként, akkor a szorzatuk is felírható ilyen alakban. Erre a segédtételre tekintettel, elegendő igazolni, hogy az

$$(15) \quad x^2 + y^2 = p, \text{ ahol } p\ 4k+1 \text{ alakú prím}$$

diofantikus egyenlet megoldható (*tetszőleges* $4k+1$ alakú p prímre).

Biz.

Tegyük fel ugyanis, hogy (15) megoldhatóságát már igazoltuk (minden $4k+1$ alakú p prímre). Legyen n tetszőleges természetes szám, mely kielégíti a (12) megoldhatóságára vonatkozó feltételt. Ekkor n nyilván a

következő alakban írható:

$$n = p_1 p_2 \dots p_r n_1^2,$$

ahol a p_i prímszámok mindegyike $4k+1$ alakú, vagy pedig $p_i=2$, és n_1 természetes szám (melynek prímosztói $4k-1$ alakúak). Ha a p_i prím $4k+1$ alakú, akkor a (15) megoldhatóságára vonatkozó feltevésünk, ha pedig $p_i=2$, akkor az

$$1^2+1^2 = 2$$

összefüggés szerint p_i felírható két négyzetszám összegeként. Így (14)-et ismételten alkalmazva, nyerjük, hogy e p_i prímek szorzata is felírható ilyen alakban, tehát léteznek olyan u, v egész számok, melyekre

$$u^2+v^2 = p_1 p_2 \dots p_r.$$

Mindkét oldalt szorozva n_1^2-nel:

$$(un_1)^2+(vn_1)^2 = p_1 p_2 \dots p_r n_1^2 = n,$$

ehát $x=un_2$, $y=vn_2$ megoldása (12)-nek.

Így (12) megoldhatósága (a (14) azonosság alapján) valóban könnyen következik (15) megoldhatóságából, tehát *a* (12) *megoldhatóságára adott feltétel elégségességének igazolása* (15) *megoldhatóságának igazolására redukálható.*

(15) megoldhatóságát elsőként a descente infinie módszer segítségével fogjuk igazolni. E módszernek ugyanis kidolgozható egy olyan változata is, amely diofantikus egyenletek *megoldhatóságának* igazolására alkalmas.

Tegyük fel például, hogy valamely

$$(16) \quad f(x_1, \dots, x_k) = n$$

alakú diofantikus egyenlet megoldhatóságát akarjuk igazolni. E célból először bizonyítjuk, hogy létezik olyan m pozitív egész szám, hogy

$$(17) \quad f(x_1, \dots, x_k) = mn$$

megoldható. Jelöljük a legkisebb olyan m természetes számot, melyre (17) megoldható, m_0-lal. Ezután igazoljuk, hogy $m_0>1$ esetén található olyan m_1 természetes szám, melyre $m_1<m_0$ teljesül és (17) m helyén m_1-gyel megoldható. Ez azonban ellentmond m_0 minimumtulajdonságának, tehát az $m_0>1$ feltevésből ellentmondásra jutottunk. Így csak $m_0=1$ lehetséges, vagyis (16) valóban megoldható.

Az 5. példa kapcsán ezen az úton igazolni fogjuk (15) megoldhatóságát.

Itt nincs módunk arra, hogy a descente infinie módszer további alkalmazásait is tárgyaljuk; megemlítjük azonban, hogy a descente infinie módszer elsőként említett változata alkalmazható lenne például a Fermat-sejtés (l. a 7. pontot) $k=4$ speciális esetének igazolására, míg a második változat a négy négyzetszám-tétel (l. a 6. pontot) bizonyítására.

Példák

4. Bizonyítsuk be, hogy ha az n természetes szám nagyobb 1-nél és a (12) diofantikus egyenlet megoldható, akkor n kanonikus alakjában valamennyi $4k-1$ alakú prímszám kitevője páros szám!

Megoldás:

Elegendő igazolni a következő segédtételt: ha p $4k-1$ alakú prímszám, mely osztója az n természetes számnak, és x_0, y_0 megoldása (12)-nek, vagyis

(18) $x_0^2+y_0^2 = n,$

akkor szükségképpen

(19) $p|x_0,$

(20) $p|y_0,$

(21) $p^2|n$

is teljesül. Innen ugyanis következnék, hogy a (18) egyenlőség minden tagját oszthatjuk p^2-nel. Ha p még mindig osztója a jobb oldalon álló konstansnak $\left(\frac{n}{p^2}\text{-nek}\right)$, akkor az említett segédtétel szerint ismét oszthatnánk p^2-nel s í. t. Így a (18) jobb oldalán álló számot, n-et ismételten oszthatjuk p^2-nel, amíg végül egy p-vel nem osztható számot kapunk; ez pedig nyilván azt jelenti, hogy p kitevője n kanonikus alakjában páros. Továbbá az említett segédtételt ismételten alkalmazva, az is látható, hogy ha p $4k-1$ alakú prímszám, és $p^{2l}|n$, akkor a (18)-at kielégítő x_0, y_0 egész számok szükségképpen oszthatók p^l-nel.

Bizonyítanunk kell tehát, hogy ha p $4k-1$ alakú prímszám, melyre

(22) $p|n$

teljesül, akkor (18)-ból következik (19), (20) és (21). (18) és (22) szerint x_0, y_0 megoldása az

$$x^2+y^2 \equiv 0 \pmod{p}$$

kongruenciának. Minthogy p $4k-1$ alakú, innen a II. fejezet 92*. feladata szerint következik, hogy x_0, y_0 csak triviális megoldása lehet ennek a kongruenciának, vagyis (19) és (20) teljesül. Továbbá (19)-ből és (20)-ból következik, hogy a (18) egyenlőség bal oldala osztható p^2-nel, tehát a jobb oldal, azaz n is, ezért (21) is teljesül. Ezzel az említett segédtételt és így a (12) diofantikus egyenlet megoldhatóságára adott feltétel szükségességét is igazoltuk.

5. Igazoljuk a descente infinje módszer segítségével, hogy a (15) diofantikus egyenlet megoldható!

Megoldás:

Mivel p $4k+1$ alakú prímszám, a Legendre-szimbólum $E)$ tulajdonsága (II. fejezet 6. pont) szerint létezik olyan z_0 egész szám, melyre

(23) $z_0^2+1 \equiv 0 \pmod{p}$

teljesül. Nyilván feltehető, hogy $0 \leqq z_0 \leqq p-1$; ekkor

(24) $0 < z_0^2+1 \leqq (p-1)^2+1 = p^2-2(p-1) < p^2.$

(23) szerint $x=z_0$, $y=1$-et írva, alkalmas m egész számra

$$x^2+y^2 = z_0^2+1 = mp,$$

ahol (24) szerint

$$0 < m < p.$$

Így p-nek az m-szerese x^2+y^2 alakban írható. Jelöljük p-nek az ilyen alakban írható legkisebb pozitív többszörösét pm_0-lal; ekkor tehát alkalmas x_0, y_0 egész számokra

(25) $x_0^2+y_0^2 = m_0p.$

Tegyük fel indirekte, hogy

(26) $1 < m_0.$

m_0 minimumtulajdonságából az is következik, hogy

(27) $m_0 \leqq m < p.$

Osszuk el x_0-t és y_0-t m_0-lal, az abszolút legkisebb maradékok segítségével végezve az osztást:

(28) $x_0 = qm_0+x_1, \quad y_0 = sm_0+y_1,$

ahol

(29) $|x_1| \leqq \frac{m_0}{2}, \quad |y_1| \leqq \frac{m_0}{2}.$

Nem lehetséges az, hogy mind $m_0 = x_1$, mind $m_0 = y_1$ teljesüljön, hiszen ekkor (28)-ból $m_0 | x_0$ és $m_0 | y_0$ is következnék, és így (25)-ből nyernénk, hogy $m_0 | p$, ami azonban a (26) indirekt feltevés és (27) szerint nem teljesülhet (mivel p prímszám). Így $m_0 \nmid x_1$ és $m_0 \nmid y_1$ közül legalább az egyik teljesül; ebből következik, hogy

$$(30) \qquad 0 < x_1^2 + y_1^2.$$

Másrészt (29) alapján

$$(31) \qquad x_1^2 + y_1^2 \leqq \left(\frac{m_0}{2}\right)^2 + \left(\frac{m_0}{2}\right)^2 = \frac{m_0^2}{2} < m_0^2.$$

Továbbá (25)-ből és (28)-ból nyerjük, hogy

$$x_1^2 + y_1^2 \equiv x_0^2 + y_0^2 \equiv 0 \pmod{m_0},$$

tehát alkalmas m_1 egész számra

$$(32) \qquad x_1^2 + y_1^2 = m_1 m_0,$$

ahol (30) és (31) szerint

$$(33) \qquad 0 < m_1 < m_0.$$

Összeszorozva (25)-öt és (32)-t, a (14) azonosságra tekintettel azt kapjuk, hogy

$$(34) \qquad m_0^2 m_1 p = (x_0^2 + y_0^2)(x_1^2 + y_1^2) = (x_0 x_1 + y_0 y_1)^2 + (x_0 y_1 - y_0 x_1)^2.$$

Azonban (25)-ből és (28)-ból következik, hogy

$$x_0 x_1 + y_0 y_1 \equiv x_0^2 + y_0^2 \equiv 0 \pmod{m_0},$$

$$x_0 y_1 - y_0 x_1 \equiv x_0 y_0 - y_0 x_0 \equiv 0 \pmod{m_0},$$

tehát léteznek olyan x_2, y_2 egész számok, melyekre

$$x_0 x_1 + y_0 y_1 = m_0 x_2, \qquad x_0 y_1 - y_0 x_1 = m_0 y_2.$$

(34)-be helyettesítve:

$$m_0^2 m_1 p = (m_0 x_2)^2 + (m_0 y_2)^2,$$

ahonnan m_0^2-nel osztva:

$$m_1 p = x_2^2 + y_2^2.$$

$m_1 p$ tehát felírható $x^2 + y^2$ alakban, ami — (33)-ra tekintettel — ellentmond m_0 minimumtulajdonságának. Így a (26) indirekt feltevésből ellentmondásra jutottunk, és ezzel az állítást igazoltuk.

3. AZ $x^2+y^2=n$ DIOFANTIKUS EGYENLET MEGOLDHATÓSÁGÁNAK VIZSGÁLATA A THUE-LEMMA SEGÍTSÉGÉVEL

Mint az előző pontban láttuk, a (12) diofantikus egyenlet megoldhatóságának vizsgálata során a kritikus pont a (15) diofantikus egyenlet megoldhatóságának vizsgálata. Ebben a pontban (15) megoldhatóságát a Thue-lemma néven ismert segédtétel segítségével fogjuk igazolni. A *Thue-lemma* — mely gyakran alkalmazható diofantikus egyenletek vizsgálatakor — a következőképpen hangzik:

$n \in \mathbb{N}$ p prím

Legyen n tetszőleges természetes szám, p tetszőleges prímszám, az a_{ij} (ahol $i=1, 2, \ldots, n$; $j=1, 2, \ldots, n$) számok tetszőleges egész számok, $u_1, \ldots, u_n, v_1, \ldots, v_n$ pedig p-nél nem nagyobb természetes számok, melyekre

$$u_1 \ldots u_n v_1 \ldots v_n > p^n.$$

Ekkor léteznek olyan $x_1, \ldots, x_n, y_1, \ldots, y_n$ egész számok, melyekre

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &\equiv y_1 \pmod{p}, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &\equiv y_2 \pmod{p}, \\ &\vdots \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n &\equiv y_n \pmod{p}, \end{aligned}$$

valamint

$$|x_1| < u_1, \ldots, |x_n| < u_n, \qquad |y_1| < v_1, \ldots, |y_n| < v_n$$

teljesül, tovább $x_1, x_2, \ldots, x_n$ közül legalább az egyik 0-tól különböző.

Az $n=1$ speciális esetben a tétel következő alakot ölti: Legyen p prímszám, a egész szám, u, v pedig p-nél nem nagyobb egész számok, melyekre

(35) $uv > p.$

Ekkor léteznek olyan x, y egész számok, melyekre

(36) $ax \equiv y \pmod{p}$

és

(37) $0 < |x| < u$,

(38) $|y| < v$

teljesül. (L. a 15. feladatot.)

(15) megoldhatóságát viszonylag egyszerűen bizonyíthatjuk, ha a Thue-lemmának ezt a speciális esetét kombináljuk azzal a segédtétellel, mely szerint létezik (23)-at kielégítő z_0 egész szám (l. az alábbi példát).

Példa

6. Bizonyítsuk be a Thue-lemma segítségével, hogy ha p $4k+1$ alakú prímszám, akkor a (12) diofantikus egyenlet megoldható!

Megoldás:

Alkalmazzuk a Thue-lemma $n=1$ speciális esetét $a=z_0$ (ahol z_0 kielégíti (23)-at), $u=v=[\sqrt{p}]+1$ választással. Ekkor nyilván $u \leqq p$, $v \leqq p$, továbbá

$$uv = ([\sqrt{p}]+1)^2 > (\sqrt{p})^2 = p,$$

tehát a (34) feltétel is teljesül. Így nyerjük, hogy léteznek olyan x, y egész számok, melyekre

(39) $z_0 x \equiv y \pmod{p}$,

(40) $0 < |x| < [\sqrt{p}]+1$,

(41) $|x| < [\sqrt{p}]+1$

teljesül. Ekkor (23) és (39) szerint

$$x^2+y^2 \equiv x^2+(z_0x)^2 = x^2(z_0^2+1) \equiv x^2 \cdot 0 = 0 \pmod{p},$$

továbbá (40) és (41) értelmében

$$0 < x^2+y^2 \leqq ([\sqrt{p}])^2+([\sqrt{p}])^2 < (\sqrt{p})^2+(\sqrt{p})^2 = 2p.$$

Így x^2+y^2 osztható p-vel, továbbá 0 és $2p$ közé esik, tehát szükségképpen p-vel egyenlő, vagyis az így definiált x, y egész számok kielégítik (15)-öt.

4. AZ $x^2+y^2=n$ DIOFANTIKUS EGYENLET MEGOLDHATÓSÁGÁNAK VIZSGÁLATA GAUSS-EGÉSZEK SEGÍTSÉGÉVEL. AZ ALGEBRAI SZÁMELMÉLET ELEMEI

A (12) diofantikus egyenlet bal oldala a komplex számok körében szorzattá alakítható:

$$(x+iy)(x-iy)=n.$$

Itt a bal oldal mindkét tényezője olyan $a+bi$ alakú szám, ahol a és b racionális egész számok; ez a tény indokolja, hogy a (12) egyenlet az ilyen alakú számok vizsgálata révén próbáljuk megoldani.

Ha a, b racionális egészek, ill. racionális számok, akkor az $a+bi$ komplex számot *Gauss-egésznek*, ill. *Gauss-racionálisnak* nevezzük. A Gauss-egészeket a továbbiakban görög betűkkel fogjuk jelölni.

Könnyen ellenőrizhető, hogy a Gauss-egészek körében az összeadás, kivonás, szorzás a szokásos műveleti szabályok szerint végezhető el, a Gauss-racionális számok körében pedig az osztás is elvégezhető.

Az absztrakt algebra terminológiáját használva, a Gauss-egészek gyűrűt, a Gauss-racionális számok testet alkotnak.

A Gauss-egészek körében kiépíthető a racionális számelmélet analogonja. Itt csupán arra szorítkozunk, hogy felsoroljuk a legfontosabb lépéseket.

A) Első lépésként az *oszthatóság* fogalmát definiáljuk: ha adott α, β Gauss-egészekhez található olyan γ Gauss-egész, hogy $\alpha=\beta\gamma$, akkor azt mondjuk, hogy α *osztható* β-val. Igazolható, hogy a Gauss-egészek körében definiált oszthatóság alaptulajdonságai megegyeznek a racionális egész számok körében definiált oszthatóság alaptulajdonságaival (csupán az egységek különböznek; l. alább).

B) Valamely ε Gauss-egészet akkor nevezünk egységnek, ha osztója bármely Gauss-egésznek. Igazolható, hogy a Gauss-egészek körében az egységek a következők: $-1, +1, -i, +i$. Ha a β Gauss-egész egységszerese α-nak, akkor β-t α *asszociáltjának* mondjuk. Könnyen látható, hogy ha $\varepsilon_1, \varepsilon_2$ tetszőleges egységek, akkor valamely α, β Gauss-egészekre $\varepsilon_1\alpha|\varepsilon_2\beta$ akkor

és csak akkor teljesül, ha $\alpha|\beta$ is teljesül. (Az oszthatóság szempontjából tehát egy Gauss-egész és asszociáltjai azonos szerepet játszanak.) Igazolható továbbá, hogy ha az α, β Gauss-egészekre $\alpha|\beta$ és $\beta|\alpha$ egyidejűleg teljesül, akkor szükségképpen β egységszerese α-nak.

A racionális számelmélet alapjainak tárgyalása során hangsúlyoztuk, hogy a legnagyobb közös osztó létezése, és ezen keresztül a maradékos osztás tétele milyen fontos szerepet játszik. Felmerül a kérdés, hogy a maradékos osztás tétele átvihető-e a Gauss-egészekre, és ha igen, hogyan? Ennek a kérdésnek a megválaszolásához nyújt segítséget az alábbi definíció:

C) Az $\alpha = a + bi$ Gauss-egész *normájának* a

$$N(\alpha) = |\alpha|^2 = a^2 + b^2$$

nemnegatív egész számot nevezzük. $N(\alpha) = 0$ nyilván akkor és csak akkor teljesül, ha $\alpha = 0$; így $\alpha \neq 0$ esetén a norma *pozitív egész* szám. Könnyen látható, hogy a norma *multiplikatív*, azaz

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Innen következik, hogy

(42) $\alpha|\beta$ esetén $N(\alpha)|N(\beta)$.

(Az előző pontban említett egységek e segédtétel alapján határozhatók meg legegyszerűbben.)

A racionális egész számok körében a következőképpen hangzik a *maradékos osztás tétele:* ha a, b adott egész számok, és $b \neq 0$, akkor léteznek olyan q, r egész számok, melyekre

$$a = qb + r$$

és

(43) $0 \leqq r < |b|$

teljesül. E tétel megfelelőjét keresve a Gauss-egészek körében, a tulajdonképpeni probléma az, hogy a (43) feltétel mivel pótolható? A tétel a következő:

D) Ha α, β adott Gauss-egészek, és $\beta \neq 0$, akkor találhatók olyan γ, δ Gauss-egészek, melyekre

$$\alpha = \beta\gamma + \delta$$

és

$$(44) \quad (0 \leqq) N(\delta) < N(\beta)$$

teljesül (l. a 17. feladatot). A (43) feltétel helyébe tehát itt a (44) feltétel lép.

E) A maradékos osztás tételére építve, az *euklideszi algoritmus* ugyanúgy definiálható, mint a racionális egész számok körében (az algoritmus végességét a (44) feltétel garantálja).

F) A legnagyobb közös osztó definíciója analóg a racionális számelméletben (általunk másodikként említett) definícióval: ha adott α, β Gauss-egészekhez található olyan δ Gauss-egész, hogy $\delta|\alpha$ és $\delta|\beta$, másrészt $\gamma|\alpha$ és $\gamma|\beta$ esetén szükségképpen $\gamma|\delta$ is teljesül, akkor δ-t α és β legnagyobb közös osztójának mondjuk. Az euklideszi algoritmus segítségével igazolható (ugyanúgy, mint a racionális számelméletben), hogy *bármely* α, β *Gauss-egészeknek létezik a legnagyobb közös osztója*, és az *lényegében* — egység szorzótól eltekintve — *egyértelműen van meghatározva*; ezt a legnagyobb közös osztót (α, β)-val jelöljük. Továbbá a legnagyobb közös osztó felírható a két szám lineáris kombinációjaként, azaz

$$\varphi\alpha + \psi\beta = (\alpha, \beta)$$

alakban, ahol φ, ψ alkalmas Gauss-egészek.

G) A *Gauss-prímek* ugyanúgy kétféleképpen is definiálhatók, mint a racionális prímszámok. Az első definíció:

Valamely egységtől különböző π Gauss-egészet akkor nevezünk Gauss-prímnek, ha $\pi = \alpha\beta$ (ahol α, β Gauss-egészek) esetén szükségképpen α vagy β egység.

A másik definíció:

Legyen π 0-tól és egységtől különböző Gauss-egész. Ha $\pi|\alpha\beta$ (ahol α, β Gauss-egészek) esetén szükségképpen $\pi|\alpha$ vagy $\pi|\beta$ is teljesül, akkor π-t Gauss-prímnek nevezzük.

A legnagyobb közös osztóról fent elmondottakat felhasználva, igazolható (ugyanúgy, mint a racionális számelméletben), hogy e két definíció *ekvivalens*. Ezt felhasználva viszont igazolható a (racionális) számelmélet alaptételének analogonja:

H) Bármely 0-tól és egységtől különböző Gauss-egész lényegében — sorrendtől és egység szorzóktól eltekintve — egyértelműen felírható Gauss-prímek szorzataként.

Felmerül az a kérdés, hogy mely Gauss-egészek a Gauss-prímek; van-e valami kapcsolat Gauss-prímek és racionális prímek között? Mint látni fogjuk, e kérdés szorosan összefügg a (12) diofantikus egyenlet megoldhatóságának vizsgálatával.

Könnyen belátható, hogy $1+i$ (és asszociáltjai) Gauss-prímek. Az is igazolható (l. a 7. példát), hogy a $4k-1$ alakú racionális prímszámok egyúttal Gauss-prímek is. Végül bizonyítható (l. a 8. példát), hogy ha p $4k+1$ alakú racionális prímszám, akkor felírható két Gauss-prím szorzataként, melyek egymás konjugáltjai; legyenek ezek $\pi=a+bi$, $\bar{\pi}=a-bi$. Ekkor

$$\pi\bar{\pi} = (a+bi)(a-bi) = a^2+b^2 = p,$$

tehát $x=a$, $y=b$ megoldása a (15) diofantikus egyenletnek. Ez azt jelenti, hogy a 8. példából következik (15) megoldhatósága, abból pedig — mint már a 2. pontban láttuk — könnyen következik a (12) diofantikus egyenlet megoldhatóságára adott feltétel elégségessége is. Így a Gauss-egészek segítségével a (12) diofantikus egyenlet megoldhatósága teljes egészében tisztázható.

Sőt, egy racionális egész szám Gauss-egészek körében felírt kanonikus alakját, ill. a (12) egyenletet finomabban analizálva, (12) megoldásszáma is meghatározható. Nevezetesen ezen az úton igazolható, hogy ha az n természetes számot $n=n_1n_2$ alakban írjuk, ahol n_1 páratlan és prímosztói $4k+1$ alakúak, n_2 prímosztói pedig — esetleg a 2-től eltekintve — $4k-1$ alakúak, akkor a (12) diofantikus egyenlet x, y egész megoldásainak száma $4d(n_1)$.

A 20*. feladat kapcsán a Gauss-egészek elméletét egy másik diofantikus egyenlet megoldására fogjuk alkalmazni. Azonban például a (12)-re emlékeztető

$$x^2+2y^2 = n$$

diofantikus egyenlet megoldhatóságának vizsgálatára a Gauss-egészek nem alkalmasak; itt a Gauss-egészek elmélete helyett nyilván az $a+bi\sqrt{2}$ (ahol a, b racionális egész számok) alakú

számokéra lenne szükségünk, hiszen x^2+2y^2 e számok körében szorzattá alakítható:

$$x^2+2y^2 = (x+yi\sqrt{2})(x-yi\sqrt{2}).$$

Az

$$x^2+xy+y^2 = n$$

vagy

$$x^2+3y^2 = n$$

diofantikus egyenletek megoldhatósága pedig az ún. *Euler-egészek* segítségével tárgyalható. Euler-egészeknek az $a+b\eta$ alakú számokat nevezzük, ahol a, b racionális egész számok, η pedig az

$$x^2+x+1 = 0$$

egyenlet egyik gyöke (tehát η primitív harmadik egységgyök), azaz $\eta = -\frac{1}{2}+i\frac{\sqrt{3}}{2}$ vagy $\eta = -\frac{1}{2}-i\frac{\sqrt{3}}{2}$. *Euler-racionális számoknak* pedig az olyan $r+s\eta$ alakú számokat nevezzük, ahol r, s racionális számok.

A Gauss-egészek, az $a+bi\sqrt{2}$ alakú számok és az Euler-egészek elmélete sok hasonlóságot mutat. Ezért célszerűnek tűnik egy olyan egységes elméletet kiépíteni, melynek keretein belül e három elmélet speciális esetként tárgyalható. Ez a probléma már az *algebrai számelmélet* tárgykörébe vág.

Az algebrai számelmélet a modern számelmélet igen gyorsan fejlődő ága, melynek igen sok alkalmazása van a diofantikus egyenletek elméletében, valamint a diofantikus approximációelméletben, de a számelmélet egyes más területein is. Itt csupán arra van módunk, hogy vázoljuk az algebrai számelmélet problematikáját, valamint egyes alapvető definíciókat, ill. tételeket.

Mindenekelőtt egy definíció: ha az α valós szám gyöke valamely egész együtthatós (nem azonosan 0) polinomnak, akkor *algebrai* számnak, ellenkező esetben *transzcendens* számnak nevezzük. Ha α gyöke egy olyan egész együtthatós polinomnak, melyben a legmagasabb fokú tag együtthatója 1, akkor α-t *algebrai egésznek* mondjuk. Egy α algebrai szám *fokának* a leg-

kisebb olyan n természetes számot nevezzük, melyhez még található olyan n-edfokú egész együtthatós polinom, melynek α gyöke.

Igazolható, hogy valamely 0-tól különböző ϑ algebrai számot megadva, létezik egy olyan egyértelműen definiált, rendszerint $R(\vartheta)$-val jelölt *számtest*, mely egyrészt tartalmazza ϑ-t és a racionális számokat, másrészt bármely más olyan számtest, amely tartalmazza ϑ-t és a racionális számokat, szükségképpen tartalmazza $R(\vartheta)$-t is. (A komplex számok valamely részhalmazát akkor nevezzük számtestnek, ha e részhalmaz bármely két elemének összege, különbsége, szorzata és — 0-tól különböző osztó esetén — hányadosa szintén e részhalmazhoz tartozik.)

Az absztrakt algebra terminológiáját használva, a ϑ-t és a racionális számtestet tartalmazó legszűkebb számtestet jelöljük $R(\vartheta)$-val.

$R(\vartheta)$-t *a racionális számtest ϑ-val való algebrai bővítésének* nevezzük. Ha ϑ n-edfokú algebrai szám, akkor $R(\vartheta)$-t *n-edfokú* algebrai bővítésnek mondjuk; speciálisan a másodfokú bővítéseket *kvadratikus bővítésnek* nevezzük. Igazolható, hogy ha $R(\vartheta)$ n-edfokú, akkor $R(\vartheta)$ bármely α eleme felírható

$$\alpha = a_0 + a_1\vartheta + \ldots + a_{n-1}\vartheta^{n-1}$$

alakban, ahol $a_0, a_1, \ldots, a_{n-1}$ racionális számok és ez a felírás egyértelmű.

Valamely $R(\vartheta)$ algebrai bővítésben szereplő algebrai *egészek* összességét $K(\vartheta)$-val fogjuk jelölni (az $I(\vartheta)$ jelölés is használatos). Igazolható, hogy $K(\vartheta)$ bármely két elemének összege, különbsége, szorzata szintén $K(\vartheta)$-hoz tartozik.

Algebrai terminológiát használva, $K(\vartheta)$ elemei *gyűrűt* alkotnak.

Visszatérve az említett konkrét pédákra, a Gauss-racionális számokhoz, az $r+si\sqrt{2}$ (ahol r, s racionális számok) alakú számokhoz, ill. az Euler-racionális számokhoz nyilván a racionális számtestnek rendre i-vel, $i\sqrt{2}$-vel, ill. η-val való kvadratikus bővítéseként juthatunk el, míg a Gauss-egészek, az $a+bi\sqrt{2}$ (ahol a, b racionális egész számok) alakú számok, az Euler-egészek összessége rendre $K(i)$-vel, $K(i\sqrt{2})$-vel, ill. $K(\eta)$-val

azonos. Mint említettük, mindhárom esetben felépíthető a racionális számelmélet analogonja, tehát definiálható a maradékos osztás, és ennek következményeként létezik az euklideszi algoritmus, létezik és lényegében egyértelmű a legnagyobb közös osztó, és *igaz a számelmélet alaptételének alnalogonja.*

Felmerül a kérdés, hogy elmondható-e ugyanaz $K(\vartheta)$-ról *tetszőleges* ϑ algebrai számot tekintve? Sajnálatos módon, a válasz negatív.

Sőt, még ha a legegyszerűbb esetnél, a kvadratikus bővítéseknél maradunk, akkor is „majdnem minden" ϑ-ra negatív a válasz a feltett kérdésre. Pontosabban, igazolható, hogy csak *véges sok* (kilenc) olyan $K(\vartheta)$ létezik, ahol ϑ másodfokú algebrai szám, és igaz a számelmélet alaptétele. (Ez a tétel úgy értendő, hogy a *különböző* ilyen $K(\vartheta)$-k száma véges; egy-egy ilyen $K(\vartheta)$-hoz azonban végtelen sok ϑ-ból kiindulva eljuthatunk. Így például tetszőleges α *nem valós* Gauss-racionális számot tekintve, $K(\alpha)=K(i)$.) A 23. feladat kapcsán igazolni fogjuk, hogy például $K(i\sqrt{5})$-ben nem igaz a számelmélet alaptétele.

Kummer vette észre elsőként — a Fermat-probléma (l. a 7. pontot) kapcsán —, hogy a legnagyobb közös osztó fogalma általánosítható oly módon, hogy a racionális számelmélet bizonyos elemei átmenthetők legyenek $K(\vartheta)$-ra, most már *tetszőleges* (algebrai) ϑ esetén. Így jutunk el a *Kummer—Dedekind-féle ideálelmélethez;* ezzel itt nincs módunk foglalkozni.

Példák

7. Bizonyítsuk be, hogy ha p $4k-1$ alakú racionális prímszám, akkor egyúttal Gauss-prím is!

Megoldás:

Tegyük fel indirekte, hogy p nem Gauss-prím, vagyis léteznek olyan α, β (egységtől különböző) Gauss-egészek, melyekre $\alpha\beta=p$. Innen következik, hogy

$$N(\alpha\beta) = N(p) = p^2,$$

vagyis a norma multiplikativitására tekintettel

$$N(\alpha)N(\beta) = p^2.$$

Minthogy Gauss-egész normája mindig nemnegatív egész szám, innen következik, hogy $N(\alpha)$ és $N(\beta)$ az $1, p, p^2$ számok közül kerülnek ki. Azonban könnyen látható, hogy valamely γ Gauss-egész akkor és csak akkor egység, ha $N(\gamma)=1$ (ennek belátását az Olvasóra bízzuk). Így szükségképpen

$N(\alpha)\neq 1$ és $N(\beta)\neq 1$, hiszen feltevésünk szerint α, β nem egységek. Ezért csak

(45) $N(\alpha) = N(\beta) = p$

lehetséges. Legyen $\alpha = a+bi$. Ekkor (45) szerint

$$N(\alpha) = a^2+b^2 = p,$$

tehát p felírható lenne két négyzetszám összegeként. Azonban feltevésünk szerint p $4k-1$ alakú, tehát a 2. pontban mondottak szerint nem állítható elő x^2+y^2 alakban; így az indirekt feltevésből ellentmondásra jutottunk, és ezzel az állítást igazoltuk.

8. Bizonyítsuk be, hogy ha p $4k+1$ alakú prímszám, akkor két olyan Gauss-prím szorzataként írható, melyek egymás konjugáltjai! (Mint már említettük, innen következik (15) megoldhatósága.)

Megoldás:

Először igazolni fogjuk, hogy p nem Gauss-prím. Ennek bizonyítása céljából tegyük fel indirekte, hogy p Gauss-prím. Az előző pontban láttuk, hogy létezik olyan z_0 egész szám, melyre (23) teljesül. Ekkor

$$p|z_0^2+1 = (z_0+i)(z_0+i).$$

Minthogy indirekt feltevésünk szerint p Gauss-prím, innen következik, hogy p osztója a $(z_0+i)(z_0-i)$ szorzat valamelyik tényezőjének is; feltehető, hogy az elsőnek (ha a másodiknak, a bizonyítás analóg). Ekkor tehát $p|z_0+i$, vagyis létezik olyan $\alpha = a+bi$ Gauss-egész, melyre

$$z_0+i = p\alpha = p(a+bi) = pa+pbi.$$

Két komplex szám egyenlőségéből következik a képzetes részeik egyenlősége: $1 = pb$. Így a racionális egész számok körében teljesülne a $p|1$ osztathatósági reláció, ami nyilván lehetetlen (hiszen p 1-nél nagyobb egész szám). Az indirekt feltevésből tehát ellentmondásra jutottunk, és ezzel igazoltuk, hogy p nem Gauss-prím.

p tehát nem Gauss-prím és nyilván nem egység (továbbá $p\neq 0$), tehát p felírható valamely $\pi_1, \pi_2, \ldots, \pi_k$ Gauss-prímek szorzataként:

$$\pi_1\pi_2 \ldots \pi_k = p,$$

ahol $k \geqq 2$. Innen következik, hogy

$$N(\pi_1\pi_2 \ldots \pi_k) = N(p),$$

vagyis a norma multiplikativitására tekintettel

(46) $N(\pi_1)N(\pi_2) \ldots N(\pi_k) = p^2.$

Minthogy $\pi_1, \pi_2, \ldots, \pi_k$ nem egységek, az előző példa megoldása során mondottak szerint $N(\pi_1), \ldots, N(\pi_k)$ különbözik 1-től. Így (46) bal oldalán legalább két, 1-nél nagyobb egész szám szorzata áll. A jobb oldalon álló szám, p^2 azonban nyilván csak egyféleképpen írható fel ilyen alakban, nevezetesen $p \cdot p = p^2$. Így (46)-ban $k=2$ és

$$N(\pi_1) = N(\pi_2) = p.$$

A norma definíciójára tekintettel innen $|\pi_1| = |\pi_2|$ következik. Továbbá a π_1, π_2 komplex számok szorzata. p *pozitív valós* szám; innen következik, hogy π_1 és π_2 argumentumai egymás negatívjai. Így π_1 és π_2 abszolút értéke egyenlő, argumentumaik pedig egymás negatívjai, tehát $\pi_2 = \bar{\pi}_1$. Végeredményben tehát $p = \pi_1 \pi_2$, ahol π_1, π_2 Gauss-prímek és $\pi_2 = \bar{\pi}_1$, és ezzel az állítást maradéktalanul igazoltuk.

(Megjegyezzük, hogy az is könnyen igazolható, hogy π_1 és π_2 lényegesen különböző Gauss-prímek, azaz nem asszociáltjai egymásnak.)

5. A GEOMETRIAI SZÁMELMÉLET ELEMEI. AZ $x^2+y^2=n$ DIOFANTIKUS EGYENLET MEGOLDHATÓSÁGÁNAK VIZSGÁLATA MINKOWSKI TÉTELE SEGÍTSÉGÉVEL

A diofantikus egyenletek vizsgálata során és a diofantikus approximációelméletben gyakran alkalmazhatók *geometriai módszerek* is; ezeket a módszereket tárgyalja az ún. *geometriai számelmélet*. Itt csupán a geometriai számelmélet egyik legfonfontosabb témáját, az ún. *paralelogrammarácsokat* és azok alkalmazásait fogjuk tárgyalni.

Tekintsünk a síkban egymással párhuzamos, egymástól egyenlő távolságra levő egyenesek által alkotott egyenessereget, majd egy másik ugyanilyen egyenessereget, mely az előző egyenessereg egyeneseit metsző egyenesekből áll. A két egyenessereg olyan paralelogrammákra osztja a síkot, melyek egybevágóak, oldalaik párhuzamosak, és hézagtalanul és átfedés nélkül lefedik a síkot; két-két ilyen paralelogrammának vagy nincsen közös pontja, vagy egy csúcsuk közös, vagy pedig egy oldaluk közös. Az így nyert hálózatot *paralelogrammarácsnak* nevezzük, az említett paralelogrammák valamelyikét pedig *alapparalelogrammának*. A paralelogrammák csúcsait *rácspontoknak*, a rácspontok összességét *pontrácsnak* nevezzük. Nyilván egy paralelogrammarácsot egy alapparalelogramma egyértelműen meghatároz („*kifeszíti*" azt).

Egy paralelogrammarács a fentiek szerint egyértelműen meghatároz egy pontrácsot; egy pontrácshoz viszont végtelen sok paralelogrammarács tartozik. Tekintsünk ugyanis valamely rögzített pontrácsban négy olyan rácspontot, melyek egy olyan paralelogramma csúcsai, melynek sem belsejébe, sem oldalaira nem esik további rácspont e négyen kívül; egy ilyen paralelogrammát *üres rácsparalelogrammának* nevezünk. Igazolható, hogy bármely üres rácsparalelogramma, mint alapparalelogramma olyan paralelogrammarácsot feszít ki, mely az adott pontrácsot definiálja. Igazolható továbbá, hogy egy pontrács üres rácsparalelogrammáinak területe azonos; e paralelogrammák területét (mely tehát a pontrácstól függő állandó) Δ-val fogjuk jelölni.

Gyakran előfordul, hogy egy paralelogrammarácsot vagy pontrácsot a derékszögű koordináta-rendszerben adunk meg. Ha ilyenkor az origó rácspont, akkor a rácsot *homogénnek*, ellenkező esetben *inhomogénnek* nevezzük. Rögzítsünk a derékszögű koordináta-rendszerben egy *homogén pontrácsot;* mint láttuk, ez egyértelműen megadható egy alapparalelogrammája (vagyis egy üres rácsparalelogramma) által. Válasszunk egy olyan alapparalelogrammát, melynek egyik csúcsa az origó; jelöljük az origót O-val, a paralelogramma O-val szomszédos csúcsait P, Q-val. Ekkor az $\overrightarrow{OP}, \overrightarrow{OQ}$ *vektorok* egyértelműen meghatározzák — „*kifeszítik*" — a szóban forgó paralelogrammát, és így az adott rácsot is.

Jelöljük az $\overrightarrow{OP}$ vektort α-val, és legyenek skalárkomponensei (a P pont derékszögű koordinátái) a_1, a_2; ekkor tehát $\alpha = \overrightarrow{OP} = (a_1; a_2)$. Hasonlóan, legyen $\beta = \overrightarrow{OQ} = (b_1; b_2)$. Legyen továbbá R a sík tetszőleges pontja, melynek derékszögű koordinátái x, y. A vektorok összeadásának, ill. skalárral való szorzásának geometriai interpretációját figyelembe véve, könnyen igazolható, hogy az R pont akkor és csak akkor rácspont, ha a $\gamma = \overrightarrow{OR}$ vektor a következő alakban írható:

$$(47) \quad \gamma = m\alpha + n\beta, \quad \text{ahol} \quad m = 0, \pm 1, \pm 2, \ldots,$$

$$n = 0, \pm 1, \pm 2, \ldots.$$

Vektorok segítségével tehát igen egyszerűen leírható egy pontrács. Továbbá a γ és $m\alpha+n\beta$ vektorok akkor és csak akkor egyenlők, ha a megfelelő komponenseik egyenlők. Így nyerjük a (47) feltétel következő átfogalmazását: az R pont akkor és csak akkor rácspont, ha x, y derékszögű koordinátái

$$x = ma_1 + nb_1,$$

$$y = ma_2 + nb_2$$

alakban írhatók, ahol m, n egész számok.

Könnyen igazolható továbbá, hogy a fenti rács egy alapparalelogrammájának területe a következőképpen számítható ki:

$$(48) \quad \Delta = |a_1 b_2 - a_2 b_1|.$$

Ebben a könyvben a geometriai számelmélet, közelebbről a paralelogrammarácsok elméletének alkalmazásai közül csupán a *Minkowski tételén* alapulókkal fogunk foglalkozni. Mielőtt ennek a tételnek az ismertetésére rátérnénk, előre kell bocsátanunk néhány geometriai alapfogalmat.

Legyen adott a síkban egy H ponthalmaz. Ha H bármely két pontjával együtt az azokat összekötő szakasz pontjait is tartalmazza, akkor H-t *konvexnek* mondjuk.

Ha P a sík tetszőleges pontja, ϱ tetszőleges pozitív szám, akkor a P-től ϱ-nál közelebb levő pontok összességét *a P pont ϱ sugarú környezetének* nevezzük. Ha egy H síkbeli ponthalmaz *bármely* P pontjához található olyan ϱ pozitív szám, hogy H tartalmazza a P pont ϱ sugarú környezetének minden pontját, akkor H-t *nyílt halmaznak* mondjuk. Valamely H síkbeli ponthalmaz pontjait elhagyva a síkból, az így megmaradó pontok összességét *H komplementerének* nevezzük, és $\bar{H}$-val jelöljük. Ha a H halmaz $\bar{H}$ komplementere nyílt halmaz, akkor H-t *zárt halmaznak* mondjuk.

Legyen adott a síkban egy H ponthalmaz és egy P pont. Ha H pontjait a P ponton át tükrözve, H önmagába megy át, akkor H-t *P-re nézve centrálszimmetrikusnak* mondjuk.

Ezek után *Minkowski tétele* a következőképpen hangzik:

Legyen adott a (síkbeli) derékszögű koordináta rendszerben egy homogén pontrács, és legyen e pontrács egy alapparalelog-

rammájának területe Δ. Legyen adott továbbá egy H konvex, zárt, az origóra nézve centrálszimmetrikus ponthalmaz, melynek területe legalább 4Δ. Ekkor H szükségképpen tartalmaz az origótól különböző — vagyis ún. *nemtriviális* — rácspontot.

(Itt csupán a Minkowski-tételnek egy speciális esetét fogalmaztuk meg; a fenti tétel ugyanis általánosítható többdimenziós rácsokra is.)

A Minkowski-tétel egy-egy konkrét alkalmazása során először a vizsgált számelméleti problémát át kell fogalmaznunk rácsgeometriai feladattá. Pontosabban, definiálnunk kell egy alkalmas rácsot, majd egy alkalmas H ponthalmazt, melyre Minkowski tételét alkalmazva, adódik a bizonyítandó állítás. A lényeges nehézséget rendszerint a megfelelő rács megkonstruálása jelenti; a rácsot rögzítve, a megfelelő H halmaz általában már adódik.

A 9. példában Minkowski tételének segítségével fogjuk igazolni — (23)-at kielégítő z_0 egész szám létezését felhasználva — a (15) diofantikus egyenlet megoldhatóságát. A 24. feladatban ismertetjük Minkowski tételének egy másik, hasonló jellegű alkalmazását. Megjegyezzük továbbá, hogy Minkowski tétele, ill. általában a geometriai számelmélet módszerei gyakran alkalmazhatók a diofantikus approximációelméletben is (l. a következő fejezetet).

Példa

9. Minkowski tételét felhasználva, igazoljuk, hogy a (15) diofantikus egyenlet megoldható!

Megoldás:

Minthogy p $4k+1$ alakú prím, a 2. pontban mondottak szerint létezik olyan z_0 egész szám, melyre (23) teljesül. Tekintsük azt a pontrácsot, melyet azon rácspontok alkotnak, melyek derékszögű koordinátái

(49) $x = mp + nz_0$,

(50) $y = n$

alakban írhatók, ahol m, n egész számok.

Ha x, y egy rácspont koordinátái (ekkor x, y nyilván egész számok), akkor (23)-ra tekintettel

$$x^2+y^2 = (mp+nz_0)^2+n^2 \equiv (nz_0)^2+n^2 = n^2(z_0^2+1) \equiv 0 \pmod{p},$$

vagyis

(51) $p \mid x^2+y^2$.

Ha tovább e rácspont különbözik az origótól, akkor nyilván

(52) $0 < x^2+y^2$.

Ha az x, y egész számokra (51) és (52) mellett

(53) $x^2+y^2 < 2p$

is teljesül, akkor x, y nyilván kielégítik (15)-öt, tehát a (15) diofantikus egyenlet valóban megoldható. Így elég azt igazolnunk, hogy léteznek olyan x, y egész számok, melyekre (51) és (52) teljesül, vagyis létezik olyan *nemtriviális rácspont*, amelyet az (53)-at kielégítő $(x; y)$ pontok által alkotott H ponthalmaz tartalmaz.

Ilyen rácspont létezésének igazolása céljából Minkowski tételét kívánjuk alkalmazni. Az (53) feltétel által definiált H ponthalmaz azonban egy ún. nyílt körlemez, mely konvex és az origóra nézve centrálszimmetrikus ugyan, de nem zárt, és így nem felel meg a Minkowski-tétel feltételeinek. Ezen a problémán úgy segíthetünk, hogy a H nyílt körlemezt egy kicsit kisebb sugarú, H' *zárt* körlemezzel helyettesítjük, például azzal, melyet az

(54) $x^2+y^2 \leqq 1,9p$

egyenlőtlenséget kielégítő $(x; y)$ pontok alkotnak. Az így definiált H' halmaz nyilván körlemez, mely konvex, az origóra nézve centrálszimmetrikus és zárt. E körlemez sugara $\sqrt{1,9p}$, tehát területére teljesül, hogy

(55) $(\sqrt{1,9p})^2 \cdot \pi = 1,9p \cdot \pi > 1,9p \cdot 3 = 5,7p > 4p$.

Végül (48) szerint a (49) és (50) feltételek által definiált rács alapparalelogrammájának területe

$$\Delta = |p \cdot 1 - z_0 \cdot 0| = |p| = p.$$

Ennek négyszerese, $4p$ (55) szerint kisebb H' területénél. Így a fenti rácsra és H'-re a Minkowski-tétel valamennyi feltétele teljesül, tehát a tétel alkalmazható. Ennek alapján H' tartalmaz nemtriviális rácspontot, tehát léteznek olyan x, y egész számok, melyekre (51), (52) és (54) teljesül. E feltételekből azonban — mint láttuk — következik, hogy x, y megoldása (15)-nek, és ezzel az állítást maradéktalanul igazoltuk.

6. A HÁROM- ÉS NÉGY NÉGYZETSZÁMTÉTEL. A WARING-PROBLÉMA

Az eddigiekben tisztáztuk, hogy mely természetes számok írhatók fel *két* négyzetszám összegeként. Felmerül a kérdés, hogy melyek írhatók fel *három* négyzetszám összegeként, más

szóval az

$$x^2+y^2+z^2 = n$$

diofantikus egyenlet mely n természetes számokra oldható meg? A. M. Legendre bizonyította, hogy ez a diofantikus egyenlet akkor és csak akkor oldható meg, ha n nem $4^k(8l+7)$ alakú (ahol k, l nemnegatív egész számok). A 10. példa kapcsán igazolni fogjuk, hogy ez a feltétel *szükséges* feltétele a megoldhatóságnak; az elégségesség bizonyítása lényegesen nehezebb. Legendre tétele szerint tehát végtelen sok olyan n természetes szám létezik, mely nem írható fel *három* négyzetszám összegeként. Másrészt J. L. Lagrange bizonyította, hogy *négy* négyzetszám összegeként már *bármely* n természetes szám felírható.

Ez a tétel a 2—5. pontokban tárgyalt módszerek bármelyikével igazolható (bár a két négyzetszám-tételnél komplikáltabban). A 31. és 32. feladat kapcsán olyan bizonyítást fogunk adni, mely a Thue-lemmára épül.

A továbbiakban Legendre, ill. Lagrange tételére mint három-, ill. négy négyzetszám-tételre fogunk hivatkozni.

E. Waring vetette fel a XVIII. században a következő problémát: található-e tetszőleges, 1-nél nagyobb k természetes számhoz olyan l (k-tól függő) természetes szám, hogy bármely n természetes szám felírható legfeljebb l számú k-adik hatvány összegeként, más szóval az

$$x_1^k+x_2^k+\ldots+x_l^k = n$$

diofantikus egyenlet megoldható a *nemnegatív* egész számok körében? Ezt a problémát *Waring-problémának* nevezzük. $k=2$ esetén a négy négyzetszám-tétel szerint a válasz igenlő (nevezetesen ekkor $l=4$ választható). A 11. példában pedig igazolni fogjuk J. Liouville tételét, mely szerint $k=4$ esetén is létezik a mondott tulajdonságú l szám (nevezetesen $l=53$ választható). Azt azonban csak 1909-ben sikerült D. Hilbertnek bebizonyítania, hogy a felvetett kérdésre a válasz az általános esetben is igenlő, tehát $k\geqq 2$ esetén található olyan l természetes szám, hogy bármely n természetes szám felírható legfeljebb l számú k-adik hatvány összegeként. Jelöljük az ilyen tulajdonságú l

számok legkisebbikét $g(k)$-val. Jelöljük tovább $G(k)$-val a legkisebb olyan l természetes számot, melyhez található olyan n_0 szám, hogy bármely n_0-nál nagyobb természetes szám felírható legfeljebb l számú k-adik hatvány összegeként.

A három-, ill. négy négyzetszám-tétel szerint

$$g(2) = G(2) = 4.$$

Továbbá nyilván bármely k természetes számra

$$g(k) \geqq G(k).$$

Hilbert bizonyítása nem volt alkalmas $G(k)$ felső becslésére. Az első érdemleges felső becslést $G(k)$-ra G. Hardy és J. Littlewood adták 1919-ben; nevezetesen komplex függvénytani segédeszközök felhasználásával igazolták, hogy $k \geqq 2$ esetén

$$G(k) \leqq k \cdot 2^{k-1}.$$

1934-ben I. M. Vinogradov a Hardy—Littlewood-módszert továbbfejlesztve, trigonometrikus összegek segítségével igazolta, hogy $k \geqq 2$ esetén

$$G(k) \leqq 3k(\log k + 11). \tag{56}$$

(A Hardy—Littlewood—Vinogradov-módszerre vonatkozóan l. a VII. fejezet 2. pontját.)

A 12. példában igazoljuk, hogy

$$g(k) \geqq 2^k - 1. \tag{57}$$

Ezt a becslést (56)-tal egybevetve, látható, hogy $g(k)$ általában lényegesen nagyobb $G(k)$-nál. Ez azért van így, mert ahhoz, hogy bizonyos „kis" számokat k-adik hatványok összegeként állítsunk elő, „sok" k-adik hatvány szükséges, és az n szám ilyen alakban való előállításához szükséges k-adik hatványok száma n növekedtével rohamosan csökkenő tendenciát mutat ((56) és (57) szerint a 2^k nagyságrendet elérő maximumról $k \log k$ egy konstans többszöröse alá csökken).

Lényegében az imént mondottakon múlik, hogy $g(k)$ értékét $k > 5$ esetén — a Hardy—Littlewood—Vinogradov-módszer segítségével — sikerült meghatározni; $g(4)$ és $g(5)$ értéke azonban még ma sem ismeretes.

Továbbá a 35*. feladat kapcsán igazolni fogjuk, hogy $k \geqq 2$ esetén

$$(58) \quad G(k) \geqq k.$$

Ez azt mutatja, hogy a Vinogradov által adott (56) becslés meglehetősen közel van a lehető legjobbhoz; az alsó és felső becslés közti eltérés lényegében mindössze egy $\log k$ faktor. (Valószínűnek látszik, hogy létezik olyan c pozitív állandó, hogy $k \geqq 2$ esetén $G(k) < ck$.)

J. Linnik a későbbiekben elemi úton is igazolta Hilbert tételét.

Példák

10. Bizonyítsuk be, hogy a $4^k(8l+7)$ alakú természetes számok (ahol k, l nemnegatív egész számok) nem írhatók fel három négyzetszám összegeként!

Megoldás:

Először is megjegyezzük, hogy az I. fejezet 25. feladatát felhasználva, könnyen igazolható, hogy egész szám négyzete 8-cal osztva 0, 1 vagy 4 maradékot ad (a részleteket az Olvasóra bízzuk).

Tegyük fel indirekte, hogy valamely k, l nemnegatív egész számokra $4k(8l+7)$ felírható három négyzetszám összegeként, tehát léteznek olyan x, y, z természetes számok, melyekre

$$(59) \quad x^2+y^2+z^2 = 4^k(8l+7).$$

A jobb oldal 8-cal osztva nyilván 0 vagy 4 maradékot ad. Ugyanakkor előbbi megjegyzésünk szerint a bal oldal valamennyi tagja 0, 1 vagy 4 maradékot ad 8-cal osztva; könnyen ellenőrizhető, hogy három ilyen szám összege csak akkor adhat 0 vagy 4 maradékot (8-cal osztva), ha minden egyes tag 0 vagy 4 maradékot ad, azaz x, y, z mindegyike páros. Így (59)-et egyszerűsíthetjük 4-gyel, vagyis $x_0=\frac{x}{2}$, $y_0=\frac{y}{2}$, $z_0=\frac{z}{2}$-t írva,

$$x_0^2+y_0^2+z_0^2 = 4^{k-1}(8l+7).$$

Ha itt a jobb oldalon 4 kitevője még mindig pozitív, az előbbi lépést megismételve, ismét oszthatunk 4-gyel s í. t. Végül (59)-ből következik olyan x_1, y_1, z_1 egész számok létezése, melyekre

$$(60) \quad x_1^2+y_1^2+z_1^2 = 8l+7.$$

Itt a bal oldal mindhárom tagja 0, 1 vagy 4 maradékot ad 8-cal osztva. Három ilyen szám összege azonban — mint könnyen ellenőrizhető — 8-cal osztva nem adhat 7 maradékot, tehát (60) nem állhat fenn, és így az indirekt feltevésből ellentmondásra jutottunk.

11. A

$$(61) \quad \sum_{1 \leqq i < j \leqq 4} (x_i+x_j)^4+(x_i-x_j)^4 = 6(x_1^2+x_2^2+x_3^2+x_4^2)^2$$

azonosságot és a négy négyzetszám-tételt felhasználva, igazoljuk, hogy bármely n természetes szám felírható legfeljebb 53 negyedik hatvány összegeként!

Megoldás:

Vizsgáljuk először az $n=6k^2$ (ahol k nemnegatív egész szám) alakú számokat. A négy négyzetszám-tételre tekintettel k felírható négy négyzetszám összegeként, tehát léteznek olyan x_1, x_2, x_3, x_4 egész számok, melyekre

$$k = x_1^2+x_2^2+x_3^2+x_4^2.$$

Ekkor

$$n = 6k^2 = 6(x_1^2+x_2^2+x_3^2+x_4^2)^2;$$

a kapott kifejezés megegyezik (61) jobb oldalával. A (61) bal oldalán álló összegnek azonban $\binom{4}{2}=6$ tagja van, melyek mindegyike két negyedik hatvány összege; így végeredményben $n=6k^2$ felírható $6\cdot 2=12$ negyedik hatvány összegeként.

Legyen most n tetszőleges természetes szám. n-et 6-tal osztva, legyen a hányados q, a maradék r:

$$n = 6q+r, \quad \text{ahol} \quad 0 \leqq r \leqq 5.$$

A négy négyzetszám-tétel szerint léteznek olyan k_1, k_2, k_3, k_4 nemnegatív egész számok, melyekre

$$q = k_1^2+k_2^2+k_3^2+k_4^2.$$

Ekkor

$$n = 6q+r = 6k_1^2+6k_2^2+6k_3^2+6k_4^2+r.$$

Itt az első négy tag $6k^2$ alakú, tehát az előbbiek szerint mindegyikük felírható 12 negyedik hatvány összegeként. Az utolsó tag, r pedig felírható r számú 1-es, vagyis r számú negyedik hatvány összegeként. Így végeredményben n felírható legfeljebb $4\cdot 12+r=48+r\leqq 48+5=53$ negyedik hatvány összegeként, és ezt kellett igazolnunk.

12. Igazoljuk, hogy $k\geqq 2$ esetén (57) teljesül!

Megoldás:

Nyilván elegendő igazolni, hogy az $n=2^k-1$ számot k-adik hatványok összegeként felírva, a tagok száma szükségképpen legalább 2^k-1, vagyis

(62) $\quad x_1^k+x_2^k+\ldots+x_l^k = n = 2^k-1$

(ahol $x_1, x_2, \ldots, x_l$ természetes számok) esetén szükségképpen

(63) $\quad l \geqq 2^k-1.$

Azonban (62) bal oldalán valamennyi tag csak 1-es lehet, hiszen $x_i \geqq 2$-ből $x_i^k \geqq 2^k > n$ következne, tehát (62) bal oldala nagyobb lenne a jobb oldalnál. Így (62) bal oldalán l számú 1-esnek az összege áll, tehát szükségképpen $l = n = 2^k - 1$. Ezzel (63)-at és így (57)-et is igazoltuk.

7. A PYTHAGORASZI SZÁMHÁRMASOK. A FERMAT-SEJTÉS

Ha az x, y, z természetes számok kielégítik az

(64) $x^2 + y^2 = z^2$

diofantikus egyenletet, akkor az x, y, z számokat *pythagoraszi számhármasnak* mondjuk. Az

$$x^2 = z^2 - y^2 = (z-y)(z+y)$$

átalakításból kiindulva, igazolható, hogy a (64) diofantikus egyenlet *alapmegoldásai*, vagyis az $(x_0, y_0, z_0) = 1$ feltételt kielégítő x_0, y_0, z_0 megoldások, az ún. *primitív pythagoraszi számhármasok* a következő alakban adhatók meg:

(65) $x_0 = 2mn, \quad y_0 = m^2 - n^2, \quad z_0 = m^2 + n^2,$

ahol m, n természetes számok, melyekre

(66) $m > n,$

(67) $(m, n) = 1,$

(68) $m \not\equiv n \pmod 2$

teljesül. Ha x_0-t és y_0-t felcseréljük, nyilván ismét alapmegoldást kapunk; igazolható, hogy az említetteken kívül több alapmegoldás nincs.

Megjegyezzük, hogy a

(69) $(2mn)^2 + (m^2 - n^2)^2 = (m^2 + n^2)^2$

azonosság értelmében a (65) alatti x_0, y_0, z_0 számhármas (66) teljesülése esetén — a (67) és (68) feltételektől függetlenül — nyilván pythagoraszi számhármast alkot; a (67) és (68) feltételek csupán $(x_0, y_0, z_0) = 1$ garantálásához szükségesek.

Minthogy a (64) diofantikus egyenlet homogén, a fent leírt alapmegoldásokon kívül pythagoraszi számhármast alkotnak az $x=x_0t$, $y=y_0t$, $z=z_0t$ alakú számhármasok is, ahol x_0, y_0, z_0 alapmegoldás, és $t=1, 2, 3, \ldots$; ezeken kívül több pythagoraszi számhármas nem létezik.

A (64) diofantikus egyenlet általánosításaként vizsgálható az

$$(70) \quad x^k+y^k = z^k$$

diofantikus egyenlet, ahol k adott — 1-nél nagyobb — természetes szám. Ennek az egyenletnek nyilván végtelen sok olyan megoldása van, melyre $xyz=0$ teljesül; az ilyen megoldásokat triviális, az $xyz\neq 0$ feltételt kielégítőket *nemtriviális megoldásoknak* nevezzük. P. Fermat a XVII. században azt sejtette, hogy a (70) egyenletnek $k\geqq 3$ esetén nincs nemtriviális megoldása. Ez az ún. *Fermat-sejtés* ebben az általánosságban azóta is bebizonyítatlan, csupán bizonyos részeredmények születtek.

Először is megjegyezzük, hogy a Fermat-sejtés igazolásához elegendő lenne belátni, hogy a Fermat-sejtés igaz akkor, ha $k=4$ vagy k (2-nél nagyobb) prímszám (l. a 14. példát). A $k=4$ speciális esetben a Fermat-sejtés a descente infinie módszerrel igazolható, felhasználva a pythagoraszi számhármasok fent adott explicit előállítását. (Ha ugyanis $k=4$ esetén az x, y, z természetes számok kielégítik a (70) Fermat-egyenletet, akkor x^2, y^2, z^2 nyilván pythagoraszi számhármast alkotnak.)

A $k=3$ speciális esetben pedig abból indulhatunk ki, hogy ekkor a (70) Fermat-egyenlet bal oldala az Euler-egészek körében a következőképpen alakítható szorzattá:

$$x^3+y^3 = (x+y)(x+\eta y)(x+\eta^2 y) = (x+y)(x+\eta y)[(x-y)-\eta y].$$

$\left(\text{ahol } \eta=-\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)$. Így célszerű (70)-et $K(\eta)$-beli egyenletként felfogni. Ezen az úton valóban eljuthatunk a Fermat-sejtés $k=3$ speciális esetének igazolásához.

Ha most $k=p$ 3-nál nagyobb prímszám, akkor a $k=3$ speciális eset analógiájára azzal próbálkozhatnánk, hogy a p-edik primitív egységgyökök valamelyikét ε-nal jelölve, (70)-et $K(\varepsilon)$-beli egyenletként fogjuk fel. Ekkor azonban felmerül egy olyan nehézség, melyre a 4. pontban már utaltunk; nevezetesen az, hogy $K(\varepsilon)$-ben nem igaz a számelmélet alaptételének analogonja. E nehézség áthidalásával próbálkozva jutott el 1847-ben E. E. Kummer — éppen a Fermat-sejtés kapcsán — az ideálelmélet kialakításáig (melyre a 4. pontban már utaltunk). Így az algebrai számelmélet tulajdon-

képpen a Fermat-sejtés kapcsán alakult ki. Azóta az algebrai számelmélet módszereinek segítségével sikerült a Fermat-sejtést igen sok speciális esetre bebizonyítani, így például minden olyan k kitevőre, melyre $k \leqq 2000$ teljesül. Az általános esetben azonban — mint említettük — a sejtés még ma is bebizonyítatlan.

Példák

13. Bizonyítsuk be, hogy ha a 2-nél nagyobb természetes szám, akkor létezik olyan pythagoraszi számhármas, melynek egyik eleme a.

Megoldás:

Ha a 2-nél nagyobb páros szám, akkor legyen $m=\frac{a}{2}$, $n=1$; ha viszont a 1-nél nagyobb páratlan szám, akkor legyen $m=\frac{a+1}{2}$, $n=\frac{a-1}{2}$. Definiáljuk az x_0, y_0, z_0 számokat (65) által. Ekkor az előbbi esetben

$$x_0 = 2mn = 2\cdot\frac{a}{2}\cdot 1 = a,$$

míg az utóbbiban

$$y_0 = m^2-n^2 = \left(\frac{a+1}{2}\right)^2-\left(\frac{a-1}{2}\right)^2 = \frac{a^2+2a+1}{4}-\frac{a^2-2a+1}{4} = a,$$

továbbá (66) nyilván teljesül, tehát — a (69) azonosságra tekintettel — x_0, y_0, z_0 pythagoraszi számhármast alkotnak.

14. Bizonyítsuk be, hogy ha a Fermat-sejtés igaz abban a speciális esetben, amikor $k=4$ vagy k 2-nél nagyobb prímszám, akkor ebből következik, hogy a Fermat-sejtés tetszőleges k természetes számra igaz!

Megoldás:

Tegyük fel indirekte, hogy létezik olyan k természetes szám, melyre

(71) $k \geqq 3$

teljesül, és a (70) egyenletnek létezik x_0, y_0, z_0 nemtriviális megoldása, vagyis

(72) $x_0^k+y_0^k = z_0^k$,

(73) $x_0y_0z_0 \neq 0$.

Ha k nem osztható 4-gyel, akkor $2l+1$ vagy $2(2l+1)$ alakú. (71)-ből mindkét esetben következik, hogy $2l+1>1$; így $2l+1$-nek van legalább egy p prímosztója, mely szükségképpen páratlan prím, tehát 2-nél nagyobb. k tehát vagy 4-gyel vagy egy ilyen p prímmel osztható, vagyis $k=dt$ alakban írható, ahol $d=4$ vagy d 2-nél nagyobb prímszám. Ekkor (72) a követ-

kező alakban írható:

$$(x_0^t)^d + (y_0^t)^d = (z_0^t)^d.$$

Továbbá (73)-ból nyilván következik, hogy

$$(x_0^t)(y_0^t)(z_0^t) \neq 0.$$

Így $k=d$ esetén $x=x_0^t$, $y=y_0^t$, $z=z_0^t$ nemtriviális megoldása lenne a (70) Fermat-egyenletnek, holott feltevésünk szerint ezekben az esetekben nem létezik nemtriviális megoldás. Így az indirekt feltevésből ellentmondásra jutottunk, és ezzel az állítást igazoltuk.

FELADATOK

1. Határozzuk meg az

$$x^2 - 4y^2 = 116$$

diofantikus egyenlet pozitív egész megoldásait!

2. Keressük meg az

$$x^3 + y^3 + z^3 = u^3$$

egyenlet összes olyan megoldását, ahol x, y, z és u ($x<y<z<u$) egymást követő egész számok!

3. Legyen p 2-nél nagyobb prímszám. Határozzuk meg az

$$\frac{1}{x} + \frac{1}{y} = \frac{2}{p}$$

egyenlet pozitív egész megoldásait!

4. Keressük meg az

$$\frac{x}{y} + \frac{y}{z} + \frac{z}{x} = 3$$

egyenlet pozitív egész megoldásait!

5*. Keressük meg az

$$(x+y+z)^3 = x^3 + y^3 + z^3$$

egyenlet egész megoldásait!

6. Bizonyítsuk be, hogy nem léteznek olyan x, y, z egész számok, melyekre

$$x^2+9y^2-2z^2 = 3.$$

7*. Bizonyítsuk be, hogy az

$$x^2+y^2+z^2 = 2xyz$$

diofantikus egyenletnek nincs nemtriviális ($x=y=z=0$-tól különböző) megoldása!

8*. Bizonyítsuk be, hogy a

$$4xy-x-y = z^2$$

diofantikus egyenlet megoldhatatlan a természetes számok körében, de végtelen sok megoldása van a negatív egész számok körében!

9. Határozzuk meg az

$$x!+y! = z!$$

egyenlet pozitív egész megoldásait!

10*. Bizonyítsuk be, hogy az

$$x!y! = z!$$

egyenletnek végtelen sok olyan megoldása van, ahol x, y és z 1-nél nagyobb természetes számok!

11. Legyen D olyan természetes szám, mely nem négyzetszám. Bizonyítsuk be, hogy ha az x_0, y_0 egész számok kielégítik az

$$(74) \quad x^2-Dy^2 = 1$$

diofantikus egyenletet, akkor az

$$(75) \quad u+v\sqrt{D} = (x_0+y_0\sqrt{D})^n \quad (n = 1, 2, \ldots)$$

feltétellel definiált u, v egész számok is!

Megjegyezzük, hogy a (74) egyenletet *Pell-egyenletnek* nevezzük. Igazolható, hogy a (74) Pell-egyenletnek bármely — négyzetszámtól különböző — D természetes számra van nemtriviális, azaz $x=\pm 1$, $y=0$-tól különböző megoldása. Innen viszont e feladat alapján következik *végtelen sok* megoldás létezése.

12. Tudva azt, hogy $7^2+3^2=58$ és $6^2+7^2=85$, írjuk fel a 4930 ($=58\cdot 85$) számot két négyzetszám összegeként!

13. Bizonyítsuk be, hogy ha az

$$(76)\quad x^2+2y^2=n$$

(ahol n természetes szám) diofantikus egyenlet megoldható, akkor szükségképpen $n=1$, vagy pedig n kanonikus alakjában valamennyi $8k-1$ és $8k-3$ alakú prímszám kitevője páros szám!

14. Bizonyítsuk be, hogy ha két természetes szám felírható x^2+2y^2 alakban, akkor a szorzatuk is felírható ilyen alakban!

15*. Igazoljuk a Thue-lemma $n=1$ speciális esetét!

16*. Bizonyítsuk be a Thue-lemma segítségével, hogy ha a p prímszám $8k+1$ vagy $8k+3$ alakú, akkor felírható x^2+2y^2 alakban!

17. Állapítsuk meg, hogy teljesülnek-e az

a. $1-i|5+7i$,

b. $2-i|4+7i$

oszthatósági relációk?

18. Igazoljuk, hogy a Gauss-egészek körében elvégezhető a maradékos osztás (l. a 4. pont *D)* állítását)!

19. Határozzuk meg az $\alpha=6+6i$, $\beta=5+3i$ Gauss-egészek legnagyobb közös osztóját!

20*. Bizonyítsuk be, hogy az

$$x^2+1=y^3$$

diofantikus egyenlet egyetlen megoldása $x=0$, $y=1$.

21*. Igazoljuk a 16*. feladat állítását $K(i\sqrt{2})$ vizsgálata révén!

22. Határozzuk meg a $K(i\sqrt{5})$-beli egységeket (azaz, $K(i\sqrt{5})$ azon elemeit, melyek $K(i\sqrt{5})$ bármely elemének osztói)!

23. $K(i\sqrt{5})$ valamely 0-tól és egységtől különböző elemét *felbonthatatlannak* nevezzük, ha nem írható fel $K(i\sqrt{5})$ két, egységtől különböző elemének szorzataként. Igazoljuk, hogy a 6 szám két, lényegesen — nem csupán egység tényezőkben vagy sorrendben — különböző módon is felírható ($K(i\sqrt{5})$-ben) felbonthatatlan számok szorzataként!

Megjegyezzük, hogy „prím" helyett „felbonthatatlant" mondtunk, ugyanis most a szokásos értelemben nem beszélhetünk prímszámokról.

24*. Adjunk Minkowski tételének segítségével új bizonyítást a 16*. feladat állítására!

25*. Jelöljük a (12) diofantikus egyenlet megoldásszámát $r(n)$-nel ($n=0, 1, 2, \ldots$). Bizonyítsuk be, hogy létezik olyan c pozitív állandó, hogy $N \geqq 1$ esetén

$$\left|\sum_{n \leqq N} r(n) - \pi N\right| < cN.$$

Megjegyezzük, hogy a bal oldalon álló kifejezés nagyságrendjének vizsgálata — a III. fejezet 9. példája kapcsán említett Dirichlet-féle osztóproblémához hasonlóan — igen fontos szerepet játszik a számelméletben.

26. Mutassunk példát a következőre: előfordulhat, hogy két természetes szám külön-külön felírható három négyzetszám összegeként, de a szorzatuk nem!

27. Bizonyítsuk be (a három négyzetszámtételt felhasználva), hogy végtelen sok olyan n természetes szám létezik, mely felírható három négyzetszám összegeként, de háromnál kevesebb négyzetszám összegeként nem!

28*. Bizonyítsuk be (a három négyzetszámtételt felhasználva), hogy az

$$x^2 + y^2 + 2z^2 = n$$

(ahol n adott természetes szám) diofantikus egyenlet akkor és csak akkor oldható meg, ha n nem $2^{2k+1}(8l+7)$ alakú szám, ahol k, l nemnegatív egész számok!

29. Legyen k tetszőleges természetes szám. Írjuk fel az

$$x^2 + y^2 + z^2 + u^2 = 15 \cdot 2^k$$

diofantikus egyenlet legalább egy megoldását!

30. Az (Eulertől származó)

$$(77) \quad (a^2+b^2+c^2+d^2)(x^2+y^2+z^2+u^2) = (ax+by+cz+du)^2 + \\ + (ay-bx+cu-dz)^2 + (az-bu-cx+dy)^2 + \\ + (au+bz-cy-dx)^2$$

azonosságot felhasználva, írjuk fel a

$$4331 = 61 \cdot 71 = (2^2+4^2+4^2+5^2)(1^2+3^2+5^2+6^2)$$

számot négy négyzetszám összegeként!

31. Legyen p tetszőleges prímszám. Bizonyítsuk be, hogy léteznek olyan x_0, y_0 egész számok, melyekre

$$(78) \quad x_0^2+y_0^2+1 \equiv 0 \pmod{p}.$$

32*. Az előző feladat állítását és a Thue-lemma $n=2$ speciális esetét felhasználva, igazoljuk, hogy bármely p prímszám felírható négy négyzetszám összegeként!

Megjegyezzük, hogy innen a (77) azonosság alapján következik, hogy *bármely* természetes szám felírható négy négyzetszám összegeként.

33*. Bizonyítsuk be (a négy négyzetszám-tételt felhasználva), hogy

a. minden 8-cal osztható természetes szám felírható nyolc páratlan négyzetszám összegeként;

b. egyetlen 8-cal osztható természetes szám sem írható fel nyolcnál kevesebb páratlan négyzetszám összegeként!

34*. Bizonyítsuk be, hogy

a. $g(3) \geqq 9$,

b. $g(4) \geqq 19$.

35*. Bizonyítsuk be, hogy $k=2, 3, \ldots$ esetén (58) teljesül!

36. Adjunk meg olyan pythagoraszi számhármast, melynek egyik eleme 198.

37. Bizonyítsuk be, hogy nem létezik olyan *primitív* pythagoraszi számhármas, melynek egyik eleme 198!

38. Bizonyítsuk be, hogy ha x, y és z pythagoraszi számhármast alkotnak, akkor xyz osztható 5-tel!

39. Bizonyítsuk be (anélkül, hogy hivatkoznánk arra, hogy a Fermat-sejtés $k=3$ esetén már bizonyított), hogy a (70) Fermat-egyenletnek $k=3$ esetén nincs olyan megoldása, ahol x, y, z (ebben a sorrendben) egymást követő egész számok!

40. Bizonyítsuk be, hogy az

$$x^{15}+y^{27} = z^{33}$$

diofantikus egyenlet megoldhatatlan a természetes számok körében!

41. Bizonyítsuk be, hogy $k>2$ esetén a (70) Fermat-egyenletnek nincs olyan megoldása, ahol x, y és z is (pozitív) prímszámok!

42*. Bizonyítsuk be, hogy az

$$x^3+y^3 = z^3+1$$

diofantikus egyenletnek végtelen sok megoldása van a természetes számok körében!

AZ V. FEJEZETBEN KITŰZÖTT FELADATOK MEGOLDÁSAI

1. A bal oldalon szorzattá alakítva:

$$(x-2y)(x+2y) = 116.$$

Így

(79) $x-2y = d_1,$

(80) $x+2y = d_2$

116-nak olyan osztói, melyekre

(81) $d_1 d_2 = 116,$

(82) $0 < d_1 < d_2 \leqq 116$

teljesül. Továbbá (80)-ból kivonva (79)-et és 4-gyel osztva:

(83) $y = \dfrac{d_2-d_1}{4}.$

Így szükségképpen

(84) $4 | d_2-d_1.$

A $116=2^2\cdot 29$ szám azonban csak egyféleképpen írható fel a (81) alakban úgy, hogy (82) és (84) is teljesüljön, nevezetesen $d_1=2$ és $d_2=2\cdot 29=58$. Ekkor (83)-ból

$$y = \frac{58-2}{4} = \frac{56}{4} = 14$$

és (79)-ből

$$x = 2y+d_1 = 2\cdot 14+2 = 30.$$

2. x, z, u-t kifejezve y-nal:

(85) $x = y-1, \quad z = y+1, \quad u = y+2.$

Így a vizsgált egyenlet a következő alakra hozható:

$$(y-1)^3+y^3+(y+1)^3 = (y+2)^3,$$

$$(y^3-3y^2+3y-1)+y^3+(y^3+3y^2+3y+1) = y^3+6y^2+12y+8,$$

$$3y^3+6y = y^3+6y^2+12y+8,$$

$$2y^3-6y^2-6y-8 = 0,$$

$$y^3-3y^2-3y-4 = 0. \tag{86}$$

Ismeretes, hogy egy egész együtthatós polinom egész gyökei a konstans tag osztói közül kerülnek ki. Így itt $y|-4$, tehát y lehetséges értékei $y=-4, -2, -1, +1, +2, +4$. Sorra (86)-ba helyettesítve, nyerjük, hogy csak $y=+4$ gyök. Továbbá ekkor (85)-ből adódik, hogy $x=3$, $z=5$, $u=6$.

3. Mindkét oldalt $2pxy$-nal szorozva, a vizsgált egyenlet a következő alakra hozható:

$$2py+2px = 4xy.$$

Adjunk mindkét oldalhoz p^2-ct:

$$4xy-2px-2py+p^2 = p^2,$$

$$(2x-p)(2y-p) = p^2.$$

Így $2x-p$ osztója p^2-nek, tehát

$$2x-p = \pm 1, \pm p \quad \text{vagy} \quad \pm p^2,$$

míg y megfelelő értékeire

$$2y-p = \pm p^2, \pm p, \quad \text{ill.} \quad \pm 1$$

adódik. Innen x-et és y-t kifejezve, három pozitív egész megoldást nyerünk:

$$x_1 = \frac{p+1}{2}, \quad y_1 = \frac{p^2+p}{2}; \quad x_2 = y_2 = p; \quad x_3 = \frac{p^2+p}{2},$$

$$y_3 = \frac{p+1}{2}.$$

4. A számtani és mértani közép közti egyenlőtlenség szerint, tetszőleges x, y, z pozitív számokra

$$\frac{\frac{x}{y}+\frac{y}{z}+\frac{z}{x}}{3} \geqq \sqrt[3]{\frac{x}{y}\cdot\frac{y}{z}\cdot\frac{z}{x}} = \sqrt[3]{1} = 1,$$

vagyis

$$\frac{x}{y}+\frac{y}{z}+\frac{z}{x} \geqq 3,$$

és itt egyenlőség akkor és csak akkor áll, ha a három szám egyenlő:

$$(87) \qquad \frac{x}{y}=\frac{y}{z}=\frac{z}{x}=k,$$

ahol k alkalmas pozitív szám. Innen

$$k^3=\frac{x}{y}\cdot\frac{y}{z}\cdot\frac{z}{x}=1,$$

ahonnan $k=1$ következik. Így (87)-ből $x=y=z$; másrészt, ha az x, y, z pozitív egész számok egyenlők, akkor nyilván kielégítik az adott diofantikus egyenletet.

5*. Átrendezve és szorzattá a akítva:

$$(x+y+z)^3-(x^3+y^3+z^3)=3(x+y)(y+z)(z+x)=0.$$

Innen látható, hogy az x, y, z (egész számokból álló) számhármas akkor és csak akkor megoldás, ha a három szám közt van két olyan, melyek egymás ellentettjei (míg a harmadik szám tetszőleges).

6. Tegyük fel indirekte, hogy létezik x_0, y_0, z_0 megoldás, vagyis

$$(88) \qquad x_0^2+9y_0^2-2z_0^2=3.$$

Innen következik, hogy

$$x_0^2+9y_0^2-2z_0^2 \equiv 3 \pmod 3,$$

$$(89) \qquad x_0^2+z_0^2 \equiv 0 \pmod 3.$$

Ha valamely u egész szám osztható 3-mal, vagyis 0-val kongruens modulo 3, akkor u^2 is 0-val kongruens modulo 3; ha viszont u nem osztható 3-mal, vagyis ± 1-gyel kongruens modulo 3, akkor u^2 1-gyel kongruens modulo 3. Így (89) bal oldalán mindkét tag 0-val vagy 1-gyel kongruens modulo 3. Innen nyilván következik, hogy (89) csak úgy teljesülhet, ha

$$x_0^2 \equiv z_0^2 \equiv 0 \pmod 3,$$

következésképpen $3|x_0$ és $3|z_0$. Ekkor azonban a (88) bal oldalán álló összeg mindhárom tagja és így maga az összeg is osztható 9-cel, míg a jobb oldal nem osztható 9-cel. Az indirekt feltevésből tehát ellentmondásra jutottunk, és ezzel az állítást igazoltuk.

7*. Tegyük fel indirekte, hogy létezik x_0, y_0, z_0 nemtriviális megoldás:

$$(90) \qquad x_0^2+y_0^2+z_0^2=2x_0y_0z_0$$

és $x_0y_0z_0 \neq 0$. Ez utóbbiból következik, hogy x_0, y_0, z_0 a következő alakban írhatók: $x_0=2^kx_1$, $y_0=2^ky_1$, $z_0=2^kz_1$, ahol k nemnegatív egész szám, és x_1, y_1, z_1 közül legalább az egyik páratlan szám. (90)-be helyettesítve:

$$(2^kx_1)^2+(2^ky_1)^2+(2^kz_1)^2 = 2(2^kx_1)(2^ky_1)(2^kz_1),$$

vagyis 2^{2k}-val osztva:

$$x_1^2+y_1^2+z_1^2 = 2^{k+1}x_1y_1z_1.$$

Itt a jobb oldal páros, tehát a bal oldalnak is párosnak kell lennie. Így az $x_1^2+y_1^2+z_1^2$ összeg páros, és legalább egy tagja páratlan; következésképpen x_1, y_1, z_1 közül az egyik — mondjuk x_1 — páros, és a másik kettő — tehát y_1, z_1 — páratlan. Ekkor x_1^2 0-val, y_1^2 és z_1^2 — az I. fejezet 20. feladatára tekintettel — 1-gyel kongruens modulo 4, tehát a bal oldal $0+1+1=2$-vel kongruens modulo 4. Ugyanakkor a jobb oldalon két páros tényező van — 2 és x_1 —, tehát a jobb oldal 0-val kongruens modulo 4. Így az indirekt feltevésből ellentmondásra jutottunk, és ezzel az állítást igazoltuk.

8*. Mindkét oldalt 4-gyel szorozva, majd mindkét oldalhoz 1-et adva:

$$16xy-4x-4y+1 = 4z^2+1,$$

vagyis

$$(4x-1)(4y-1) = (2z)^2+1.$$

Ha x, y természetes számok, akkor a bal oldalon mindkét tényező 1-nél nagyobb páratlan szám, tehát felírható páratlan prímszámok szorzataként. Ezek mindegyike nem lehet $4k+1$ alakú, hiszen akkor a szorzatuk is ilyen alakú lenne. Így a bal oldalnak van $4k-1$ alakú prímosztója. Ugyanakkor a II. fejezet 91. feladata szerint a jobb oldal valamennyi prímosztója $4k+1$ alakú. Így az adott egyenlet valóban megoldhatatlan a természetes számok körében.

Másrészt az adott egyenletnek végtelen sok olyan x, y, z egész megoldása van, melyre $x=-1$ teljesül; így például $x=-1$, $y=-5n^2-2n$, $z=5n+1$ (ahol n tetszőleges egész szám) megoldás.

9. Nyilván elegendő azon x, y, z megoldásokat meghatározni, melyekre $x \leqq y < z$ teljesül (ezekből ugyanis x és y felcserélésével megkapjuk az összes megoldást). Átrendezve:

$$(91) \qquad x! = z!-y! = y![(y+1)(y+2)\dots z-1].$$

Ha $y>x$, akkor $x!$-sal osztva, a következőt nyerjük:

$$1 = (x+1)(x+2)\dots y[(y+1)(y+2)\dots z-1].$$

Innen nyilván következik, hogy $y|1$, másrészt $1 \leqq x < y$-ra tekintettel $y \geqq 2$; y azonban e két feltételt egyidejűleg nem elégítheti ki. Így csak $x=y$ lehet-

séges. Ekkor (91)-et $x!$-sal osztva, a következőt nyerjük:

$$1 = \frac{y!}{x!}\left((y+1)(y+2)\dots z-1\right) = (x+1)(x+2)\dots z-1,$$

$$(x+1)(x+2)\dots z = 2.$$

Ha $x>1$, akkor a bal oldal első tényezője és így az egész bal oldal is nagyobb lenne 2-nél, vagyis a jobb oldalnál. Így csak $x=1$ lehetséges. Továbbá a bal oldalon csak egyetlen tényező szerepelhet, vagyis $x+1=z=2$, hiszen ellenkező esetben a bal oldal ismét nagyobb lenne a jobb oldalnál. Végeredményben tehát az egyetlen lehetséges megoldás $x=y=1$, $z=2$; behelyettesítéssel ellenőrizhető, hogy e számhármas valóban megoldás.

10*. Ellenőrizhető, hogy $x=n!-1$, $y=n$, $z=n!$ (ahol $n=2, 3, \dots$) megoldás. Nem tudunk arról, hogy a fentiekből x és y felcserélésével keletkező megoldásokon, valamint az $x=6$, $y=7$, $z=10$ megoldáson kívül van-e az egyenletnek további megoldása.

11. Minthogy $x=x_0$, $y=y_0$ megoldás, ezért

$$x_0^2 - Dy_0^2 = 1. \tag{92}$$

Ha D nem négyzetszám, akkor $\sqrt{D}$ irracionális szám (l. az I. fejezet 16. példájához fűzött megjegyzést). Ebből viszont nyilván következik, hogy ha $a_1+b_1\sqrt{D}=a_2+b_2\sqrt{D}$ (ahol a_1, a_2, b_1, b_2 egész számok), akkor szükségképpen $a_1=a_2$, $b_1=b_2$. Más szóval, egy $a+b\sqrt{D}$ alakú szám egyértelműen írható fel ilyen alakban. Így (75)-ből a binomiális tételre tekintettel könnyen következik, hogy

$$u-v\sqrt{D} = (x_0-y_0\sqrt{D})^n. \tag{93}$$

(75)-öt és (93)-at összeszorozva:

$$(u+v\sqrt{D})(u-v\sqrt{D}) = [(x_0+y_0\sqrt{D})(x_0-y_0\sqrt{D})]^n,$$

vagyis (92)-re tekintettel

$$u^2-Dv^2 = (x_0^2-Dy_0^2)^n = 1^n = 1,$$

tehát u, v valóban megoldása (74)-nek.

12. A (14) azonosságot alkalmazva $a=7$, $b=3$, $x=6$, $y=7$ választással:

$$4930 = 58\cdot 85 = (7^2+3^2)(6^2+7^2) = (7\cdot 6+3\cdot 7)^2+(7\cdot 7-3\cdot 6)^2 =$$

$$= 63^2+31^2.$$

13. A II. fejezet 90*. és 93*. feladatából kiindulva, ugyanúgy okoskodhatunk, mint ahogyan a 2. pont elején a II. fejezet 92*. feladatából kiindulva levezettük (12) megoldhatóságának szükséges feltételét; a részletek kidolgozását az Olvasóra bízzuk.

14. Az állítás következik az

$$(a^2+2b^2)(x^2+2y^2) = (ax+2by)^2+2(ay-bx)^2$$

azonosságból.

15*. Legyen

$$f(x, y) = ax-y.$$

Írjuk itt x helyére az $x=1, 2, \ldots, u$ számokat, y helyére az $y=1, 2, \ldots, v$ értékeket. Így uv számú helyettesítési értéket nyerünk; nyilván ezek mindegyike egész szám. Minthogy (35) szerint uv nagyobb p-nél, e helyettesítési értékek száma p-nél nagyobb. Van tehát köztük két olyan — mondjuk az $x=x_1$, $y=y_1$-nek, ill. az $x=x_2$, $y=y_2$-nek megfelelő —, melyek ugyanabba a maradékosztályba esnek modulo p:

$$f(x_1, y_1) \equiv f(x_2, y_2) \pmod{p},$$

vagyis

$$ax_1-y_1 \equiv ax_2-y_2 \pmod{p},$$

$$a(x_1-x_2) \equiv y_1-y_2 \pmod{p}.$$

Így $x=x_1-x_2$-t, $y=y_1-y_2$-t választva, (36) teljesül. Könnyen ellenőrizhető, hogy x, y ilyen választása mellett (37) és (38) is teljesül.

16*. A II. fejezet 93*. feladata szerint, ha p a mondott alakú prímszám, akkor létezik olyan z_0 egész szám, melyre

$$z_0^2+2 \equiv 0 \pmod{p}. \tag{94}$$

Alkalmazzuk a Thue-lemma $n=1$ speciális esetét $a=z_0$, $u=v=[\sqrt{p}]+1$ választással (ekkor a (35) feltétel nyilván teljesül). Azt kapjuk, hogy léteznek olyan x_1, y_1 egész számok, melyekre

$$z_0x_1 \equiv y_1 \pmod{p}, \tag{95}$$

$$0 < |x_1| < [\sqrt{p}]+1, \quad |y_1| < [\sqrt{p}]+1 \tag{96}$$

teljesül. (94) és (95) szerint

$$2x_1^2+y_1^2 \equiv 2x_1^2+(z_0x_1)^2 = x_1^2(2+z_0^2) \equiv 0 \pmod{p}, \tag{97}$$

továbbá (96)-ra tekintettel

$$0 < 2x_1^2+y_1^2 < 2([\sqrt{p}]+1)^2+([\sqrt{p}]+1)^2 < 2(\sqrt{p})^2+(\sqrt{p})^2 = 3p. \tag{98}$$

(97)-ből és (98)-ból következik, hogy

$$2x_1^2+y_1^2 = p \tag{99}$$

vagy

(100) $2x_1^2+y_1^2 = 2p.$

Ha (99) teljesül, akkor $x=y_1$, $y=x_1$-et írva,

(101) $x^2+2y^2 = p,$

tehát ekkor készen vagyunk. Ha viszont (100) teljesül, akkor (100) jobb oldala és a bal oldal első tagja is páros, tehát a második tagnak, y_1^2-nek is párosnak kell lennie, vagyis $\frac{y_1}{2}$ egész szám. Így (100)-at 2-vel osztva:

$$x_1^2+2\cdot\left(\frac{y_1}{2}\right)^2 = p$$

$\left(\text{ahol } \frac{y_1}{2} \text{ egész szám}\right)$, tehát (101) most $x=x_1$, $y=\frac{y_1}{2}$ választással teljesül.

17.

a. $$\frac{5+7i}{1-i} = \frac{(5+7i)(1+i)}{(1-i)(1+i)} = \frac{-2+12i}{2} = -1+6i.$$

b. $$\frac{4+7i}{2-i} = \frac{(4+7i)(2+i)}{(2-i)(2+i)} = \frac{1+18i}{5} = \frac{1}{5}+\frac{18}{5}i.$$

Az előbbi hányados Gauss-egész, míg az utóbbi nem, tehát az *a.* osztható-sági reláció teljesül, míg a *b.* reláció nem.

18. Legyen α tetszőleges, β pedig 0-tól különböző Gauss-egész, és legyen $\frac{\alpha}{\beta}=a+bi$ (ahol a, b valós számok). Jelöljük az a-hoz legközelebbi egész számot m-mel, a b-hez legközelebbit n-nel. Ekkor tehát

(102) $|a-m| \leqq \frac{1}{2}, \qquad |b-n| \leqq \frac{1}{2}.$

Legyen továbbá $\gamma=m+ni$ és $\delta=\alpha-\beta\gamma$. Ekkor (102)-re tekintettel

$$N(\delta) = |\delta|^2 = |\alpha-\beta\gamma|^2 = |\beta|^2\left|\frac{\alpha}{\beta}-\gamma\right|^2 =$$

$$= N(\beta)|(a+bi)-(m+ni)|^2 = N(\beta)|(a-m)+(b-n)i|^2 =$$

$$= N(\beta)\left((a-m)^2+(b-n)^2\right) \leqq N(\beta)\left(\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2\right) = \frac{1}{2}N(\beta),$$

ahonnan következik (44).

19. $$\frac{\alpha}{\beta}=\frac{6+6i}{5+3i}=\frac{(6+6i)(5-3i)}{(5+3i)(5-3i)}=\frac{48+12i}{34}=\frac{24}{17}+\frac{6}{17}i.$$

A $\frac{24}{17}$-hez legközelebbi egész szám az 1, a $\frac{6}{17}$-hez legközelebbi a 0, legyen tehát $\gamma_1=1+0\cdot i=1$ és

$$\delta_1=\alpha-\beta\gamma_1=(6+6i)-(5+3i)\cdot 1=1+3i.$$

Az előbbi osztót, β-t az előbbi maradékkal, δ_1-gyel osztva:

$$\frac{\beta}{\delta_1}=\frac{5+3i}{1+3i}=\frac{(5+3i)(1-3i)}{(1+3i)(1-3i)}=\frac{14-12i}{10}=\frac{7}{5}-\frac{6}{5}i.$$

A $\frac{7}{5}$-höz, ill. $-\frac{6}{5}$-höz legközelebbi egész szám 1, ill. -1, legyen tehát $\gamma_2=1-i$ és

$$\delta_2=\beta-\varrho_1\gamma_2=(5+3i)-(1+3i)(1-i)=1+i.$$

Az előbbi osztót, δ_1-et az előbbi maradékkal, δ_2-vel osztva:

$$\frac{\delta_1}{\delta_2}=\frac{1+3i}{1+i}=\frac{(1+3i)(1-i)}{(1+i)(1-i)}=\frac{4+2i}{2}=2+i.$$

A hányados Gauss-egész, tehát a maradék 0. Így a legnagyobb közös osztó az előző osztás maradéka:

$$(\alpha,\beta)=\delta_2=1+i.$$

20*. Ha x páratlan szám, akkor — az I. fejezet 20. feladata alapján — a bal oldal $8k+2$ alakú szám, tehát 2-vel osztható, de 4-gyel nem; ekkor azonban — az I. fejezet 16. példájára tekintettel — nem lehet köbszám. Így ha $x=x_0$, $y=y_0$ megoldás, vagyis

(103) $$x_0^2+1=y_0^3,$$

akkor x_0 szükségképpen páros szám. A bal oldal a Gauss-egészek körében szorzattá alakítható:

(104) $$(x_0+i)(x_0-i)=y_0^3.$$

Legyen $\delta=(x_0+i, x_0-i)$. Ekkor δ osztója a két szám különbségének:

$$\delta\,|\,(x_0+i)-(x_0-i)=2i.$$

Minthogy δ osztója x_0+i-nek és $2i$-nek, osztója e két szám lineáris kombinációinak is, tehát

$$\delta|(x_0+i)+\frac{x_0 i}{2}\cdot 2i = (x_0+i)-x_0 = i.$$

A legnagyobb közös osztó tehát

(105) $(x_0+i, x_0-i) = 1.$

(104)-ből és (105)-ből következik, hogy mind x_0+i, mind x_0-i Gauss-egész harmadik hatványa (ez egyrészt abból következik, hogy a Gauss-egészek körében igaz a számelmélet alaptételének analogonja, másrészt a Gauss-egységek mindegyike felírható egy másik Gauss-egység köbeként). Így létezik olyan $\gamma=u+vi$ Gauss-egész, melyre

(106) $x_0+i = \gamma^3 = (u+vi)^3 = (u^3-3uv^2)+(3u^2v-v^3)i.$

Ha két komplex szám egyenlő, akkor képzetes részeik is egyenlők, tehát

$$1 = 3u^2v-v^3 = v(3u^2-v^2).$$

Innen következik, hogy

$$v = 3u^2-v^2 = 1$$

vagy pedig

(107) $v = 3u^2-v^2 = -1.$

Az előbbi esetben azonban

$$3u^2 = v^2+1 = 1+1 = 2;$$

az innen u-ra adódó értékek nem egész számok. Így szükségképpen (107) teljesül, ahonnan

$$3u^2 = v^2-1 = (-1)^2-1 = 0,$$

tehát $u=0$ és $\gamma=u+vi=0+(-1)i=-i$. Így (106)-ból

$$x_0+i = \gamma^3 = (-i)^3 = -i,$$

ahonnan következik, hogy $x_0=0$, továbbá (103)-ból $y_0=1$ is adódik.

21*. $K(i\sqrt{2})$-ben a racionális számelmélet analogonja ugyanúgy építhető fel, mint a Gauss-egészek körében; a részleteket az Olvasóra bízzuk. A normát most a következőképpen definiáljuk: valamely $K(i\sqrt{2})$-beli $\alpha=a+bi\sqrt{2}$ számra legyen

$$N(\alpha) = |\alpha|^2 = a^2+2b^2.$$

Ekkor $N(\alpha)$ nemnegatív egész szám, továbbá $\alpha|\beta$ esetén $N(\alpha)|N(\beta)$. Ha tehát ε egység, akkor $\varepsilon|1$-re tekintettel $N(\varepsilon)|N(1)=1$, ahonnan könnyen levezethető, hogy itt csak két egység van: -1 és $+1$. A maradékos osztás tételének megfelelője ugyanúgy igazolható, mint a Gauss-egészeknél (l. a 18. feladatot), és e tétel következményei is ugyanazok.

A 16*. feladat állításának igazolása céljából induljunk ki ismét abból, hogy ha p $8k+1$ vagy $8k+3$ alakú prímszám, akkor a II. fejezet 93*. feladata szerint létezik olyan z_0 egész szám, melyre (94) teljesül, vagyis

$$p|z_0^2+2 = (z_0+i\sqrt{2})(z_0-i\sqrt{2}).$$

Ezután a 7. példa megoldásához hasonlóan okoskodva, innen levezethető, hogy p $\pi_1\pi_2$ alakban írható, ahol π_1, π_2 $K(i\sqrt{2})$-beli prímek, melyek egymás konjugáltjai. (A részleteket ismét az Olvasóra bízzuk.) Legyen $\pi_1=a+bi\sqrt{2}$. Ekkor

$$p = \pi_1\pi_2 = \pi_1\bar{\pi}_1 = |\pi_1|^2 = |a+bi\sqrt{2}|^2 = a^2+2b^2,$$

tehát p valóban felírható a kívánt alakban.

22. Definiáljuk valamely $K(i\sqrt{5})$-beli $\alpha=a+bi\sqrt{5}$ szám normáját a következőképpen:

$$N(\alpha) = |\alpha|^2 = |a+bi\sqrt{5}|^2 = a^2+5b^2.$$

Ekkor egy $K(i\sqrt{5})$-beli szám normája nyilván nemnegatív egész szám. Továbbá a komplex számok abszolút értékének multiplikativitásából következik $N(\alpha)$ multiplikativitása. Innen viszont következik, hogy $\alpha|\beta$ esetén $N(\alpha)|N(\beta)$. Ha tehát $\varepsilon=x+yi\sqrt{5}$ egység, akkor $\varepsilon|1$-re tekintettel $N(\varepsilon)|N(1)=1$; így szükségképpen

$$N(\varepsilon) = x^2+5y^2 = 1.$$

Ez azonban nyilván akkor és csak akkor teljesül, ha $x=\pm 1$, $y=0$, tehát $\varepsilon=\pm 1+0\cdot i\sqrt{5}=\pm 1$; másrészt a -1 és $+1$ nyilván egységek. $K(i\sqrt{5})$-ben tehát két egység van: -1 és $+1$.

23. A 6 szám $K(i\sqrt{5})$-ben felbontható például a következőképpen:

(108) $6 = 2\cdot 3,$

(109) $6 = (1+i\sqrt{5})(1-i\sqrt{5}).$

Állítjuk, hogy az itt szereplő $2, 3, 1+i\sqrt{5}, 1-i\sqrt{5}$ tényezők mindegyike felbonthatatlan $K(i\sqrt{5})$-ben.

Ha ugyanis például 2 nem volna felbonthatatlan, akkor léteznének olyan α, β egységtől különböző $K(i\sqrt{2})$-beli számok, melyekre

(110) $\alpha\beta = 2.$

Minthogy α, β egységtől különbözők,

(111) $N(\alpha) \neq 1, \quad N(\beta) \neq 1.$

Továbbá (110)-ből következik, hogy

$$N(\alpha)N(\beta) = 4.$$

Innen (111)-re tekintettel adódik, hogy

$$N(\alpha) = N(\beta) = 2,$$

tehát $\alpha = x + yi\sqrt{5}$-öt írva,

$$N(\alpha) = |\alpha|^2 = x^2 + 5y^2 = 2.$$

Ilyen x, y egész számok azonban nyilván nem léteznek, tehát a 2 szám felbonthatatlan.

Hasonlóan igazolható, hogy a $3, 1+i\sqrt{5}, 1-i\sqrt{5}$ számok is felbonthatatlan számok.

Végül a (108) és (109) felbontások nyilván lényegesen különbözők, hiszen nem csupán sorrendben és egység szorzóban (vagyis — az előző feladat eredménye alapján — előjelben) különböznek.

24. Induljunk ki ismét abból, hogy ha p $8k+1$ vagy $8k+3$ alakú prímszám, akkor létezik olyan z_0 egész szám, melyre (94) teljesül. Tekintsük azt a pontrácsot, melyet azon rácspontok alkotnak, melyek derékszögű koordinátái

$$x = mp + nz_0,$$

$$y = n$$

alakban írhatók, ahol m, n egész számok. Ha tehát $(x; y)$ rácspont, akkor

(112) $x^2 + 2y^2 = (mp + nz_0)^2 + 2n^2 \equiv (nz_0)^2 + 2n^2 = n^2(z_0^2 + 2) \equiv 0 \pmod{p}.$

Elegendő megmutatni, hogy létezik olyan $(x; y)$ nemtriviális — vagyis a

(113) $0 < x^2 + y^2$

feltételt kielégítő — rácspont, melyre

(114) $x^2 + 2y^2 \leqq 1{,}99p$

teljesül. (112)-ből, (113)-ból és (114)-ből ugyanis nyilván következik, hogy

$$x^2 + 2y^2 = p.$$

A (114) feltételt kielégítő $(x; y)$ pontok origó centrumú ellipszist alkotnak, mely nyilván konvex, zárt és az origóra nézve centrálszimmetrikus. Továbbá $1{,}99p$-vel osztva, a következőt nyerjük:

$$\frac{x^2}{1{,}99p}+\frac{y^2}{\frac{1{,}99}{2}p} \leqq 1.$$

Innen látható ,hogy az ellipszis fél nagytengelye $a=\sqrt{1{,}99p}$, fél kistengelye $b=\sqrt{\frac{1{,}99}{2}p}$, tehát területe:

$$(115)\quad ab\pi = \sqrt{1{,}99p}\sqrt{\frac{1{,}99}{2}p}\pi = \frac{1{,}99}{2}\sqrt{2}\pi p > 0{,}99\cdot 1{,}4\cdot 3p =$$

$$= 0{,}99\cdot 4{,}2p = 4{,}158p > 4p.$$

Végül (48) szerint a rács alapparalelogrammájának területe:

$$\Delta = |p\cdot 1 - z_0\cdot 0| = |p| = p,$$

ami (115) szerint kisebb az ellipszis területének negyedénél. Így a Minkowski tételében előírt feltételek mindegyike teljesül, tehát a tétel alkalmazható. Ezért létezik olyan nemtriviális rácspont, melyre (114) teljesül, és éppen ezt kellett igazolnunk.

25*. $\sum\limits_{n\leqq N} r(n)$ nyilván azonos az

$$(116)\quad x^2+y^2 \leqq N$$

feltételt kielégítő, egész számokból álló $(x; y)$ számpárok számával. Ha egy $(x; y)$ számpárhoz hozzárendeljük a derékszögű koordináta-rendszer azon pontját, melynek koordinátái x, ill. y, akkor az egész számokból álló számpárok egy pontrácsot határoznak meg. Ez nyilván az a négyzetrács, mely a (0; 0), (0; 1), (1; 0), (1; 1) csúcsokkal rendelkező egységnégyzettel generálható. Továbbá ekkor a (116)-ot kielégítő x, y valós számoknak az origó középpontú, $\sqrt{N}$ sugarú kör pontjai felelnek meg. Végeredményben tehát azoknak a rácspontoknak a számát kell becsülnünk, amelyeket ez a kör tartalmaz.

Rendeljük hozzá minden egyes, az említett körbe eső rácsponthoz azt az egységnégyzetet (vagyis a koordinátatengelyekkel párhuzamos, egységnyi hosszúságú oldalakkal határolt négyzetet), melynek „bal alsó" csúcspontja a szóban forgó rácspont. E négyzetek együttvéve valamely S_N síkidomot fednek le. S_N területe — jelöljük ezt t_N-nel — nyilván azonos az S_N-et alkotó négyzetek számával (hiszen egy-egy négyzet egységnyi területű), vagyis a szóban forgó rácspontok számával. Másrészt könnyen látható, hogy az origó középpontú, $\sqrt{N}+\sqrt{2}$ sugarú kör lefedi S_N-et, míg S_N lefedi

az origó középpontú, $\sqrt{N}-\sqrt{2}$ sugarú kört (ennek belátását az Olvasóra bízzuk). Így S_N területe e két kör területe közé esik, tehát $N \geqq 1$ esetén

$$t_N \leqq (\sqrt{N}+\sqrt{2})^2\pi = (N+2\sqrt{2}\sqrt{N}+2)\pi \leqq (N+2\sqrt{2}\sqrt{N}+2\sqrt{N})\pi =$$

$$= \pi N+4\sqrt{2}\pi\sqrt{N} < \pi N+20\sqrt{N},$$

$$t_N \geqq (\sqrt{N}-\sqrt{2})^2\pi = (N-2\sqrt{2}\sqrt{N}+2)\pi > \pi N-2\sqrt{2}\pi\sqrt{N} >$$

$$> \pi N-20\sqrt{N}.$$

$N \geqq 1$ esetén tehát

$$|t_N-\pi N| < 20\sqrt{N}.$$

Minthogy $t_N = \sum_{n \leqq N} r(n)$, innen adódik a bizonyítandó egyenlőtlenség, $c=20$ választással.

26. $(1^2+1^2+1^2)(2^2+1^2+0^2) = 3\cdot 5 = 15.$

Másrészt a 15 szám $8k+7$ alakú, tehát a három négyzetszám tétel szerint nem írható fel három négyzetszám összegeként.

27. Mint már többször említettük, egy négyzetszám 8-cal osztva 0, 1 vagy 4 maradékot ad. Ebből következik, hogy a két négyzetszám összegeként felírható számok 8-cal osztva 0, 1, 2, 4 vagy 5 maradékot adnak. A $8k+3$ vagy $8k+6$ alakú számok tehát nem írhatók fel két négyzetszám összegeként. Másrészt a három négyzetszám-tétel szerint az ilyen alakú számok felírhatók három négyzetszám összegeként.

28*. Tegyük fel, hogy az adott diofantikus egyenlet megoldható, vagyis léteznek olyan x_0, y_0, z_0 egész számok, melyekre

$$x_0^2+y_0^2+2z_0^2 = n.$$

Mindkét oldalt 2-vel szorozva és felhasználva a

$$(117) \quad 2(a^2+b^2) = (a+b)^2+(a-b)^2$$

azonosságot:

$$(x_0+y_0)^2+(x_0-y_0)^2+(2z_0)^2 = 2n.$$

Így, ha az adott diofantikus egyenlet megoldható, akkor az

$$(118) \quad x^2+y^2+z^2 = 2n$$

diofantikus egyenlet is megoldható.

Másrészt tegyük fel, hogy (118) megoldható, vagyis léteznek olyan x_1, y_1, z_1 egész számok, melyekre

$$(119) \quad x_1^2+y_1^2+z_1^2 = 2n.$$

Minthogy a jobb oldal páros, a bal oldal három tagja közül az egyik páros, a másik kettő pedig azonos paritású. Feltehető, hogy például z_1 páros, és x_1 és y_1 azonos paritású. Ekkor (119) mindkét oldalát 2-vel osztva és az

$$(120)\qquad \frac{a^2+b^2}{2} = \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2$$

azonosságot felhasználva:

$$\left(\frac{x_1+y_1}{2}\right)^2 + \left(\frac{x_1-y_1}{2}\right)^2 + 2\cdot\left(\frac{z_1}{2}\right)^2 = n,$$

tehát az adott diofantikus egyenlet is megoldható.

Így az adott diofantikus egyenlet akkor és csak akkor oldható meg, ha a (118) diofantikus egyenlet is megoldható, vagyis $2n$ felírható három négyzetszám összegeként. Azonban a három négyzetszám tételre tekintettel $2n$ akkor és csak akkor *nem* írható fel ilyen alakban, ha $2n=4^{k+1}(8l+7)=2^{2k+2}(8l+7)$ alakú (ahol k, l nemnegatív egész számok). 2-vel egyszerűsítve, adódik az állítás.

29. Ha k páros, akkor $x = 3\cdot 2^{\frac{k}{2}}$, $y = 2\cdot 2^{\frac{k}{2}}$, $z = u = 2^{\frac{k}{2}}$, ha k páratlan, akkor $x=4\cdot 2^{\frac{k-1}{2}}$, $y=3\cdot 2^{\frac{k-1}{2}}$, $z=2\cdot 2^{\frac{k-1}{2}}$, $u=2^{\frac{k-1}{2}}$ megoldás.

30. $4331 = 61\cdot 71 = (2^2+4^2+4^2+5^2)(1^2+3^2+5^2+6^2) =$

$$= (2\cdot 1+4\cdot 3+4\cdot 5+5\cdot 6)^2+(2\cdot 3-4\cdot 1+4\cdot 6-5\cdot 5)^2+$$

$$+(2\cdot 5-4\cdot 6-4\cdot 1+5\cdot 3)^2+(2\cdot 6+4\cdot 5-4\cdot 3-5\cdot 1)^2 =$$

$$= 64^2+1^2+(-3)^2+15^2 = 1^2+3^2+15^2+64^2.$$

31. x^2-et p-vel osztva, maradékként 0-t vagy kvadratikus maradékot kapunk; ez utóbbiak száma $\frac{p-1}{2}$, tehát összesen $\frac{p+1}{2}$ inkongruens maradékot nyerünk. Ugyanúgy, $-y^2-1$ p-vel osztva $\frac{p+1}{2}$ inkongruens maradékot ad. A kétfajta maradék száma összesen $\frac{p+1}{2}+\frac{p+1}{2}=p+1$, tehát p-nél nagyobb. Így létezik legalább egy olyan maradék, mely mindkét esetben fellép, tehát léteznek olyan x_0, y_0 egész számok, melyekre

$$x_0^2 \equiv -y_0^2-1 \pmod{p}.$$

Ezt átrendezve, adódik (78).

32*. Legyen $n=2$, $a_{11}=x_0$, $a_{12}=a_{21}=y_0$, $a_{22}=-x_0$, ahol x_0, y_0 (78)-at kielégítő egész számok, és legyen $u_1=u_2=v_1=v_2=[\sqrt{p}]+1$. Ekkor

$$u_1u_2v_1v_2 = ([\sqrt{p}]+1)^4 > (\sqrt{p})^4 = p^2,$$

tehát a Thue-lemma alkalmazható. Ennek alapján léteznek olyan x_1, x_2, y_1, y_2 egész számok, melyekre

(121) $x_0x_1+y_0x_2 \equiv y_1 \pmod{p}$,

(122) $y_0x_1-x_0x_2 \equiv y_2 \pmod{p}$,

(123) $|x_1| < [\sqrt{p}]+1,\ |x_2| < [\sqrt{p}]+1,\ |y_1| < [\sqrt{p}]+1,\ |y_2| < [\sqrt{p}]+1$

és

(124) $x_1^2+x_2^2+y_1^2+y_2^2 > 0$

teljesül. Ekkor (78)-ra, (121)-re és (122)-re tekintettel

(125) $$x_1^2+x_2^2+y_1^2+y_2^2 \equiv x_1^2+x_2^2+(x_0x_1+y_0x_2)^2+(y_0x_1-x_0x_2)^2 =$$
$$= x_1^2+x_2^2+x_0^2x_1^2+y_0^2x_2^2+y_0^2x_1^2+x_0^2x_2^2 = (x_1^2+x_2^2)(1+x_0^2+y_0^2) \equiv 0 \pmod{p},$$

továbbá (123) alapján

(126) $x_1^2+x_2^2+y_1^2+y_2^2 \leqq 4[\sqrt{p}]^2 < 4(\sqrt{p})^2 = 4p.$

(124)-ből, (125)-ből és (126)-ból következik, hogy

(127) $x_1^2+x_2^2+y_1^2+y_2^2 = p,$

(128) $x_1^2+x_2^2+y_1^2+y_2^2 = 2p$

vagy

(129) $x_1^2+x_2^2+y_1^2+y_2^2 = 3p$

teljesül.

Ha (127) teljesül, akkor készen vagyunk. Ha (128) teljesül, akkor a jobb oldal páros, tehát a bal oldalon álló négy tag közül kettő-kettő egyező paritású. Feltehető, hogy például x_1 és x_2, ill. y_1 és y_2 egyező paritásúak. Ekkor (128) mindkét oldalát 2-vel osztva és a (120) azonosságot alkalmazva:

$$\left(\frac{x_1+x_2}{2}\right)^2+\left(\frac{x_1-x_2}{2}\right)^2+\left(\frac{y_1+y_2}{2}\right)^2+\left(\frac{y_1-y_2}{2}\right)^2 = p,$$

tehát p most is felírható négy négyzetszám összegeként.

Végül tegyük fel, hogy (129) teljesül. Ha $p=3$, akkor a feladat állítása nyilvánvaló; feltehető tehát, hogy $p>3$. Ekkor (129) jobb oldala osztható 3-mal, de 9-cel nem; így a bal oldal is osztható 3-mal, de 9-cel nem. Ebből következik, hogy x_1, x_2, y_1, y_2 közt van legalább egy olyan, mely nem osztható 3-mal. Továbbá könnyen látható, hogy egy négyzetszám 3-mal osztva 0 vagy 1 maradékot ad. Így (129) bal oldala nyilván csak úgy lehet 3-mal osztható (figyelembe véve, hogy nem lehet x_1, x_2, y_1, y_2 mindegyike osztható 3-mal), hogy az x_1, x_2, y_1, y_2 számok közül egy — mondjuk y_2

— osztható 3-mal, a többi — tehát x_1, x_2, y_1 — nem osztható 3-mal. Ha továbbá például x_1 nem $3k+1$ alakú szám, hanem $3k-1$ alakú, akkor $-x_1$ már $3k+1$ alakú, és x_1-et $-x_1$-gyel helyettesítve, (129) továbbra is fennáll. Ezért feltehetjük, hogy x_1, x_2, y_1 mindegyike $3k+1$ alakú szám. Ekkor azonban a

$$z_1 = \frac{x_1+x_2+y_1}{3}, \quad z_2 = \frac{x_1-x_2+y_2}{3}, \quad z_3 = \frac{x_2-y_1+y_2}{3},$$

$$z_4 = \frac{y_1-x_1+y_2}{3}$$

számok mindegyike egész szám, másrészt (129) mindkét oldalát 3-mal osztva és a bal oldalt átalakítva, éppen

$$z_1^2+z_2^2+z_3^2+z_4^2 = p$$

adódik. Így p ebben az esetben is felírható négy négyzetszám összegeként, és ezzel az állítást maradéktalanul igazoltuk.

33. *a.* Legyen $n=8k$, ahol k természetes szám. A négy négyzetszámtétel szerint $k-1$ felírható négy négyzetszám összegeként:

$$k-1 = x^2+y^2+z^2+u^2.$$

Mindkét oldalhoz 1-et adva, majd 8-cal szorozva:

$$(130) \quad (n =)\ 8k = 8x^2+8y^2+8z^2+8u^2+8.$$

Könnyen ellenőrizhető azonban, hogy

$$(131) \quad 8x^2+8y^2+8z^2+8u^2+8 = (2x+1)^2+(2x-1)^2+(2y+1)^2+$$
$$+(2y-1)^2+(2z+1)^2+(2z-1)^2+(2u+1)^2+(2u-1)^2.$$

(130)-ból és (131)-ből adódik a bizonyítandó állítás.

b. Az I. fejezet 20. feladatára tekintettel $1 \leqq k \leqq 7$ esetén k számú páratlan négyzetszám összege 8-cal osztva k maradékot ad, tehát nem osztható 8-cal. Innen következik az állítás.

34. *a.* Ha a 23 számot köbszámok összegeként akarjuk felírni, akkor a tagok között 3^3 vagy annál nagyobb köbszám nem szerepelhet, hiszen $3^3=27>23$. Így csak $1^3=1$ és $2^3=8$ léphetnek fel tagként. Továbbá a 23 szám fenti alakú optimális (azaz, lehető legkevesebb tagból álló) előállítását nyilván úgy nyerjük, ha a lehető legtöbb 8-ast használjuk fel. Azonban $3\cdot 8=24>23$, tehát csak két 2^3 alakú tag szerepelhet, és szükségképpen szerepelnie kell $23-2\cdot 2^3=7$ darab 1^3 alakú tagnak. Ez összesen $2+7=9$ tag, tehát a 23 szám köbszámok összegeként való felírásához legalább 9 tag szükséges, és ezzel az állítást igazoltuk.

b. Hasonlóan igazolható, hogy a 79 szám negyedik hatványok összegeként való előállításához legalább 19 negyedik hatvány szükséges.

35*. Tegyük fel indirekte, hogy

$$(132) \quad G(k) \leqq k-1.$$

Ebből következik, hogy létezik olyan n_0 szám, hogy $n > n_0$ esetén az n természetes szám felírható

$$(133) \quad x_1^k + x_2^k + \ldots + x_{k-1}^k = n$$

alakban, ahol $x_1, x_2, \ldots, x_{k-1}$ nemnegatív egész számok. Jelöljük (133) megoldásszámát $f(n)$-nel.

Rögzítsünk most valamely n_0-nál nagyobb N természetes számot, és legyen $n_0 < n \leqq N$. Ekkor (133)-ból nyilván következik, hogy

$$(134) \quad 0 \leqq x_i \leqq \sqrt[k]{n} \leqq \sqrt[k]{N} \quad (\text{ahol } i = 1, 2, \ldots, k-1).$$

E feltétel nyilván legfeljebb $1 + \sqrt[k]{N} \leqq 2\sqrt[k]{N}$ számú x_i egész számra teljesül. Továbbá az i szám itt $(k-1)$-féleképpen választható, tehát azon $(k-1)$-esek száma, melyekre

$$(135) \quad x_1^k + x_2^k + \ldots + x_{k-1}^k \leqq N$$

teljesül, legfeljebb $(2\sqrt[k]{N})^{k-1} = 2^{k-1} N^{\frac{k-1}{k}}$.

Másrészt, ha $n_0 < n \leqq N$, és az $x_1, x_2, \ldots, x_{k-1}$ $(k-1)$-esre (133) teljesül, akkor szükségképpen (135) is fennáll. Így (135) megoldásszáma legalább

$$f(n_0+1) + f(n_0+2) + \ldots + f(N) \geqq 1 + 1 + \ldots + 1 = N - n_0.$$

Ezt egybevetve a megoldásszám előbbi felső becslésével, nyerjük, hogy

$$N - n_0 \leqq 2^{k-1} N^{\frac{k-1}{k}}.$$

Mindkét oldalt N-nel osztva:

$$1 - \frac{n_0}{N} \leqq \frac{2^{k-1}}{\sqrt[k]{N}}.$$

Ha N tart a végtelenhez, akkor a bal oldal 1-hez, míg a jobb oldal 0-hoz tart. Így elég nagy N-re ez az egyenlőtlenség nem állhat fenn, tehát a (132) indirekt feltevésből ellentmondásra jutottunk, és ezzel az állítást igazoltuk.

36. $m = 99$, $n = 1$-et választva, a (69) azonosságra tekintettel az $x_0 = 2mn = 2 \cdot 99 \cdot 1 = 198$, $y_0 = m^2 - n^2 = 99^2 - 1 = (99-1)(99+1) = 9800$, $z_0 = m^2 + n^2 = 99^2 + 1 = y_0 + 2 = 9802$ számhármas pythagoraszi számhármas.

37. Azt kell igazolnunk, hogy 198 nem írható fel a (65) alatti $2mn$, $m^2 - n^2$, $m^2 + n^2$ alakok egyikében sem, ahol m, n kielégítik a (66), (67) és (68) feltételeket. Valóban, a (68) feltételből következik, hogy $m^2 - n^2$ és $m^2 + n^2$ páratlan számok, míg $4 | 2mn$. Ugyanakkor 198 páros szám, de $4 \nmid 198$; innen következik az állítás.

38. Könnyen igazolható, hogy ha az n egész szám nem osztható 5-tel, akkor négyzete -1-gyel vagy $+1$-gyel kongruens modulo 5 (ennek belátá-

sát az Olvasóra bízzuk). Így ha x, y nem oszthatók 5-tel, akkor x^2+y^2 vagy $(-1)+(-1)=-2$-vel vagy $(-1)+(+1)=0$-val vagy $(+1)+(+1)=2$-vel kongruens modulo 5. Az első és harmadik esetben x^2+y^2 nem osztható 5-tel, és inkongruens -1-gyel és $+1$-gyel modulo 5, tehát nem lehet négyzetszám. Így csak a második eset fordulhat elő; tehát (64)-ből $5 \nmid xy$ esetén $5|z$ következik, és ezzel az állítást igazoltuk.

39. Tegyük fel indirekte, hogy $x=a-1, y=a, z=a+1$ megoldás, vagyis

$$(a-1)^3+a^3 = (a+1)^3,$$

vagyis

$$(a^3-3a^2+3a-1)+a^3 = a^3+3a^2+3a+1,$$

$$(136) \quad a^3-6a^2-2 = 0.$$

a tehát gyöke az x^3-6x^2-2 egész együtthatós polinomnak. Ismeretes, hogy ha egy egész szám gyöke egy egész együtthatós polinomnak, akkor osztója a konstans tagnak. Így innen $a|2$ következik, tehát a lehetséges értékei $a=-2, -1, +1, +2$. Rendre behelyettesítve, ellenőrizhető, hogy ezek egyike sem elégíti ki (136)-ot. Így az indirekt feltevésből ellentmondásra jutottunk, és ezzel az állítást igazoltuk.

40. Ha az $x=x_0, y=y_0, z=z_0$ természetes számokból álló számhármas megoldása lenne az adott egyenletnek, akkor $t=x_0^5, u=y_0^9, v=z_0^{11}$ nyilván nemtriviális megoldása lenne a

$$t^3+u^3 = z^3$$

Fermat-egyenletnek. Minthogy a Fermat-sejtés $k=3$ esetén bizonyított, innen következik az állítás.

41. Tegyük fel indirekte, hogy valamely 2-nél nagyobb k természetes számra és p, q, r pozitív prímszámokra

$$(137) \quad p^k+q^k = r^k.$$

Minthogy a két oldal paritása megegyezik, nem lehet p, q, r mindegyike páratlan. Továbbá $r=2$ nem lehetséges, mert ekkor a bal oldal nagyobb lenne a jobb oldalnál. Így p és q közül az egyik 2-vel egyenlő; feltehető, hogy $p=2$. Ekkor (137)-ből következik, hogy q, r páratlan számok, melyekre $r>q\geqq 3$. Így (137)-ból a binomiális tételre (és $k>2$-re) tekintettel

$$2^k = r^k-q^k \geqq (q+2)^k-q^k = (q^k+k\cdot q^{k-1}\cdot 2+\ldots+2^k)-q^k =$$

$$= 2kq^{k-1}+\ldots+2^k > 2^k.$$

Az indirekt feltevésből tehát ellentmondásra jutottunk, és ezzel az állítást igazoltuk.

42*. Az állítás következik az

$$(9n^4)^3+(9n^3+1)^3 = (9n^4+3n)^3+1$$

azonosságból.

VI. DIOFANTIKUS APPROXIMÁCIÓ-ELMÉLET

1. A DIOFANTIKUS APPROXIMÁCIÓELMÉLET ELEMEI

A diofantikus approximációelmélet az alábbi típusú problémák vizsgálatával foglalkozik:

Adott valamely egy- vagy többváltozós függvény (mely esetleg lehet vektor-vektor függvény is). E függvényekbe alkalmas *egész vagy racionális* számokat helyettesítve, a megfelelő függvényértékek milyen közel kerülhetnek valamilyen előre adott valós számhoz (ill. vektorhoz)?

A legegyszerűbb — és talán legfontosabb — ilyen típusú probléma a következő:

Adott valamely α valós szám. Alkalmas $\frac{p}{q}$ racionális számokra (ahol p egész szám, q természetes szám) milyen kicsivé tehető az

$$(1) \qquad \left|\alpha - \frac{p}{q}\right|$$

kifejezés? Az olyan $\frac{p}{q}$ racionális számokat, melyekre az (1) kifejezés valamilyen jól definiált értelemben (rendszerint q függvényében) kicsi, α-t *jól approximáló* számoknak, ilyen $\frac{p}{q}$ racionális számok keresését pedig α racionális számokkal való *approximációjának* mondjuk.

Az az eset, amikor α racionális szám, könnyen tárgyalható; ennek az esetnek a diszkusszióját az Olvasóra bízzuk, és a továbbiakban arra az esetre szorítkozunk, amikor α *irracionális szám*.

Könnyen látható, hogy bármely α valós számot és q természetes számot megadva, található olyan p egész szám, melyre

$$(2) \qquad |q\alpha - p| \leqq \frac{1}{2},$$

vagyis

$$(3) \qquad \left|\alpha - \frac{p}{q}\right| \leqq \frac{1}{2q}$$

teljesül. Mint a $\frac{2k+1}{2}$ alakú racionális számokhoz „közeli" α irracionális számok mutatják, ez a becslés *rögzített* q mellett általában nem javítható.

Ugyanakkor P. G. L. Dirichlet bizonyította, hogy α-t rögzítve, található *végtelen sok* olyan q természetes szám, hogy alkalmas p egész számokra

$$(4) \qquad \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$$

(ami lényegesen élesebb a (3) becslésnél). Ez a tétel az $\alpha, 2\alpha, \ldots, \ldots, N\alpha$ számok (N rögzített természetes szám) tört részének vizsgálata révén, a skatulyaelv segítségével igen egyszerűen bizonyítható (l. az 1. és 2. példát; sőt, ott valamivel élesebb tételt fogunk bizonyítani).

Másrészt a 3. példa kapcsán igazolni fogjuk, hogy $\alpha = \sqrt{2}$ esetén a (4) becslés nem javítható lényegesen, amennyiben bármely q természetes számra és p egész számra

$$(5) \qquad \left|\sqrt{2} - \frac{p}{q}\right| > \frac{1}{4q^2}.$$

Ez azt jelenti, hogy a (4) becslés legfeljebb annyiban javítható, hogy a jobb oldalon $\frac{1}{q^2}$-t még esetleg szorozhatjuk egy 1-nél kisebb — de (5) szerint $\frac{1}{4}$-nél nagyobb — c konstans szorzóval. A 15*. feladatban igazolni fogjuk, hogy $c = \frac{1}{2}$-et még írhatunk.

Végül akár a geometriai számelmélet módszereivel, akár lánctörtek (l. a 2. pontot) segítségével igazolható, hogy $c=\frac{1}{\sqrt{5}}$-öt is írhatunk, vagyis tetszőleges α irracionális számot megadva, végtelen sok q természetes számra és alkalmas p egész számokra

$$(6)\qquad \left|\alpha-\frac{p}{q}\right|<\frac{1}{\sqrt{5}q^2}.$$

Itt — $\alpha=\frac{\sqrt{5}+1}{2}$-t választva — a jobb oldalon álló $\frac{1}{\sqrt{5}}$ konstans szorzó már nem csökkenthető tovább, tehát a (6) becslés — *tetszőleges* α-ra — tovább már nem javítható. (L. 4*. feladat.)

Eddig olyan becslést kerestünk az (1) kifejezésre, mely alkalmas p, q egész számokat választva bármely α irracionális számra teljesül. Felmerül a kérdés, hogy bizonyos „kivételes" α-któl eltekintve, nem javítható-e tovább a (6) becslés? Igazolható, hogy — bizonyos, jól definiált értelemben „majdnem minden" α-hoz található végtelen sok olyan p, q számpár, amelyre (4) jobb oldalán például $\frac{1}{q^2\log q}$ is írható, másrészt „majdnem minden" α-ra

$$\left|\alpha-\frac{p}{q}\right|<\frac{1}{q^2\log q}$$

csak véges sok p, q párra áll fenn.

Pontosabban: (6) jobb oldalán $\frac{1}{5q^2}$ helyére $\frac{1}{qf(q)}$-t — ahol $f(q)>0$ — írva, az így nyert egyenlőtlenség akkor és csak akkor teljesül „majdnem minden" α-ra (végtelen sok p, q számpárra), ha a $\sum_{q=1}^{+\infty}\frac{1}{f(q)}$ végtelen sor divergens.

Itt a „majdnem minden" úgy értendő, hogy a szóban forgó α-k halmazának komplementere (Lebesgue értelemben) 0 mértékű.

Míg a most említett statisztikus tétel nem túlzottan mély, jóval nehezebb probléma annak eldöntése, hogy egy-egy konkrét α

irracionális számra mennyiben javítható a (6) egyenlőtlenség (végtelen sok p, q-ra)? A legfontosabb ilyen jellegű eredmények α *algebrai karakterére* vonatkozóan tartalmaznak megszorításokat. Azt ugyanis már az előbbiekben is láttuk, hogy az $\alpha=\sqrt{2}$, ill. $\alpha=\frac{\sqrt{5}+1}{2}$ számok „rosszul approximálhatók", azaz a (6) egyenlőtlenség ezekre az α-kra nem javítható (eltekintve — $\alpha=\sqrt{2}$ esetén — egy konstans szorzótól a jobb oldalon). Ennek a két számnak megvan az a közös tulajdonsága, hogy mindkettő gyöke egy másodfokú egész együtthatós egyenletnek, vagyis mindkettő másodfokú algebrai szám. Igazolható, hogy bármely másodfokú algebrai szám „rosszul approximálható" (pontosabban, ilyen α-kra (6) csak egy konstans szorzó erejéig javítható; l. a 3. feladatot). Még általánosabban, J. Liouville bizonyította, hogy ha α (valós) n-edfokú algebrai szám, akkor létezik olyan c (α-tól függő) pozitív állandó, hogy tetszőleges q természetes számra és p egész számra

$$(7) \qquad \left|\alpha-\frac{p}{q}\right|>\frac{c}{q^n}.$$

Liouville tétele felhasználható például annak a — távolról sem magától értetődő — ténynek a bizonyítására (mégpedig *konstruktív* bizonyítására), hogy *létezik transzcendens szám*, tehát a transzcendens számoknak a VI. fejezet 4. pontjában adott definíciója nem üres (l. a 8*. feladatot).

Liouville tételét sokan élesítették, végül K. F. Rothnak 1955-ben sikerült bebizonyítania az alábbi igen mély tételt:

Ha α algebrai szám, ε tetszőlegesen kicsi pozitív szám, akkor az

$$(8) \qquad \left|\alpha-\frac{p}{q}\right|<\frac{1}{q^{2+\varepsilon}}$$

egyenlőtlenséget csak *véges sok* q természetes szám és p egész szám elégítheti ki.

Áttérünk Dirichlet (approximációra vonatkozó) tételének „többdimenziós" általánosítására. Legyenek adottak valamely $\alpha_1, \alpha_2, \ldots, \alpha_k$ irracionális számok (k tetszőleges természetes szám). Célunk olyan racionális számok keresése, melyek *neve-*

zője azonos, és jól approximálják az egyes α_i-ket; ilyenkor *szimultán approximációról* beszélünk. Dirichlet tételének a szimultán approximációra vonatkozó analogonja az alábbi tétel:

Tetszőleges k természetes számot és $\alpha_1, \alpha_2, \ldots, \alpha_k$ irracionális számokat megadva, található végtelen sok q természetes szám és ezek mindegyikéhez olyan $p_1, p_2, \ldots, p_k$ egész számok, melyekre $i=1, 2, \ldots, k$ esetén

$$(9) \qquad \left|\alpha_i - \frac{p_i}{q}\right| < \frac{1}{q^{1+\frac{1}{k}}}.$$

(A bizonyítás is analóg az „egydimenziós" speciális esetben adott bizonyításhoz; l. a 9. feladatot.) Igazolható, hogy ez a tétel is legfeljebb annyiban javítható, hogy (9) jobb oldalát megszorozhatjuk egy 1-nél kisebb alkalmas állandóval.

Lényegesen mélyebb Dirichlet tételének egy más irányú általánosítása, mely L. Kroneckertől származik (1884-ből). Szorozzuk meg ugyanis (4) mindkét oldalát q-val:

$$|qd-p| < \frac{1}{q},$$

tehát $|q\alpha-p|$-re nyerünk felső becslést. Mármost ennél általánosabban, α mellett rögzíthetünk valamely β valós számot is, és ekkor $|q\alpha-p-\beta|$-ra keresünk felső becslést. (Tehát lényegében arról van szó, hogy $q\alpha$ tört része alkalmas q számokra milyen közel kerülhet β tört részéhez.) Ilyenkor *inhomogén approximációról* beszélünk; ha speciálisan $\beta=0$, vagy általánosabban β egész szám, akkor jutunk vissza az előbbi esetre, melyet *homogén approximációnak* nevezünk. Kronecker tételének „egydimenziós" speciális esete, mely Dirichlet tételének az inhomogén approximációra vonatkozó analogonja, a következőképpen hangzik:

Tetszőleges α irracionális számot és β valós számot megadva, található végtelen sok q természetes szám és ezekhez alkalmas p egész szám, melyekre

$$(10) \qquad |q\alpha-p-\beta| < \frac{3}{q}.$$

Kronecker tételének ez a speciális esete levezethető Dirichlet tételéből. Ugyanakkor Dirichlet tétele sokkal kevésbé mély, mint Kronecker tételének legáltalánosabb formája. Ennek kimondásához előre kell bocsátanunk egy definíciót:

Ha az $\alpha_1, \alpha_2, \ldots, \alpha_k$ valós számokra

$$r_1\alpha_1 + r_2\alpha_2 + \ldots + r_k\alpha_k = 0$$

esetén — ahol $r_1, r_2, \ldots, r_k$ racionális számok — szükségképpen fennáll, hogy $r_1 = r_2 = \ldots = r_k = 0$, akkor azt mondjuk, hogy $\alpha_1, \alpha_2, \ldots, \alpha_k$ *lineárisan függetlenek a racionális számtest felett.*

Ezek után *Kronecker tétele* legáltalánosabb formájában a következőképpen hangzik:

Tegyük fel, hogy az $1, \alpha_1, \alpha_2, \ldots, \alpha_k$ számok lineárisan függetlenek a racionális számtest felett, és legyenek $\beta_1, \beta_2, \ldots, \beta_k$ tetszőleges valós számok, ε pedig tetszőlegesen kicsi pozitív szám. Ekkor létezik végtelen sok olyan q természetes szám, hogy alkalmas $p_1, p_2, \ldots, p_k$ egész számokra $i = 1, 2, \ldots, k$ esetén

$$|q\alpha_i - p_i - \beta_i| < \varepsilon.$$

A diofantikus approximációelmélet igen gyakran alkalmazható diofantikus egyenletek vizsgálata során. Így például Roth tételéből viszonylag könnyen levezethető, hogy bizonyos típusú diofantikus egyenleteknek legfeljebb véges sok megoldásuk van (a diofantikus egyenletek elméletében kevés olyan tétel ismeretes, mely az egyenletek ilyen nagy csoportjára vonatkozik). Felhasználható azonban a diofantikus approximációelmélet a számelmélet egyes más területein is, így például az algebrai számelméletben (l. a 8*. feladatot). Sőt, újabban alkalmazzák az approximációelméletet a matematika más ágaiban is, így például a numerikus analízisben (határozott integrálok közelítő kiszámítására).

Példák

1. Igazoljuk Dirichlet tételét: tetszőleges α irracionális számot és Q természetes számot megadva, található olyan q természetes szám, hogy alkalmas p egész számra:

$$(11) \qquad \left|\alpha - \frac{p}{q}\right| < \frac{1}{qQ},$$

továbbá

(12) $q \leqq Q$

teljesül!

Megoldás:

Tekintsük az

(13) $\alpha-[\alpha],\ 2\alpha-[2\alpha],\ \ldots,\ (Q+1)\alpha-[(Q+1)\alpha]$

számokat. Ezek mindegyike legalább 0 és kisebb 1-nél, vagyis a $[0, 1)$ (balról zárt, jobbról nyílt) intervallumba esik. Osszuk ezt az intervallumot Q egyenlő részre, vagyis tekintsük a

(14) $\left[0, \frac{1}{Q}\right),\ \left[\frac{1}{Q}, \frac{2}{Q}\right),\ \ldots,\ \left[\frac{Q-1}{Q}, 1\right)$

részintervallumokat. Ez utóbbiak száma Q, míg a (13) alatti számoké $Q+1$, tehát a skatulyaelv értelmében a (13) számok közt van két olyan — mondjuk $i\alpha-[i\alpha]$ és $j\alpha-[j\alpha]$ (feltehető, hogy $i<j$) —, melyek ugyanabba a (14) alatti részintervallumba esnek. Ekkor e két szám különbsége kisebb az intervallum hosszánál, $\frac{1}{Q}$-nál, tehát

$$|(j\alpha-[j\alpha])-(i\alpha-[i\alpha])| < \frac{1}{Q},$$

vagyis

$$|(j-i)\alpha-([j\alpha]-[i\alpha])| < \frac{1}{Q}.$$

Itt $q=j-i$-t és $p=[j\alpha]-[i\alpha]$-t írva, q természetes szám, p egész szám, továbbá

(15) $|q\alpha-p| < \frac{1}{Q}$

és nyilván $q \leqq Q$. (15)-öt q-val osztva, adódik (11), és ezzel az állítást igazoltuk.

2. Az előző példát felhasználva, bizonyítsuk be, hogy tetszőleges α irracionális számot megadva, létezik *végtelen sok* olyan q természetes szám és p egész szám, melyekre (4) teljesül, vagyis $\left|\alpha-\frac{p}{q}\right| < \frac{1}{q^2}$.

Megoldás:

Nyilván elegendő igazolni, hogy tetszőleges $\frac{p_1}{q_1}$ racionális számot megadva, található olyan $\frac{p_2}{q_2}$ racionális szám (p_2 egész szám, q_2 termé-

szetes szám), melyre

$$(16) \qquad \left|\alpha-\frac{p_2}{q_2}\right| < \left|\alpha-\frac{p_1}{q_1}\right|$$

és

$$(17) \qquad \left|\alpha-\frac{p_2}{q_2}\right| < \frac{1}{q_2^2}$$

teljesül. Ha ugyanis ez az állítás igaz, akkor ismételten alkalmazva azt, racionális számoknak $\frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots, \frac{p_k}{q_k}, \ldots$ végtelen sorozatát nyerjük, melyre

$$(18) \qquad \left|\alpha-\frac{p_1}{q_1}\right| > \left|\alpha-\frac{p_2}{q_2}\right| > \ldots > \left|\alpha-\frac{p_k}{q_k}\right| > \ldots$$

és

$$(19) \qquad \left|\alpha-\frac{p_k}{q_k}\right| < \frac{1}{q_k^2} \quad (\text{ahol } k = 1, 2, \ldots)$$

teljesül. (19) szerint e $\frac{p_k}{q_k}$ törtek kielégítik (4)-et, másrészt (18) szerint különbözők, tehát így (4)-nek végtelen sok megoldását nyerjük.

Rögzítsünk tehát valamely $\frac{p_1}{q_1}$ racionális számot. Mivel α irracionális szám, $\left|\alpha-\frac{p_1}{q_1}\right|$ nem lehet 0, tehát pozitív szám. Így, ha a Q természetes számot elég nagyra választjuk, akkor nyilván

$$(20) \qquad \left|\alpha-\frac{p_1}{q_1}\right| > \frac{1}{Q}.$$

Alkalmazzuk az 1. példa állítását egy ilyen Q természetes számra. Nyerjük, hogy létezik olyan $\frac{p}{q}$ tört, melyre

$$(21) \qquad \left|\alpha-\frac{p}{q}\right| < \frac{1}{qQ}$$

és

$$(22) \qquad 1 \leqq q \leqq Q$$

teljesül. (21)-ből és (22)-ből következik, hogy

$$\left|\alpha-\frac{p}{q}\right| < \frac{1}{qQ} \leqq \frac{1}{q \cdot q} = \frac{1}{q^2},$$

továbbá (20)-ból, (21)-ből és (22)-ből kapjuk, hogy

$$\left|\alpha-\frac{p}{q}\right|<\frac{1}{qQ}\leqq\frac{1}{1\cdot Q}=\frac{1}{Q}<\left|\alpha-\frac{p_1}{q_1}\right|.$$

Így $p_2=p$, $q_2=q$ választással (16) és (17) teljesül, és ezzel az állítást igazoltuk.

3. Bizonyítsuk be, hogy tetszőleges q természetes számra és p egész számra teljesül (5), vagyis az

$$\left|\sqrt{2}-\frac{p}{q}\right|<\frac{1}{4q^2}$$

egyenlőtlenség!

Megoldás:

$$(23)\quad \left|\sqrt{2}-\frac{p}{q}\right|=\left|\left(\sqrt{2}-\frac{p}{q}\right)\left(\sqrt{2}+\frac{p}{q}\right)\cdot\frac{1}{\sqrt{2}+\frac{p}{q}}\right|=$$

$$=\left|\left(2-\frac{p^2}{q^2}\right)\cdot\frac{1}{\sqrt{2}+\frac{p}{q}}\right|=\frac{|2q^2-p^2|}{q^2}\cdot\frac{1}{\left|\sqrt{2}+\frac{p}{q}\right|}.$$

Minthogy $\sqrt{2}$ irracionális szám, $2q^2-p^2$ nem lehet 0. Másrészt $2q^2-p^2$ nyilván egész szám, következésképpen $|2q^2-p^2|\geqq 1$. Így (23)-ból

$$(24)\quad \left|\sqrt{2}+\frac{p}{q}\right|\geqq\frac{1}{q^2}\cdot\frac{1}{\left|\sqrt{2}+\frac{p}{q}\right|}.$$

Most esetszétválasztást végzünk.

a. Ha $\left|\sqrt{2}-\frac{p}{q}\right|\geqq 1$, akkor nyilván

$$\left|\sqrt{2}-\frac{p}{q}\right|\geqq 1\geqq\frac{1}{q^2}>\frac{1}{4q^2}.$$

b. Ha $\left|\sqrt{2}-\frac{p}{q}\right| < 1$, akkor (24)-ből

$$\left|\sqrt{2}-\frac{p}{q}\right| \geqq \frac{1}{q^2}\cdot\frac{1}{\left|\sqrt{2}+\frac{p}{q}\right|} = \frac{1}{q^2}\cdot\frac{1}{\left|2\sqrt{2}+\left(\frac{p}{q}-\sqrt{2}\right)\right|} \geqq$$

$$\geqq \frac{1}{q^2}\cdot\frac{1}{2\sqrt{2}+\left|\frac{p}{q}-\sqrt{2}\right|} > \frac{1}{q^2}\cdot\frac{1}{2\sqrt{2}+1} > \frac{1}{4q^2}.$$

2*. LÁNCTÖRTEK

Eddig csak jól approximáló törtek *létezésével* foglalkoztunk, azt azonban nem vizsgáltuk, hogy ezek hogyan határozhatók meg? Ebben a pontban egy olyan eljárást fogunk ismertetni, mely lehetővé teszi *a jól approximáló törtek meghatározását* (legalábbis a homogén, egydimenziós esetben; a többi esetben fellépnek bizonyos nehézségek).

Lánctörtön

$$(25)\qquad a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\ddots+\cfrac{1}{a_{n-1}+\cfrac{1}{a_n}}}}$$

alakú emeletes törtet értünk, ahol n tetszőleges nemnegatív egész szám, és az $a_0, a_1, \ldots, a_n$ számokról egyelőre csak annyit teszünk fel, hogy azok olyan valós számok, melyekre a kijelölt műveletek elvégezhetők (vagyis azok végrehajtása során egyszer sem kell 0-val osztanunk); ha például feltesszük, hogy $a_1, a_2, \ldots, a_n$ pozitív számok, akkor ez a feltétel nyilván teljesül. A (25) lánctörtet rövidség kedvéért $[a_0, a_1, a_2, \ldots, a_n]$-nel fogjuk jelölni.

Ez megegyezik az $a_0, a_1, \ldots, a_n$ számok legkisebb közös többszörösének jelölésével; ez az egyezés azonban nem fog félreértést okozni, mert ebben a pontban nem fogjuk használni a legkisebb közös többszörös fogalmát.

Továbbá az $a_0, a_1, \ldots, a_n$ számokat a (25) lánctört *jegyeinek* fogjuk nevezni.

A lánctörtek definíciójából nyilván következik, hogy $n \geqq 2$ esetén

$$(26) \quad [a_0, a_1, \ldots, a_{n-2}, a_{n-1}, a_n] = \left[a_0, a_1, \ldots, a_{n-2}, a_{n-1} + \frac{1}{a_n}\right] =$$

$$= [a_0, a_1, a_{n-2}, [a_{n-1}, a_n]],$$

vagy még általánosabban, $n \geqq 1$, $1 \leqq k \leqq n$ esetén

$$(27) \quad [a_0, a_1, \ldots, a_{k-1}, a_k, \ldots, a_n] = [a_0, a_1, \ldots, a_{k-1}, [a_k, \ldots, a_n]].$$

Igazolható, hogy a (25) lánctört értéke a következőképpen számítható ki: ha a $P_0, P_1, \ldots, P_n, Q_0, Q_1, \ldots, Q_n$ számokat a

$$(28) \quad P_0 = a_0, \quad P_1 = a_1 a_0 + 1, \quad P_{k+1} = a_{k+1} P_k + P_{k-1},$$

$$(29) \quad Q_0 = 1, \quad Q_1 = a_1, \quad Q_{k+1} = a_{k+1} Q_k + Q_{k-1}$$

(ahol $k = 1, 2, \ldots, n-1$) rekurzió által határozzuk meg, akkor

$$(30) \quad [a_0, a_1, \ldots, a_n] = \frac{P_n}{Q_n}.$$

(Ez az állítás n-re vonatkozó teljes indukcióval igazolható, felhasználva (26)-ot.) Tekintve valamely (25) alakú lánctörtet, képezzük a $\frac{P_0}{Q_0}, \frac{P_1}{Q_1}, \ldots, \frac{P_n}{Q_n}$ hányadosokat; ezeket a (25) szám *közelítő törtjeinek* nevezzük.

(28)-ból és (29)-ből könnyen levezethető (l. a 6. példát), hogy $1 \leqq k \leqq n$ esetén

$$(31) \quad P_k Q_{k-1} - P_{k-1} Q_k = (-1)^{k-1},$$

vagyis $Q_{k-1} Q_k$-val osztva:

$$(32) \quad \frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{(-1)^{k-1}}{Q_{k-1} Q_k},$$

továbbá $2 \leqq k \leqq n$ esetén

$$(33) \quad P_k Q_{k-2} - P_{k-2} Q_k = (-1)^k a_k,$$

vagyis $Q_{k-2}Q_k$-val osztva:

$$(34)\quad \frac{P_k}{Q_k}-\frac{P_{k-2}}{Q_{k-2}}=\frac{(-1)^k a_k}{Q_{k-2}Q_k}.$$

A továbbiakban olyan (25) alakú lánctörtek vizsgálatára fogunk szorítkozni, melyek jegyei — eltekintve esetleg az elsőtől — *pozitívak:*

$$(35)\quad a_1>0,\quad a_2>0,\quad \ldots,\quad a_n>0.$$

Ekkor (32)-ből és (34)-ből könnyen következik, hogy

$$(36)\quad \frac{P_0}{Q_0}<\frac{P_2}{Q_2}<\frac{P_4}{Q_4}<\ldots\leqq[a_0,a_1,\ldots,a_n]\leqq\ldots<$$

$$<\frac{P_5}{Q_5}<\frac{P_3}{Q_3}<\frac{P_1}{Q_1}.$$

Így ekkor a „közelítő tört" elnevezés jogosult legalábbis annyiban, hogy a $\frac{P_k}{Q_k}$ közelítő törtek k növekedtével valóban közelednek a szóban forgó lánctört értékéhez, mégpedig a páros indexűek alulról, a páratlan indexűek felülről (mindkét esetben szigorúan monoton módon).

Eddig csak *véges* lánctörtekkel foglalkoztunk. A *végtelen lánctörtek* a következőképpen definiálhatók:

Legyen adott valamely $a_0, a_1, \ldots, a_n, \ldots$ végtelen sorozat. Ha az $[a_0], [a_0, a_1], \ldots, [a_0, a_1, \ldots, a_n], \ldots$ végtelen számsorozatnak létezik és véges a határértéke, és ez a határérték α-val egyenlő, akkor azt mondjuk, hogy az $[a_0, a_1, \ldots, a_n, \ldots]$ végtelen lánctört *konvergens,* és

$$\alpha=[a_0,a_1,\ldots,a_n,\ldots].$$

A (30) formulára tekintettel ekkor

$$(37)\quad \alpha=[a_0,a_1,\ldots,a_n,\ldots]=\lim_{n\to+\infty}\frac{P_n}{Q_n},$$

ahol a $P_0, P_1, \ldots, Q_0, Q_1, \ldots$ számokat a (28) és (29) rekurziók definiálják.

A fentiekben a legáltalánosabb alakú lánctörteket vizsgáltuk; ebben az általánosságban találkozhatunk lánctörtekkel például az ortogonális sorok elméletében, sőt műszaki alkalmazásaik is ismeretesek. Számelméleti szempontból azonban kitüntetett szerepet játszanak az olyan lánctörtek, melyekre (35) mellett az a feltétel is teljesül, hogy jegyei egész számok; más szóval feltesszük, hogy a_0 *egész szám*, $a_1, a_2, \ldots$ pedig *természetes számok*. Egy ilyen lánctörtet *egyszerű lánctörtnek* fogunk nevezni; minthogy a számelméletben csaknem kizárólag ilyen lánctörtekkel találkozunk, az „egyszerű:" jelzőt — ha ez nem okozhat félreértést — el fogjuk hagyni.

Az egyszerű lánctörtek közelítő törtjeinek egy fontos tulajdonsága kiolvasható (31)-ből. Innen ugyanis nyilván következik, hogy $(P_n, Q_n)|1$, tehát

$$(38) \quad (P_n, Q_n) = 1.$$

Továbbá, ha egyelőre formálisan (tekintet nélkül a konvergenciára) felírunk valamely $[a_0, a_1, \ldots, a_n, \ldots]$ (végtelen) *egyszerű lánctörtet*, akkor a (29) által definiált Q_k természetes számokra $k=1, 2, \ldots$ esetén

$$(39) \quad Q_{k+1} = a_{k+1}Q_k + Q_{k-1} \geqq Q_k + Q_{k-1} > Q_k.$$

Innen következik, hogy $k=1, 2, \ldots$ esetén

$$Q_k \geqq k.$$

Ezt az egyenlőtlenséget felhasználva (32)-ből könnyen levezethető, hogy *bármely végtelen, egyszerű lánctört* konvergens, ezért a továbbiakban nem kell az ilyen lánctörtek konvergenciáját vizsgálnunk.

Tekintsünk valamely $[a_0, a_1, \ldots]$ végtelen lánctörtet; legyen

$$(40) \quad \alpha = [a_0, a_1, \ldots].$$

Minthogy az $[a_1, a_2, \ldots]$, $[a_2, a_3, \ldots]$, ..., $[a_n, a_{n+1}, \ldots]$, ... végtelen lánctörtek szintén egyszerű lánctörtek, ezek is konvergensek. Az $[a_n, a_{n+1}, \ldots]$ lánctörtet az $[a_0, a_1, \ldots]$ lánctört *n-edik maradéktörtjének* nevezzük, és a következőképpen fogjuk jelölni:

$$\alpha_n = [a_n, a_{n+1}, \ldots] \quad (\text{ahol } n = 0, 1, 2. \ldots).$$

A végtelen lánctörtek definíciójából könnyen következik, hogy

$$(41)\quad \alpha = [a_0, a_1, \ldots] = \alpha_0 = a_0 + \frac{1}{\alpha_1} = [a_0, \alpha_1] =$$

$$= \left[a_0, a_1 + \frac{1}{\alpha_2}\right] = [a_0, a_1, \alpha_2] = \ldots = [a_0, a_1, \ldots, a_{n-1}, \alpha_n] = \ldots.$$

A (40) *végtelen*, egyszerű lánctört tehát felírható $[a_0, a_1, \ldots, \ldots, a_{n-1}, \alpha_n]$ alakban, vagyis *véges* lánctörtként; így a véges lánctörtekre fent levezetett formulák alkalmazhatók végtelen egyszerű lánctörtek vizsgálatára is.

Az egyszerű lánctörtek jelentősége abban áll, hogy bármely α valós szám felírható a (40) alakban, ahol a jobb oldalon álló egyszerű lánctört lehet véges és végtelen is. A megfelelő lánctört $a_0, a_1, \ldots, a_n, \ldots$ jegyei az ún. *lánctörtalgoritmus* segítségével határozhatók meg, mely (41)-ből olvasható ki:

Legyen $\alpha_0 = \alpha$, és legyen a_0 ennek egész része, tehát $a_0 = [\alpha] = [\alpha_0]$. Most tegyük fel, hogy α_{k-1}, a_{k-1} már definiálva vannak (ahol $k = 1, 2, \ldots$). Ha $\alpha_{k-1} = a_{k-1}$ (tehát α_{k-1} egész szám), akkor itt megállunk, vagyis α_k-t és a_k-t már nem definiáljuk. Ha pedig $\alpha_{k-1} > a_{k-1}$ (vagyis α_{k-1} nem egész szám), akkor definiáljuk α_k-t az

$$(42)\quad \alpha_{k-1} = a_{k-1} + \frac{1}{\alpha_k}$$

azaz

$$\alpha_k = \frac{1}{\alpha_{k-1} - a_{k-1}}$$

egyenlőséggel, és legyen $a_k = [\alpha_k]$. Igazolható, hogy az $a_0, a_1, \ldots$ (véges vagy végtelen) sorozatot így definiálva, (40) teljesül.

Adott α mellett a (40)-et kielégítő $[a_0, a_1, \ldots]$ lánctört jegyeinek meghatározását α *lánctörtbe fejtésének* mondjuk.

Nyilvánvaló, hogy bármely *véges* egyszerű lánctört *racionális* számot állít elő. Másrészt állítjuk, hogy bármely $\alpha = \frac{c}{d}$ (ahol c egész szám, d természetes szám) racionális számot a fentiek

szerint lánctörtbe fejtve, szükségképpen *véges* lánctörtet nyerünk. Ez következik abból a szoros kapcsolatból, mely a $\frac{c}{d}$ szám lánctörtbe fejtésére szolgáló *lánctörtalgoritmus*, ill. a (c, d) meghatározására szolgáló *euklideszi algoritmus* közt fennáll.

Legyenek ugyanis ez utóbbi egyes lépései az alábbiak:

$$c = q_1 d + r_1,$$

$$d = q_2 r_1 + r_2,$$

$$r_1 = q_3 r_2 + r_3,$$

$$\cdots\cdots\cdots\cdots$$

$$r_{n-2} = q_n r_{n-1} + r_n,$$

$$r_{n-1} = q_{n+1} r_n.$$

Az első egyenlőséget d-vel osztva:

$$\alpha = \frac{c}{d} = q_1 + \frac{r_1}{d},$$

ahonnan kiolvasható, hogy $a_0 = q_1, \alpha_1 = \frac{d}{r_1}$. A második egyenlőséget r_1-gyel osztva:

$$\alpha_1 = \frac{d}{r_1} = q_2 + \frac{r_2}{r_1},$$

ahonnan nyerjük, hogy $a_1 = q_2, \alpha_2 = \frac{r_1}{r_2}$ s í. t. Látható, hogy az euklideszi algoritmus egyes egyenlőségeit elosztva az osztóval, tehát rendre $q, r_1, r_2, \ldots, r_n$-nel, éppen a lánctörtalgoritmus (42) alakú egyenlőségeit kapjuk. Az euklideszi algoritmusról azonban már tudjuk, hogy véges sok lépés után véget ér, tehát a megfelelő lánctörtalgoritmus (mely ugyanannyi lépésből áll) szintén véget ér véges sok lépés után, és így valóban véges lánctörtet nyerünk.

Végeredményben tehát egy valós szám akkor és csak akkor fejthető *véges* lánctörtbe, ha *racionális* szám, és akkor és csak akkor *végtelen* lánctörtbe, ha *irracionális* szám.

Ha $[a_0, a_1, \ldots, a_{n-1}, a_n]$ tetszőleges véges lánctört, akkor $a_n \geqq 2$ esetén nyilván

$$[a_0, a_1, \ldots, a_{n-1}, a_n] = [a_0, a_1, \ldots, a_{n-1}, a_n - 1, 1],$$

míg $a_n = 1$ esetén

$$[a_0, a_1, \ldots, a_{n-1}, a_n] = [a_0, a_1, \ldots, a_{n-1}, 1] =$$
$$= [a_0, a_1, \ldots, a_{n-1} + 1],$$

tehát bármely racionális szám kétféleképpen is lánctörtbe fejthető. Másrészt meglehetősen könnyen igazolható, hogy ettől a kivételtől eltekintve, a valós számok lánctörtbe fejtése egyértelmű. Pontosabban: ha $[a_0, a_1, \ldots]$ *végtelen*, $[b_0, b_1, \ldots]$ tetszőleges egyszerű lánctört és

$$[a_0, a_1, \ldots] = [b_0, b_1, \ldots],$$

akkor szükségképpen a jobb oldalon álló lánctört is végtelen, és

$$a_0 = b_0, \quad a_1 = b_1, \quad \ldots, \quad a_n = b_n, \quad \ldots;$$

ha továbbá valamely véges, egyszerű lánctörtekre

$$[a_0, a_1, \ldots, a_M] = [b_0, b_1, \cdots, b_N]$$

és

$$a_M > 1, \quad b_N > 1$$

teljesül, akkor szükségképpen $M = N$ és

$$a_0 = b_0, \quad a_1 = b_1, \quad \ldots, \quad a_M = b_N.$$

Ezt a tényt röviden úgy fejezhetjük ki, hogy a valós számok lánctörtbe fejtése *lényegében egyértelmű.*

Ezzel befejeztük a lánctörtek alaptulajdonságainak ismertetését. Foglaljuk össze az eddigieket (figyelembe véve, hogy a (41) összefüggés alapján a véges lánctörtekről elmondottak a végtelen lánctörtekre is adaptálhatók):

Bármely valós szám a leírt lánctört algoritmus segítségével egyszerű lánctörtbe fejthető. Irracionális számot lánctörtbe fejtve, egy egyértelműen meghatározott végtelen lánctörtet, míg racionális számot lánctörtbe fejtve, egy lényegében egyértelműen meghatározott véges lánctörtet nyerünk. Valamely $[a_0, a_1, \ldots]$ egyszerű lánctört közelítő törtjei a (28) és (29) rekurzív összefüggések segítségével határozhatók meg, és kielégítik a (31), (32), (34), (36) (végtelen lánctört esetén $[a_0, a_1, \ldots, a_n]$ helyére $[a_0, a_1, \ldots]$-et írva), (41) összefüggéseket, valamint véges lánctörtek esetén (30)-at, végtelen lánctörtek esetén (37)-et.

Áttérünk a lánctörteknek a Dirichlet-tétellel kapcsolatos alkalmazásaira. Legyen α tetszőleges irracionális szám, és fejtsük (végtelen) lánctörtbe. Ekkor

$$\alpha = [a_0, a_1, \ldots, a_n, a_{n+1}, \ldots] = [a_0, a_1, \ldots, a_n, \alpha_{n+1}].$$

Legyenek $[a_0, a_1, \ldots]$ közelítő törtjei $\frac{P_0}{Q_0}, \frac{P_1}{Q_1}, \ldots$, az

(43) $[a_0, a_1, \ldots, a_n, \alpha_{n+1}]$

lánctörtéi pedig $\frac{P_0}{Q_0}, \frac{P_0}{Q_1}, \ldots, \frac{P_n}{Q_n}, \frac{P'_{n+1}}{Q'_{n+1}}$ (az első $n+1$ közelítő tört nyilván megegyezik). A (43) lánctörtre alkalmazva (30)-at (n helyén $n+1$-gyel):

$$(44) \quad \alpha = [a_0, a_1, \ldots, a_n, \alpha_{n+1}] = \frac{P'_{n+1}}{Q'_{n+1}},$$

továbbá (32)-ből (k helyén $n+1$-gyel):

$$(45) \quad \frac{P'_{n+1}}{Q'_{n+1}} - \frac{P_n}{Q_n} = \frac{(-1)^n}{Q_n Q'_{n+1}}.$$

Itt (29)-re tekintettel

$$(46) \quad Q'_{n+1} = \alpha_{n+1} Q_n + Q_{n-1} > 1 \cdot Q_n + 0 = Q_n$$

(nyilván az $\alpha_1, \alpha_2, \ldots$ maradéktörtek mindegyike legalább 1). (44)-ből és (45)-ből (46)-ra tekintettel nyerjük, hogy

$$\left|\alpha - \frac{P_n}{Q_n}\right| = \left|\frac{P'_{n+1}}{Q'_{n+1}} - \frac{P_n}{Q_n}\right| = \frac{1}{Q_n Q'_{n+1}} < \frac{1}{Q_n \cdot Q_n} = \frac{1}{Q_n^2}.$$

Ezzel új — mégpedig konstruktív — bizonyítást nyertünk Dirichlet tételére, amennyiben igazoltuk, hogy egy α irracionális számot lánctörtbe fejtve, e lánctört közelítő törtjei (melyek (38) és (39) szerint különböznek egymástól) kielégítik a Dirichlet tételében szereplő (4) egyenlőtlenséget. (Tehát valóban teljes mértékben jogosult a „közelítő tört" elnevezés, hiszen ezek szerint — egyszerű lánctörtek esetén — a közelítő törtek kivétel nélkül jól approximáló törtek.) Sőt, némi fárad-

sággal az is igazolható, hogy bármely két egymást követő közelítő tört közül az egyik kielégíti az

$$(47) \quad \left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$$

egyenlőtlenséget (l. a 15*. feladatot), bármely három közül az egyik (6)-ot.

Másrészt igazolható, hogy ha valamely $\frac{p}{q}$ racionális szám kielégíti (47)-et és a $(p, q)=1$ feltételt, akkor $\frac{p}{q}$ szükségképpen közelítő törtje α-nak.

Példák

4. Fejtsük lánctörtbe az $\alpha=\frac{43}{19}$ számot!

Megoldás:

A 43 és 19 számokra vonatkozó euklideszi algoritmust az ismertetett módon lánctörtalgoritmussá átalakítva:

$$\frac{43}{19} = 2+\frac{5}{19},$$

$$\frac{19}{5} = 3+\frac{4}{5},$$

$$\frac{5}{4} = 1+\frac{1}{4},$$

$$\frac{4}{1} = 4.$$

A jobb oldalak első tagjai adják a lánctörtjegyeket:

$$\frac{43}{19} = [2, 3, 1, 4].$$

5. Fejtsük lánctörtbe az $\alpha = \frac{\sqrt{5}+1}{2}$ számot!

Megoldás:

$$a_0 = [\alpha] = \left[\frac{2,2\ldots+1}{2}\right] = [1,6\ldots] = 1,$$

$$\alpha_1 = \frac{1}{\alpha - a_0} = \frac{1}{\frac{\sqrt{5}+1}{2}-1} = \frac{2}{\sqrt{5}-1} = \frac{2(\sqrt{5}+1)}{(\sqrt{5}-1)(\sqrt{5}+1)} =$$

$$= \frac{2(\sqrt{5}+1)}{4} = \frac{\sqrt{5}+1}{2} = \alpha.$$

Így

$$\alpha = [a_0, \alpha_1] = [1, \alpha] = [1, [a_0, \alpha_1]] = [1, 1, \alpha] =$$

$$= [1, 1, [a_0, \alpha_1]] = [1, 1, 1, \alpha] = \ldots = [1, 1, 1, \ldots],$$

tehát α lánctörtbe fejtésének valamennyi jegye 1-es.

Megjegyezzük, hogy α közelítő törtjei érdekes kapcsolatban vannak az ún. *Fibonacci-sorozattal.* Fibonacci-sorozatnak a

$$b_0 = b_1 = 1, \quad b_k = b_{k-1} + b_{k-2} \quad (\text{ahol } k = 2, 3, \ldots)$$

rekurzióval definiált végtelen sorozatot nevezzük. Ezt a rekurziót egybevetve a (28) és (29) rekurziókkal, látható, hogy $k=0, 1, 2, \ldots$ esetén $P_k = b_{k+1}$ és $Q_k = b_k$, tehát $\frac{\sqrt{5}+1}{2}$ közelítő törtjei $\frac{P_n}{Q_n} = \frac{b_{n+1}}{b_n}$ alakúak.

6. Igazoljuk (31)-et!

Megoldás:

A (28) és (29) rekurziókat alkalmazva:

$$P_k Q_{k-1} - P_{k-1} Q_k = (a_k P_{k-1} + P_{k-2}) Q_{k-1} - P_{k-1}(a_k Q_{k-1} + Q_{k-2}) =$$

$$= P_{k-2} Q_{k-1} - P_{k-1} Q_{k-2} = -(P_{k-1} Q_{k-2} - P_{k-2} Q_{k-1}).$$

Ezt az átalakítást megismételve k helyén $k-1$-gyel, majd $k-2$-vel s í. t., nyerjük, hogy

$$P_k Q_{k-1} - P_{k-1} Q_k = -(P_{k-1} Q_{k-2} - P_{k-2} Q_{k-1}) =$$

$$= (-1)^2 (P_{k-2} Q_{k-3} - P_{k-3} Q_{k-2}) = \ldots = (-1)^{k-1} (P_1 Q_0 - P_0 Q_1) =$$

$$= (-1)^{k-1} ((a_1 a_0 + 1) \cdot 1 - a_0 \cdot a_1) = (-1)^{k-1}.$$

FELADATOK

1. Legyen α adott valós szám. Bizonyítsuk be, hogy ha tetszőlegesen kicsi ε pozitív számhoz található p egész szám és q természetes szám, melyekre

$$(48)\quad 0 < \left|\alpha - \frac{p}{q}\right| < \frac{\varepsilon}{q}$$

teljesül, akkor α irracionális szám!

2*. Bizonyítsuk be, hogy az

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{n!} + \ldots$$

szám irracionális!

3. Legyen D négyzetszámtól különböző természetes szám. Bizonyítsuk be, hogy bármely p egész számra és q természetes számra

$$\left|\sqrt{D} - \frac{p}{q}\right| > \frac{1}{(2\sqrt{D}+1)q^2}.$$

4*. Bizonyítsuk be, hogy tetszőlegesen kicsi ε pozitív számot megadva, található olyan q_0 szám, hogy ha p, q egészek, és $q > q_0$, akkor

$$(49)\quad \left|\frac{\sqrt{5}+1}{2} - \frac{p}{q}\right| > \frac{1}{(\sqrt{5}+\varepsilon)q^2}.$$

5. Legyen n 1-nél nagyobb természetes szám. Bizonyítsuk be, hogy tetszőleges p egész számra és q természetes számra

$$\left|\sqrt[n]{2} - \frac{p}{q}\right| > \frac{1}{n2^{n-1}q^n}.$$

6. Bizonyítsuk be, hogy tetszőlegesen kicsi ε pozitív számot megadva, található végtelen sok olyan n természetes szám, melyre

$$|\sin n| < \varepsilon.$$

7. Legyenek α, β tetszőleges valós számok, ε tetszőlegesen kicsi pozitív szám. Bizonyítsuk be, hogy létezik végtelen sok olyan m, n — egész számokból álló — számpár, melyre

$$(50) \quad |m\alpha + n\beta| < \varepsilon.$$

8*. Liouville tételét felhasználva, igazoljuk, hogy az

$$\alpha = \sum_{k=1}^{+\infty} \frac{1}{2^{k!}}$$

szám transzcendens!

9*. Bizonyítsuk be, hogy tetszőleges α_1, α_2 irracionális számokat megadva, található végtelen sok q természetes szám és ezekhez p_1, p_2 egész számok, melyekre

$$(51) \quad \left|\alpha_1 - \frac{p_1}{q}\right| < \frac{1}{q^{\frac{3}{2}}}$$

és

$$(52) \quad \left|\alpha_2 - \frac{p_2}{q}\right| < \frac{1}{q^{\frac{3}{2}}}$$

teljesül!

10. Legyen D négyzetszámtól különböző természetes szám. Bizonyítsuk be, hogy ha az x_0, y_0 természetes számok kielégítik az

$$(53) \quad x^2 - Dy^2 = 1$$

Pell-egyenletet (l. az V. fejezet 11. feladatát), akkor szükségképpen

$$\left|\sqrt{D} - \frac{x_0}{y_0}\right| < \frac{1}{\sqrt{D}y_0^2}.$$

Megjegyezzük, hogy fordított irányban is okoskodhatunk, amennyiben $\sqrt{D}$-t „jól approximáló" $\frac{x_0}{y_0}$ racionális számok létezéséből levezethető, hogy (54)-nek létezik nemtriviális — $x=1, y=0$-tól különböző — megoldása.

11. Keressük meg $\pi=3{,}1415926\ldots$ első három közelítő törtjét, és e $\frac{p}{q}$ közelítő törtekre hasonlítsuk össze $\left|\pi-\frac{p}{q}\right|$ és $\frac{1}{q^2}$ értékét!

12. Fejtsük lánctörtbe az $\alpha=-\frac{69}{32}$ számot!

13. Fejtsük lánctörtbe az $\alpha=\sqrt{2}$ számot!

14*. Legyen n 1-nél nagyobb természetes szám. Fejtsük lánctörtbe az $\alpha=\sqrt{n^2-1}$ számot!

15*. Bizonyítsuk be, hogy valamely α irracionális szám két egymást követő közelítő törtje közül az egyik kielégíti a (47) egyenlőtlenséget!

16*. Bizonyítsuk be, hogy ha az α irracionális szám lánctörtjegyeinek sorozata valahonnan kezdve periodikus, akkor α másodfokú algebrai szám (l. az V. fejezet 4. pontját)!

A VI. FEJEZETBEN KITŰZÖTT FELADATOK MEGOLDÁSAI

1. Tegyük fel indirekte, hogy $\alpha=\frac{r}{s}$, ahol r, s egész számok, $s\neq 0$. Ekkor tetszőleges p egész számra és q természetes számra $\left|\alpha-\frac{p}{q}\right|\neq 0$ esetén

$$\left|\alpha-\frac{p}{q}\right| = \left|\frac{r}{s}-\frac{p}{q}\right| = \frac{|rq-ps|}{|sq|} \geqq \frac{1}{|sq|} = \frac{1}{|s|}\cdot\frac{1}{q},$$

tehát $\varepsilon=\frac{1}{|s|}$-et választva, a (48) feltétel semmilyen p, q párra sem teljesülhet. Így az indirekt feltevésből ellentmondásra jutottunk, és ezzel az állítást igazoltuk.

2*. $n=1, 2, \ldots$ esetén nyilván

$$1+\frac{1}{1!}+\frac{1}{2!}+\ldots+\frac{1}{n!} = \frac{a_n}{n!},$$

ahol a_n alkalmas természetes szám. Ekkor a végtelen mértani sor összegképletét felhasználva:

$$(54)\qquad 0 < e-\frac{a_n}{n!} = \frac{1}{(n+1)!}+\frac{1}{(n+2)!}+\ldots+\frac{1}{(n+k)!}+\ldots =$$

$$= \frac{1}{n!}\left(\frac{1}{n+1}+\frac{1}{(n+1)(n+2)}+\ldots+\frac{1}{(n+1)\ldots(n+k)}+\ldots\right) <$$

$$< \frac{1}{n!}\left(\frac{1}{n+1}+\frac{1}{(n+1)^2}+\ldots+\frac{1}{(n+1)^k}+\ldots\right) =$$

$$= \frac{1}{n!}\cdot\frac{1}{n+1}\cdot\frac{1}{1-\frac{1}{n+1}} \leqq \frac{1}{n!}\cdot\frac{1}{n+1}\cdot\frac{1}{1-\frac{1}{2}} = \frac{2}{n+1}\cdot\frac{1}{n!}.$$

Tetszőlegesen kicsi ε pozitív számot megadva, elég nagy n-re nyilván $\frac{2}{n+1}<\varepsilon$. Ekkor azonban (54)-ből

$$0 < e-\frac{a_n}{n!} < \frac{\varepsilon}{n!},$$

tehát $p=a_n$, $q=n!$ választással (48) teljesül (bárhogyan választottuk is ε-t), és így az 1. feladat szerint e valóban irracionális szám.

3. Minthogy D nem négyzetszám,

$$\left|\sqrt{D}-\frac{p}{q}\right| = \frac{1}{\left|\sqrt{D}+\frac{p}{q}\right|}\cdot\left|\sqrt{D}-\frac{p}{q}\right|\left|\sqrt{D}+\frac{p}{q}\right| =$$

$$= \frac{1}{\left|\sqrt{D}+\frac{p}{q}\right|}\cdot\left|D-\frac{p^2}{q^2}\right| = \frac{1}{\left|\sqrt{D}+\frac{p}{q}\right|}\cdot\frac{|Dq^2-p^2|}{q^2} \geqq \frac{1}{\left|\sqrt{D}+\frac{p}{q}\right|q^2}.$$

Ha $\left|\sqrt{D}-\frac{p}{q}\right| < 1$, akkor innen az

(55) $\quad |a+b| \leqq |a|+|b|$

egyenlőtlenség alapján

$$\left|\sqrt{D}-\frac{p}{q}\right| \geqq \frac{1}{\left|\sqrt{D}+\frac{p}{q}\right|q^2} = \frac{1}{\left|2\sqrt{D}+\left(\frac{p}{q}-\sqrt{D}\right)\right|q^2} \geqq$$

$$\geqq \frac{1}{\left(2\sqrt{D}+\left|\frac{p}{q}-\sqrt{D}\right|\right)q^2} > \frac{1}{(2\sqrt{D}+1)q^2}.$$

Ha viszont $\left|\sqrt{D}-\frac{p}{q}\right| \geqq 1$, akkor

$$\left|\sqrt{D}-\frac{p}{q}\right| \geqq 1 \geqq \frac{1}{q^2} > \frac{1}{(2\sqrt{D}+1)q^2}.$$

4*. Tetszőleges p, q $(q\neq 0)$ egészekre

$$\left|\frac{\sqrt{5}+1}{2}-\frac{p}{q}\right|\left|\frac{-\sqrt{5}+1}{2}-\frac{p}{q}\right| = \left|\frac{p^2}{q^2}-\frac{p}{q}-1\right| = \frac{|p^2-pq-q^2|}{q^2}.$$

Itt a számlálóban nemnegatív egész szám áll. Ez a szám 0-tól különböző (ellenkező esetben innen az következnék, hogy $\sqrt{5}$ racionális szám), tehát legalább 1:

$$(56)\qquad \left|\frac{\sqrt{5}+1}{2}-\frac{p}{q}\right|\left|\frac{-\sqrt{5}+1}{2}-\frac{p}{q}\right| \geqq \frac{1}{q^2}.$$

Tegyük fel most indirekte, hogy valamely ε pozitív számhoz találhatók $q_1, q_2, \ldots, q_n, \ldots$ természetes számok és ezekhez $p_1, p_2, \ldots, p_n, \ldots$ egész számok, melyekre

$$(57)\qquad \left|\frac{\sqrt{5}+1}{2}-\frac{p_n}{q_n}\right| \leqq \frac{1}{(\sqrt{5}+\varepsilon)q_n^2} \qquad (n = 1, 2, \ldots)$$

és

$$(58)\qquad q_1 < q_2 < \ldots < q_n < \ldots$$

teljesül.

(56) bal oldalán $p=p_n$-et, $q=q_n$-et írva, az így nyert kifejezés (55) és (57) alapján a következőképpen becsülhető felülről:

$$(59)\qquad \left|\frac{\sqrt{5}+1}{2}-\frac{p_n}{q_n}\right|\left|\frac{-\sqrt{5}+1}{2}-\frac{p_n}{q_n}\right| =$$

$$= \left|\frac{\sqrt{5}+1}{2}-\frac{p_n}{q_n}\right|\left|-\sqrt{5}+\left(\frac{\sqrt{5}+1}{2}-\frac{p_n}{q_n}\right)\right| \leqq$$

$$\leqq \left|\frac{\sqrt{5}+1}{2}-\frac{p_n}{q_n}\right|\left(\sqrt{5}+\left|\frac{\sqrt{5}+1}{2}-\frac{p_n}{q_n}\right|\right) \leqq$$

$$\leqq \frac{1}{(\sqrt{5}+\varepsilon)q_n^2}\left(\sqrt{5}+\frac{1}{(\sqrt{5}+\varepsilon)q_n^2}\right) \leqq \frac{1}{(\sqrt{5}+\varepsilon)q_n^2}\left(\sqrt{5}+\frac{1}{q_n^2}\right).$$

(58)-ra tekintettel létezik olyan n_0 szám, hogy $n>n_0$ esetén $\frac{1}{q_n^2}<\varepsilon$. (59)-ből $n>n_0$ esetén

$$\left|\frac{\sqrt{5}+1}{2}-\frac{p_n}{q_n}\right|\left|\frac{-\sqrt{5}+1}{2}-\frac{p_n}{q_n}\right| < \frac{1}{(\sqrt{5}+\varepsilon)q_n^2}(\sqrt{5}+\varepsilon) = \frac{1}{q_n^2},$$

ami ellentmond (56)-nak (mely *bármely* p egész számra és q természetes számra fennáll). Így az indirekt feltevésből ellentmondásra jutottunk, és ezzel az állítást igazoltuk.

5. Minthogy $\sqrt[n]{2}$ ($n>1$-re tekintettel) irracionális szám, nyilván

$$(60)\qquad \frac{|2q^n-p^n|}{q^n} \geqq \frac{1}{q^n},$$

Másrészt az I. fejezetben szereplő (7) azonosság alapján

$$\frac{|2q^n-p^n|}{q^n} = \left|2-\frac{p^n}{q^n}\right| =$$

$$= \left|\sqrt[n]{2}-\frac{p}{q}\right| \left|\left(\sqrt[n]{2}\right)^{n-1}+\left(\sqrt[n]{2}\right)^{n-2}\cdot\frac{p}{q}+\left(\sqrt[n]{2}\right)^{n-3}\left(\frac{p}{q}\right)^2+\ldots+\right.$$

$$\left.+\sqrt[n]{2}\left(\frac{p}{q}\right)^{n-2}+\left(\frac{p}{q}\right)^{n-1}\right|.$$

Ha $0<\frac{p}{q}<2$, akkor innen nyilván

$$(61)\qquad \frac{|2q^n-p^n|}{q^n} < \left|\sqrt[n]{2}-\frac{p}{q}\right| \left|\left(\sqrt[n]{2}\right)^{n-1}+\left(\sqrt[n]{2}\right)^{n-2}\cdot 2+\left(\sqrt[n]{2}\right)^{n-3}\cdot 2^2+\right.$$

$$\left.+\ldots+\sqrt[n]{2}\cdot 2^{n-2}+2^{n-1}\right| \leqq$$

$$< \left|\sqrt[n]{2}-\frac{p}{q}\right| |2^{n-1}+2^{n-2}\cdot 2+2^{n-3}\cdot 2^2+\ldots+2\cdot 2^{n-2}+2^{n-1}| =$$

$$= \left|\sqrt[n]{2}-\frac{p}{q}\right|\cdot n2^{n-1}.$$

(60)-ból és (61)-ből nyerjük, hogy

$$\left|\sqrt[n]{2}-\frac{p}{q}\right|\cdot n2^{n-1} > \frac{1}{q^n},$$

ahonnan $n2^{n-1}$-gyel osztva, adódik az állítás.

Ha viszont $\frac{p}{q}\leqq 0$ vagy $\frac{p}{q}\geqq 2$, akkor ($n>1$-re tekintettel) nyilván

$$\left|\sqrt[n]{2}-\frac{p}{q}\right| \geqq \left|2-\sqrt[n]{2}\right| \geqq |2-\sqrt{2}| > \frac{1}{2} \geqq \frac{1}{n} \geqq \frac{1}{n2^{n-1}q^n},$$

tehát a bizonyítandó egyenlőtlenség ebben az esetben is teljesül.

6. A $\sin x$ függvény periódushossza 2π, tehát teszőleges m egész számra

(62) $\sin(n-2m\pi) = \sin n.$

Továbbá a $\sin x$ függvény folytonos, és $\sin 0=0$, tehát tetszőleges ε pozitív számot megadva, létezik olyan δ pozitív szám, hogy $|x|<\delta$ esetén

(63) $|\sin x| < \varepsilon \quad (|x| < \delta).$

Ha tehát az n természetes számra és az m egész számra

(64) $|n-2m\pi| < \delta$

teljesül, akkor (62) és (63) szerint szükségképpen

$$|\sin n| = |\sin(n-2m\pi)| < \varepsilon$$

is fennáll. Elég tehát azt igazolni, hogy létezik végtelen sok olyan n természetes szám, hogy alkalmas m egész számmal (64) teljesül.

(64)-et elosztva $2\pi n$-nel, ekvivalens egyenlőtlenséget kapunk:

(65) $$\left|\frac{1}{2\pi}-\frac{m}{n}\right| < \frac{\delta}{2\pi}\cdot\frac{1}{n}.$$

Minthogy π irracionális szám, $\frac{1}{2\pi}$ is az. Így Dirichlet tétele szerint létezik végtelen sok olyan q természetes szám, hogy alkalmas p egész számra

(66) $$\left|\frac{1}{2\pi}-\frac{p}{q}\right| < \frac{1}{q^2}.$$

Ha itt q elég nagy, akkor $q>\frac{2\pi}{\delta}$. Ekkor (66)-ból

$$\left|\frac{1}{2\pi}-\frac{p}{q}\right| < \frac{1}{q^2} = \frac{1}{q}\cdot\frac{1}{q} < \frac{\delta}{2\pi}\cdot\frac{1}{q},$$

tehát $m=p$, $q=n$ választással (65) teljesül, és ezzel az állítást igazoltuk.

7. Tegyük fel először, hogy léteznek olyan m_0, n_0 egész számok, melyek közül legalább az egyik 0-tól különböző, és

(67) $m_0\alpha+n_0\beta = 0$

(vagyis α, β lineárisan összefüggők a racionális számtest felett). Mindkét oldalt szorozva valamely t egész számmal:

$$(m_0 t)\alpha+(n_0 t)\beta = 0.$$

Így $m=m_0t$, $n=n_0t$ (ahol $t=0, \pm 1, \pm 2, \ldots$) választással (50) teljesül *bármely* ε pozitív számra.

Most tegyük fel, hogy ha az m_0, n_0 egész számok kielégítik (67)-et, akkor szükségképpen $m_0=n_0=0$ (vagyis α, β lineárisan függetlenek a racionális számtest felett). Ha $\beta=0$, akkor $m_0=0$, $n_0=\pm 1$, ± 2, ± 3, ... választással, ha pedig $\frac{\alpha}{\beta}=\frac{p}{q}$ (ahol p, q egész számok, $q\neq 0$), akkor $m_0=qt$, $n_0=-pt$ (ahol $t=\pm 1$, ± 2, ...) választással (67) teljesülne; így feltevésünkből következik, hogy $\beta\neq 0$ és $\frac{\alpha}{\beta}$ irracionális szám. Ekkor Dirichlet tétele szerint léteznek $q_1, q_2, \ldots, q_k, \ldots$ természetes számok és ezekhez $p_1, p_2, \ldots, p_k, \ldots$ egész számok, melyekre

$$\left|\frac{\alpha}{\beta}-\frac{p_k}{q_k}\right|<\frac{1}{q_k^2}.$$

Mindkét oldalt $q_k\beta$-val szorozva:

$$|q_k\alpha-p_k\beta|<\frac{\beta}{q_k}.$$

Innen látható, hogy tetszőlegesen kicsi ε pozitív számot megadva, $\frac{\beta}{q_k}<\varepsilon$, vagyis $\frac{\beta}{\varepsilon}<q_k$ esetén (tehát minden elég nagy q_k-ra) $m=q_k$, $n=-p_k$ választással (50) teljesül, és ezzel az állítást igazoltuk.

8*. Meg fogjuk mutatni, hogy az α-t definiáló végtelen sor részletösszegei olyan „jól" approximálják α-t, hogy α — Liouville tétele alapján — nem lehet algebrai szám.

Az említett végtelen sor N-edik ($N=1, 2, \ldots$) részletösszege az összegzés elvégzése után nyilván a következő alakban írható:

$$\sum_{k=1}^{N}\frac{1}{2^{k!}}=\frac{a_N}{2^{N!}},$$

ahol a_N (pozitív) egész szám. Továbbá $i=2, 3, \ldots$ esetén

$$\frac{1}{2^{(N+i)!}}=\frac{1}{2^{(N+1)!}}\cdot\frac{1}{2^{(N+i)!-(N+1)!}}=$$

$$=\frac{1}{2^{(N+1)!}}\cdot\frac{1}{2^{(N+1)![(N+2)\ldots(N+i)-1]}}\leqq$$

$$\leqq\frac{1}{2^{(N+1)!}}\cdot\frac{1}{2^{(N+1)![(N+i)-1]}}\leqq\frac{1}{2^{(N+1)!}}\cdot\frac{1}{2^{i-1}}.$$

Így (a végtelen mértani sor összegképletét felhasználva):

$$\left|\alpha-\frac{a_N}{2^{N!}}\right| = \left|\alpha-\sum_{k=1}^{N}\frac{1}{2^{k!}}\right| = \sum_{k=N+1}^{+\infty}\frac{1}{2^{k!}} =$$

$$= \sum_{i=1}^{+\infty}\frac{1}{2^{(N+i)!}} = \frac{1}{2^{(N+1)!}}+\sum_{i=2}^{+\infty}\frac{1}{2^{(N+i)!}} \leqq$$

$$\leqq \frac{1}{2^{(N+1)!}}+\sum_{i=2}^{+\infty}\frac{1}{2^{(N+1)!}}\cdot\frac{1}{2^{i-1}} = \frac{1}{2^{(N+1)!}}\sum_{i=0}^{+\infty}\frac{1}{2^i} =$$

$$= \frac{1}{2^{(N+1)!}}\cdot\frac{1}{1-\frac{1}{2}} = \frac{2}{2^{(N+1)!}} = \frac{2}{(2^{N!})^{N+1}} \leqq \frac{2^{N!}}{(2^{N!})^{N+1}} =$$

$$= \frac{1}{(2^{N!})^N}.$$

Ha tehát $p_N = a_N$, $q_N = 2^{N!}$, akkor azt nyerjük, hogy

$$\left|\alpha-\frac{p_N}{q_N}\right| < \frac{1}{q_N^N}.$$

Innen nyilván következik, hogy tetszőleges c pozitív számot és n természetes számot rögzítve, elég nagy N-re

$$\left|\alpha-\frac{p_N}{q_N}\right| < \frac{1}{q_N^N} = \frac{1}{q_N^n}\cdot\frac{1}{q_N^{N-n}} < \frac{c}{q_N^n},$$

tehát a (7) egyenlőtlenség nem teljesül. Így Liouville tétele szerint α nem lehet n-edfokú algebrai szám semmilyen n-re sem, vagyis α szükségképpen transzcendens szám.

9*. Legyen Q tetszőleges természetes szám. Tekintsük a (síkbeli) derékszögű koordináta rendszerben azon $P_1, P_2, \ldots, P_{Q^2+1}$ pontokat, melyek derékszögű koordinátái rendre $(\alpha_1-[\alpha_1];\ \alpha_2-[\alpha_2])$, $(2\alpha_1-[2\alpha_1];\ 2\alpha_2-[2\alpha_2]), \ldots, ((Q^2+1)\alpha_1-[(Q^2+1)\alpha_1];\ (Q^2+1)\alpha_2-[(Q^2+1)\alpha_2])$. E pontok mindegyikét tartalmazza az az egységnégyzet, melyet a $0\leqq x<1$, $0\leqq y<1$ feltételt kielégítő $(x; y)$ pontok alkotnak. Osszuk fel ezt a négyzetet $\frac{1}{Q}$ oldalhosszúságú, Q^2 számú „kis" négyzetre úgy, hogy az egyes négyzetek az $\frac{i}{Q}\leqq x<\frac{i+1}{Q}$, $\frac{j}{Q}\leqq y<\frac{j+1}{Q}$ feltételt kielégítő $(x; y)$ pontokból álljanak (ahol $0\leqq i\leqq Q-1$, $0\leqq j\leqq Q-1$). E „kis" négyzetek száma

Q^2, és a Q^2+1 számú P_i pont mindegyike a „kis" négyzetek valamelyikébe esik; így a skatulyaelv értelmében található két olyan pont, mondjuk P_i és P_j — ahol $1 \leqq i < j \leqq Q^2+1$ —, melyek ugyanabba a „kis" négyzetbe senek. Ekkor a két pont abszcisszáinak, ill. ordinátáinak különbsége kisebb, mint a „kis" négyzetek oldalhossza, vagyis $\frac{1}{Q}$:

$$|(j\alpha_1 - [j\alpha_1]) - (i\alpha_1 - [i\alpha_1])| < \frac{1}{Q},$$

$$|(j\alpha_2 - [j\alpha_2]) - (i\alpha_2 - [i\alpha_2])| < \frac{1}{Q}.$$

Legyen $j-i=q$, $[j\alpha_1]-[i\alpha_1]=p_1$, $[j\alpha_2]-[i\alpha_2]=p_2$. Ekkor nyilván

$$(68) \qquad 1 \leqq q \leqq Q^2,$$

továbbá a fenti egyenlőtlenségek a következő alakban írhatók:

$$|q\alpha_1 - p_1| < \frac{1}{Q},$$

$$|q\alpha_2 - p_2| < \frac{1}{Q},$$

vagyis q-val osztva:

$$(69) \qquad \left|\alpha_1 - \frac{p_1}{q}\right| < \frac{1}{qQ},$$

$$(70) \qquad \left|\alpha_2 - \frac{p_2}{q}\right| < \frac{1}{qQ}.$$

(68)-ból következik, hogy $q^{\frac{1}{2}} \leqq Q$; így (69)-ből, ill. (70)-ből adódik (51), ill. (52).

Bizonyítanunk kell még, hogy abból, hogy *tetszőleges* Q természetes számhoz találhatók (69)-et és (70)-et kielégítő p_1, p_2, q számok, következik, hogy *végtelen sok* olyan p_1, p_2, q számhármas létezik, melyre (51) és (52) teljesül. Ez ugyanúgy igazolható, mint az 1. példa állításából kiindulva a 2. példa állítása; a részletek kidolgozását az Olvasóra bízzuk.

10*. Ha x_0, y_0 megoldása az (53) egyenletnek, akkor

$$x_0^2 - Dy_0^2 = (x_0 - \sqrt{D}y_0)(x_0 + \sqrt{D}y_0) = 1.$$

Mindkét oldalt osztva $y_0(x_0+\sqrt{D}y_0)$-lal:

$$\frac{x_0}{y_0}-\sqrt{D}=\frac{1}{y_0(x_0+\sqrt{D}y_0)}.$$

Így

$$\left|\frac{x_0}{y_0}-\sqrt{D}\right|=\frac{1}{y_0(x_0+\sqrt{D}y_0)}\leqq\frac{1}{y_0\cdot\sqrt{D}y_0}=\frac{1}{\sqrt{D}y_0^2}.$$

11. $a_0=[\pi]=3,$

$$\alpha_1=\frac{1}{\alpha_0-a_0}=\frac{1}{\pi-3},$$

$$a_1=[\alpha_1]=\left[\frac{1}{\pi-3}\right]=\left[\frac{1}{0{,}14159\ldots}\right]=7,$$

$$\alpha_2=\frac{1}{\alpha_1-a_1}=\frac{1}{\frac{1}{\pi-3}-7}=\frac{1}{\frac{1}{0{,}1415926\ldots}-7}=$$

$$=\frac{1}{7{,}0625\ldots-7}=\frac{1}{0{,}0625\ldots}=15{,}9\ldots,$$

$$a_2=[\alpha_2]=[15{,}9\ldots]=15.$$

Így

$$P_0=a_0=3,\quad P_1=a_1a_0+1=7\cdot3+1=22,\quad P_2=a_2P_1+P_0=$$

$$=15\cdot22+3=333,$$

$Q_0=1$, $Q_1=a_1=7$, $Q_2=a_2Q_1+Q_0=15\cdot7+1=106$.
Az első három közelítő tört tehát

$$\frac{P_0}{Q_0}=\frac{3}{1},\quad\frac{P_1}{Q_1}=\frac{22}{7},\quad\frac{P_2}{Q_2}=\frac{333}{106},$$

továbbá

$$\left|\pi-\frac{P_0}{Q_0}\right|=\pi-3=0{,}14\ldots,\quad\frac{1}{Q_0^2}=1;$$

$$\left|\pi-\frac{P_1}{Q_1}\right|=\left|\pi-\frac{22}{7}\right|=|3{,}14159\ldots-3{,}14285\ldots|\approx0{,}00126,$$

JATE Móra Ferenc Kollégium
KÖNYVTÁRA

$$\frac{1}{Q_1^2} = \frac{1}{49} = 0{,}02040\ldots;$$

$$\left|\pi - \frac{P_2}{Q_2}\right| = \left|\pi - \frac{333}{106}\right| = |3{,}1415926\ldots - 3{,}1415094\ldots| \approx$$

$$\approx 0{,}0000832\ldots, \quad \frac{1}{Q_2^2} = \frac{1}{106^2} = 0{,}0000889\ldots.$$

A $\pi \approx \frac{P_i}{Q_i}$ közelítés hibája $\frac{1}{Q_i^2}$-hez viszonyítva különösen $i=1$ esetén kicsi; másrészt a lánctörtekről mondottakból következik, hogy nem létezik más olyan $\frac{p}{q}$ tört, melyre $q \leqq Q_2 = 106$ teljesül és π-t $\frac{1}{q^2}$-hez viszonyítva ilyen jól approximálja. Ez az oka annak, hogy a $\pi \approx \frac{P_1}{Q_1} = \frac{22}{7} = 3\frac{1}{7}$ közelítés gyakran használatos.

12. $-\frac{69}{32} = -3 + \frac{27}{32}$,

$$\frac{32}{27} = 1 + \frac{5}{27},$$

$$\frac{27}{5} = 5 + \frac{2}{5},$$

$$\frac{5}{2} = 2 + \frac{1}{2},$$

$$\frac{2}{1} = 2.$$

Így

$$-\frac{69}{32} = [-3, 1, 5, 2, 2].$$

13. $a_0 = [\alpha] = [\sqrt{2}] = [1{,}41\ldots] = 1,$

$$\alpha_1 = \frac{1}{\alpha_0 - a_0} = \frac{1}{\sqrt{2}-1} \cdot \frac{\sqrt{2}+1}{\sqrt{2}+1} = \sqrt{2}+1,$$

$$a_1 = [\alpha_1] = [\sqrt{2}+1] = [2{,}41\ldots] = 2,$$

$$\alpha_2 = \frac{1}{\alpha_1 - a_1} = \frac{1}{(\sqrt{2}+1)-2} = \frac{1}{\sqrt{2}-1}.$$

Minthogy $\alpha_1=\alpha_2$, $\sqrt{2}$ lánctörtbe fejtése nyilván periodikus, mégpedig $a_1=a_2=a_3=\ldots=2$. Így

$$\sqrt{2} = [1, 2, 2, 2, \ldots].$$

14. $a_0 = [\alpha] = [\sqrt{n^2-1}]$.

Azonban

$$\sqrt{n^2-1} < \sqrt{n^2} = n$$

és $n \geqq 2$-re tekintettel

$$\sqrt{n^2-1} = \sqrt{(n-1)(n+1)} > \sqrt{(n-1)(n-1)} = n-1,$$

tehát nyilván

(71) $[\sqrt{n^2-1}] = n-1$,

és így $a_0 = n-1$.

Továbbá

$$\alpha_1 = \frac{1}{\alpha_0 - a_0} = \frac{1}{\sqrt{n^2-1}-(n-1)} = \frac{1}{\sqrt{n^2-1}-(n-1)} \cdot \frac{\sqrt{n^2-1}+(n-1)}{\sqrt{n^2-1}+(n-1)} =$$

$$= \frac{\sqrt{n^2-1}+(n-1)}{(n^2-1)-(n-1)^2} = \frac{\sqrt{n^2-1}+(n-1)}{2(n-1)} = \frac{1}{2}\sqrt{\frac{n+1}{n-1}}+\frac{1}{2}.$$

Nyilván

(72) $\alpha_1 = \frac{1}{2}\sqrt{\frac{n+1}{n-1}}+\frac{1}{2} > \frac{1}{2}\cdot 1+\frac{1}{2} = 1.$

Másrészt állítjuk, hogy $n \geqq 2$-ből következik, hogy

(73) $\frac{n+1}{n-1} \leqq 3.$

Innen ugyanis ekvivalens átalakítások révén a következőt nyerjük:

$$n+1 \leqq 3(n-1) = 3n-3,$$

$$4 \leqq 2n,$$

$$2 \leqq n,$$

ami feltevésünk szerint valóban teljesül. (73)-ból azonban következik, hogy

$$(74)\qquad \alpha_1 = \frac{1}{2}\sqrt{\frac{n+1}{n-1}}+\frac{1}{2} \leqq \frac{1}{2}\sqrt{3}+\frac{1}{2} < \frac{1}{2}\sqrt{4}+\frac{1}{2} = \frac{3}{2}.$$

(72)-ből és (74)-ből következik, hogy

$$a_1 = [\alpha_1] = 1.$$

Továbbá

$$\alpha_2 = \frac{1}{\alpha_1 - a_1} = \frac{1}{\left(\frac{1}{2}\sqrt{\frac{n+1}{n-1}}+\frac{1}{2}\right)-1} = \frac{1}{\frac{1}{2}\sqrt{\frac{n+1}{n-1}}-\frac{1}{2}} =$$

$$= \frac{2\sqrt{n-1}}{\sqrt{n+1}-\sqrt{n-1}} = \frac{2\sqrt{n-1}}{\sqrt{n+1}-\sqrt{n-1}}\cdot\frac{\sqrt{n+1}+\sqrt{n-1}}{\sqrt{n+1}+\sqrt{n-1}} =$$

$$= \frac{2\sqrt{n^2-1}+2(n-1)}{(n+1)-(n-1)} = \frac{2\sqrt{n^2-1}+2(n-1)}{2} = \sqrt{n^2-1}+(n-1).$$

Így (71)-re tekintettel

$$a_2 = [\alpha_2] = [\sqrt{n^2-1}+(n-1)] = [\sqrt{n^2-1}]+(n-1) =$$

$$= (n-1)+(n-1) = 2n-2.$$

Továbbá

$$\alpha_3 = \frac{1}{\alpha_2 - a_2} = \frac{1}{(\sqrt{n^2-1}+(n-1))-(2n-2)} = \frac{1}{\sqrt{n^2-1}-(n-1)}.$$

Így $\alpha_3 = \alpha_1$, tehát α lánctörtbe fejtése (a_1-től kezdve) periodikus, mégpedig egy periódus hossza 2:

$$a_1 = a_3 = a_5 = a_7 = \ldots = 1, \quad a_2 = a_4 = a_6 = a_8 = \ldots = 2n-2.$$

$\alpha = \sqrt{n^2-1}$ lánctörtbe fejtése tehát

$$\sqrt{n^2-1} = [n-1, 1, 2n-2, 1, 2n-2, 1, 2n-2, \ldots]$$

15*. Mint láttuk, (36) végtelen lánctörtekre is teljesül ($[a_1, a_2, \ldots, a_n]$ helyén $[a_1, a_2, \ldots, a_n, \ldots]$-nel), tehát valamely α irracionális szám $\frac{P_{k-1}}{Q_{k-1}}$, $\frac{P_k}{Q_k}$ (k tetszőleges természetes szám) egymást követő közelítő törtjei

közrefogják α-t. Így

$$(75)\quad \left|\frac{P_k}{Q_k}-\frac{P_{k-1}}{Q_{k-1}}\right| = \left|\left(\frac{P_k}{Q_k}-\alpha\right)+\left(\alpha-\frac{P_{k-1}}{Q_{k-1}}\right)\right| =$$

$$= \left|\frac{P_k}{Q_k}-\alpha\right|+\left|\alpha-\frac{P_{k-1}}{Q_{k-1}}\right|.$$

Másrészt (32)-re tekintettel

$$(76)\quad \left|\frac{P_k}{Q_k}-\frac{P_{k-1}}{Q_{k-1}}\right| = \frac{1}{Q_{k-1}Q_k}.$$

(75)-ből és (76)-ból nyerjük, hogy

$$(77)\quad \left|\frac{P_k}{Q_k}-\alpha\right|+\left|\alpha-\frac{P_{k-1}}{Q_{k-1}}\right| = \frac{1}{Q_{k-1}Q_k}.$$

Most tegyük fel indirekte, hogy a $\frac{P_{k-1}}{Q_{k-1}}$ és $\frac{P_k}{Q_k}$ közelítő törtek egyike sem elégíti ki (47)-et, vagyis

$$(78)\quad \left|\alpha-\frac{P_{k-1}}{Q_{k-1}}\right| \geqq \frac{1}{2Q_{k-1}^2} \quad \text{és} \quad \left|\alpha-\frac{P_k}{Q_k}\right| \geqq \frac{1}{2Q_k^2}.$$

Minthogy α irracionális szám, itt egyik helyen sem állhat egyenlőségjel. Így innen

$$(79)\quad \left|\alpha-\frac{P_{k-1}}{Q_{k-1}}\right|+\left|\alpha-\frac{P_k}{Q_k}\right| > \frac{1}{2Q_{k-1}^2}+\frac{1}{2Q_k^2}.$$

(77)-ből és (79)-ből következik, hogy

$$\frac{1}{Q_{k-1}Q_k} > \frac{1}{2Q_{k-1}^2}+\frac{1}{2Q_k^2}.$$

Mindkét oldalt $2Q_{k-1}^2Q_k^2$-nel szorozva:

$$2Q_{k-1}Q_k > Q_k^2+Q_{k-1}^2,$$

vagyis

$$Q_k^2-2Q_{k-1}Q_k+Q_{k-1}^2 < 0,$$

$$(Q_k-Q_{k-1})^2 < 0.$$

A bal oldalon azonban nyilván nemnegatív szám áll, tehát ez az egyenlőtlenség nem teljesülhet. Így a (78) indirekt feltevésből ellentmondásra jutottunk, és ezzel az állítást igazoltuk.

16*. Ha az α szám $a_0, a_1, a_2, \ldots$ lánctörtjegyeinek sorozata periodikus, akkor találhatók olyan m, n természetes számok, hogy $k=0, 1, 2, \ldots$ esetén

$$a_{n+k} = a_{n+m+k}.$$

Ekkor

$$\alpha_n = [a_n, a_{n+1}, \ldots] = \alpha_{n+m} = [a_{n+m}, a_{n+m+1}, \ldots].$$

Az $[a_0, a_1, \ldots, a_{n-1}, \alpha_n]$ $(=\alpha)$ lánctörtre alkalmazva a (28)–(30) formulákat, a következőt nyerjük:

$$\alpha = \frac{P_n}{Q_n} = \frac{\alpha_n P_{n-1} + P_{n-2}}{\alpha_n Q_{n-1} + Q_{n-2}}. \tag{80}$$

Az $[a_0, a_1, \ldots, a_{n+m-1}, \alpha_{n+m}]$ lánctörtet vizsgálva ugyanígy kapjuk, hogy

$$\alpha = \frac{P_{n+m}}{Q_{n+m}} = \frac{\alpha_{n+m} P_{n+m-1} + P_{n+m-2}}{\alpha_{n+m} Q_{n+m-1} + Q_{n+m-2}}. \tag{81}$$

Az $x = \alpha_n = \alpha_{n+m}$ jelölést bevezetve, (80)-ból és (81)-ből adódik, hogy

$$\frac{xP_{n-1} + P_{n-2}}{xQ_{n-1} + Q_{n-2}} = \frac{xP_{n+m-1} + P_{n+m-2}}{xQ_{n+m-1} + Q_{n+m-2}}.$$

Mindkét oldalt szorozva a nevezők szorzatával, majd rendezve, x-re

$$bx^2 + cx + d = 0 \tag{82}$$

alakú egyenletet nyerünk, ahol b, c, d egész számok, speciálisan

$$b = P_{n-1} Q_{n+m-1} - Q_{n-1} P_{n+m-1}.$$

Állítjuk, hogy $b \neq 0$. Ellenkező esetben ugyanis

$$b = P_{n-1} Q_{n+m-1} - Q_{n-1} P_{n+m-1} = 0,$$

vagyis

$$P_{n-1} Q_{n+m-1} = Q_{n-1} P_{n+m-1}$$

teljesülne. Innen következnék, hogy $Q_{n+m-1} | Q_{n-1} P_{n+m-1}$. Továbbá (38) szerint $(Q_{n+m-1}, P_{n+m-1}) = 1$. Így innen nyerjük, hogy $Q_{n+m-1} | Q_{n-1}$, következésképpen $Q_{n+m-1} \leqq Q_{n-1}$. Másrészt (39)-re tekintettel $Q_{n+m-1} > Q_{n-1}$, tehát a $b=0$ indirekt feltevésből ellentmondásra jutottunk.

x tehát gyöke a (82) egész együtthatós egyenletnek, mely $b \neq 0$-ra tekintettel másodfokú. Könnyen igazolható, hogy ha valamely y valós szám gyöke egy egész együtthatós, legfeljebb másodfokú egyenletnek, akkor tetszőleges r racionális számot megadva ry, $y+r$ és — $y \neq 0$ esetén — $\frac{1}{y}$ is gyöke egy ilyen típusú egyenletnek (ennek belátását az Olvasóra bízzuk). Így x-szel együtt

$$\alpha = \frac{xP_{n-1}+P_{n-2}}{xQ_{n-1}+Q_{n-2}} = \left(\frac{xP_{n-1}+P_{n-2}}{xQ_{n-1}+Q_{n-2}} - \frac{P_{n-1}}{Q_{n-1}}\right) + \frac{P_{n-1}}{Q_{n-1}} =$$

$$= \frac{Q_{n-1}P_{n-2}-P_{n-1}Q_{n-2}}{Q_{n-1}} \cdot \frac{1}{xQ_{n-1}+Q_{n-2}} + \frac{P_{n-1}}{Q_{n-1}}$$

is gyöke egy legfeljebb másodfokú egész együtthatós egyenletnek, tehát α legfeljebb másodfokú algebrai szám. Másrészt α nem lehet elsőfokú algebrai szám, vagyis racionális szám, hiszen feltevésünk szerint α-t lánctörtbe fejtve, végtelen lánctörtet kapunk, és ezzel az állítást igazoltuk.

VII*. AZ ANALITIKUS SZÁMELMÉLET ELEMEI

1. A GENERÁTORFÜGGVÉNY-ELV

A számelméletnek azt az ágát, melynek módszerei a (valós) analízisre és főképpen a komplex változós függvénytanra épülnek, *analitikus számelméletnek* hívjuk. Az analitikus számelmélet eredményeinek bizonyítása általában komoly analízisbeli felkészültséget igényel, és e bizonyítások többnyire meglehetősen sok számolással járnak. Ezért itt nincs módunk arra, hogy rendszeres áttekintését adjuk az analitikus számelméletnek. Csak arra szorítkozunk, hogy az analitikus számelmélet egyes fontosabb módszereit, összefüggéseit vázoljuk néhány illusztráció kapcsán.

A — legalábbis részben — *valós* analízisen alapuló módszerek közül legjelentősebb az ún. *generátorfüggvény-elv*, melyről két értelemben is szoktunk beszélni. Tágabb értelemben a következőt értjük generátorfüggvény-elven: Adott valamely $f(n)$ számelméleti függvény (vagy más megfogalmazásban, valamely $a_1, a_2, \ldots$ — véges vagy végtelen — sorozat). Ennek vizsgálata céljából az adott számelméleti függvényhez (ill. sorozathoz) hozzárendelünk valamely $F(x)$ (valós vagy komplex változós) függvényt, melyet az adott számelméleti függvény (ill. sorozat) *generátorfüggvényének* nevezünk. Ezután analízisbeli segédeszközök segítségével vizsgáljuk ezt az $F(x)$ generátorfüggvényt, majd az így $F(x)$-re nyert információkból visszakövetkeztetünk az adott számelméleti függvény (ill. sorozat) bizonyos tulajdonságaira.

Szűkebb értelemben viszont csak akkor beszélünk generátorfüggvény-elvről, ha az említett $F(x)$ generátorfüggvény *polinom*, vagy pedig *hatványsor összegfüggvényeként* van definiálva. Ebben a pontban a generátorfüggvény-elv kifejezést ez utóbbi, szűkebb értelemben fogjuk használni.

A generátorfüggvény-elv az alábbi tételen alapul:

Legyenek $f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n$ és $g(x)=b_0x^n+b_1x^{n-1}+\ldots+b_n$ (valós vagy komplex változós) legfeljebb n-edfokú polinomok (n tetszőleges természetes szám). Tegyük fel, hogy a két polinom helyettesítési értékei (legalább) $n+1$ helyen megegyeznek, vagyis léteznek olyan $x_1, x_2, \ldots, x_{n+1}$ (páronként különböző) számok, hogy $i=1, 2, \ldots, n+1$ esetén

(1) $f(x_i) = g(x_i)$

teljesül. Ekkor szükségképpen $a_0=b_0$, $a_1=b_1$, ..., $a_n=b_n$ (tehát a két polinom megfelelő együtthatói megegyeznek).

E tételnek hatványsorokra vonatkozó analogonja:

Legyenek $f(x)$ és $g(x)$ olyan (valós vagy komplex változós) függvények, melyek hatványsor összegfüggvényeként vannak definiálva: $f(x)=a_0+a_1x+\ldots+a_nx^n+\ldots$ és $g(x)=b_0+b_1x+\ldots+b_nx^n+\ldots$. Tegyük fel, hogy a két hatványsor valamely c pozitív számra $|x|<c$ esetén abszolút konvergens (következésképpen az $f(x)$ és $g(x)$ függvények $|x|<c$ esetén definiálva vannak). Tegyük fel továbbá, hogy található valamely d pozitív szám és egy $x_1, x_2, \ldots, x_n, \ldots$ végtelen számsorozat úgy, hogy a következő feltételek teljesülnek: $(0<)d<c$, $i=1, 2, \ldots$ esetén $|x_i|\leqq d$, $1\leqq i<j$ esetén $x_i\neq x_j$, és $i=1, 2, \ldots$ esetén (1) teljesül. Ekkor szükségképpen $a_0=b_0$, $a_1=b_1$, ...

Megjegyezzük, hogy ha a generátorfüggvény nem polinom, hanem (végtelen) hatványsor, akkor a gyakorlatban némi többletmunkát jelent az abszolút konvergencia vizsgálata. Ez a többletmunka az absztrakt algebra módszereinek segítségével részben kiküszöbölhető; ennek a kérdésnek a részletezésére itt nincs módunk.

Az alábbiakban a generátorfüggvény-elv illusztrációjaként az ún. *Fibonacci-sorozatot* fogjuk vizsgálni.

Példa

1. Írjuk fel a VI. fejezet 5. példájának kapcsán definiált $b_0, b_1, \ldots, b_n, \ldots$ Fibonacci-sorozat b_n elemét n függvényeként (zárt alakban)!

Megoldás:

A Fibonacci-sorozatot az említett példa kapcsán a következő rekurzióval definiáltuk:

(2) $b_0 = b_1 = 1,$

(3) $b_n = b_{n-1}+b_{n-2} \quad (n = 2, 3, \ldots).$

(2) és (3) alapján indukcióval könnyen igazolható (a részleteket az Olvasóra bízzuk), hogy $n=0, 1, 2, \ldots$ esetén $0<b_n<2^n$. Innen következik, hogy a $b_0+b_1x+\ldots+b_nx^n+\ldots$ (valós) hatványsor $|x|<\frac{1}{2}$ esetén abszolút konvergens. Jelöljük összegfüggvényét (vagyis a Fibonacci-sorozat generátorfüggvényét) $F(x)$-szel:

$$(4) \qquad F(x) = b_0+b_1x+b_2x^2+\ldots+b_nx^n+\ldots \left(\text{ahol } |x| < \frac{1}{2}\right).$$

Szorozzuk meg (4) mindkét oldalát $-x$-szel, majd $-x^2$-nel:

$$(5) \qquad -xF(x) = -b_0x-b_1x^2-\ldots-b_{n-1}x^n-\ldots,$$

$$(6) \qquad -x^2F(x) = -b_0x^2-\ldots-b_{n-2}x^n-\ldots.$$

(4)-et, (5)-öt és (6)-ot összeadva:

$$(7) \qquad (1-x-x^2)F(x) = b_0+(b_1-b_0)x+(b_2-b_1-b_0)x^2+\ldots+$$
$$+(b_n-b_{n-1}-b_{n-2})x^n+\ldots.$$

A jobb oldalon (2) szerint a konstans tag $b_0=1$, x együtthatója $b_1-b_0=$ $=1-1=0$, továbbá (3) szerint $n=2, 3, \ldots$ esetén x^n együtthatója b_n- $-b_{n-1}-b_{n-2}=0$.
Így (7) a következő alakban írható:

$$(1-x-x^2)F(x) = 1,$$
$$F(x) = \frac{1}{1-x-x^2}.$$

A jobb oldalon parciális törtekre bontva, majd a végtelen mértani sor összegképletét alkalmazva:

$$(8) \qquad F(x) = \frac{1}{1-x-x^2} = \frac{1}{\left(1-\frac{\sqrt{5}+1}{2}x\right)\left(1-\frac{-\sqrt{5}+1}{2}x\right)} =$$
$$= \frac{\sqrt{5}+1}{2\sqrt{5}}\cdot\frac{1}{1-\frac{\sqrt{5}+1}{2}x}+\frac{\sqrt{5}-1}{2\sqrt{5}}\cdot\frac{1}{1-\frac{-\sqrt{5}+1}{2}x} =$$
$$= \frac{\sqrt{5}+1}{2\sqrt{5}}\sum_{n=0}^{+\infty}\left(\frac{\sqrt{5}+1}{2}\right)^n x^n+\frac{\sqrt{5}-1}{2\sqrt{5}}\sum_{n=0}^{+\infty}\left(\frac{-\sqrt{5}+1}{2}\right)^n x^n =$$
$$= \sum_{n=0}^{+\infty}\frac{1}{\sqrt{5}}\left(\left(\frac{\sqrt{5}+1}{2}\right)^{n+1}-\left(\frac{-\sqrt{5}+1}{2}\right)\right)^{n+1} x^n \quad \left(|x| < \frac{1}{2}\right).$$

A (4), ill. (8) jobb oldalán álló hatványsorok összegfüggvényei $|x|<\frac{1}{2}$ esetén megegyeznek egymással (egyaránt az $F(x)$ generátorfüggvénnyel azonosak). Így a fent említett tétel szerint a két hatványsor megfelelő együtthatói megegyeznek, tehát $n=0, 1, 2, \ldots$ esetén

$$b_n = \frac{1}{\sqrt{5}}\left(\left(\frac{\sqrt{5}+1}{2}\right)^{n+1} - \left(\frac{-\sqrt{5}+1}{2}\right)^{n+1}\right).$$

2. TRIGONOMETRIKUS MÓDSZEREK (EXPONENCIÁLIS ÖSSZEGEK)

Már az V. fejezet 4. pontjában találkoztunk a komplex számok egy számelméleti alkalmazásával, a Gauss-egészekkel kapcsolatban. Igazán hatékony segédeszközzé azonban akkor válnak a komplex számok, ha a *komplex analízis* eredményeit is felhasználjuk. Ebben a pontban a komplex analízis olyan számelméleti alkalmazásaival fogunk foglalkozni, melyekben csak *valós változós* — de komplex értékeket is felvevő — függvények (röviden: *valós változós komplex* függvények) szerepelnek. Az ilyen alkalmazásokhoz lényegében elegendő a valós analízis ismerete. Valamely $f(t)$ valós változós komplex függvény ugyanis felírható

(9) $\quad f(t) = \varphi(t) + i\psi(t)$

alakban, ahol $\varphi(t)$ és $\psi(t)$ valós változós és *valós értékű* (röviden: *valós*) függvények; így az $f(t)$ valós változós komplex függvény analitikus tulajdonságainak vizsgálata visszavezethető a $\varphi(t)$ és $\psi(t)$ *valós* függvények vizsgálatára.

Valós változós komplex függvények folytonossága, differenciálhatósága, integrálhatósága lényegében ugyanúgy definiálható, mint a valós függvényeké. (A különbség csupán az, hogy az egyes definíciókban szereplő számsorozatok valós számok helyett komplex számokból állnak.) Igazolható, hogy a (9) alatti $f(t)$ valós változós komplex függvény akkor és csak akkor differenciálható, ha a $\varphi(t)$ és $\psi(t)$ valós függvények is differenciálhatók, és ekkor

(9) $\quad f'(t) = \varphi'(t) + i\psi'(t).$

Hasonlóan,

$$(10)\quad \int_a^b f(t)\,dt = \int_a^b \varphi(t)\,dt + i\int_a^b \varphi(t)\,dt,$$

ahol a bal oldali integrál akkor és csak akkor létezik, ha a jobb oldali integrálok is léteznek. (9)-ből és (10)-ből következik, hogy a valós analízis deriválásra és integrálásra vonatkozó szabályai valós változós komplex függvényekre is átvihetők.

A valós változós komplex függvények számelméleti alkalmazásai során (de sok egyéb alkalmazásban is) kitüntetett szerepet játszik az a függvény, melyhez úgy juthatunk el, hogy a (valós) $f(x)=e^x$ exponenciális függvény értelmezését kiterjesztjük arra az esetre, amikor a kitevő tiszta képzetes szám. A definíció a következő: legyen tetszőleges t valós számra

$$(11)\quad e^{it} = \cos t + i \sin t$$

(tehát e^{it} az 1 abszolút értékű, t argumentumú komplex számot jelöli). Igazolható, hogy ekkor tetszőleges u, v valós számokra és tetszőleges n természetes számra

$$e^{i(u+v)} = e^{iu}\cdot e^{iv},$$

$$(e^{iu})^n = e^{i(un)}$$

(összhangban a hatványozás jól ismert azonosságaival).

Megjegyezzük, hogy az exponenciális függvény értelmezése kiterjeszthető arra a legáltalánosabb esetre is, amikor a kitevő tetszőleges komplex szám. A definíció a következő: legyen valamely $z=a+bi$ (ahol a, b tetszőleges valós számok) komplex számra

$$e^z = e^{a+bi} = e^a\cdot e^{bi} = e^a(\cos b + i \sin b).$$

Az így definiált $f(z)=e^z$ *komplex változós* függvény alapvető szerepet játszik a komplex analízisben; itt azonban nincs szükségünk erre az általánosságra.

A (11) definícióból (9) és (10) alapján könnyen levezethető, hogy az e^{it} függvény — durván szólva — úgy differenciálható és integrálható, mint ha i valós szám lenne: $(e^{it})' = ie^{it}$, $\int e^{it} = \frac{e^{it}}{i}$.

Az $f(t)=e^{it}$ függvény (11)-re tekintettel nyilvánvalóan periodikus, mégpedig egy periódus hossza 2π. A számelméleti alkalmazásokban gyakran előnyös e függvény helyett a

$$(12)\quad g(t) = f(2\pi t) = e^{2\pi it}$$

függvényt vizsgálni; ennek periódushossza ugyanis 1, tehát *$g(t)$ értéke csak t tört részétől függ.*

A számelméleti alkalmazásokban szereplő valós változós komplex függvények igen gyakran a (12) függvény polinomjai, vagyis

$$F(t) = \sum_{k=m}^{n} a_k e^{2\pi ikt}$$

alakúak (ahol m, n egész számok, $a_m, a_{m+1}, \ldots, a_n$ adott komplex számok); az ilyen alakú függvényeket (komplex) *trigonometrikus polinomoknak* nevezzük. ((11)-re tekintettel ugyanis $F(t)$-nek mind a valós, mind a képzetes része *valós* trigonometrikus polinom.) Ha speciálisan az a_k együtthatók mindegyike 0 vagy 1, akkor

$$(13)\quad F(t) = \sum_{j=1}^{N} e^{2\pi ik_j t}$$

alakú trigonometrikus polinomot kapunk, ahol $k_1, k_2, \ldots, k_N$ egész számok. Ha egész számok valamely $k_1, k_2, \ldots, k_N$ sorozatát trigonometrikus módszerek segítségével akarjuk vizsgálni, akkor e célból az adott sorozathoz rendszerint a (13) *generátorfüggvényt* rendeljük hozzá (itt a generátorfüggvény szót természetesen a tágabb értelemben használjuk). (13) alakú trigononometrikus polinomoknak fontos tulajdonsága az alábbi:

Helyettesítsünk (13)-ban t helyére valamely $\frac{p}{q}$ racionális számot (ahol p egész szám, q természetes szám):

$$(14)\quad F\left(\frac{p}{q}\right) = \sum_{j=1}^{N} e^{2\pi i \frac{k_j p}{q}}.$$

Mint mondtuk, a (12) függvény értéke csak attól függ, hogy t tört része mennyi. Ebből következik, hogy a (14) jobb oldalán

álló összeg egyes tagjainak értéke (rögzített p, q mellett) csak attól függ, hogy a kitevőben álló k_j tényező q-val osztva mennyi maradékot ad, vagyis melyik maradékosztályba esik modulo q. Így végeredményben $F\left(\frac{p}{q}\right)$ *értéke csak attól függ, hogy a* $k_1, k_2, \ldots, k_N$ *sorozat hogyan oszlik el a modulo q maradékosztályokban.*

Sok számelméleti alkalmazásban a trigonometrikus polinomoknál általánosabb,

$$G(t) = \sum_{j=1}^{N} f_j(t) e^{2\pi i \varphi_j(t)}$$

(ahol $f_j(t)$ valós változós komplex, $\varphi_j(t)$ valós függvény) alakú *exponenciális összegek* szerepelnek. (Ha itt az $f_j(t)$ függvények azonosan konstansok, a $\varphi_j(t)$ függvények pedig $k_j t$ alakúak — ahol k_j egész szám —, akkor trigonometrikus polinomot kapunk.) Fontos szerepet játszanak a számelméletben az ún. *Weyl-összegek*, melyek

$$\sum_{j=1}^{N} e^{i\varphi(j)}$$

alakú kifejezések, ahol $\varphi(x)$ valós együtthatós polinom; ha speciálisan $\varphi(x) = \frac{p}{q} x^2$ (ahol p egész szám, q természetes szám), akkor *Gauss-összegekről* beszélünk.

Az alábbiakban vázoljuk a trigonometrikus módszerek néhány különösen fontos számelméleti alkalmazását.

Elsőként a legfontosabb és leghatékonyabb trigonometrikus módszerek egyikét, az ún. *Hardy—Littlewood-módszert* említjük. Ez a következő típusú problémák vizsgálatára alkalmas:

Legyenek adottak bizonyos egész számokból álló

$$A_1 = \{a_{(1,1)}, a_{(1,2)}, \ldots, a_{(1,N_1)}\}, \quad A_2 = \{a_{(2,1)}, a_{(2,2)}, \ldots, a_{(2,N_2)}\}, \ldots, \quad A_k = \{a_{(k,1)}, a_{(k,2)}, \ldots, a_{(k,N_k)}\}$$

véges sorozatok. Kérdés, hogy az

$$(15) \quad a_{(1,x_1)} + a_{(2,x_2)} + \ldots + a_{(k,x_k)} = 0$$

egyenletnek hány megoldása van, vagyis a 0 hányféleképpen állítható elő olyan k tagú összegként, melynek j-edik tagja a j-edik sorozatból van véve ($j=1, 2, \ldots, k$)? Így például legyen adott valamely n páratlan természetes szám, és jelöljük az n-nél nem nagyobb páratlan prímszámok sorozatát P-vel. Legyen $k=4$, $A_1=A_2=A_3=P$, $A_4=\{-n\}$. Ekkor a (15) egyenlet a

$$p+q+r=n$$

(ahol p, q, r páratlan prímszámok) egyenletbe megy át, vagyis a páratlan számokra vonatkozó Goldbach-problémához jutunk (a páratlan számokra vonatkozó Goldbach-sejtés ugyanis úgy fogalmazható, hogy ennek az egyenletnek a megoldásszáma minden 7-nél nagyobb n páratlan számra legalább 1). Hasonlóan, a Waring-probléma is átfogalmazható a fenti módon.

Jelöljük (15) megoldásszámát M-mel, és képezzük az A_1, $A_2, \ldots, A_k$ sorozatok generátorfüggvényeit:

$$F_r(t)=\sum_{j_r=1}^{N_r} e^{2\pi i a_{(r,j_r)} t} \quad (\text{ahol } r=1, 2, \ldots, k).$$

Ekkor könnyen igazolható (l. a 16. feladatot), hogy (15) megoldásszáma a következőképpen számítható ki:

$$(16) \quad \int_0^1 F_1(t)F_2(t)\ldots F_k(t)\,dt = M.$$

Az M megoldásszám vizsgálata tehát az $F_1(t)F_2(t)\ldots F_k(t)$ integrandus vizsgálatára vezethető vissza. Ennek becslése a Hardy—Littlewood-módszer értelmében a következőképpen történik:

Tegyük fel, hogy az integrandust a $t=t_0$ (ahol $0\leqq t_0\leqq 1$) helyen akarjuk becsülni. E célból Dirichlet (approximációelméleti) tételének — a VI. fejezet 1. példája kapcsán bizonyított — élesebb alakját felhasználva, t_0-t approximáljuk valamely $\frac{p}{q}$ racionális számmal (ahol $1\leqq q\leqq Q$; itt a Q korlát megválasztása az $A_1, A_2, \ldots, A_k$ sorozatoktól függ). Minthogy $\frac{p}{q}$ „közel"

van t_0-hoz, várható, hogy $\left|F_i\left(\frac{p}{q}\right)-F_i(t_0)\right|$ (ahol $i=1, 2, \ldots, k$) „kicsi", következésképpen

$$\left|F_1\left(\frac{p}{q}\right)F_2\left(\frac{p}{q}\right)\ldots F_k\left(\frac{p}{q}\right)-F_1(t_0)F_2(t_0)\ldots F_k(t_0)\right|$$

is „kicsi"; ennek igazolása a következő lépés. Ha ezt már igazoltuk, akkor $F_1(t_0)F_2(t_0)\ldots F_k(t_0)$ becslése céljából elegendő $F_1\left(\frac{p}{q}\right)F_2\left(\frac{p}{q}\right)\ldots F_k\left(\frac{p}{q}\right)$-t, vagyis az integrandus („kis" nevezőjű) racionális helyeken vett helyettesítési értékeit becsülnünk. Ez viszont az egyes $F_i\left(\frac{p}{q}\right)$ tényezők becslésére redukálható. Az $F_i\left(\frac{p}{q}\right)$ helyettesítési értékek viszont (14) alakúak, tehát az ott mondottak szerint $F_i\left(\frac{p}{q}\right)$ becsléséhez elég azt tudni, hogy az A_i sorozat elemei hogyan oszlanak el a modulo q maradékosztályokban. Így a (16) bal oldalán álló integrandus (és így egyúttal M) becslése *annak vizsgálatára redukálható, hogy az adott sorozatok hogyan oszlanak el a „kis" modulusú maradékosztályokban.*

Míg a Hardy—Littlewood-módszer alkalmazásai során az adott sorozatok adott modulusú maradékosztályokban való eloszlásának vizsgálata csupán segédeszköz, addig bizonyos más esetekben éppen az adott sorozat (például a prímszámok által alkotott sorozat) maradékosztályokban, azaz számtani sorozatokban való eloszlásának vizsgálata a végcél. Ilyen esetekben — például Dirichlet (prímszámelméleti) tételének igazolása során — fontos szerepet játszanak a 17. feladatban vizsgált *karakterek.*

A számelméletben gyakran találkozunk a következő típusú problémával: adott valamely *valós* számból álló $a_1, a_2, \ldots$ sorozat. Kérdés, hogy az $a_1, a_2, \ldots$ számok *tört részei* hogyan helyezkednek el (például *mennyire „egyenletesen" oszlanak el*) a $[0, 1)$ intervallumban? Ilyen típusú problémák vizsgálata során szintén igen fontos szerepet játszanak az exponenciális összegek (lényegében azért, mert — mint megjegyeztük — a (12) alatti $g(t)$ függvény értéke csak t tört részétől függ).

Példa

2. Legyen a tetszőleges egész szám, p 2-nél nagyobb prímszám, és legyen

$$S(a,p) = \sum_{x=0}^{p-1} e^{2\pi i \frac{ax^2}{p}}.$$

(tehát $S(a,p)$ ún. *Gauss-összeg*). Bizonyítsuk be, hogy

$$|S(a,p)| = \begin{cases} p, & \text{ha } p|a; \\ \sqrt{p}, & \text{ha } p\nmid a. \end{cases}$$

Megoldás:

Ha $p|a$, akkor nyilván az $S(a,p)$ összeg valamennyi tagja 1, tehát az összeg értéke p.

Tegyük fel most, hogy $p\nmid a$. Ekkor

$$(17) \quad |S(a,p)|^2 = S(a,p)\overline{S(a,p)} = \sum_{x=0}^{p-1} e^{2\pi i \frac{ax^2}{p}} \sum_{y=0}^{p-1} e^{-2\pi i \frac{ay^2}{p}} =$$

$$= \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} e^{2\pi i \frac{a(x^2-y^2)}{p}} = \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} e^{2\pi i \frac{a(x-y)(x+y)}{p}}.$$

Itt az egyes tagok értéke csak attól függ, hogy a kitevőben szereplő $a(x-y)(x+y)$ szorzat p-vel osztva mennyi maradékot ad. Legyen

$$(18) \quad x-y = t \pmod{p}, \quad \text{ahol } 0 \leqq t \leqq p-1$$

(ezáltal t-t egyértelműen definiáljuk). Ekkor az említett szorzat a következő alakban írható:

$$a(x-y)(x+y) \equiv at(t+2y) \pmod{p}.$$

Így a (17)-ben szereplő összeget t értéke szerint csoportosítva:

$$|S(a,p)|^2 = \sum_{t=0}^{p-1} \sum_{y} e^{2\pi i \frac{at(t+2y)}{p}} = \sum_{t=0}^{p-1} e^{2\pi i \frac{at^2}{p}} \sum_{y} e^{2\pi i \frac{2aty}{p}}.$$

Itt a $\sum_y$ jelölés úgy értendő, hogy az összegzés azon y értékekre terjed ki, melyekre $0 \leqq y \leqq p-1$ teljesül, és melyekhez található (18)-at és a $0 \leqq x \leqq p-1$ feltételt kielégítő x egész szám. Azonban nyilván *bármely* y (és t) egész számokhoz egy (és csak egy) ilyen x egész szám található, tehát a $\sum_y$ összegzésben y a $0, 1, \ldots, p-1$ értékeket veheti fel:

$$|S(a,p)|^2 = \sum_{t=0}^{p-1} e^{2\pi i \frac{at^2}{p}} \sum_{y=0}^{p-1} e^{2\pi i \frac{2aty}{p}}.$$

A belső összegben mértani sor áll, melynek kvociense $e^{2\pi i \frac{2at}{p}}$. Ez a kvociens

akkor és csak akkor 1, ha $p|2at$. Feltevésünk szerint $p>2$ és $p\nmid a$; így $(p, 2a)=1$, tehát $p|2at$ akkor és csak akkor teljesül, ha $p|t$. Ez viszont $0\leq t\leq p-1$-re tekintettel akkor és csak akkor teljesül, ha $t=0$. $t\neq 0$ esetén az említett összeg kiszámítása céljából alkalmazható a mértani sor összegképlete. Így különválasztva a $t=0$-nak megfelelő tagot:

$$|S(a,p)|^2 = e^{2\pi i \frac{a\cdot 0^2}{p}} \sum_{y=0}^{p-1} e^{2\pi i \frac{2a\cdot 0\cdot y}{p}} + \sum_{t=1}^{p-1} e^{2\pi i \frac{at^2}{p}} \sum_{y=0}^{p-1} e^{2\pi i \frac{2aty}{p}} =$$

$$= 1\cdot \sum_{y=0}^{p-1} 1 + \sum_{t=1}^{p-1} e^{2pi \frac{at^2}{p}} \cdot \frac{e^{2\pi i \frac{2at}{p}\cdot p} - 1}{e^{2\pi i \frac{2at}{p}} - 1} =$$

$$= p + \sum_{t=1}^{p-1} e^{2\pi i \frac{at^2}{p}} \cdot \frac{1-1}{e^{2\pi i \frac{2at}{p}} - 1} = p + \sum_{t=1}^{p-1} 0 = p,$$

ahonnan

$$|S(a,p)| = \sqrt{p}$$

következik, és ezzel az állítást igazoltuk.

(Megjegyezzük, hogy a 20. feladatban e példa állítását alkalmazni fogjuk egy kongruencia megoldásszámának meghatározása céljából.)

3. DIRICHLET-SOROK. A RIEMANN-FÉLE ζ-FÜGGVÉNY

A komplex változós függvénytanra építve, igen hatékony analitikus módszerek dolgozhatók ki, melyek különösen a prímszámelméletben játszanak döntő szerepet. Itt csupán arra szorítkozunk, hogy ismertetjük azokat az alapfogalmakat, segédeszközöket, összefüggéseket, melyekre e módszerek épülnek, mégpedig a technikai részleteket mellőzve és lehetőleg csupán a valós analízisre hivatkozva.

Mindenekelőtt a *Dirichlet-sorok* definíciójával és alaptulajdonságaival kell megismerkednünk. Dirichlet-soron $\sum_{n=1}^{+\infty} \frac{a_n}{n^s}$ alakú végtelen sort értünk, ahol $a_1, a_2, \ldots$ adott valós vagy komplex számok, s valós vagy komplex változó. Az alábbiakban arra az esetre fogunk szorítkozni, amikor $a_1, a_2, \ldots$ valós

számok és s valós változó; ilyenkor *valós Dirichlet-sorról* beszélünk.

Igazolható, hogy ha valamely (valós) Dirichlet-sor az s_0 helyen konvergens, ill. abszolút konvergens, akkor $s>s_0$ esetén is az. Így azok a pontok, melyekben egy Dirichlet-sor konvergens, ill. abszolút konvergens, egy-egy *félegyenest* alkotnak (melyek kezdőpontjában az adott Dirichlet-sor lehet konvergens, ill. abszolút konvergens, de az is előfordulhat, hogy nem az).

Az 1. pontban láttuk, hogy egy hatványsor összegfüggvénye egyértelműen meghatározza a hatványsor együtthatóit. Hasonló tétel igaz Dirichlet-sorokra is:

Jelöljük a $\sum_{n=1}^{+\infty} \frac{a_n}{n^s}$ Dirichlet-sor összegfüggvényét (mindazon s-ekre, melyekre a sor konvergens) $f(s)$-sel, a $\sum_{n=1}^{+\infty} \frac{b_n}{n^s}$ Dirichlet-sorét $g(s)$-sel. Ha található olyan s_0 szám, hogy $s \geqq s_0$ esetén $f(s)=g(s)$, akkor szükségképpen $a_1=b_1, a_2=b_2, \ldots, a_n=b_n, \ldots$.

A Dirichlet-sorok *szorzási szabálya* a következő:

Tegyük fel, hogy a $\sum_{n=1}^{+\infty} \frac{a_n}{n^s}$ és $\sum_{n=1}^{+\infty} \frac{b_n}{n^s}$ Dirichlet-sorok $s \geqq s_0$ esetén abszolút konvergensek, és jelöljük összegfüggvényüket $f(s)$-sel, ill. $g(s)$-sel. Legyen $n=1, 2, \ldots$ esetén

$$c_n = \sum_{d|n} a_d b_{\frac{n}{d}}.$$

Ekkor $s \geqq s_0$ esetén a $\sum_{n=1}^{+\infty} \frac{c_n}{n^s}$ Dirichlet-sor is abszolút konvergens, és

$$f(s)g(s) = \left(\sum_{n=1}^{+\infty} \frac{a_n}{n^s}\right)\left(\sum_{n=1}^{+\infty} \frac{b_n}{n^s}\right) = \sum_{n=1}^{+\infty} \frac{c_n}{n^s}.$$

A Dirichlet-sorok közt kitüntetett szerepet játszik a $\sum_{n=1}^{+\infty} \frac{1}{n^s}$ Dirichlet-sor. A valós analízisből jól ismert, hogy ez a végtelen sor (az ún. *hiperharmonikus sor*) $s>1$ esetén konvergens, míg $s \leqq 1$ esetén divergens (speciálisan $s=1$ esetén *harmonikus sorról* beszélünk). Jelöljük a sor összegfüggvényét $\zeta(s)$-sel:

$$(19) \quad \zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s} \quad (\text{ahol } s > 1).$$

Az így definiált $\zeta(s)$ függvényt *Riemann-féle ζ-függvénynek* nevezzük.

A Riemann-féle ζ-függvény felírható végtelen szorzat formájában is. Jelöljük ugyanis az i-edik prímszámot p_i-vel (tehát $p_1=2, p_2=3, p_3=5, \ldots$). Ekkor a végtelen mértani sor összegképletét alkalmazva, majd tagonkénti beszorzást végezve, és alkalmazva a számelmélet alaptételét, $s>1$ esetén a következőt nyerjük:

$$(20)\quad \prod_{i=1}^{+\infty} \frac{1}{1-\frac{1}{p_i^s}} = \prod_{i=1}^{+\infty}\left(1+\sum_{k_i=1}^{+\infty}\frac{1}{p_i^{k_i s}}\right) =$$

$$= 1+\sum \frac{1}{p_{i_1}^{\alpha_1 s} p_{i_2}^{\alpha_2 s} \cdots p_{i_r}^{\alpha_r s}} = 1+\sum \frac{1}{(p_{i_1}^{\alpha_1} p_{i_2}^{\alpha_2} \cdots p_{i_r}^{\alpha_r})^s} =$$

$$= \sum_{n=1}^{+\infty} \frac{1}{n^s} = \zeta(s).$$

Itt két helyen csak Σ jelet írtunk, annak feltüntetése nélkül, hogy az összegzés mely számokra vonatkozik. Mindkét összegzés úgy értendő, hogy $r, \alpha_1, \alpha_2, \ldots, \alpha_r$ tetszőleges természetes számok lehetnek, $p_{i_1}, p_{i_2}, \ldots, \ldots, p_{i_r}$ pedig tetszőleges prímszámok, melyekre $p_{i_1}<p_{i_2}<\ldots<p_{i_r}$ teljesül. Megjegyezzük továbbá, hogy a végzett átalakítások jogosultsága következik abból, hogy az itt szereplő végtelen sorok tagjai pozitívak.

$\prod_{i=1}^{+\infty} f(p_i)$ típusú végtelen szorzat jelölésére gyakran használjuk a rövidebb $\prod_p f(p)$ írásmódot. Ezt a jelölést használva, a levezetett összefüggés a következő alakban írható:

$$\zeta(s) = \prod_p \frac{1}{1-\frac{1}{p^s}} \quad (\text{ahol } s>1).$$

A ζ-függvénynek ezt az előállítását a ζ-függvény *Euler-féle szorzatelőállításának* nevezzük.

Végeredményben tehát igazoltuk, hogy

$$(21)\quad \prod_p \frac{1}{1-\frac{1}{p^s}} = \sum_{n=1}^{+\infty} \frac{1}{n^s} \quad (=\zeta(s)).$$

Ez az (Eulertől származó) összefüggés kulcsszerepet játszik az analitikus számelméletben. Ez lényegében azzal magyarázható, hogy a jobb oldalon álló összegben az összegzés az *összes* természetes számra kiterjed, tehát összegfüggvénye a prímszámok eloszlásától függetlenül, analitikus szempontból viszonylag könnyen kezelhető. Ugyanakkor a bal oldalon álló szorzatban a p változó a *prímszámokon* fut végig, és ezért e szorzat analitikus tulajdonságai (melyeket az előbbiek szerint a végtelen sor alakban való előállításból kiindulva vizsgálhatunk) összefüggésbe hozhatók a prímszámok eloszlásával.

Így például a (20) átalakítás nyilván $s=1$ esetén is jogosult abban az értelemben, hogy az ott szereplő $\prod_p \frac{1}{1-\frac{1}{p^s}}$ szorzat részletszorzatai, ill. a végeredményként kapott végtelen sor részletösszegei ugyanazon — véges vagy végtelen — határértékhez tartanak; ezért ebben az értelemben (21) ekkor is teljesül. Azonban mint mondtuk, $s=1$ esetén a (21) jobb oldalán álló harmonikus sor divergens; következésképpen nyilván nem lehetséges, hogy a bal oldalon álló $\prod_p \frac{1}{1-\frac{1}{p}}$ szorzatnak csak véges sok tényezője legyen, tehát *végtelen sok prímszám létezik*. Így a (21) összefüggésből — mint ezt lényegében már a IV. fejezet 21*. feladatában is láttuk — következik végtelen sok prímszám létezése (természetesen mélyebb segédeszközökkel (21)-ből ennél lényegesen több információt is levezethetünk a prímszámokra vonatkozóan).

A prímszámelméletben gyakran találkozunk a ζ-függvény logaritmikus deriváltjának, azaz $(\log \zeta(s))' = \frac{\zeta'(s)}{\zeta(s)}$-nek, ill. az $\frac{1}{\zeta(s)}$ függvénynek a Dirichlet-sorával is. A ζ-függvény Euler-féle szorzatelőállítását felhasználva, könnyen igazolható (l. a 22., ill. 23. feladatot), hogy az említett függvények Dirichlet-sora:

$$(22) \quad \frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{+\infty} -\frac{\Lambda(n)}{n^s},$$

$$(23) \quad \frac{1}{\zeta(s)} = \sum_{n=1}^{+\infty} \frac{\mu(n)}{n^s},$$

ahol $s>1$, és $\Lambda(n)$ a III. fejezet 17. feladatában definiált Mangoldt-szimbólum, $\mu(n)$ pedig a Möbius-függvényt jelöli.

A 3. példa, valamint a 24—27. feladatok kapcsán a Dirichlet-sorok elméletének, valamint a ζ-függvénynek néhány olyan alkalmazását fogjuk ismertetni, mely rokon az 1. pontban tárgyalt analitikus módszerek alkalmazásaival; más szóval most is a generátorfüggvény-elv egy verzióját fogjuk alkalmazni. A különbség csupán az, hogy itt a generátorfüggvények hatványsorok helyett Dirichlet-sorok lesznek. Ismételten hangsúlyozzuk azonban, hogy a Dirichlet-sorok és a ζ-függvény csupán a komplex függvénytan felhasználásával válnak igazán hatékony segédeszközzé.

A valós Dirichlet-sorokról fent elmondottak lényegében változatlanul átvihetők komplex Dirichlet-sorokra is, csupán az $s>s_0$ feltétel helyett végig $\operatorname{Re} s>\operatorname{Re} s_0$ írandó. Ezek alapján egy komplex Dirichlet-sor egy *félsík* pontjaiban konvergál (beleértve a félsíkot határoló egyenes egyes pontjait is). A Riemann-féle ζ-függvény értelmezése is kiterjeszthető a $\operatorname{Re} s>1$ félsíkra, mégpedig a kiterjesztett ζ-függvény változatlanul a (19) formula által definiálható, és arra továbbra is érvényes marad a (21) Euler-féle szorzatelőállítás. Alapvető fontosságú és az előbbinél jóval mélyebb tény, hogy a ζ-függvény értelmezése az egész komplex számsíkra kiterjeszthető; $\operatorname{Re} s\leqq 1$ esetén azonban már a (19) és (21) előállítások egyike sem marad érvényben. A számelmélet legfontosabb problémái közé tartozik annak vizsgálata, hogy az így kiterjesztett ζ-függvény hogyan viselkedik a $0\leqq\operatorname{Re} s\leqq 1$ ún. *kritikus sávban*, speciálisan, hol helyezkednek el a ζ-függvény kritikus sávba eső gyökei? Ez utóbbi problémára vonatkozik az ún. *Riemann-sejtés*, melynek igazolása (vagy akár csak az eddigieken túlmenő részeredmények elérése is) a számelmélet sok területén lényeges előrelépést tenne lehetővé.

Végül megemlítjük, hogy a prímszámok számtani sorozatokban való eloszlásának vizsgálata során igen fontos szerepet játszanak a ζ-függvény bizonyos általánosításai. Valamely $\chi(n)$ karaktert (lásd a 17. feladatot) megadva, a $\sum_{n=1}^{+\infty}\frac{\chi(n)}{n^s}$ Dirichlet-sor összegfüggvényét $L(s,\chi)$-vel jelöljük. Igazolható, hogy $\operatorname{Re} s>1$ esetén ez a végtelen sor abszolút konvergens, és

$$(24)\quad L(s,\chi)=\sum_{n=1}^{+\infty}\frac{\chi(n)}{n^s}=\prod_p\frac{1}{1-\frac{\chi(p)}{p^s}}.$$

Az így definiált $L(s, \chi)$ függvényeket *Dirichlet-féle L-függvényeknek* nevezzük.

Példa

3. Bizonyítsuk be, hogy tetszőleges n természetes számra

$$2 \sum_{k|n} \Lambda(k) d\left(\frac{n}{k}\right) = d(n) \log n.$$

Megoldás:

Induljunk ki a

$$(25) \qquad 2\frac{\zeta'(s)}{\zeta(s)} \cdot \zeta^2(s) = 2\zeta(s)\zeta'(s) = (\zeta^2(s))' \quad (\text{ahol } s > 1)$$

összefüggésből. A Dirichlet-sorok szorzási szabálya szerint $\zeta^2(s)$ Dirichlet-sora

$$\zeta^2(s) = \left(\sum_{n=1}^{+\infty} \frac{1}{n^s}\right)\left(\sum_{n=1}^{+\infty} \frac{1}{n^s}\right) = \sum_{n=1}^{+\infty} \frac{\sum_{d|n} 1}{n^s} = \sum_{n=1}^{+\infty} \frac{d(n)}{n^s}.$$

(22)-ből és (23)-ból ismét a szorzási szabály alapján következik, hogy a (25) bal oldalán álló függvény Dirichlet-sora:

$$(26) \qquad 2\frac{\zeta'(s)}{\zeta(s)} \cdot \zeta^2(s) = \left(\sum_{n=1}^{+\infty} -\frac{2\Lambda(n)}{n^s}\right)\left(\sum_{n=1}^{+\infty} \frac{d(n)}{n^s}\right) =$$

$$= \sum_{n=1}^{+\infty} \frac{-\sum_{k|n} 2\Lambda(k) d\left(\frac{n}{k}\right)}{n^s}.$$

Másrészt könnyen látható, hogy $s > 1$ esetén $\zeta^2(s)$ deriváltját kiszámíthatjuk Dirichlet-sorának tagonkénti deriválása révén:

$$(27) \qquad (\zeta^2(s))' = \left(\sum_{n=1}^{+\infty} \frac{d(n)}{n^s}\right)' = \sum_{n=1}^{+\infty} \left(\frac{d(n)}{n^s}\right)' = \sum_{n=1}^{+\infty} (d(n) \cdot n^{-s})' =$$

$$= \sum_{n=1}^{+\infty} d(n)(-\log n) n^{-s} = \sum_{n=1}^{+\infty} \frac{-d(n) \log n}{n^s}.$$

Minthogy valamely Dirichlet-sor összegfüggvénye egyértelműen meghatározza a sor együtthatóit, (25)-ből következik, hogy a (26), ill. (27) alatt nyert Dirichlet-sorok megfelelő együtthatói megegyeznek:

$$-\sum_{k|n} 2\Lambda(k) d\left(\frac{n}{k}\right) = -d(n) \log n \quad (\text{ahol } n = 1, 2, \ldots).$$

Mindkét oldalt -1-gyel szorozva és a bal oldalon 2-t kiemelve, adódik a bizonyítandó összefüggés.

FELADATOK

1. Definiáljuk az $a_0, a_1, a_2, \ldots$ végtelen sorozatot a következő rekurzióval: legyen $a_0=1, a_1=3$ és $a_{n+2}=4a_{n+1}-3a_n$ (ahol $n=0, 1, 2, \ldots$). Fejezzük ki a_n-et n függvényeként (zárt alakban)!

2. Jelöljük az $f(n)$ számelméleti függvény összegzési függvényét $F(n)$-nel: $F(n)=\sum_{d|n} f(d)$. Bizonyítsuk be, hogy ha tetszőlegesen kicsi ε pozitív számhoz található olyan n_0 szám, hogy $n>n_0$ esetén

$$|f(n)| < (1+\varepsilon)^n,$$

akkor $|x|<1$ esetén

$$\sum_{n=1}^{+\infty} F(n)x^n = \sum_{i=1}^{+\infty} f(i)\frac{x^i}{1-x^i}$$

(a szóban forgó végtelen sorok abszolút konvergensek)!

3. Bizonyítsuk be, hogy $|x|<1$ esetén

a. $$\sum_{n=1}^{+\infty} d(n)x^n = \sum_{i=1}^{+\infty} \frac{x^i}{1-x^i},$$

b. $$\sum_{n=1}^{+\infty} \sigma(n)x^n = \sum_{i=1}^{+\infty} \frac{ix^i}{1-x^i} = \sum_{k=1}^{+\infty} \frac{x^k}{(1-x^k)^2},$$

c. $$\sum_{n=1}^{+\infty} \nu(n)x^n = \sum_{p} \frac{x^p}{1-x^p},$$

d. $$\sum_{n=1}^{+\infty} \frac{\mu(n)x^n}{1-x^n} = x,$$

e. $$\sum_{n=1}^{+\infty} \frac{\varphi(n)x^n}{1-x^n} = \frac{x}{(1-x)^2}$$

(a szereplő végtelen sorok abszolút konvergensek)!

4. Legyenek $k, a_1, a_2, \ldots, a_k$ adott természetes számok, n adott nemnegatív egész szám. Jelöljük az

$$a_1x_1+a_2x_2+\ldots+a_kx_k = n$$

diofantikus egyenlet nemnegatív egész megoldásainak a számát $f(a_1, a_2, \ldots, a_k; n)$-nel. Bizonyítsuk be, hogy $|x|<1$ esetén

$$F(x) = \sum_{n=0}^{+\infty} f(a_1, a_2, \ldots, a_n; n)x^n = \prod_{i=1}^{k} \frac{1}{1-x^{a_i}}.$$

5*. Határozzuk meg a

$$2x+3y = n$$

(n adott nemnegatív egész szám) diofantikus egyenlet nemnegatív egész megoldásainak a számát!

6*. Bizonyítsuk be, hogy tetszőleges k, n természetes számokra

$$\left\{\frac{n}{k}\right\} = \frac{1}{2} - \frac{1}{2k} - \frac{1}{2k} \sum_{j=1}^{k-1} \frac{\sin \frac{(2n+1)j\pi}{k}}{\sin \frac{j\pi}{k}}.$$

7. Legyen n tetszőleges természetes szám. Jelöljük az

$$x_1+x_2+\ldots+x_k = n, \quad x_1 \geqq x_2 \geqq \ldots \geqq x_k \geqq 1$$

(ahol k bármely természetes szám lehet) rendszer természetes számokból álló $x_1, x_2, \ldots, x_k$ megoldásainak a számát $p(n)$-nel, és legyen $p(0)=1$. Bizonyítsuk be, hogy $|x|<1$ esetén

$$F(x) = \sum_{n=0}^{+\infty} p(n)x^n = \prod_{i=1}^{+\infty} \frac{1}{1-x^i}.$$

8. Az előző feladatot felhasználva, számítsuk ki $p(n)$ értékét $0 \leqq n \leqq 5$ esetén!

9*. Bizonyítsuk be, hogy tetszőleges n természetes számra

$$np(n) = p(0)\sigma(n)+p(1)\sigma(n-1)+p(2)\sigma(n-2)+$$
$$+\ldots+p(n-1)\sigma(1).$$

10. Az előző két feladatot felhasználva, számítsuk ki $p(n)$ értékét $n=6, 7, 8$ esetén!

11. Legyen b tetszőleges természetes szám. Jelöljük az

$$x_1+x_2+\ldots+x_k = n, \quad x_1 > x_2 > \ldots > x_k \geqq 1$$

(ahol k bármely természetes szám lehet) rendszer természetes számokból álló $x_1, x_2, \ldots, x_k$ megoldásainak a számát $g(n)$-nel, és legyen $g(0)=1$. Bizonyítsuk be, hogy $|x|<1$ esetén

$$G(x) = \sum_{n=0}^{+\infty} g(n)x^n = \prod_{i=1}^{+\infty} (1+x^i).$$

12. Legyen n tetszőleges természetes szám. Jelöljük az

$$x_1+x_2+\ldots+x_k = n, \quad x_1 \geqq x_2 \geqq \ldots \geqq x_k \geqq 1$$

(ahol k bármely természetes szám lehet) rendszer *páratlan* egész számokból álló $x_1, x_2, \ldots, x_k$ megoldásainak a számát $h(n)$-nel, és legyen $h(0)=1$. Bizonyítsuk be, hogy $|x|<1$ esetén

$$H(x) = \sum_{n=0}^{+\infty} h(n)x^n = \prod_{i=1}^{+\infty} \frac{1}{1-x^{2i-1}}.$$

13. Az előző két feladat jelöléseit használva, igazoljuk, hogy tetszőleges n nemnegatív egész számra $g(n)=h(n)$.

14*. Igazoljuk, hogy tetszőleges n természetes számra az n-edik primitív egységgyökök összege $\mu(n)$-nel egyenlő!

15. Az előző feladat állítását felhasználva, adjunk új bizonyítást a III. fejezet (24) összefüggésére!

16. Igazoljuk a (16) összefüggést!

17. Legyen p tetszőleges prímszám, g prímitív gyök modulo p, ε a ($p-1$ számú) $p-1$-edik egységgyök valamelyike. Definiáljuk a $\chi(n)$ számelméleti függvényt a következőképpen:

Ha az n természetes számra $(n, p)>1$ teljesül (vagyis $p|n$), akkor legyen $\chi(n)=0$. Ha viszont $(n, p)=1$, akkor létezik olyan t nemnegatív egész szám, melyre

$$g^t \equiv n \pmod{p};$$

legyen ekkor $\chi(n)=\varepsilon^t$. Az így definiált $\chi(n)$ számelméleti függvényeket (modulo p) *karaktereknek* nevezzük. A definícióból nyilván következik, hogy a modulo p karakterek száma $p-1$. Speciálisan, $\varepsilon=1$ esetén

$$\chi(n) = \begin{cases} 0, & \text{ha } p|n; \\ 1, & \text{ha } p\nmid n. \end{cases}$$

Ezt a karaktert *főkarakternek* nevezzük, és χ_0-lal szoktuk jelölni.

Igazoljuk a karakterek alábbi alaptulajdonságait:

a. ha $a \equiv b \pmod{p}$,

akkor $\chi(a) = \chi(b)$.

b. Tetszőleges a, b természetes számokra

$\chi(ab) = \chi(a)\chi(b)$.

c. Bármely χ karakterre $\chi(1) = 1$.

d. $$\sum_{n=0}^{p-1} \chi(n) = \begin{cases} p-1, & \text{ha } \chi = \chi_0; \\ 0, & \text{ha } \chi \not\equiv \chi_0. \end{cases}$$

e. $$\sum_{\chi} \chi(n) = \begin{cases} p-1, & \text{ha } n \equiv 1 \pmod{p}; \\ 0, & \text{ha } n \not\equiv 1 \pmod{p}. \end{cases}$$

(Itt a $\sum_{\chi}$ jelölés úgy értendő, hogy χ a $p-1$ számú modulo p karaktereken fut végig.)

f. $(a, b) = 1$ esetén

$$\sum_{\chi} \chi(a)\overline{\chi(b)} = \begin{cases} p-1, & \text{ha } a \equiv b \pmod{p}; \\ 0, & \text{ha } a \not\equiv b \pmod{p}. \end{cases}$$

Megjegyezzük, hogy a karakterek összetett modulus esetén is definiálhatók. E célból azonban általánosítanunk kellene a primitív gyök fogalmát az összetett modulus esetére, ami bizonyos nehézségekkel járna.

18. Legyen $f(x_1, x_2, \ldots, x_r)$ tetszőleges egész együtthatós (r változós) polinom, m tetszőleges természetes szám. Jelöljük az

$$f(x_1, x_2, \ldots, x_r) \equiv 0 \pmod{m}$$

kongruencia lényegesen különböző megoldásainak a számát N-nel. (A fenti kongruencia $x_1', x_2', \ldots, x_r'$ és $x_1'', x_2'', \ldots, x_r''$ megoldásait akkor és csak akkor tekintjük lényegesen különbözőknek, ha létezik legalább egy olyan i index, melyre

$$x_i' \not\equiv x_i'' \pmod{m}$$

teljesül.) Bizonyítsuk be, hogy

$$(28)\quad Nm = \sum_{k=0}^{m-1} \sum_{x_1=0}^{m-1} \dots \sum_{x_r=0}^{m-1} e^{2\pi i \frac{kf(x_1, x_2, \dots, x_r)}{m}}.$$

19*. Legyenek m, r tetszőleges természetes számok, $a_1, a_2, \dots, \dots, a_r, b$ tetszőleges egész számok. Jelöljük az

$$a_1x_1 + a_2x_2 + \dots + a_rx_r + b \equiv 0 \pmod{m}$$

kongruencia lényegesen különböző megoldásainak a számát N-nel, és legyen $(a_1, a_2, \dots, a_r, m) = d$. Bizonyítsuk be, hogy

$$N = \begin{cases} m^{r-1}d, & \text{ha } d|b; \\ 0, & \text{ha } d|b. \end{cases}$$

20. A 2. példa és a 18. feladat állítását felhasználva, igazoljuk Lagrange következő tételét: ha p 2-nél nagyobb prímszám, a tetszőleges egész szám, akkor az

$$x^2 - y^2 \equiv a \pmod{p}$$

kongruencia lényegesen különböző megoldásainak a száma:

$$N = \begin{cases} p-1, & \text{ha } p \nmid a; \\ 2p-1, & \text{ha } p|a. \end{cases}$$

(Lagrange tétele szerint tehát a megoldásszám $p \nmid a$ esetén *független a-tól.*)

21. Adjuk meg valós számoknak valamely $a_1, a_2, \dots, a_n, \dots$ végtelen sorozatát; jelöljük ezt A-val. Jelöljük továbbá

$$(29)\quad 0 \leqq \alpha < \beta \leqq 1$$

esetén az $\alpha \leqq \{a_i\} < \beta$, $1 \leqq i \leqq n$ feltételeket kielégítő a_i számok számát $N(\alpha, \beta, n)$-nel. Az A sorozatot akkor mondjuk *egyenletes eloszlásúnak modulo* 1, ha bármely, a (29) feltételt kielégítő α, β valós számokra

$$\lim_{n=+\infty} \frac{N(\alpha, \beta, n)}{n} = \beta - \alpha.$$

Az ún. *Weyl kritérium* szerint valamely A sorozat akkor és csak akkor egyenletes eloszlású modulo 1, ha bármely 0-tól különböző k egész számra

$$\lim_{n=+\infty} \frac{\sum_{j=1}^{n} e^{2\pi i k a_j}}{n} = 0.$$

Ezt a kritériumot felhasználva, igazoljuk, hogy tetszőleges α irracionális számra az $\alpha, 2\alpha, \ldots, n\alpha, \ldots$ sorozat egyenletes eloszlású modulo 1.

22. Igazoljuk a (22) összefüggést!

23. Igazoljuk a (23) összefüggést!

24. Igazoljuk, hogy $s>2$ esetén

a. $$\zeta(s-1)\zeta(s) = \sum_{n=1}^{+\infty} \frac{\sigma(n)}{n^s},$$

b. $$\frac{\zeta(s-1)}{\zeta(s)} = \sum_{n=1}^{+\infty} \frac{\varphi(n)}{n^s}.$$

25. Dirichlet-sorok segítségével adjunk új bizonyítást a III. fejezet 21. feladatának állítására!

26. Igazoljuk, hogy tetszőleges n természetes számra

a. $$\sum_{k|n} \varphi(k) d\left(\frac{n}{k}\right) = \sigma(n),$$

b. $$\sum_{k|n} \varphi(k) \sigma\left(\frac{n}{k}\right) = n d(n).$$

27. Igazoljuk, hogy tetszőleges n természetes számra

$$\sum_{k|n} \mu(k) d\left(\frac{n}{k}\right) \log \frac{n}{k} = 2 \log n.$$

28. Igazoljuk, hogy tetszőleges p prímszámra és tetszőleges (modulo p) karakterre teljesül a (24) összefüggés!

ÚTMUTATÁSOK A VII*. FEJEZETBEN KITŰZÖTT FELADATOK MEGOLDÁSÁHOZ

Az 1. pont elején említett szempontokra tekintettel itt arra szorítkozunk, hogy útmutatást adunk egyes feladatokhoz.

1. A generátorfüggvény:

$$F(x) = \sum_{n=0}^{+\infty} a_n x^n = \frac{1-x}{1-4x+3x^2} = \frac{1}{1-3x}.$$

Eredmény: $a_n = 3^n$ (ahol ($n = 0, 1, 2, \ldots$).

2. $$\sum_{n=1}^{+\infty} F(n)x^n = \sum_{n=1}^{+\infty}\left(\sum_{i|n} f(i)\right)x^n = \sum_{i=1}^{+\infty}\left(\sum_{j=1}^{+\infty} f(i)x^{ij}\right) =$$

$$= \sum_{i=1}^{+\infty} f(i)\frac{x^i}{1-x^i}.$$

3. Alkalmazzuk az előző feladat állítását, mégpedig $f(n)$-et a következőképpen választva:

a. $f(n) = 1$;

b. $f(n) = n$;

c. $f(n) = \begin{cases} 1, & \text{ha } n \text{ prímszám,} \\ 0, & \text{ha } n \text{ nem prímszám;} \end{cases}$

d. $f(n) = \mu(n)$;

e. $f(n) = \varphi(n)$.

Hivatkozzunk továbbá a III. fejezet (18), (19) és (24) formuláira, 15. feladatára, ill. 4. példájára!

4. $$\prod_{i=1}^{k} \frac{1}{1-x^{a_i}} = \prod_{i=1}^{k}\left(\sum_{x_i=0}^{+\infty} x^{a_i x_i}\right) =$$

$$= \sum_{x_1=0}^{+\infty} \ldots \sum_{x_k=0}^{+\infty} x^{a_1x_1+a_2x_2+\ldots+a_kx_k} = \sum_{n=0}^{+\infty} f(a_1, a_2, \ldots, a_k; n)x^n.$$

5*. A megoldásszámot $f(n)$-nel jelölve, az előző feladat szerint $f(n)$ generátorfüggvénye:

$$F(x) = \sum_{n=0}^{+\infty} f(n)x^n = \frac{1}{1-x^2}\cdot\frac{1}{1-x^3} = \frac{1}{(1-x)^2(1+x)(1-\varepsilon x)(1-\varepsilon^2 x)},$$

ahol x komplex változó, ε pedig a primitív harmadik egységgyökök valamelyike. Parciális törtekre bontva:

$$F(x) = \frac{1}{6(1-x)^2}+\frac{1}{4(1-x)}+\frac{1}{4(1+x)}+\frac{1-\varepsilon^2}{9(1-\varepsilon x)}+\frac{1-\varepsilon}{9(1-\varepsilon^2 x)}.$$

Eredmény:

$$f(n) = \frac{1}{6}(n+1)+\frac{1}{4}(1+(-1)^n)+\frac{1}{9}[(1-\varepsilon^2)\varepsilon^n+(1-\varepsilon)\varepsilon^{2n}].$$

Ez a következő alakra hozható:

$$f(n) = \frac{1}{6}(n+1)+\frac{1}{4}(1+(-1)^n)+\frac{2}{3\sqrt{3}}\sin(n+1)\frac{2\pi}{3}.$$

6*. Az $\left\{\frac{n}{k}\right\} = \frac{n}{k}-\left[\frac{n}{k}\right]$ összefüggésre tekintettel $\left[\frac{n}{k}\right]$ vizsgálatára szorítkozhatunk. Továbbá az

$$x+ky = n$$

diofantikus egyenlet nemnegatív egész megoldásainak számát $f(n)$-nel jelölve, könnyen látható, hogy

$$\left[\frac{n}{k}\right] = f(n)-1.$$

Így $\left\{\frac{n}{k}\right\}$ vizsgálata végeredményben $f(n)$ vizsgálatára redukálható. A 4. feladat szerint azonban $f(n)$ generátorfüggvénye:

$$F(x) = \sum_{n=0}^{+\infty} f(n)x^n = \frac{1}{(1-x)(1-x^k)} = \frac{1}{(1-x)^2\prod_{j=1}^{k-1}(1-\varepsilon_j x)},$$

ahol x komplex változó, $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{k-1}$ az 1-től különböző k-adik egységgyökök. Ez a racionális törtfüggvény a következőképpen bontható parciális törtekre:

$$F(x) = \frac{1}{k}\cdot\frac{1}{(1-x)^2}+\frac{k-1}{2k}\cdot\frac{1}{1-x}+\sum_{j=1}^{k-1}\frac{1}{k(1-\varepsilon_j)}\cdot\frac{1}{1-\varepsilon_j x}.$$

7. A 4. feladat megoldásához hasonlóan okoskodhatunk.

8. Eredmény: $p(0)=p(1)=1$, $p(2)=2$, $p(3)=3$, $p(4)=5$, $p(5)=7$.

9*. Legyen $F(x) = \sum_{n=0}^{+\infty} p(n)x^n$ (ahol $|x| < 1$).

Nyilván

$$F'(x) = \frac{F'(x)}{F(x)} \cdot F(x) = (\log F(x))' \cdot F(x). \tag{30}$$

A 3.*b.* és 7. feladatokra tekintettel

$$(\log F(x))' = \left(\log \prod_{i=1}^{+\infty} \frac{1}{1-x^i}\right)' = \left(\sum_{i=1}^{+\infty} -\log(1-x^i)\right)' =$$

$$= \sum_{i=1}^{+\infty} (-\log(1-x^i))' = \sum_{i=1}^{+\infty} \frac{ix^{i-1}}{1-x^i} = \frac{1}{x} \sum_{i=1}^{+\infty} \frac{ix^i}{1-x^i} =$$

$$= \frac{1}{x} \sum_{n=1}^{+\infty} \sigma(n)x^n = \sum_{n=1}^{+\infty} \sigma(n)x^{n-1}.$$

(30) tehát a következő alakban írható:

$$\sum_{n=1}^{+\infty} np(n)x^{n-1} = \left(\sum_{n=1}^{+\infty} \sigma(n)x^{n-1}\right)\left(\sum_{n=0}^{+\infty} p(n)x^n\right).$$

A jobb oldalon álló hatványsorokat összeszorozva, majd x^{n-1} együtthatóját vizsgálva, adódik az állítás.

10. Eredmény: $p(6)=11$, $p(7)=15$, $p(8)=22$.

11. A felírt végtelen szorzat átalakítása céljából végezzünk tagonkénti beszorzást!

12. A felírt végtelen szorzat egyes tényezőit írjuk fel végtelen mértani sor alakjában, majd végezzünk tagonkénti beszorzást!

13. Az előző két feladat jelöléseit használva:

$$G(x) = \lim_{n=+\infty} \prod_{i=1}^{n} (1+x^i) = \lim_{n=+\infty} \prod_{i=1}^{n} \frac{1-x^{2i}}{1-x^i} =$$

$$= \lim_{n=+\infty} \frac{\prod\limits_{\frac{n}{2}<i\leqq n} (1-x^{2i})}{\prod\limits_{0\leqq i<\frac{n}{2}} (1-x^{2i+1})} = \lim_{n=+\infty} \prod_{0\leqq i<\frac{n}{2}} \frac{1}{1-x^{2i+1}} \cdot$$

$$\cdot \lim_{n=+\infty} \prod_{\frac{n}{2}<i\leqq n} (1-x^{2i}) = H(x)\cdot 1 = H(x).$$

14*. Azt kell bizonyítanunk, hogy

$$\sum_{\substack{k:(k,n)=1,\\ 0\leqq k\leqq n-1}} e^{2\pi i\frac{k}{n}} = \mu(n).$$

Minthogy a jobb oldalon álló $\mu(n)$ függvény multiplikatív, elegendő igazolni, hogy a bal oldalon álló összeg is multiplikatív függvénye n-nek, továbbá a fenti összefüggés teljesül abban a speciális esetben, amikor $n=1$, vagy pedig n prímszámhatvány.

15. Mint jól ismert, az n-edik egységgyökök összege $n>1$ esetén 0-val egyenlő. Másrészt bizonyítsuk be és használjuk fel, hogy valamely komplex szám akkor és csak akkor n-edik egységgyök, ha az valamely $d|n$ számra d-edik primitív egységgyök.

16. Igazoljuk először, hogy valamely k egész számra

$$\int_0^1 e^{2\pi ikt}\,dt = \begin{cases} 1, & \text{ha } k=0;\\ 0, & \text{ha } k\neq 0.\end{cases}$$

Ezután

$$\int_0^1 F_1(t)\dots F_k(t)\,dt = \int_0^1 \left(\sum_{j_1=1}^{N_1} e^{2\pi i a_{(1,j_1)}t}\right)\dots\left(\sum_{j_k=1}^{N_k} e^{2\pi i a_{(k,j_k)}t}\right)dt$$

kiszámítása céljából végezzünk először az integrandusban tagonkénti beszorzást, majd a nyert összeget integráljuk tagonként.

17. *d.* Tekintettel *a.*-ra és *b.*-re:

$$\sum_{n=0}^{p-1}\chi(n) = \chi(0)+\sum_{n=1}^{p-1}\chi(n) = 0+\sum_{t=0}^{p-2}\chi(g^t) =$$

$$= \sum_{t=0}^{p-2}(\chi(g))^t = \sum_{t=0}^{p-2}\varepsilon^t.$$

e. Ha $(n,p)=1$ és

$$n\equiv g^t \pmod p,$$

akkor *a.*-ra és *b.*-re tekintettel

$$\sum_{\chi}\chi(n) = \sum_{\chi}\chi(g^t) = \sum_{\chi}(\chi(g))^t = \sum_{\varepsilon}\varepsilon^t,$$

ahol ε a $p-1$-edik egységgyökökön fut végig. A *primitív* $p-1$-edik egységgyökök valamelyikét ε_0-lal jelölve, ez az összeg a következő alakban írható:

$$\sum_{\chi}\chi(n) = \sum_{j=0}^{p-2}\varepsilon_0^{jt}.$$

f. Ha $(b, p)=1$, akkor létezik olyan b^* egész szám, melyre

$$bb^* \equiv 1 \pmod{p}.$$

Innen *a.*, *b.* és *c.* alapján következik, hogy

$$\chi(b)\chi(b^*) = \chi(bb^*) = \chi(1) = 1,$$

tehát

$$\chi(b) = \frac{1}{\chi(b^*)} = \overline{\chi(b^*)}.$$

Így ekkor b.-re tekintettel

$$\sum_{\chi} \chi(a)\overline{\chi(b)} = \sum_{\chi} \chi(a)\overline{(\overline{\chi(b^*)})} = \sum_{\chi} \chi(a)\chi(b^*) = \sum_{\chi} \chi(ab^*),$$

ahonnan *a.* és *e.* alapján következik az állítás.

18. A bizonyítandó összefüggés jobb oldalán cseréljük fel az összegezés sorrendjét úgy, hogy először a k-ra vonatkozó összegezést végezzük el; továbbá ez utóbbi összegezés elvégzése során válasszuk külön az olyan $x_1, x_2, \ldots, x_r$ szám-r-eseknek megfelelő tagokat, melyek kielégítik a vizsgált kongruenciát, vagyis $m|f(x_1, x_2, \ldots, x_r)$ teljesül.

19*. Az előző feladat alapján

$$(32) \qquad N = \frac{1}{m} \sum_{k=0}^{m-1} \sum_{x_1=0}^{m-1} \cdots \sum_{x_r=0}^{m-1} e^{2\pi i \left(\frac{ka_1x_1}{m}+\ldots+\frac{ka_rx_r}{m}+\frac{kb}{m}\right)} =$$

$$= \frac{1}{m} \sum_{k=0}^{m-1} \left[e^{2\pi i \frac{kb}{m}} \prod_{j=1}^{r} \left(\sum_{x_j=0}^{m-1} e^{2\pi i \frac{ka_jx_j}{m}} \right) \right].$$

Az itt szereplő produktum j-edik tényezőjének (a kerek zárójelben levő kifejezésnek) az értéke $m|ka_j$ esetén nyilván m, $m\nmid ka_j$ esetén pedig 0. Így a szögletes zárójelben álló kifejezés csak azokra a k számokra nem 0, melyekre az $m|ka_1, m|ka_2, \ldots, m|ka_r$ oszthatósági relációk mindegyike teljesül; ekkor az említett kifejezés értéke $m^r e^{2\pi i \frac{kb}{m}}$. Azonban e relációk akkor és csak akkor teljesülnek egyidejűleg, ha létezik olyan j egész szám, melyre $k=j\frac{m}{d}$ és $0 \leqq j < d$ teljesül. Így

$$N = \frac{1}{m} \sum_{j=0}^{d-1} m^r e^{2\pi i \cdot j \frac{m}{d} \cdot \frac{b}{m}} = m^{r-1} \sum_{j=0}^{d-1} e^{2\pi i \frac{jb}{d}}.$$

20. A 18. feladat értelmében

$$N = \frac{1}{p} \sum_{k=0}^{p-1} \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} e^{2\pi i \frac{k(x^2-y^2-a)}{p}} =$$

$$= \frac{1}{p} \sum_{k=0}^{p-1} \left[e^{-2\pi i \frac{ka}{p}} \left(\sum_{x=0}^{p-1} e^{2pi \frac{kx^2}{p}} \right) \left(\sum_{y=0}^{p-1} e^{-2\pi i \frac{ky^2}{p}} \right) \right] =$$

$$= \frac{1}{p} \sum_{k=0}^{p-1} e^{-2\pi i \frac{ka}{p}} \cdot S(k,p) \cdot \overline{S(k,p)} = \frac{1}{p} \sum_{k=0}^{p-1} e^{-2\pi i \frac{ka}{p}} \cdot |S(k,p)|^2$$

(ahol $S(k,p)$ a 2. példában definiált összeg).

21. Azt kell bizonyítanunk, hogy bármely 0-tól különböző k egész számra

$$\lim_{n=+\infty} \frac{\sum_{j=1}^{n} e^{2\pi i k j \alpha}}{n} = 0.$$

Mivel α irracionális szám, a számlálóban álló mértani sor kvociense, $e^{2\pi i k \alpha}$ különbözik 1-től. Így akalmazható a mértani sor összegképlete:

$$\lim_{n=+\infty} \frac{\sum_{j=1}^{n} e^{2\pi i k j \alpha}}{n} = \lim_{n=+\infty} \frac{1}{n} \cdot \frac{e^{2\pi i k \alpha}(1-e^{2\pi i n k \alpha})}{1-e^{2\pi i k \alpha}} =$$

$$= \frac{e^{2\pi i k \alpha}}{1-e^{2\pi i k \alpha}} \lim_{n=+\infty} \frac{1-e^{2\pi i n k \alpha}}{n}.$$

Az itt álló $1-e^{2\pi i n k \alpha}$ kifejezés abszolút értéke a következőképpen becsülhető:

$$|1-e^{2\pi i n k \alpha}| \leqq |1| + |e^{2\pi i n k \alpha}| = 1+1 = 2.$$

22. A ζ-függvény Euler-féle szorzatelőállítását felhasználva:

$$\frac{\zeta'(s)}{\zeta(s)} = (\log \zeta(s))' = \left(\log \prod_p \frac{1}{1-\frac{1}{p^s}} \right)' =$$

$$= \left(-\sum_p \log \left(1 - \frac{1}{p^s} \right) \right)' = -\sum_p (\log(1-p^{-s}))' =$$

$$= -\sum_p \frac{\log p}{1-p^{-s}} = -\sum_p \log p \cdot \sum_{k=0}^{+\infty} p^{-ks}.$$

23. $s>1$ esetén nyilván $\zeta(s)>0$; így ekkor képezhetjük a ζ-függvény reciprokát. Az Euler-féle szorzatelőállításra tekintettel

$$\frac{1}{\zeta(s)} = \prod_p \left(1-\frac{1}{p^s}\right).$$

A jobb oldalon tagonkénti beszorzást végezve, adódik az állítás.

24. *a.* A Dirichlet-sorok szorzási szabálya értelmében

$$\zeta(s-1)\zeta(s) = \left(\sum_{n=1}^{+\infty} \frac{1}{n^{s-1}}\right)\left(\sum_{n=1}^{+\infty} \frac{1}{n^s}\right) =$$

$$= \left(\sum_{n=1}^{+\infty} \frac{n}{n^s}\right)\left(\sum_{n=1}^{+\infty} \frac{1}{n^s}\right) = \sum_{n=1}^{+\infty} \frac{\sum\limits_{d|n} d}{n^s} = \sum_{n=1}^{+\infty} \frac{\sigma(n)}{n^s}.$$

b. Az *a.* állításhoz hasonlóan igazolható, felhasználva (23)-at és a III. fejezet (27) formuláját.

25. Induljunk ki a

$$\frac{\zeta'(s)}{\zeta(s)} = \frac{\zeta'(s)}{\zeta^2(s)}\cdot\zeta(s) \quad \left(=\left(-\frac{1}{\zeta(s)}\right)'\cdot\zeta(s)\right)$$

összefüggésből.

26. Induljunk ki az

a. $$\frac{\zeta(s-1)}{\zeta(s)}\cdot\zeta^2(s) = \zeta(s-1)\zeta(s),$$

b. $$\frac{\zeta(s-1)}{\zeta(s)}\cdot\zeta(s-1)\zeta(s) = \zeta^2(s-1)$$

összefüggésből!

27. Induljunk ki az

$$\frac{1}{\zeta(s)}\cdot 2\zeta(s)\zeta'(s) = 2\zeta'(s)$$

összefüggésből!

28. (21)-hez hasonlóan igazolható, felhasználva a karakterek multiplikativitását.

Műszaki vezető: Hegedűs Ernő
Műszaki szerkesztő: Mózer István
A borítót tervezte: Serediuk Péter

A könyv formátuma: FR5 — Ívterjedelem: 19,5 (A5)
Példányszám: 8900
Papír minősége: 80 g-os ofszet
Betűcsalád és méret: Times gm/gm
Azonossági szám: 60 685 — **MÜ: 2271-i-7678**
Készült az MSZ 5601—59 és 5602—55 szerint

75-316—Szegedi Nyomda

32,— Ft