Kiss Péter—Mátyás Ferenc

A SZÁMELMÉLET ELEMEI

EKF LÍCEUM KIADÓ, EGER
2005

Lektor:

Dr. Varecza Árpád

a matematikai tudomány kandidátusa

Megjelent az EKF Líceum Kiadó műszaki gondozásában
A szedés a MiKTEX—plainTEX szövegformázó programmal történt
Kiadóvezető: Hekeli Sándor
Felelős szerkesztő: Tömösközi Péter
Műszaki szerkesztő: Szabó Tünde és Tómács Tibor
Megjelent: 2005

Első kiadás digitális változata

Tartalom

Bevezetés

A könyvben a klasszikus számelmélet néhány fontos és érdekes fejezetét tárgyaljuk. A szereplő problémákat, definíciókat és tételeket legtöbbször a $(\mathbf{Z}, +, \cdot)$ integritástartományban fogalmazzuk meg, azaz alaphalmazunk a jól ismert egész számok halmaza az összeadás és szorzás műveletekkel. A szövegben $\mathbf{N}$ alatt a természetes számok halmazát értjük a nullát is beleértve, $\mathbf{N}^+$ pedig a pozitív egészek halmazát jelöli. Néhány fogalmat, tételt a $(\mathbf{T}[x], +, \cdot)$ polinomgyűrűben is megfogalmazunk, ahol $\mathbf{T}[x]$ valamely $\mathbf{T}$ (racionális, valós vagy komplex) számtest feletti polinomok halmaza.

Tapasztalatunk szerint a rendelkezésre álló idő kevés a könyv anyagának tanórákon való teljes feldolgozására. Alkalmas azonban a könyv arra, hogy az oktató ízlése szerint súlypontozza az anyagot, korlátozza a bebizonyítandó tételek számát, esetleg kihagyjon egyes fejezeteket. A könyv segítségével az előadásokon kihagyott fejezeteket, bizonyításokat viszont a hallgatók tanórán kívül is megismerhetik érdeklődésből vagy kötelező jelleggel.

A fejezetek végén néhány feladat található, melyek elősegítik a téma jobb megértését, és megmutatják az elméleti anyag alkalmazásainak lehetőségeit. A feladatmegoldásban való kellő jártasság eléréséhez jól használhatók az irodalomjegyzékben szereplő feladatgyűjtemények, melyek a megoldásokat is tartalmazzák.

A szerzők

1. Oszthatóság a $(\mathbf{Z}, +, \cdot)$ integritástartományban

Ismeretes, hogy az egész számok $(\mathbf{Z}, +, \cdot)$ gyűrűje integritástartomány és elemei a

$$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$$

egész számok. A 0 egész szám a gyűrű additív zérusa és zéruseleme, míg a multiplikatív egységelem az 1. Tudjuk továbbá, hogy a $(\mathbf{Z}, +, \cdot)$ gyűrű a $\leq$ rendezési reláció szerint rendezett. A $\mathbf{Z}^- = \{\ldots, -3, -2, -1\}$, illetve a $\mathbf{Z}^+ = \mathbf{N}^+ = \mathbf{N} \setminus \{0\} = \{1, 2, 3, \ldots\}$ halmaz elemeit negatív (vagy 0-nál kisebb), illetve pozitív (vagy 0-nál nagyobb) egészeknek nevezzük.

Az $a \in \mathbf{Z}$ egész szám $|a|$ abszolút értékét

$$|a| = \begin{cases} a, & \text{ha} \quad a \geq 0, \\ -a, & \text{ha} \quad a < 0 \end{cases}$$

módon definiálva, bármely $a, b \in \mathbf{Z}$ egészre igaz, hogy

$$|a + b| \leq |a| + |b|\,,$$
$$|ab| = |a|\,|b|\,.$$

Euklideszi vagy maradékos osztás Z-ben

A számelmélet egyik legegyszerűbb, de nagyon sokszor idézett tétele a következő.

1.1. Tétel. (A maradékos osztás tétele) *Bármely a és b $(\neq 0)$ egész számhoz egyértelműen léteznek olyan q és r egész számok, amelyekre*

$$a = bq + r \quad \text{és} \quad 0 \leq r < |b| \tag{1.1}$$

teljesül.

(1.1)-ben az a-t osztandónak, a b-t osztónak, a q-t hányadosnak, míg az r-et legkisebb nemnegatív maradéknak nevezzük.

Bizonyítás. Tekintsük az alábbi M halmazt:

$$M = \{m : m = a - bk \geq 0,\ k \in \mathbf{Z}\}\,.$$

Nyilvánvaló, hogy $M \neq \emptyset$ és $M \subseteq \mathbf{N}$. Mivel $\mathbf{N}$ jólrendezett a $\leq$ reláció szerint, ezért M-nek van legkisebb eleme, melyet jelöljünk r-rel, míg az

$r = a - bk$ egyenlőségben a konkrét k-t q-val, azaz, $r = a - bq$. Ekkor $r < |b|$, mert ha $r \geq |b|$ teljesülne, akkor

$$r > r - |b| = a - bq - |b| = \begin{cases} (a - bq) - b \geq 0, & \text{ha} \quad b > 0, \\ (a - bq) + b \geq 0, & \text{ha} \quad b < 0 \end{cases}$$

lenne, mely ellentmond r minimális voltának.

q és r egyértelműségét indirekt módon bizonyítjuk. Tegyük fel, hogy a és b ($\neq 0$) olyan egészek, amelyekre nem egyértelmű a maradékos osztás, azaz

$$\begin{aligned} a &= bq_1 + r_1, \quad 0 \leq r_1 < |b|\,, \\ a &= bq_2 + r_2, \quad 0 \leq r_2 < |b| \end{aligned}$$

és $q_1 \neq q_2$. Kivonás után a

$$0 = b(q_1 - q_2) + r_1 - r_2, \quad \text{illetve} \quad |b|\,|q_1 - q_2| = |r_1 - r_2|$$

egyenlőséget kapjuk. Mivel a feltevésünk szerint $q_1 \neq q_2$, ezért $|b|\,|q_1 - q_2| \geq$ $\geq |b|$, ugyanakkor $0 \leq |r_1 - r_2| < |b|$. Ez ellentmondás, tehát a $q_1 \neq q_2$ feltevésünk hamis. Viszont a $q_1 = q_2$ esetén már $r_1 = r_2$ is következik. ∎

Példa:

$$\begin{aligned} 15 &= 4 \cdot 3 + 3; & -15 &= 4(-4) + 1; \\ 15 &= (-4)(-3) + 3; & -15 &= (-4)4 + 1. \end{aligned}$$

A maradékos osztás tételével kapcsolatban felvetődhet az a kérdés, hogy szükséges-e a legkisebb nemnegatív maradékot szerepeltetni a tételben. Nos, ha nem ragaszkodunk a q hányados és az r maradék egyértelműségéhez, akkor lehet ,,enyhébb" feltételt is szabni az r maradékra. Ha például az alábbi módokon fogalmazzuk meg a tételt, akkor az egyértelműség már nem biztosítható.

1. Bármely a és b ($\neq 0$) egészhez léteznek olyan q' és r' egészek, amelyekre

$$a = bq' + r' \quad \text{és} \quad |r'| < |b|\,.$$

(Az 1.1 Tételbeli q és r számokkal $q' = q$, $r' = r$, vagy $q' = q+1$, $r' = r-b$.)

Példa:

$$\begin{aligned} 13 &= 5 \cdot 2 + 3, \quad 3 < 5; \\ 13 &= 5 \cdot 3 - 2, \quad |-2| < 5. \end{aligned}$$

2. Bármely a és $b(\neq 0)$ egészhez léteznek olyan q'' és r'' egészek, amelyekre

$$a = bq'' + r'' \quad \text{és} \quad |r''| \leq \frac{|b|}{2}.$$

Példa:

$$\begin{aligned} 14 &= 4 \cdot 3 + 2, \quad 2 \leq 2; \\ 14 &= 4 \cdot 4 - 2, \quad |-2| \leq 2. \end{aligned}$$

Az euklideszi algoritmus

Legyenek adottak az a és b $(\neq 0)$ egész számok. A maradékos osztás tétele szerint a alakja

$$a = bq_0 + r_1, \quad \text{ahol} \quad 0 \leq r_1 < |b|\,.$$

Ha $r_1 \neq 0$, akkor a b és r_1 egészekkel elvégezve a maradékos osztást

$$b = r_1 q_1 + r_2, \quad \text{ahol} \quad 0 \leq r_2 < r_1$$

adódik. Ha $r_2 \neq 0$, akkor

$$r_1 = r_2 q_2 + r_3, \quad \text{ahol} \quad 0 \leq r_3 < r_2.$$

$r_i \neq 0$ $(i \geq 3)$ esetben hasonlóan folytatva, a maradékos osztások alábbi sorozatát, az úgynevezett euklideszi algoritmust kapjuk:

$$\begin{aligned} a &= bq_0 + r_1, & 0 < r_1 < |b|\,, \\ b &= r_1 q_1 + r_2, & 0 < r_2 < r_1, \\ r_1 &= r_2 q_2 + r_3, & 0 < r_3 < r_2, \\ &\vdots & \vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n, & 0 < r_n < r_{n-1}, \\ r_{n-1} &= r_n q_n + r_{n+1}, & r_{n+1} = 0. \end{aligned} \tag{1.2}$$

Az osztások során fellépő maradékok természetes számok szigorúan csökkenő sorozatát alkotják, ezért a fenti algoritmus nem lehet végtelen hosszú. Azaz, véges sok lépés után a maradéknak (r_{n+1}) 0-nak kell lennie.

Az algoritmus hosszára könnyen adható az alábbi „durva” becslés. Mivel $|b| > r_1 > r_2 > \cdots > r_n > 0$, ezért (1.2) legfeljebb $|b|$ lépésből állhat. Megemlítjük, hogy szomszédos Fibonacci-számokon végrehajtott euklideszi algoritmus a lehető leghosszabb, és a maradékok és a hányadosok is Fibonacci-számok. (A Fibonacci-számokat az $F_0 = 0$, $F_1 = 1$ kezdőtagokkal és az $F_n = F_{n-1} + F_{n-2}$ $(n \geq 2)$ rekurzióval definiáljuk.)

Példa: $F_7 = 13$ és $F_6 = 8$ esetén

$$\begin{aligned} 13 &= 8 \cdot 1 + 5, \\ 8 &= 5 \cdot 1 + 3, \\ 5 &= 3 \cdot 1 + 2, \\ 3 &= 2 \cdot 1 + 1, \\ 2 &= 1 \cdot 2 + 0. \end{aligned}$$

A későbbiek szempontjából is fontos az alábbi tétel.

1.2. Tétel. *Legyen r_n (1.2)-ben az utolsó zérustól különböző maradék. Végtelen sok X_n és Y_n egész szám létezik, amelyekre*

$$aX_n + bY_n = r_n.$$

Bizonyítás. Először megmutatjuk, hogy minden $1 \leq k \leq n$ esetén léteznek olyan x_k és y_k egészek, amelyekre $ax_k + by_k = r_k$.

Rendezzük át (1.2)-t az alábbiak szerint:

$$\begin{aligned} r_1 &= a - bq_0, \\ r_2 &= b - r_1 q_1, \\ r_3 &= r_1 - r_2 q_2, \\ &\vdots \\ r_{k-1} &= r_{k-3} - r_{k-2} q_{k-2}, \\ r_k &= r_{k-2} - r_{k-1} q_{k-1} \\ &\vdots \\ r_n &= r_{n-2} - r_{n-1} q_{n-1}, \end{aligned} \tag{1.3}$$

majd alkalmazzunk k szerinti teljes indukciót. $k = 1$ és $k = 2$ esetben igaz az állítás, mert

$$\begin{aligned} r_1 &= a1 + b(-q_0), \\ r_2 &= b - r_1 q_1 = b - (a - bq_0)q_1 = a(-q_1) + b(1 + q_0 q_1), \end{aligned}$$

azaz $x_1 = 1$, $y_1 = -q_0$, $x_2 = -q_1$ és $y_2 = 1 + q_0q_1$. Tegyük fel, hogy k-nál kisebb indexekre már bizonyítottuk az állítást, azaz léteznek olyan x_{k-2}, y_{k-2}, x_{k-1} és y_{k-1} egészek, amelyekre

$$\begin{aligned} r_{k-2} &= ax_{k-2} + by_{k-2}, \\ r_{k-1} &= ax_{k-1} + by_{k-1}, \end{aligned} \tag{1.4}$$

ahol $k \geq 3$. Így (1.3)-ból és (1.4)-ből kapjuk, hogy

$$\begin{aligned} r_k = r_{k-2} - r_{k-1}q_{k-1} = ax_{k-2} + by_{k-2} - (ax_{k-1} + by_{k-1})q_{k-1} = \\ = a(x_{k-2} - x_{k-1}q_{k-1}) + b(y_{k-2} - y_{k-1}q_{k-1}), \end{aligned}$$

amelyben a és b együtthatóit x_k-val, illetve y_k-val jelölve

$$r_k = ax_k + by_k.$$

A fentiek alapján láthatjuk, hogy (1.3)-ból mindig nyerhető egy konkrét x_n, y_n számpár, amelyre $ax_n + by_n = r_n$. Ugyanakkor az $X_n = x_n + bt$ és $Y_n = y_n - at$ egészek bármely $t \in \mathbf{Z}$-vel szintén kielégítik az $aX_n + bY_n = r_n$ egyenlőséget, mivel

$$aX_n + bY_n = a(x_n + bt) + b(y_n - at) = ax_n + by_n + abt - abt = r_n. \ \blacksquare$$

Például $a = 13$ és $b = 8$ esetén az algoritmus és r_n előállítása a következő:

$$\begin{aligned} 13 &= 8 \cdot 1 + 5, & 5 &= 13 - 8, \\ 8 &= 5 \cdot 1 + 3, & 3 &= 8 - 5, \\ 5 &= 3 \cdot 1 + 2, & 2 &= 5 - 3, \\ 3 &= 2 \cdot 1 + 1, & 1 &= 3 - 2, \\ 2 &= 1 \cdot 2 + 0, \end{aligned}$$

$$\begin{aligned} 3 &= 8 - (13 - 8) = -13 + 8 \cdot 2, \\ 2 &= (13 - 8) - (-13 + 8 \cdot 2) = 13 \cdot 2 - 8 \cdot 3, \\ 1 &= -13 + 8 \cdot 2 - (13 \cdot 2 - 8 \cdot 3) = 13 \cdot (-3) + 8 \cdot 5, \end{aligned}$$

$$1 = 13(-3 + 8t) + 8(5 - 13t), \quad t \in \mathbf{Z}.$$

A maradékos osztás tételét alkalmazzuk akkor is, amikor egy c pozitív egész számot g alapú számrendszerben írunk fel.

1.3. Tétel. *Bármely c pozitív egész szám egyértelműen írható fel*

$$c = a_n g^n + a_{n-1} g^{n-1} + \cdots + a_1 g + a_0 \tag{1.5}$$

alakban, ahol n, g és a_i $(i = 0, 1, \ldots, n)$ természetes számok, továbbá $g \geq 2$ rögzített, $0 \leq a_i \leq g - 1$ $(i = 0, 1, 2, \ldots, n)$ és $a_n \neq 0$.

Bizonyítás. Végezzük el az alábbi maradékos osztásokat:

$$\begin{aligned}
c &= gq_0 + a_0, && 0 \leq a_0 \leq g-1,\\
q_0 &= gq_1 + a_1, && 0 \leq a_1 \leq g-1,\\
q_1 &= gq_2 + a_2, && 0 \leq a_2 \leq g-1,\\
&\vdots && \vdots\\
q_{n-2} &= gq_{n-1} + a_{n-1}, && 0 \leq a_{n-1} \leq g-1,\\
q_{n-1} &= gq_n + a_n, && 0 < a_n \leq g-1 \quad \text{és} \quad q_n = 0.
\end{aligned} \tag{1.6}$$

Az (1.6) algoritmusban $q_i \in \mathbf{N}$, $c > q_0 > q_1 > \cdots > q_{n-1} > q_n$, ezért (1.6) nem lehet végtelen hosszú, azaz, $q_n = 0$ és $q_{n-1} = a_n$. (1.6) utolsó sorából q_{n-1}-et az utolsó előtti sorba helyettesítve kapjuk, hogy

$$q_{n-2} = ga_n + a_{n-1}.$$

A továbbiakban is helyettesítsük q_k-t a $q_{k-1} = gq_k + a_k$ egyenlőségbe $(n-2 \leq \leq k \leq 1)$, és így a következőt kapjuk:

$$q_0 = a_n g^{n-1} + a_{n-1} g^{n-2} + \cdots + a_2 g + a_1.$$

Ezt az (1.6) első egyenlőségébe helyettesítve a

$$c = gq_0 + a_0 = a_n g^n + a_{n-1} g^{n-1} + \cdots + a_1 g + a_0$$

alakhoz jutunk, amely egyezik (1.5)-tel.

Az (1.5)-beli egyértelműséget indirekt úton igazoljuk. Tegyük fel, hogy a $c(> 0)$ természetes számnak két különböző, (1.5) típusú előállítása van:

$$c = a_n g^n + a_{n-1} g^{n-1} + \cdots + a_0 = b_m g^m + \cdots + b_0, \tag{1.7}$$

ahol feltehető, hogy $n \leq m$. (1.7)-ből

$$g\left|a_n g^{n-1} + \cdots + a_1 - \left(b_m g^{m-1} + \cdots + b_1\right)\right| = |b_0 - a_0| \tag{1.8}$$

következik. Ha (1.8)-ban a bal oldal nem nulla, akkor legalább $g(\geq 2)$, ugyanakkor (1.8) jobb oldala maximum $g-1$. Ezért (1.8)-ban és (1.7)-ben is $a_0 = b_0$, és így (1.7)-ből kapjuk a következő egyenlőséget:

$$g\left|a_n g^{n-2} + \cdots + a_2 - (b_m g^{m-2} + \cdots + b_2)\right| = |b_1 - a_1|\,.$$

A bal és a jobb oldal összehasonlításából, hasonlóan az előbb leírtakhoz, $b_1 = a_1$ következik. Ezt folytatva (1.7)-ből az $a_2 = b_2$, $a_3 = b_3, \ldots, a_n = b_n$ egyenlőségekhez jutunk, azaz (1.7)-ből végül a

$$0 = b_m g^m + \cdots + b_{n+1} g^{n+1}$$

egyenlőséget nyerjük. De ez a b_i és g számokra tett feltételek miatt csak $b_m = b_{m-1} = \cdots = b_{n+1} = 0$ esetén teljesül, és ez ellentmondás. Ezzel bebizonyítottuk az (1.5)-beli előállítás egyértelműségét. ∎

A rövidebb írásmód kedvéért (1.5)-öt

$$c = (a_n a_{n-1} \cdots a_1 a_0)_g$$

alakban szokás írni, melyet a $c(>0)$ természetes szám $g(\geq 2)$ alapú számrendszerbeli alakjának nevezzük, ahol $a_n, a_{n-1}, \ldots, a_0$ a g alapú számrendszerben használt számjegyek ($0 \leq a_i \leq g-1$, ha $i = 0, \ldots, n$ és $a_n \neq 0$).

A különböző alapú számrendszerben való számolás (összeadás, kivonás, szorzás és osztás) több-kevesebb gyakorlással elsajátítható. Például adjuk meg a $c = (124)_5$ szám 4-es (alapú) számrendszerbeli alakját. Az (1.6) algoritmus most a következő:

$$\begin{aligned}(124)_5 &= (4)_5(14)_5 + (3)_5,\\ (14)_5 &= (4)_5(2)_5 + (1)_5,\\ (2)_5 &= (4)_5(0)_5 + (2)_5,\end{aligned}$$

így $(124)_5 = (213)_4$.

E feladat kapcsán megjegyezzük, hogy ha egy g_1 alapú számrendszerben felírt számot $g_2(>g_1)$ alapú számrendszerbe írunk át, akkor új számjegyek bevezetése válik szükségessé.

Oszthatóság Z-ben

A $(\mathbf{Z}, +, \cdot)$ integritástartományban az $ax = b$ alakú egyenletek nem mindig oldhatók meg, illetve a b és $a(\neq 0)$ elemeken végrehajtott euklideszi osztás nem mindig ad nulla maradékot. Ha az a és b egész számpárra ez mégis teljesül, akkor érdemes ezt a relációt külön is megvizsgálni.

Definíció. Az a egész szám osztója a b egész számnak (vagy b osztható a-val), ha az $ax = b$ egyenlet megoldható $\mathbf{Z}$-ben. Ezt az $a \mid b$, míg ennek tagadását az $a \nmid b$ szimbólummal jelöljük.

Az oszthatóság mint binér reláció rendelkezik az alábbi tulajdonságokkal.

1.4. Tétel. *$\mathbf{Z}$-ben az oszthatósági reláció*
(a) *reflexív*,
(b) *nem szimmetrikus*,
(c) *nem antiszimmetrikus*,
(d) *tranzitív.*

Bizonyítás. Mivel bármely $a \in \mathbf{Z}$ esetén az $ax = a$ egyenletnek megoldása az $x = 1$, ezért (a) igaz. A reláció nem szimmetrikus, valamint nem antiszimmetrikus volta konkrét példával igazolható:
például $5 \mid 10$, de $10 \nmid 5$, illetve $5 \mid -5$ és $-5 \mid 5$, de $5 \neq -5$.
A (d) bizonyításánál az $a \mid b$ és $b \mid c$ feltételek szerint léteznek olyan x_0 és y_0 egész számok, amelyekre

$$ax_0 = b \text{ és } by_0 = c.$$

Ebből

$$a(x_0y_0) = (ax_0)y_0 = by_0 = c$$

miatt $a \mid c$ következik, azaz az oszthatóság rendelkezik a tranzitív tulajdonsággal. ∎

Érdemes megfigyelni, hogy bár az oszthatóság nem antiszimmetrikus reláció, mégis igaz a következő állítás.

1.5. Tétel. *Bármely a és b egész számra, ha $a \mid b$ és $b \mid a$, akkor $|a| = |b|$.*

Bizonyítás. $a \mid b$ és $b \mid a$ miatt léteznek olyan x_0 és y_0 egészek, amelyekre $ax_0 = b$ és $by_0 = a$. Ezért

$$a(x_0y_0) = (ax_0)y_0 = by_0 = a. \tag{1.9}$$

Ha $a \neq 0$, akkor (1.9)-ből $x_0 y_0 = 1$ következik, azaz, vagy $x_0 = y_0 = 1$, vagy $x_0 = y_0 = -1$. Ha $a = 0$, akkor $0x_0 = b = 0$ miatt szintén igaz az állítás. ∎

Az oszthatósági problémák vizsgálatánál nem játszik fontos szerepet a számok előjele. Erről szól az alábbi tétel.

1.6. Tétel. *Bármely $a, b \in \mathbf{Z}$ esetén, ha $a \mid b$, akkor $a \mid -b$, $-a \mid b$ és $-a \mid -b$.*

Bizonyítás. Mivel $a \mid b$, ezért $ax_0 = b$ valamely $x_0 \in \mathbf{Z}$-re. De ekkor a $-b = a(-x_0)$, $b = (-a)(-x_0)$ és $-b = (-a)x_0$ egyenlőségek szintén igazak, és így a tétel állítása is. ∎

Definíció. A $(\mathbf{Z}, +, \cdot)$ integritástartomány 1 egységelemének osztóit egységeknek nevezzük.

Definíció. Az a egész számot b egész szám asszociáltjának nevezzük, ha van olyan e egység, amellyel $ae = b$. Ezt az $a \sim b$ szimbólummal jelöljük.

Így az egész számok halmazában nyilvánvalóan két egység van, és ezek a ± 1 egészek. Továbbá a és b pontosan akkor asszociáltak, ha $|a| = |b|$. Látható, hogy az 1.5. és 1.6. Tétel az asszociáltság segítségével is megfogalmazható lenne.

Az asszociáltság segítségével értelmezzük a valódi, illetve a triviális osztó fogalmát.

Definíció. Legyenek a és $b(\neq 0)$ egész számok. Ha $a \mid b$ és se $a \sim 1$, se $a \sim b$ nem teljesül, akkor a-t a b valódi osztójának, ellenkező esetben triviális osztójának nevezzük.

E definíció szerint a ± 1 egészeknek csak két triviális osztója (± 1) létezik, míg valódi osztójuk nincs. Bármely $a \in \mathbf{Z} \setminus \{-1, 0, 1\}$ egésznek pontosan négy $(\pm 1, \pm a)$ triviális osztója van.

A következőkben megvizsgáljuk, hogy milyen kapcsolat van az oszthatósági reláció és a $(\mathbf{Z}, +, \cdot)$ integritástartomány műveletei között.

1.7. Tétel. *Bármely $a, b, c, d \in \mathbf{Z}$-re*

(a) *ha $a \mid b$ és $a \mid c$, akkor $a \mid (b + c)$;*

(b) *ha $a \mid b$ és $c \mid d$, akkor $ac \mid bd$.*

(Az (a), illetve (b) tulajdonságokat az oszthatóság additív, illetve multiplikatív tulajdonságának nevezzük.)

Bizonyítás. Az (a) részben a feltétel szerint léteznek olyan x_0, y_0 egészek, amelyekre

$$ax_0 = b \quad \text{és} \quad ay_0 = c.$$

Ebből összeadással az

$$a(x_0 + y_0) = b + c$$

egyenlőséget kapjuk, azaz $a \mid (b + c)$.

A (b) rész feltétele szerint léteznek olyan x_0, y_0 egészek, amelyekre

$$ax_0 = b \quad \text{és} \quad cy_0 = d.$$

Ebből az oldalak összeszorzásával kapjuk az

$$ac(x_0y_0) = bd$$

egyenlőséget, azaz $ac \mid bd$. ∎

Az 1.4. és 1.7. Tételek következményeként bizonyítható az alábbi, feladatmegoldáskor gyakran alkalmazott tétel.

1.8. Tétel. *Ha* $a \mid a_i$ $(i = 1, 2, \ldots, n)$, *akkor*

$$a \mid (c_1a_1 + c_2a_2 + \cdots + c_na_n),$$

ahol $c_1, c_2, \ldots, c_n$ *tetszőleges egész számok.* (*A* $c_1a_1 + c_2a_2 + \cdots + c_na_n$ *összeget az* $a_1, a_2, \ldots, a_n$ *egészek lineáris kombinációjának is szokás nevezni.*)

Bizonyítás. Az 1.7. Tétel (b) pontja szerint, $1 \mid c_i$ és $a \mid a_i$ miatt, $a \mid c_ia_i$ $(i = 1, 2, \ldots, n)$. Az 1.7. Tétel (a) pontjának ismételt alkalmazásával kapjuk, hogy $a \mid (c_1a_1 + \cdots + c_na_n)$. ∎

Külön is érdemes kiemelni a $(\mathbf{Z}, +, \cdot)$ struktúra nevezetes elemeivel kapcsolatos oszthatósági tulajdonságokat.

1.9. Tétel. *Bármely* $a \in \mathbf{Z}$*-re igaz, hogy*

(a) $a \mid 0$*;*

(b) $0 \mid a$ *akkor és csak akkor, ha* $a = 0$*;*

(c) *az* e *egész szám akkor és csak akkor osztója bármely* a *egésznek, ha* $e = \pm 1$.

Bizonyítás. Mivel az $ax = 0$ egyenletnek minden $a \in \mathbf{Z}$-re $x = 0$ megoldása, ezért (a) igaz.

A (b) állításban $0 \mid a$ miatt $0x_0 = a$ valamely $x_0 \in \mathbf{Z}$-re, azaz $a = 0$. Ugyanakkor $0 \mid 0$, mert a $0x = 0$ egyenlet megoldható $\mathbf{Z}$-ben.

A (c) állításban ha $e \mid a$ bármely a egész számra, akkor speciálisan $e \mid 1$ is teljesül, azaz $e = \pm 1$. Ugyanakkor $\pm 1 \mid a$ valóban teljesül minden $a \in \mathbf{Z}$-re. ∎

Az osztók nagyságára és számára vonatkozik az alábbi tétel.

1.10. Tétel. *Bármely a és $b(\neq 0)$ egész számra igaz, hogy*

(a) *ha $a \mid b$, akkor $|a| \leq |b|$;*

(b) *b-nek véges sok osztója van.*

Bizonyítás. Mivel $b \neq 0$ és $a \mid b$, ezért van olyan $x_0 \in \mathbf{Z}$, amelyre $ax_0 = b$ és $|x_0| \geq 1$. Így

$$|b| = |a|\,|x_0| \geq |a|\,,$$

tehát (a) igaz. Ugyanakkor, az (a) részből már következik, hogy b minden osztója a $[-b, b]$ intervallumban van, azaz számuk csak véges lehet. ∎

Definíció. A 2-vel osztható egészeket párosnak, a 2-vel nem oszthatókat pedig páratlannak nevezzük. Ha a és b mindkettője páros vagy mindkettő páratlan, akkor azonos paritásúaknak nevezzük őket. Ellenkező esetben különböző paritásúak.

Oszthatósági feladatok megoldásakor sokszor alkalmazzuk az alábbi összefüggéseket:

Bármely $n \in \mathbf{N} \setminus \{0\}$ és $a, b \in \mathbf{Z}$-re

(a) $a^n - b^n = (a-b)\left(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}\right)$ miatt

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

(b) $a^{2n} - b^{2n} = (a^2 - b^2)(a^{2n-2} + a^{2n-4}b^2 + \cdots + b^{2n-2})$ miatt

$$(a^2 - b^2) \mid (a^{2n} - b^{2n});$$

(c) $a^{2n+1} + b^{2n+1} = (a+b)\left(a^{2n} - a^{2n-1}b + \cdots - ab^{2n-1} + b^{2n}\right)$ miatt

$$(a+b) \mid (a^{2n+1} + b^{2n+1}).$$

Legnagyobb közös osztó

A legnagyobb közös osztó definíciója a *legnagyobb* és a *közös* jelzők pontosításából áll.

Definíció. Az a és $b(\neq 0)$ egész számok legnagyobb közös osztójának nevezünk egy d egész számot, ha

1. d közös osztó, azaz $d \mid a$ és $d \mid b$;

2. d a legnagyobb abban az értelemben, hogy a és b bármely d' közös osztójának többszöröse, azaz, ha $d' \mid a$ és $d' \mid b$, akkor $d' \mid d$.

A definíció kapcsán azonnal felvethető az egyértelműség kérdése.

1.11. Tétel. *Ha az a és $b(\neq 0)$ egészeknek létezik legnagyobb közös osztója, akkor az asszociáltság erejéig egyértelműen maghatározott.*

Bizonyítás. Tételezzük fel, hogy d_1 és d_2 is kielégíti a fenti definíciót. Ekkor $d_1 \mid d_2$ és $d_2 \mid d_1$, melyből az 1.5. Tétel szerint $|d_1| = |d_2|$ következik, azaz $d_1 \sim d_2$. ∎

E tétel szerint, ha d az a és $b(\neq 0)$ elemek legnagyobb közös osztója, akkor $-d$ is az. A d és $-d$ közül a pozitívat (a, b)-vel szokás jelölni. Ugyanakkor az is igaz, hogy ha $a \sim a_1$ és $b \sim b_1$, akkor $(a_1, b_1) = (a, b)$. Ezért a továbbiakban, ha (a, b) legnagyobb közös osztóról beszélünk, feltételezhetjük, hogy $a \in \mathbf{N}$ és $b \in \mathbf{N} \setminus \{0\}$.

Ezek után bizonyítjuk a legnagyobb közös osztó létezését.

1.12. Tétel. *Bármely a és $b(\neq 0)$ természetes számnak van legnagyobb közös osztója, és $b \nmid a$ esetén $(a, b) = r_n$, ahol r_n az a és b egészeken végrehajtott euklideszi algoritmus utolsó zérustól különböző maradéka, míg $b \mid a$ esetén $(a, b) = b$.*

Bizonyítás. Tekintsük $b \nmid a$ esetén az

$$
\begin{aligned}
a &= bq_0 + r_1, && 0 < r_1 < |b|, \\
b &= r_1 q_1 + r_2, && 0 < r_2 < r_1, \\
r_1 &= r_2 q_2 + r_3, && 0 < r_3 < r_2, \\
&\vdots && \vdots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n, && 0 < r_n < r_{n-1}, \\
r_{n-1} &= r_n q_n + 0
\end{aligned}
\tag{1.10}
$$

algoritmust. (1.10) soraival visszafelé haladva látható, hogy

$$r_n \mid r_{n-1},\ r_n \mid r_{n-2},\ \ldots,\ r_n \mid r_1,\ r_n \mid b \text{ és } r_n \mid a,$$

azaz r_n közös osztója az a és b egészeknek. Most tegyük fel, hogy $d' \mid a$ és $d' \mid b$. (1.10) soraival fentről lefelé haladva kapjuk, hogy

$$d' \mid r_1,\ d' \mid r_2,\ \ldots,\ d' \mid r_{n-1} \text{ és } d' \mid r_n,$$

tehát a legnagyobb közös osztó definíciója miatt valóban $(a,b) = r_n$. Ugyanakkor $b \mid a$ esetén $(a,b) = b$ nyilvánvaló. ∎

Érdemes külön kiemelni, hogy az 1.2. Tétel és a most bebizonyított 1.12. Tétel szerint végtelen sok X_n, Y_n egész létezik, amelyre

$$aX_n + bY_n = (a,b),$$

azaz (a,b) előállítható az a és b egészek lineáris kombinációjaként.

A továbbiakban a legnagyobb közös osztó tulajdonságaival foglalkozunk.

1.13. Tétel. *Bármely $a, b(\neq 0), c$ természetes számra igazak az alábbiak:*

(a) $(a,b) = (b,a)$;

(b) $((a,b),c) = (a,(b,c))$;

(c) $(b,b) = b$;

(d) $(a,b)c = (ac,bc)$, *ha* $c \neq 0$;

(e) $(a,b) = b$ *akkor és csak akkor, ha* $b \mid a$;

(f) $(a,b) = (a+kb,b)$, *ahol* $k \in \mathbf{Z}$.

Bizonyítás. Az (a), (b) és (c) állítások a legnagyobb közös osztó definíciója alapján könnyen bizonyíthatók. A (d) rész bizonyításához tekintsük (1.10)-et, melynek minden sorát c-vel szorozva az alábbiakat kapjuk:

$$\begin{aligned} ac &= bcq_0 + cr_1, \quad 0 < cr_1 < cb, \\ bc &= cr_1q_1 + cr_2, \quad 0 < cr_2 < cr_1, \\ &\vdots \\ cr_{n-1} &= cr_nq_n. \end{aligned} \tag{1.11}$$

De (1.11) azonos az ac és bc elemeken végrehajtott algoritmussal, ezért az 1.12. Tétel szerint

$$(ac,bc) = cr_n = c(a,b).$$

Az (e) állítás nyilvánvaló, ezért nem igényel részletes bizonyítást. Az (f) rész igazolása szintén (1.10) segítségével történhet. Mivel (1.10) első sorából

$$a + kb = b(q_0 + k) + r_1, \quad 0 < r_1 < b$$

adódik, ezért az $a + kb$ és b egészeken végrehajtott euklideszi algoritmus utolsó zérustól különböző maradéka azonos az (1.10)-beli r_n-nel, azaz

$$(a+kb,b) = r_n = (a,b). \ ∎$$

Az előbbi tétel (b) állítása lehetőséget ad véges sok egész szám legnagyobb közös osztójának alábbi rekurzív definíciójára.

DEFINÍCIÓ. Az $a_1, a_2, \ldots, a_n$ egész számok $(a_1, a_2, \ldots, a_n)$-nel jelölt legnagyobb közös osztója alatt értjük $n \geq 3$ esetén az

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

pozitív egész számot.

E definíció alapján n egész szám legnagyobb közös osztójának meghatározása visszavezethető két egész szám legnagyobb közös osztója meghatározására alkalmas algoritmus $n-1$-szer való elvégzésére. Igaz az alábbi tétel is.

1.14. TÉTEL. *Az $a_1, a_2, \ldots, a_n$ egészek legnagyobb közös osztója kifejezhető az $a_1, a_2, \ldots, a_n$ egészek lineáris kombinációjaként, azaz léteznek olyan $x_1, x_2, \ldots, x_n$ egészek, amelyekkel*

$$(a_1, a_2, \ldots, a_n) = a_1x_1 + a_2x_2 + \cdots + a_nx_n.$$

BIZONYÍTÁS. Az $(a_1, a_2, \ldots, a_n)$ definíciója alapján, n szerinti teljes indukcióval könnyen elvégezhető a bizonyítás, ezért részletezésétől eltekintünk. ∎

Példaként állítsuk elő 40, 24 és 5 legnagyobb közös osztóját 40, 24 és 5 lineáris kombinációjaként:

$$\begin{aligned} 40 &= 24 \cdot 1 + 16, & 16 &= 40 - 24, \\ 24 &= 16 \cdot 1 + 8, & 8 &= 24 - 16. \\ 16 &= 8 \cdot 2 + 0, \end{aligned}$$

Ez alapján

$$(40, 24) = 8 = 40(-1 + 24k) + 24(2 - 40k), \quad k \in \mathbf{Z}.$$

Mivel $(40, 24, 5) = \big((40, 24), 5\big) = (8, 5)$, ezért meghatározzuk $(8, 5)$ lineáris kombinációs előállítását:

$$\begin{aligned} 8 &= 5 \cdot 1 + 3, & 3 &= 8 - 5, \\ 5 &= 3 \cdot 1 + 2, & 2 &= 5 - 3, & 2 &= -8 + 5 \cdot 2, \\ 3 &= 2 \cdot 1 + 1, & 1 &= 3 - 2, & 1 &= 8 - 5 + 8 - 5 \cdot 2 = 8 \cdot 2 + 5 \cdot (-3). \\ 2 &= 1 \cdot 2 + 0, \end{aligned}$$

Így

$$(8,5) = 1 = 8(2+5t) + 5(-3-8t), \quad t \in \mathbf{Z}.$$

Tehát $(40,24,5) = 1 = 40(-1+24k)(2+5t)+24(2-40k)(2+5t)+5(-3-8t)$, $k, t \in \mathbf{Z}$.

Foglalkozzunk most azzal az esettel, amikor $(a_1, a_2, \ldots, a_n) = 1$.

Definíció. Ha $(a_1, a_2, \ldots, a_n) = 1$ $(n \geq 2)$, akkor az $a_1, a_2, \ldots, a_n$ egészeket relatív prímeknek nevezzük. Ha $(a_i, a_j) = 1$ bármely $1 \leq i < j \leq n$ esetén, akkor páronként relatív prím egészekről beszélünk.

Nyilvánvaló, hogy páronként relatív prím egészek relatív prímek is, de ennek fordítottja nem feltétlenül igaz.

Relatív prím számpár előállításáról szól a következő tétel.

1.15. Tétel. *Bármely* $a, b(\neq 0)$ *természetes számra*

$$\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1.$$

Bizonyítás. Az 1.13. Tétel (d) állítása szerint

$$\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right)(a,b) = (a,b)\,,$$

ahonnan

$$(a,b)\left(\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) - 1\right) = 0.$$

Mivel $(a,b) \geq 1$, ezért igaz a tétel állítása. ∎

1.16. Tétel. *Legyen* $a(\neq 0), b, c \in \mathbf{N}$. $(a,b) = 1$ *és* $(a,c) = 1$ *akkor és csak akkor teljesül, ha* $(a,bc) = 1$.

Bizonyítás. Az 1.13. Tételt alkalmazva kapjuk, hogy ha $(a,b) = 1$ és $(a,c) = 1$, akkor

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

Másrészt ha $(a,bc) = 1$ és például $(a,b) = d > 1$, akkor $a = a_1 d$ és $b = b_1 d$ $(a_1(\neq 0), b_1 \in \mathbf{N})$ miatt

$$(a,bc) = (a_1 d, b_1 dc) = d(a_1, b_1 c) \geq d > 1,$$

amely ellentmond $(a, bc) = 1$-nek. ∎

A következő tétel *általánosított prímtulajdonság* néven ismert.

1.17. Tétel. *Legyen* $a\ (\neq 0)$, $b, c \in \mathbf{N}$. *Ha* $a \mid bc$ *és* $(a, b) = 1$, *akkor* $a \mid c$.

Bizonyítás. Itt is az 1.13. Tétel állításait alkalmazva kapjuk, hogy

$$(a, c) = (a, (a, b)c) = (a, (ac, bc)) = ((a, ac), bc) = (a, bc) = a,$$

mivel a feltétel szerint $(a, b) = 1$ és $a \mid bc$. Ugyanakkor a kapott egyenlőség szerint $(a, c) = a$, azaz $a \mid c$. ∎

1.18. Tétel. *Legyen* $a(\neq 0), b, c \in \mathbf{N}$. *Ha* $a \mid b$, $c \mid b$ *és* $(a, c) = 1$, *akkor* $ac \mid b$.

Bizonyítás. Az 1.13. Tétel és a feltételeink szerint

$$\begin{aligned}(ac, b) = (ac, b(a, c)) = (ac, (ba, bc)) = ((ac, ba), bc) = \\ = (a(c, b), bc) = (ac, bc) = (a, b)c = ac,\end{aligned}$$

amely ekvivalens $ac \mid b$-vel. ∎

Legkisebb közös többszörös

A legkisebb közös többszörös definícióját a legnagyobb közös osztó definíciójához hasonlóan adjuk meg.

Definíció. Legyen $a, b \in \mathbf{Z} \setminus \{0\}$. Az a és a b legkisebb közös többszörösének nevezünk egy m egész számot, ha

(a) m közös többszörös, azaz $a \mid m$ és $b \mid m$;

(b) m „legkisebb” abban az értelemben, hogy a és b bármely m' közös többszörösének osztója, azaz, ha $a \mid m'$ és $b \mid m'$, akkor $m \mid m'$.

Elsőként vizsgáljuk az egyértelműség kérdését.

1.19. Tétel. *Ha az* $a, b \in \mathbf{Z} \setminus \{0\}$ *egészeknek létezik legkisebb közös többszöröse, akkor az asszociáltság erejéig egyértelműen meghatározott.*

Bizonyítás. Tegyük fel, hogy m_1 és m_2 legkisebb közös többszöröse az a és b egészeknek. Ekkor a definíció alapján $m_1 \mid m_2$ és $m_2 \mid m_1$ is teljesül, amelyből az 1.5. Tétel alapján $|m_1| = |m_2|$, azaz $m_1 \sim m_2$. ∎

A most bizonyított tétel szerint, ha m legkisebb közös többszöröse az a és b egészeknek, akkor $-m$ is az. E kettő közül a pozitívat $[a, b]$-vel jelöljük.

Ugyanakkor az is igaz, hogy ha $a_1 \sim a$ és $b_1 \sim b$, akkor $[a_1, b_1] = [a, b]$. Ezért a továbbiakban $[a, b]$ esetén feltételezzük, hogy $a, b \in \mathbf{N} \setminus \{0\}$.

Ezek után bizonyítjuk a legkisebb közös többszörös létezését.

1.20. Tétel. *Bármely a, b pozitív egész számnak van legkisebb közös többszöröse, és*

$$[a, b] = \frac{ab}{(a, b)}.$$

Bizonyítás. Mivel (a, b) létezését már bizonyítottuk (1.12. Tétel) és

$$a \mid a\frac{b}{(a, b)}, \quad \text{illetve} \quad b \mid b\frac{a}{(a, b)},$$

ezért az $\frac{ab}{(a,b)}$ valóban közös többszöröse a-nak és b-nek. Legyen m' az a és b egy tetszőleges közös többszöröse, azaz

$$ac = m' \quad \text{és} \quad bd = m' \tag{1.12}$$

valamely $c, d \in \mathbf{N}$-re. (1.12)-ből az $ac = bd$ következik, amelyből (a, b)-vel való osztás után az

$$\frac{a}{(a, b)}c = \frac{b}{(a, b)}d \tag{1.13}$$

egyenlőséget kapjuk. (1.13)-ból látható, hogy

$$\frac{a}{(a, b)} \;\Big|\; \frac{b}{(a, b)}d \quad \text{és} \quad \frac{b}{(a, b)} \;\Big|\; \frac{a}{(a, b)}c,$$

de az 1.15 tétel következtében $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$, és így az 1.17. Tétel miatt

$$\frac{a}{(a, b)} \;\Big|\; d \quad \text{és} \quad \frac{b}{(a, b)} \;\Big|\; c,$$

ezért

$$\frac{a}{(a, b)}f = d \quad \text{és} \quad \frac{b}{(a, b)}h = c \tag{1.14}$$

valamely $f, h \in \mathbf{N}$-re. (1.14)-et (1.12)-be helyettesítve kapjuk, hogy

$$\frac{ab}{(a, b)} \;\Big|\; m',$$

azaz $\frac{ab}{(a,b)}$ kielégíti a legkisebb közös többszörös definícióját. ∎

Megemlítjük, hogy a tétel bizonyításából $(a,b) = 1$ esetén $[a,b] = ab$ következik.

A továbbiakban a legkisebb közös többszörös tulajdonságaival foglalkozunk.

1.21. Tétel. *Bármely a, b, c pozitív egészekre igazak az alábbi tulajdonságok:*

(a) $[a,b] = [b,a]$;

(b) $[[a,b],c] = [a,[b,c]]$;

(c) $[a,a] = a$;

(d) $[a,b]c = [ac,bc]$;

(e) $[a,b] = b$ *akkor és csak akkor, ha* $a \mid b$.

Bizonyítás. A (b) pont kivételével valamennyi állítás könnyen bizonyítható az előző, illetve a legnagyobb közös osztó tulajdonságait taglaló 1.13. Tétel alkalmazásával. Például a (d) bizonyítását részletezve:

$$[a,b]c = \frac{ab}{(a,b)}c = \frac{abc^2}{(a,b)c} = \frac{acbc}{(ac,bc)} = [ac,bc].$$

A (b) állítás a következőképpen bizonyítható. Legyen $[[a,b],c] = m_1$ és $[a,[b,c]] = m_2$. Ekkor a legkisebb közös többszörös definíciója alapján $[a,b] \mid m_1$ és $c \mid m_1$, amiből viszont $a \mid m_1$, $b \mid m_1$ és $c \mid m_1$ következik. Ezért, szintén a definíció miatt $[b,c] \mid m_1$ és $a \mid m_1$, így $[a,[b,c]] = m_2$ osztója m_1-nek. Hasonlóan látható be, hogy $m_1 \mid m_2$, viszont $m_2 \mid m_1$ és $m_1 \mid m_2$-ből $m_1 = m_2$ következik. ∎

Az 1.21. Tétel (b) állítása alapján véges sok egész szám legkisebb közös többszöröse definícióját az alábbi rekurzív módon adhatjuk meg.

Definíció. Az $a_1, a_2, \ldots, a_n$ nemzérus egész számok $[a_1, a_2, \ldots, a_n]$-nel jelölt legkisebb közös többszörösén értjük $n \geq 3$ esetben az

$$[a_1, a_2, \ldots, a_n] = \big[[a_1, a_2, \ldots, a_{n-1}], a_n\big]$$

pozitív egész számot.

Felhívjuk az olvasó figyelmét arra, hogy általában

$$[a_1, a_2, \ldots, a_n] \neq \frac{a_1 a_2 \cdots a_n}{(a_1, a_2, \ldots, a_n)} \quad (n \geq 3),$$

ugyanakkor bizonyítható, hogy

$$[a_1, a_2, \ldots, a_n] = \frac{a_1 a_2 \cdots a_n}{(a_2 a_3 \cdots a_n, a_1 a_3 \cdots a_n, \ldots, a_1 a_2 \cdots a_{n-1})}$$

igaz minden $n \geq 2$ esetén.

Irreducibilis és prímszámok, a számelmélet alaptétele

A számelméletben alapvető szerepet játszó fogalmakat fogunk definiálni.

Definíció. A 0-tól és ± 1-től különböző p egész számot irreducibilisnek (vagy felbonthatatlannak) nevezzük, ha nincs valódi osztója, azaz ha $a \in \mathbf{Z}$ és $a \mid p$, akkor vagy $a = \pm 1$, vagy $a = \pm p$. Ellenkező esetben p-t reducibilisnek (vagy összetettnek) nevezzük.

Definíció. A 0-tól és ± 1-től különböző p egész számot prímnek nevezzük, ha az valahányszor osztója egy szorzatnak, mindannyiszor osztója a szorzat legalább egyik tényezőjének, azaz ha $a, b \in \mathbf{Z}$, $p \mid ab$, de $p \nmid a$, akkor $p \mid b$.

Külön felhívjuk az olvasó figyelmét arra, hogy definícióink szerint a 0 és a ± 1 egész számok se nem irreducibilisek, se nem reducibilisek és nem is prímek.

Mélyebb számelméleti tanulmányokat folytatva könnyen adható példa olyan integritástartományra, ahol az irreducibilis és prím fogalmak nem fedik egymást, de az általunk vizsgált $(\mathbf{Z}, +, \cdot)$-ban bizonyítható a következő tétel.

1.22. Tétel. *A $(\mathbf{Z}, +, \cdot)$ integritástartományban az irreducibilis egészek és a prímek egybeesnek, azaz a p egész szám akkor és csakis akkor irreducibilis, ha prím.*

Bizonyítás. Legyen p irreducibilis egész és tegyük fel, hogy $p \mid ab$ de $p \nmid a$. Megmutatjuk, hogy akkor $p \mid b$, azaz p prím. Mivel p irreducibilis és $p \nmid a$, ezért $(a, p) = 1$. Így azt kaptuk, hogy

$$p \mid ab \quad \text{és} \quad (a, p) = 1,$$

amelyből az általánosított prímtulajdonság (1.17. Tétel) szerint $p \mid b$ következik.

Legyen most p prím és tegyük fel indirekt módon, hogy p nem irreducibilis, azaz, $p = ab$, jóllehet sem a, sem b nem ± 1. Mivel p prím, ezért $p \mid a$ vagy $p \mid b$. Feltehető, hogy például $p \mid a$. Ugyanakkor $p = ab$ miatt $a \mid p$ is igaz, és ezért $p \sim a$, tehát b mégis vagy 1, vagy -1. Az ellentmondásból p irreducibilis volta következik. ∎

E tétel alapján az irreducibilis és prím fogalmak minden tekintetben egyenértékűek, azaz, szinonimákként használhatók a $(\mathbf{Z}, +, \cdot)$ integritástartományban.

A következő tételt szokás a számelmélet alaptételének, illetve az egyértelmű irreducibilis faktorizáció tételének is nevezni.

1.23. Tétel. *Bármely 0-tól és ±1-től különböző egész szám véges sok irreducibilis (prím) szám szorzatára bontható és ez a felbontás a tényezők sorrendjétől és egységtényezőktől (előjelektől) eltekintve egyértelmű. (Jelen esetben az egytényezős szorzat is megengedett, és az magát az egész számot jelenti.)*

Ha az egységtényezőket figyelmen kívül hagyjuk, akkor a számelmélet alaptételét az alábbi módon is megfogalmazhatjuk.

1.24. Tétel. *Miden $n \geq 2$ természetes szám sorrendtől eltekintve egyértelműen állítható elő véges sok prímszám szorzataként, ahol prímszámokon a pozitív prímeket értjük és az egytényezős szorzat is megengedett.*

A számelmélet alaptételének fenti két megfogalmazása közül nyilvánvalóan elengedő az egyiket bizonyítani. Mi az 1.24. Tételt bizonyítjuk.

Bizonyítás. Először teljes indukcióval bizonyítjuk, hogy a kívánt szorzatelőállítás létezik. Mivel $n = 2$ prímszám, ezért a tétel igaz $n = 2$-re. Tegyük fel, hogy minden k természetes szám felbontható véges sok prímszám szorzatára, ha $2 \leq k \leq n-1$. Ha n prímszám, akkor az (egytényezős) szorzatelőállítása adott. Ha n összetett, akkor léteznek olyan n_1 és n_2 természetes számok, amelyekre $n = n_1 n_2$, $2 \leq n_1 < n$ és $2 \leq n_2 < n$. De indukciós feltevésünk szerint n_1 és n_2 is előállítható véges sok prímszám szorzataként, s ezért igaz az állítás $n = n_1 n_2$-re, illetve tetszőleges $n \geq 2$ természetes számra.

A felbontás egyértelműségét indirekt módon igazoljuk. Tegyük fel, hogy létezik olyan $n \geq 2$ természetes szám, melynek két különböző prímtényezős felbontása van, azaz

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_t, \tag{1.15}$$

ahol feltehető, hogy $k \leq t$. Mivel p_1 prímszám és $p_1 \mid q_1 q_2 \cdots q_t$, ezért $p_1 \mid q_j$ valamely $1 \leq j \leq t$-re. Feltehetjük, hogy $j = 1$, azaz, $p_1 \mid q_1$. De a q_1

prímszám irreducibilis voltából következik, hogy $p_1 = q_1$. Így (1.15)-ből a

$$p_2 p_3 \cdots p_k = q_2 q_3 \cdots q_t \tag{1.16}$$

egyenlőséget kapjuk. Hasonlóan érvelve kapjuk, hogy $p_2 = q_2$, $p_3 = q_3, \ldots,$ $p_k = q_k$. (1.16)-ból így az

$$1 = q_{k+1} q_{k+2} \cdots q_t$$

egyenlőséget nyerjük, amely ellentmondás ha $k < t$. Ezért $k = t$, és így (1.15)-ben a ,,két" prímtényezős felbontás azonos. ∎

Ha $n > 1$ és az $n = p_1 p_2 \cdots p_k$ prímtényezős felbontásban az azonos prímtényezőket egy hatványba foglaljuk össze, akkor az n természetes szám

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \tag{1.17}$$

alakban is írható, ahol $p_1, p_2, \ldots, p_r$ különböző prímszámok és $\alpha_1, \alpha_2, \ldots \alpha_r$ pozitív egész számok. Az n szám (1.17)-beli alakát szokás n kanonikus alakjának is nevezni. Néha, praktikussági okokból olyan prímszámokat is szerepeltetünk az n prímtényezős felbontásában, amelyek ténylegesen nem osztói n-nek. Ekkor az n természetes szám (1.17)-beli alakjában $\alpha_i \geq 0$.

Nyilvánvaló, hogy ha $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ $(\alpha_i \geq 0)$ alakban írható és $d \mid n$, illetve $n \mid m$, akkor a d és m természetes számok prímtényezős felbontása

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r} \quad \text{és} \quad m = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_t^{\gamma_t}$$

alakú, ahol $0 \leq \beta_i \leq \alpha_i$, illetve $0 \leq \alpha_i \leq \gamma_i$ $(i = 1, 2, \ldots, r)$, továbbá $t \geq r$ és $\gamma_j \geq 0$ ha $j > r$. Ha az n és m természetes szám

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \quad \text{és} \quad m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r} \quad (\alpha_i \geq 0,\ \beta_i \geq 0)$$

prímtényezős alakkal rendelkezik, akkor — mint könnyen igazolható —

$$(n, m) = p_1^{\min\{\alpha_1, \beta_1\}} p_2^{\min\{\alpha_2, \beta_2\}} \cdots p_r^{\min\{\alpha_r, \beta_r\}},$$
$$[n, m] = p_1^{\max\{\alpha_1, \beta_1\}} p_2^{\max\{\alpha_2, \beta_2\}} \cdots p_r^{\max\{\alpha_r, \beta_r\}}.$$

A későbbiek szempontjából fontos a következő két tétel.

1.25. Tétel. *Legyen $m, n, d \in \mathbf{N} \setminus \{0\}$. Ha $(m, n) = 1$ és $d \mid mn$, akkor léteznek olyan d_1, d_2 pozitív egészek, amelyekre $d_1 \mid m$, $d_2 \mid n$, $d = d_1 d_2$ és $(d_1, d_2) = 1$.*

Bizonyítás. Legyen m és n prímtényezős alakja

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \quad \text{és} \quad n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_t^{\beta_t},$$

ahol $\alpha_i \geq 0, \beta_i \geq 0$ és $q_j \neq p_i$ egyetlen i és j indexre sem, mert $(m, n) = 1$. Mivel $d \mid mn$, ezért az előzőek alapján

$$d = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_r^{\gamma_r} q_1^{\delta_1} q_2^{\delta_2} \cdots q_t^{\delta_t},$$

ahol $0 \leq \gamma_i \leq \alpha_i$ és $0 \leq \delta_j \leq \beta_j$ $(1 \leq i \leq r,\ 1 \leq j \leq t)$. Legyen

$$d_1 = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_r^{\gamma_r} \quad \text{és} \quad d_2 = q_1^{\delta_1} q_2^{\delta_2} \cdots q_t^{\delta_t},$$

így $d = d_1 d_2,\ d_1 \mid m,\ d_2 \mid n$ és nyilván $(d_1, d_2) = 1$. ∎

1.26. Tétel. *Legyen $k \in \mathbf{N} \setminus \{0\}$. Ha $m = n^k = m_1 m_2$ és $(m_1, m_2) = 1$, akkor léteznek olyan n_1 és n_2 természetes számok, amelyekre $m_1 = n_1^k$ és $m_2 = n_2^k$.*

Bizonyítás. Legyen n prímtényezős alakja

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r},$$

ahol $\alpha_i \geq 0$, $p_i \neq p_j$, ha $i \neq j$, és így

$$m = n^k = p_1^{k\alpha_1} p_2^{k\alpha_2} \cdots p_r^{k\alpha_r}.$$

Mivel $(m_1, m_2) = 1$ és $m_1 m_2 = m$, ezért feltehető, hogy

$$m_1 = p_1^{k\alpha_1} p_2^{k\alpha_2} \cdots p_t^{k\alpha_t} \quad \text{és} \quad m_2 = p_{t+1}^{k\alpha_{t+1}} p_{t+2}^{k\alpha_{t+2}} \cdots p_r^{k\alpha_r},$$

amelyből

$$n_1 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t} \quad \text{és} \quad n_2 = p_{t+1}^{\alpha_{t+1}} p_{t+2}^{\alpha_{t+2}} \cdots p_r^{\alpha_r}$$

jelöléssel $m_1 = n_1^k$ és $m_2 = n_2^k$ adódik. ∎

Jóllehet külön fejezetben (7.) foglalkozunk a prímszámok elméletével, mégis célszerű néhány alapvető tényre már itt is kitérni.

Elsőként vizsgáljuk meg, hogyan dönthető el egy $n \geq 2$ egész számról, hogy prímszám-e, vagy összetett, illetve hogyan határozhatók meg az n-nél nem nagyobb prímszámok.

1.27. Tétel. *Ha az $n \geq 2$ természetes számnak nincs $\sqrt{n}$-nél nem nagyobb prímszám osztója, akkor n prímszám, azaz, minden összetett természetes számnak van négyzetgyökénél nem nagyobb prímosztója.*

Bizonyítás. Legyen n egy összetett szám és legyen p a legkisebb prímosztója. Ekkor $n = pm$, ahol $m \geq p$. Ezért $n \geq p^2$ és $p \leq \sqrt{n}$, tehát a legkisebb prímosztó valóban legfeljebb $\sqrt{n}$. ∎

Az adott $n \geq 2$ természetes számnál nem nagyobb prímszámok meghatározására szolgál az úgynevezett eratoszthéneszi szita módszere. Ehhez növekvő sorrendben felírjuk 2-től n-ig a természetes számokat, majd bekeretezzük a 2-t és kihúzzuk 2 minden többszörösét. Ezután bekeretezzük a legkisebb nem kihúzottat (jelen esetben a 3-at) és kihúzzuk ennek minden többszörösét. A bekeretezést legfeljebb $\sqrt{n}$-ig folytatva és a többszörösöket mindig kihúzva, az 1.27. Tétel szerint pontosan az n-nél nem nagyobb prímek lesznek bekeretezve, illetve nem kihúzva. Az elmondottakat az alábbi táblázattal mutatjuk be $n = 30$ esetén:

	$\boxed{2}$	$\boxed{3}$	$\not{4}$	$\boxed{5}$	$\not{6}$	7	$\not{8}$	$\not{9}$	$\not{10}$
11	$\not{12}$	13	$\not{14}$	$\not{15}$	$\not{16}$	17	$\not{18}$	19	$\not{20}$
$\not{21}$	$\not{22}$	23	$\not{24}$	$\not{25}$	$\not{26}$	$\not{27}$	$\not{28}$	29	$\not{30}$

Természetesen, nagy n-re a fenti szita módszer meglehetősen nehézkes.

Ezt a fejezetet a következő tétellel zárjuk.

1.28. Tétel. *Végtelen sok prímszám van.*

Bizonyítás. Erre a tételre számos bizonyítás ismert a számelméletben (lásd 7. fejezet). Ezek közül a legismertebb az alábbi, Euklidésztől származó indirekt bizonyítás. Tegyük fel, hogy véges sok prímszám létezik és ezek $p_1, p_2, \ldots, p_n$ $(n \geq 1)$. Tekintsük az

$$m = p_1 p_2 \cdots p_n + 1$$

természetes számot. Nyilvánvaló, hogy $m > 1$ és $p_i \nmid m$ $(i = 1, 2, \ldots, n)$. Így az $m > 1$ természetes számnak nincs prímosztója, amely ellentmond a számelmélet alaptételének (1.24. Tétel). Mivel az indirekt feltevés ellentmondáshoz vezetett, ezért igaz a tétel állítása. ∎

Feladatok

1. Végezzük el az összes lehetséges euklideszi osztást az a és b egészeken, ha $a = \pm 83$ és $b = \pm 19$.

2. Hajtsuk végre az euklideszi algoritmust az a és b egészeken, majd az utolsó zérustól különböző maradékot állítsuk elő a és b lineáris kombinációjaként, ha $a = 68$ és $b = 42$.

3. Bizonyítsuk be, hogy

$$1947 \mid (46^n + 296 \cdot 13^n),$$

ahol n páratlan természetes szám.

4. Igazoljuk, hogy

$$80 \mid abc(a^2 - b^2)(b^2 - c^2)(c^2 - a^2),$$

ahol a, b és c egész számok.

5. Bizonyítsuk be, hogy $2^8 \mid (n^{1984} - 1)$, ha n páratlan természetes szám.

6. Bizonyítsuk be, hogy $81 \mid (10^n(9n - 1) + 1)$, ha $n \in \mathbf{N}$.

7. Bizonyítsuk be, hogy

$$19 \mid (2^{2^{6n+2}} + 3),$$

ahol $n \in \mathbf{N}$.

8. Legyen $a = 52$, $b = 182$ és $c = 1352$. Fejezzük ki a, b és c egészek legnagyobb közös osztóját a, b és c lineáris kombinációjaként.

9. Legyen $n \in \mathbf{N}$. Bizonyítsuk be, hogy $(n! + 1, (n + 1)! + 1) = 1$.

10. Legyen $m, n \in \mathbf{N}$ és m páratlan. Igazoljuk, hogy

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

11. Legyen a, b és $c \in \mathbf{N} \setminus \{0\}$. Bizonyítsuk be, hogy

$$[a, b, c] = \frac{abc}{(ab, ac, bc)}.$$

12. Bizonyítsuk be, hogy $\sum_{n=2}^{k} \frac{1}{n}$ soha sem egész szám.

13. Bizonyítsuk be, hogy $\sum_{n=1}^{k} \frac{1}{2n+1}$ soha sem egész szám.

14. Legyen $n \geq 2$ természetes szám. Igazoljuk, hogy

$$n! = \prod_{2 \leq p \leq n} p^{\sum_{i=1}^{\infty} \left[\frac{n}{p^i} \right]},$$

ahol p prímszám, és $[x]$ az x egész részét jelöli.

15. Osztható-e 7-tel az $\binom{1000}{500}$ binomiális együttható?

16. Melyek azok az n természetes számok, amelyek esetén $n!$-nak a 10-es számrendszerbeli alakja legalább 200, és maximum 210 darab nullára végződik.

17. Legyen p prímszám. Bizonyítsuk be, hogy minden k-ra $(0 < k < p)$ $p \mid \binom{p}{k}$.

18. Legyen $p > 3$ prímszám. Igazoljuk, hogy minden k-ra $(1 < k < < p - 1)$

$$p \left| \left(\binom{p-1}{k-1} - \binom{p-1}{k+1} \right) \right. .$$

19. Legyen $m \in \mathbf{N} \setminus \{0\}$, $n = 2^m$. Bizonyítsuk be, hogy $\binom{n}{k}$ páros minden k egészre, ha $(1 \leq k \leq n-1)$.

20. Legyen $a_i \in \mathbf{N}$ $(i = 1, 2, \ldots, n)$. Bizonyítsuk be, hogy

$$\frac{\left(\sum_{i=1}^{n} a_i \right)!}{\prod_{i=1}^{n} (a_i!)} \in \mathbf{N}.$$

21. Legyen $a, b \in \mathbf{N}$. Igazoljuk, hogy

$$\frac{(ab)!}{a!(b!)^a} \in \mathbf{N}.$$

2. Test fölötti polinomgyűrűk, euklideszi gyűrűk

Az előző fejezetben áttekintettük a $(\mathbf{Z}, +, \cdot)$ integritástartományban definiált elemi számelméleti fogalmakat és az alapvető tételeket. Most egy újabb integritástartományban, az úgynevezett test fölötti polinomgyűrűk körében értelmezzük az első fejezetbeli számelméleti fogalmak polinomokra vonatkozó megfelelőit.

Definíció. Legyen $(\mathbf{T}, +, \cdot)$ egy (kommutatív) test. A $\mathbf{T}$ test fölötti egyhatározatlanú polinomon értjük és $f(x)$-szel jelöljük az

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \tag{2.1}$$

formális összeget, ahol $a_i \in \mathbf{T}$ $(i = 0, 1, 2, \ldots, n)$ és x pedig egy határozatlan.

A definícióban szereplő „határozatlan" elnevezés arra utal, hogy az x nem változó, azaz nem futja be egy adott halmaz elemeit. Ellenkező esetben $f(x)$-et az adott halmazon értelmezett polinomfüggvénynek nevezzük. Az x határozatlant célszerű olyan szimbólumnak tekinteni, amelynek képezhetjük a nemnegatív egész kitevőjű hatványait és ezen hatványoknak $\mathbf{T}$-beli elemekkel való szorzatát.

Definíció. A (2.1)-beli $f(x)$ polinom f°-rel jelölt valódi fokszáma n, ha $a_n \neq 0$. Ha $a_n = 0$, akkor n az $f(x)$ formális fokszáma. Szokás az a_n-et $f(x)$ főegyütthatójának, míg $a_n = 1$ esetben $f(x)$-et főpolinomnak nevezni.

Ebből a definícióból következik, hogy a $\mathbf{T}$ test zérustól különböző elemeinek $(f(x) = a_0 \neq 0)$ valódi fokszáma nulla, míg a $\mathbf{T}$ test zéruselemének — az $f(x) = a_0 = 0$ zéruspolinomnak — nincs valódi fokszáma. E „hiányosságot" könnyen megszüntethetjük a következő módon.

Definíció. A (2.1)-beli $f(x)$ polinom $f^{\circ\circ}$-rel jelölt módosított fokszámán értjük az

$$f^{\circ\circ} = \begin{cases} 2^{f^\circ}, & \text{ha } f(x) \text{ nem a zéruspolinom,} \\ 0, & \text{ha } f(x) \text{ a zéruspolinom} \end{cases}$$

természetes számot.

A valódi, illetve a módosított fokszámok definíciójából nyilvánvaló, hogy $f^\circ = g^\circ$ akkor és csak akkor, ha $1 \leq f^{\circ\circ} = g^{\circ\circ}$, illetve $f(x) = 0$ akkor és csak akkor, ha $f^{\circ\circ} = 0$. Így például a $\mathbf{Q}$ fölötti

$$f(x) = 0x^5 + 3x^4 + 2x^3 - x^2 - 6$$

polinom esetén a formális fokszám 5, a valódi fokszám $f^\circ = 4$ és a módosított fokszám $f^{\circ\circ} = 2^4$.

A továbbiakban bevezetjük a

$$\mathbf{T}[x] = \{h(x) \colon h(x) \text{ a } \mathbf{T} \text{ test fölötti polinom}\}$$

jelölést. Legyen $f(x)$, $g(x) \in \mathbf{T}[x]$,

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \\ g(x) &= b_n x^n + b_{n-1}x^{n-1} + \cdots + b_m x^m + \cdots b_1 x + b_0, \end{aligned} \tag{2.2}$$

ahol $b_n = b_{n-1} = \cdots = b_{m+1} = 0$, mivel feltehető, hogy $n \geq m$.

Definíció. A (2.2)-beli $f(x)$ és $g(x)$ polinomokat egyenlőnek nevezzük, ha minden $0 \leq i \leq n$ esetén $a_i = b_i$, azaz, ha a ,,megfelelő" együtthatók rendre egyenlők.

2.1. Tétel. *A $(\mathbf{T}[x], +, \cdot)$ struktúra integritástartomány, ahol az összeadás és szorzás műveletek az alábbi módon vannak értelmezve:*

$$\begin{aligned} f(x) + g(x) &= (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_0 + b_0), \\ f(x)g(x) &= (a_n b_m)x^{n+m} + (a_n b_{m-1} + a_{n-1} b_m)x^{n+m-1} + \cdots + (a_0 b_0). \end{aligned} \tag{2.3}$$

Bizonyítás. (2.3)-ból látható, hogy az összeg- és a szorzatpolinomok együtthatói továbbra is $\mathbf{T}$ elemei, ezért $(\mathbf{T}[x], +, \cdot)$ valóban algebrai struktúra. A műveleti tulajdonságok ellenőrzésével igazolhatók, hogy $(\mathbf{T}[x], +, \cdot)$ gyűrű. Ugyancsak könnyen belátható, hogy $(\mathbf{T}[x], \cdot)$-ban a szorzás kommutatív, az $f(x) = a_0 = 1$ polinom az egységelem és az $f(x) = a_0 = 0$ zéruspolinom a zéruselem, ahol 1, illetve 0 a $(\mathbf{T}, \cdot)$ struktúra egység-, illetve zéruseleme. Ha pedig sem $f(x)$, sem $g(x)$ nem a zéruspolinom, akkor feltehető, hogy $a_n \neq 0$ és $b_m \neq 0$. Mivel $(\mathbf{T}, +, \cdot)$ test, így $a_n b_m \neq 0$, azaz — (2.3) szerint — az $f(x)g(x)$ polinom nem lehet a zéruspolinom. Ezzel beláttuk, hogy $(\mathbf{T}[x], +, \cdot)$ valóban integritástartomány. ∎

E tétel kapcsán megjegyezzük, hogy a bizonyításban a $\mathbf{T}$ testnek csak azon tulajdonságait használtuk, amelyek már a $(\mathbf{T}, +, \cdot)$ integritástartományban is megtalálhatók, ugyanis sehol sem kellett nemzérus $\mathbf{T}$-beli elemmel osztani. Ezért az előző tétel akkor is igaz marad, ha $\mathbf{T}[x]$ helyett egy tetszőleges $(\mathbf{I}, +, \cdot)$ integritástartomány fölötti polinomok $\mathbf{I}[x]$ halmaza szerepel. Mivel tudjuk, hogy $(\mathbf{Z}, +, \cdot)$ integritástartomány, ezért a fentiek alapján igaz az alábbi tétel.

2.2. Tétel. *A $(\mathbf{Z}[x], +, \cdot)$ struktúra integritástartomány.*

Ugyancsak nyilvánvalóak az alábbi relációk is:

$$\mathbf{Z}[x] \subset \mathbf{Q}[x] \subset \mathbf{R}[x] \subset \mathbf{C}[x],$$

ahol rendre az egész, a racionális, a valós és a komplex együtthatós polinomok gyűrűi szerepelnek.

Maradékos osztás $\mathbf{T}[x]$-ben

Ha az egész számok integritástartományában kiépített számelméleti fogalmak megfelelőit a fenti polinomgyűrűkben kívánjuk megfogalmazni, akkor első lépésben felvetődik, hogy vajon bizonyítható-e ezen gyűrűkben a maradékos osztásnak megfelelő tétel. Tekintsük először a test fölötti polinomgyűrűket.

2.3. Tétel. *Bármely* $\mathbf{T}$ *test fölötti* $f(x), g(x)$ $(g(x) \neq 0)$ *polinomhoz egyértelműen léteznek olyan* $q(x)$ *és* $r(x)$ *ugyancsak* $\mathbf{T}[x]$*-beli polinomok, amelyekkel*

$$f(x) = g(x)q(x) + r(x),$$

ahol vagy $r(x) = 0$*, vagy* $r^\circ < g^\circ$*, azaz* $0 \leq r^{\circ\circ} < g^{\circ\circ}$*.*

Bizonyítás. Legyen $f(x)$ és $g(x)$ az alábbi alakú:

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$
$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0,$$

ahol $b_m \neq 0$, azaz $g^\circ = m \geq 0$.

Ha $m = 0$, akkor $g(x) = b_0 \neq 0$. Ekkor az

$$f(x) = b_0 \frac{1}{b_0} f(x) + 0$$

egyenlőség szerint igaz a tétel állítása $\left(q(x) = \frac{1}{b_0} f(x),\ r(x) = 0\right)$. A továbbiakban feltesszük, hogy $m \geq 1$. Ha $f(x) = 0$, vagy $f^\circ = n < m$, akkor az

$$f(x) = g(x)0 + f(x)$$

egyenlőség szerint szintén igaz a tétel állítása $(q(x) = 0,\ r(x) = f(x))$. Ha $f^\circ = n \geq m$, azaz $n = m + k$ $(k \in \mathbf{N})$, akkor $q(x)$ és $r(x)$ létezését k-szerinti teljes indukcióval igazoljuk.

Legyen $k = 0$, és definiáljuk az $f_1(x)$ polinomot az alábbi módon:

$$f_1(x) = f(x) - \frac{a_m}{b_m} g(x).$$

Így

$$f_1(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_0 - \frac{a_m}{b_m} \left(b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0 \right)$$

polinomban az összevonásokat elvégezve látható, hogy vagy $f_1(x) = 0$, vagy $0 \leq f_1^\circ \leq m - 1 < m = g^\circ$, azaz $0 \leq f_1^{\circ\circ} = 2^{f_1^\circ} \leq 2^{m-1} < 2^m = 2^{g^\circ} = g^{\circ\circ}$. Ebben az esetben tehát a

$$q(x) = \frac{a_m}{b_m} \text{ és } r(x) = f_1(x)$$

választással teljesül, hogy

$$f(x) = g(x)q(x) + r(x) \quad \text{és} \quad 0 \leq r^{\circ\circ} < g^{\circ\circ}.$$

Tegyük fel, hogy $k - 1 \geq 0$-ra, azaz $n \leq m + k - 1$-re már igazoltuk $q(x)$ és $r(x)$ létezését. Bebizonyítjuk, hogy ekkor $n = m + k$ esetén is léteznek a feltételeket kielégítő $q(x)$ és $r(x)$ polinomok. Legyen

$$f_2(x) = f(x) - \frac{a_{m+k}}{b_m} x^k g(x), \tag{2.4}$$

amelyből kapjuk, hogy

$$f_2(x) = a_{m+k} x^{m+k} + \cdots + a_0 - \frac{a_{m+k}}{b_m} x^k (b_m x^m + \cdots + b_0).$$

Nyilvánvaló, hogy vagy $f_2(x) = 0$, vagy $0 \leq f_2^\circ \leq m + k - 1$. Indukciós feltevésünk szerint az $f_2(x)$ polinomhoz léteznek olyan $q'(x)$ és $r'(x)$ $\mathbf{T}[x]$-beli polinomok, amelyekre

$$f_2(x) = g(x)q'(x) + r'(x) \tag{2.5}$$

és $0 \leq r'^{\circ\circ} < g^{\circ\circ}$. Így (2.4)-ből és (2.5)-ből adódik, hogy

$$f(x) = g(x) \left(\frac{a_{m+k}}{b_m} x^k + q'(x) \right) + r'(x).$$

A $q(x) = \frac{a_{m+k}}{b_m}x^k + q'(x)$ és $r(x) = r'(x)$ jelöléseket bevezetve kapjuk, hogy

$$f(x) = g(x)q(x) + r(x),$$

ahol $0 \le r^{\circ\circ} < g^{\circ\circ}$, azaz vagy $r(x) = 0$, vagy $0 \le r^{\circ} < g^{\circ}$. Ezzel a maradékos (vagy euklideszi) osztás elvégezhetőségét bebizonyítottuk.

A maradékos osztás egyértelműségét indirekt módon igazoljuk. Tegyük fel, hogy

$$\begin{aligned} f(x) &= g(x)q_1(x) + r_1(x), \quad 0 \le r_1^{\circ\circ} < g^{\circ\circ}, \\ f(x) &= g(x)q_2(x) + r_2(x), \quad 0 \le r_2^{\circ\circ} < g^{\circ\circ}, \end{aligned} \tag{2.6}$$

ahol $q_1(x), q_2(x), r_1(x), r_2(x) \in \mathbf{T}[x]$ és $q_1(x) \neq q_2(x)$. (2.6)-ból kivonással kapjuk, hogy

$$g(x)\left(q_2(x) - q_1(x)\right) = r_1(x) - r_2(x). \tag{2.7}$$

Mivel $q_2(x) - q_1(x) \neq 0$, ezért a (2.7) bal oldalán álló polinom valódi fokszáma legalább g°, így a módosított fokszáma legalább $2^{g^{\circ}}$. A (2.7) jobb oldalán álló polinom viszont vagy a zéruspolinom, vagy olyan polinom, amelynek a valódi fokszáma kisebb, mint g°, vagyis a módosított fokszáma kisebb, mint $2^{g^{\circ}}$. A fokszámokban megjelenő ellentmondás oka a $q_1(x) \neq q_2(x)$ feltevés. Ugyanakkor $q_1(x) = q_2(x)$ esetén (2.7)-ből az $r_1(x) = r_2(x)$ is adódik. Ezzel a tétel egyértelműségre vonaktozó állítását is bebizonyítottuk. ∎

Megjegyezzük, hogy konkrét polinomok esetén a maradékos osztás könnyen elvégezhető a (2.4)-beli lépés ismételt alkalmazásával. Példaként osszuk el maradékosan az $f(x) = 2x^4+4x^3+2x+1$ polinomot a $g(x) = 2x^2+x-1$ polinommal, ahol nyilvánvalóan $f(x), g(x) \in \mathbf{Q}[x]$.

$$\begin{array}{l} \left(\ 2x^4 + 4x^3 + 2x + 1\right) : \left(2x^2 + x - 1\right) = x^2 + \dfrac{3}{2}x - \dfrac{1}{4} \\ \underline{-(2x^4 + x^3 - x^2)} \\ 3x^3 + x^2 + 2x + 1 \\ \underline{-(3x^3 + \frac{3}{2}x^2 - \frac{3}{2}x)} \\ -\frac{1}{2}x^2 + \frac{7}{2}x + 1 \\ \underline{-(-\frac{1}{2}x^2 - \frac{1}{4}x + \frac{1}{4})} \\ \frac{15}{4}x + \frac{3}{4}. \end{array}$$

Tehát $f(x) = g(x)(x^2 + \frac{3}{2}x - \frac{1}{4}) + \frac{15}{4}x + \frac{3}{4}$, azaz $q(x) = x^2 + \frac{3}{2}x - \frac{1}{4}$ és $r(x) = \frac{15}{4}x + \frac{3}{4}$.

E feladat kapcsán megjegyezzük, hogy bár $f(x), g(x) \in \mathbf{Z}[x]$, de $q(x)$, $r(x) \notin \mathbf{Z}[x]$, amelyből azonnal adódik, hogy a maradékos osztás tétele nem igaz a $(\mathbf{Z}[x], +, \cdot)$ integritástartományban. Érdemes külön is felhívni a figyelmet arra az esetre, amikor $f(x), g(x) \in \mathbf{Z}[x]$ és a $g(x)$ főpolinom. Ekkor ugyanis az $f(x) = g(x)q(x) + r(x)$ $(r^{\circ\circ} < g^{\circ\circ})$ egyenlőségben mind a $q(x)$ mind az $r(x)$ polinomok egész együtthatós polinomok, azaz ezen polinomokon elvégezhető a maradékos osztás $\mathbf{Z}[x]$-ben.

Visszatérve a $\mathbf{T}$ test fölötti $(\mathbf{T}[x], +, \cdot)$ integritástartományra, legyen $f(x), g(x) \in \mathbf{T}[x]$ és $g(x) \neq 0$. A 2.3. Tétel szerint léteznek olyan $q_0(x), r_1(x)$ $\mathbf{T}[x]$-beli polinomok, amelyekkel

$$f(x) = g(x)q_0(x) + r_1(x), \text{ ahol } 0 \leq r_1^{\circ\circ} < g^{\circ\circ}.$$

Ha $r_1^{\circ\circ} \neq 0$, azaz $r_1(x) \neq 0$, akkor ugyancsak a 2.3. Tétel szerint léteznek olyan $q_1(x), r_2(x) \in \mathbf{T}[x]$ polinomok, amelyekkel

$$g(x) = r_1(x)q_1(x) + r_2(x), \text{ ahol } 0 \leq r_2^{\circ\circ} < r_1^{\circ\circ}.$$

Ha $r_2^{\circ\circ} \neq 0$, azaz $r_2(x) \neq 0$, akkor az $r_1(x)$ és $r_2(x)$ polinomokon hajtunk végre euklideszi osztást, majd ezt folytatva az alábbi, úgynevezett euklideszi algoritmushoz jutunk:

$$\begin{aligned}
f(x) &= g(x)q_0(x) + r_1(x), && 0 < r_1^{\circ\circ} < g^{\circ\circ},\\
g(x) &= r_1(x)q_1(x) + r_2(x), && 0 < r_2^{\circ\circ} < r_1^{\circ\circ},\\
r_1(x) &= r_2(x)q_2(x) + r_3(x), && 0 < r_3^{\circ\circ} < r_2^{\circ\circ},\\
&\vdots && \vdots\\
r_{n-2}(x) &= r_{n-1}(x)q_{n-1}(x) + r_n(x), && 0 < r_n^{\circ\circ} < r_{n-1}^{\circ\circ},\\
r_{n-1}(x) &= r_n(x)q_n(x) + 0.
\end{aligned} \tag{2.8}$$

A (2.8) algoritmus véges lépésben véget ér, ugyanis a

$$g^{\circ\circ} > r_1^{\circ\circ} > r_2^{\circ\circ} > \cdots > r_{n-1}^{\circ\circ} > r_n^{\circ\circ} > 0$$

egyenlőtlenségrendszerben természetes számok szigorúan csökkenő sorozata található, és az ilyen sorozat csak véges hosszúságú lehet.

Az 1.2. Tételhez hasonlóan igaz az alábbi állítás.

2.4. Tétel. *Legyen $r_n(x)$ az $f(x)$ és $g(x)$ $(g(x) \neq 0)$ $\mathbf{T}[x]$-beli polinomokon végrehajtott* (2.8) *euklideszi algoritmus utolsó zérustól különböző maradéka. Végtelen sok $X_n(x), Y_n(x) \in \mathbf{T}[x]$ polinom létezik, amelyekre*

$$f(x)X_n(x) + g(x)Y_n(x) = r_n(x). \tag{2.9}$$

Bizonyítás. Tételünk igazolása az 1.2. Tétel bizonyításához teljesen hasonló módon végezhető el. (A (2.9)-et kielégítő konkrét $X_n(x)$ és $Y_n(x)$ polinomok — az egész számoknál tanultakhoz hasonlóan — a (2.8)-ból előállíthatók.) ∎

Oszthatóság $\mathbf{T}[x]$-ben

A továbbiakban az 1. fejezetben megismert fogalmak és tételek polinomelméletbeli megfelelőit fogalmazzuk meg. A tételek bizonyításával csak akkor foglalkozunk, ha az lényegesen eltér az egész számok körében megismert megfelelő tétel bizonyításától. A többi esetben csak utalunk a bizonyítás módjára.

Definíció. Legyen $f(x)$ és $g(x) \in \mathbf{T}[x]$. Az $f(x)$ polinomot a $g(x)$ polinom osztójának nevezzük, ha létezik olyan $h(x) \in \mathbf{T}[x]$, amellyel

$$f(x)h(x) = g(x).$$

Az oszthatóságot $f(x) \mid g(x)$, míg ennek tagadását az $f(x) \nmid g(x)$ szimbólummal jelöljük.

2.5. Tétel. *$\mathbf{T}[x]$-ben az oszthatóság mint binér reláció*
(a) *reflexív,*
(b) *nem szimmetrikus,*
(c) *nem antiszimmetrikus,*
(d) *tranzitív.*

Bizonyítás. Az oszthatóság definíciója, illetve konkrét példák alapján a tétel egyszerűen bizonyítható (lásd 1.4. Tétel). ∎

2.6. Tétel. *Bármely $f(x)$, $g(x)$, $h(x)$ és $l(x) \in \mathbf{T}[x]$ esetén:*

(a) *ha $f(x) \mid g(x)$ és $f(x) \mid h(x)$, akkor $f(x) \mid (g(x) + h(x))$;*

(b) *ha $f(x) \mid g(x)$ és $h(x) \mid l(x)$, akkor $f(x)h(x) \mid g(x)l(x)$;*

(c) *$f(x) \mid 0$;*

(d) *$0 \mid f(x)$ akkor és csak akkor, ha $f(x) = 0$.*

(e) *Legyen $e(x)$ egy rögzített eleme $\mathbf{T}[x]$-nek. Az $e(x)$ polinom akkor és csak akkor osztója bármely $f(x) \in \mathbf{T}[x]$ polinomnak, ha $e(x) \mid 1$, azaz ha $e(x)$ nem zérus $\mathbf{T}$-beli elem.*

Bizonyítás. Az állítások igazolása az 1.7. és 1.8. Tétel bizonyításához hasonlóan történhet. ∎

Definíció. A $(\mathbf{T}[x], +, \cdot)$ integritástartomány 1 egységelemének osztóit egységeknek nevezzük, továbbá az $f(x)$ és $g(x) \in \mathbf{T}[x]$ polinomokat asszociáltaknak nevezzük, ha van olyan $e(x)$ egység $\mathbf{T}[x]$-ben, amelyre

$$f(x) = e(x)g(x).$$

Ezt a tényt az $f(x) \sim g(x)$ szimbólummal jelöljük.

Megjegyezzük, hogy míg az egész számok körében csak a $+1$ és a -1 az egység, addig $\mathbf{T}[x]$-ben a $\mathbf{T}$ test minden nemzérus eleme egység. Az előző definíciók alapján megfogalmazható a következő tétel.

2.7. Tétel. *Bármely $f(x)$ és $g(x) \in \mathbf{T}[x]$ esetén:*

(a) *ha $f(x) \mid g(x)$ és $g(x) \mid f(x)$, akkor $f(x) \sim g(x)$;*

(b) *ha $f(x) \mid g(x)$, $f(x) \sim f_1(x)$ és $g(x) \sim g_1(x)$, akkor $f_1(x) \mid g_1(x)$.*

Bizonyítás. Lásd az 1.5. és 1.6. Tételek bizonyítását. ∎

Tételünk egyszerű következménye, hogy a $\mathbf{T}[x]$-beli oszthatósági kérdések vizsgálatánál elegendő a főpolinomokra szorítkozni.

Legnagyobb közös osztó, legkisebb közös többszörös

Mivel az egész számok körében a legnagyobb közös osztóra, illetve a legkisebb közös többszörösre adott definíciókban a legnagyobb, illetve a legkisebb jelzők lényegében többszöröst, illetve osztót jelentettek, ezért e fogalmak változtatás nélkül átültethetők.

Definíció. Legyen $f(x)$, $g(x) \in \mathbf{T}[x]$ és $g(x) \neq 0$. Az $f(x)$ és $g(x)$ polinomok legnagyobb közös osztójának nevezzük a $d(x) \in \mathbf{T}[x]$ polinomot, ha

1. $d(x) \mid f(x)$ és $d(x) \mid g(x)$;
2. $f(x)$ és $g(x)$ bármely $d'(x) \in \mathbf{T}[x]$ közös osztójára igaz, hogy

$$d'(x) \mid d(x).$$

Definíció. Legyen $f(x), g(x) \in \mathbf{T}[x]$, és $f(x)g(x) \neq 0$. Az $f(x)$ és $g(x)$ polinomok legkisebb közös többszörösének nevezzük az $m(x) \in \mathbf{T}[x]$ polinomot, ha

1. $f(x) \mid m(x)$ és $g(x) \mid m(x)$;

2. $f(x)$ és $g(x)$ bármely $m'(x) \in \mathbf{T}[x]$ közös többszörösére igaz, hogy $m(x) \mid m'(x)$.

2.8. Tétel. *Ha az $f(x)$ és a $g(x)$ $\mathbf{T}[x]$-beli polinomoknak van legnagyobb közös osztója, illetve legkisebb közös többszöröse, akkor ezek asszociáltság erejéig egyértelműen meghatározottak.*

Bizonyítás. Ha $d_1(x)$ és $d_2(x)$ is legnagyobb közös osztó, ill. $m_1(x)$ és $m_2(x)$ is legkisebb közös többszörös, akkor $d_1(x) \mid d_2(x)$ és $d_2 \mid d_1(x)$ miatt $d_1(x) \sim d_2(x)$, ill. $m_1(x) \mid m_2(x)$ és $m_2(x) \mid m_1(x)$ miatt $m_1(x) \sim m_2(x)$. ∎

Megjegyezzük, hogy az $f(x)$ és a $g(x)$ polinom legnagyobb közös osztói, illetve legkisebb közös többszörösei közül a főpolinomot az $\big(f(x), g(x)\big)$, illetve az $\big[f(x), g(x)\big]$ szimbólummal szokás jelölni.

2.9. Tétel. *Bármely $f(x), g(x) \in \mathbf{T}[x]$ $(g(x) \neq 0)$ polinomoknak van legnagyobb közös osztója, és $g(x) \nmid f(x)$ esetén $\big(f(x), g(x)\big) \sim r_n(x)$, ahol $r_n(x)$ az $f(x)$ és $g(x)$ polinomokon végrehajtott euklideszi algoritmus utolsó zérustól különböző maradéka, míg $g(x) \mid f(x)$ esetén $(f(x), g(x)) \sim g(x)$.*

Bizonyítás. A (2.8) alatti algoritmusból adódik, hogy $g(x) \nmid f(x)$ esetén

$$r_n(x) \mid r_{n-1}(x),\ r_n(x) \mid r_{n-2}(x), \ldots, r_n(x) \mid g(x) \text{ és } \ r_n(x) \mid f(x).$$

Ha pedig $d'(x) \mid f(x)$ és $d'(x) \mid g(x)$, akkor szintén (2.8) alapján kapjuk, hogy

$$d'(x) \mid r_1(x),\ d'(x) \mid r_2(x), \ldots, d'(x) \mid r_n(x),$$

azaz $\big(f(x), g(x)\big) \sim r_n(x)$. Ha pedig $g(x) \mid f(x)$, akkor nyilvánvaló, hogy

$$(f(x), g(x)) \sim g(x). \ ∎$$

Most is könnyen igazolhatók az 1.12. Tételbeli tulajdonságok polinomokra vonatkozó átfogalmazásai.

2.10. Tétel. *Bármely $f(x), g(x)$ és $h(x) \in \mathbf{T}[x]$ $(g(x) \neq 0)$ polinomokra igazak az alábbiak:*

(a) $\big(f(x), g(x)\big) \sim \big(g(x), f(x)\big)$;

(b) $\big(\big(f(x), g(x)\big), h(x)\big) \sim \big(f(x), \big(g(x), h(x)\big)\big)$;

(c) $\big(g(x), g(x)\big) \sim g(x)$;

(d) $\big(f(x), g(x)\big)h(x) \sim \big(f(x)h(x), g(x)h(x)\big)$, *ha* $h(x) \neq 0$;

(e) $\big(f(x), g(x)\big) \sim g(x)$ *akkor és csak akkor, ha* $g(x) \mid f(x)$;

(f) $\big(f(x), g(x)\big) \sim \big(f(x) + t(x)g(x), g(x)\big)$ *minden* $t(x) \in \mathbf{T}[x]$ *esetén.*

Bizonyítás. Az 1.12. Tétel bizonyításának lépéseit követve itt is adódnak az állítások. ∎

Definíció. Legyen $f(x), g(x) \in \mathbf{T}[x]$ és $g(x) \neq 0$. Ha $\big(f(x), g(x)\big) \sim 1$, akkor az $f(x)$ és a $g(x)$ polinomokat relatív prím polinomoknak nevezzük.

Itt is igaz a relatív prím párok előállítására vonatkozó tétel.

2.11. Tétel. *Bármely* $f(x), g(x) \in \mathbf{T}[x]$ $\big(g(x) \neq 0\big)$ *polinomra*

$$\left(\frac{f(x)}{\big(f(x), g(x)\big)}, \frac{g(x)}{\big(f(x), g(x)\big)}\right) \sim 1.$$

Bizonyítás. A 2.10. Tétel (d) állítását alkalmazva kapjuk, hogy

$$\left(\frac{f(x)}{\big(f(x), g(x)\big)}, \frac{g(x)}{\big(f(x), g(x)\big)}\right) \big(f(x), g(x)\big) \sim \big(f(x), g(x)\big),$$

amelyből

$$\big(f(x), g(x)\big) \left(\left(\frac{f(x)}{\big(f(x), g(x)\big)}, \frac{g(x)}{\big(f(x), g(x)\big)}\right) - c\right) = 0 \tag{2.10}$$

következik, ahol $c \in \mathbf{T} \setminus \{0\}$. Mivel $\big(f(x), g(x)\big) \neq 0$, így (2.10)-ből kapjuk, hogy

$$\left(\frac{f(x)}{\big(f(x), g(x)\big)}, \frac{g(x)}{\big(f(x), g(x)\big)}\right) = c,$$

amely — az asszociáltság definíciója alapján — állításunkkal ekvivalens. ∎

2.12. Tétel. *Legyen* $f(x), g(x)$ *és* $h(x) \in \mathbf{T}[x]$. *Ha* $f(x) \mid g(x)h(x)$ *és* $\big(f(x), g(x)\big) \sim 1$, *akkor* $f(x) \mid h(x)$.

Bizonyítás. A 2.10. Tétel állításait alkalmazva, — az 1.15. tétel bizonyításának mintájára — könnyen adódik az állítás. ∎

A továbbiakban az $[f(x), g(x)]$ létezésével, illetve a tulajdonságaival foglalkozunk.

2.13. Tétel. *Bármely* $f(x), g(x) \in \mathbf{T}[x] \setminus \{0\}$ *polinomnak van legkisebb közös többszöröse és*

$$[f(x), g(x)] \sim \frac{f(x)g(x)}{\big(f(x), g(x)\big)}.$$

Bizonyítás. A tétel bizonyítása nem igényel új ötletet, így az 1.18. Tétel bizonyításának mintáját követve adódik az állítás. ∎

2.14. Tétel. *Bármely* $f(x), g(x), h(x) \in T[x] \setminus \{0\}$ *polinomra igazak az alábbi tulajdonságok:*

(a) $[f(x), g(x)] \sim [g(x), f(x)]$;

(b) $[[f(x), g(x)], h(x)] \sim [f(x), [g(x), h(x)]]$;

(c) $[f(x), f(x)] \sim f(x)$;

(d) $[f(x), g(x)]h(x) \sim [f(x)h(x), g(x)h(x)]$;

(e) $[f(x), g(x)] \sim g(x)$ *akkor és csak akkor, ha* $f(x) \mid g(x)$.

Bizonyítás. Az 1.19. Tétel bizonyításának lépéseit követve itt is egyszerűen adódnak az állítások. ∎

Irreducibilis és prímpolinomok $\mathbf{T}[x]$-ben, a polinomelmélet alaptétele

Definíció. Az $f(x)$ legalább elsőfokú ($f^\circ \geq 1$), $\mathbf{T}[x]$-beli polinomot irreducibilisnek nevezzük, ha nincs valódi osztója, azaz, ha $g(x) \in \mathbf{T}[x]$ és $g(x) \mid f(x)$, akkor vagy $g(x) \sim 1$, vagy $g(x) \sim f(x)$. Ellenkező esetben $f(x)$-et reducibilis polinomnak nevezzük.

Definíció. Az $f(x)$ legalább elsőfokú ($f^\circ \geq 1$), $\mathbf{T}[x]$-beli polinomot prímnek nevezzük, ha bármely $g(x)$, $h(x) \in \mathbf{T}[x]$ esetén az $f(x) \mid g(x)h(x)$ és $f(x) \nmid g(x)$ feltételekből $f(x) \mid h(x)$ következik.

Az egész számokhoz hasonlóan $\mathbf{T}[x]$-ben is ,,fedi egymást" az előző két definíció.

2.15. Tétel. $\mathbf{T}[x]$*-ben egy polinom akkor és csak akkor irreducibilis, ha prím.*

Bizonyítás. Tételünknek mind a szükséges, mind az elégséges része — az 1.22. Tétel bizonyításának gondolatmenetét követve — könnyen bizonyítható. ∎

Az előzőekben megfogalmazott tételek alapján nem meglepő, hogy $\mathbf{T}[x]$-ben is igaz az úgynevezett egyértelmű irreducibilis faktorizáció tétele, melyet a *polinomelmélet alaptételének* is nevezünk.

2.16. Tétel. *Minden legalább elsőfokú,* $\mathbf{T}[x]$*-beli* $f(x)$ $(f^\circ \geq 1)$ *polinom — a tényezők sorrendjétől és asszociáltságtól eltekintve — egyértelműen írható fel véges sok* $\mathbf{T}[x]$*-beli irreducibilis (prím) polinom szorzataként. (Speciálisan az egytényezős szorzat is megengedett.)*

Bizonyítás. A számelmélet alaptételének (1.24. Tétel) bizonyításához hasonlóan itt is két részből áll a bizonyítás. Először — a (valódi) fokszám szerinti teljes indukcióval — a szorzatfelbontás létezését bizonyítjuk. Az egy (valódi) fokszámú polinomok nyilván irreducibilisek $\mathbf{T}[x]$-ben, és így mint egytényezős szorzatra igaz az állítás. Tegyük fel, hogy minden legfeljebb $n-1$-edfokú $(1 \leq n-1)$ $\mathbf{T}[x]$-beli polinom már felbomlik véges sok irreducibilis polinom szorzatára. Bizonyítjuk, hogy az állítás n-edfokú polinomokra is igaz. Legyen $f(x)$ egy tetszőleges n-edfokú polinom $\mathbf{T}[x]$-ben. Ha $f(x)$ irreducibilis, akkor az egytényezős szorzatelőállítása adott, ellenkező esetben létezik olyan $g(x)$ és $h(x) \in \mathbf{T}[x]$, amelyre

$$f(x) = g(x)h(x), \tag{2.11}$$

ahol $f^\circ = n > g^\circ \geq 1$ és $f^\circ = n > h^\circ \geq 1$. Ezért az indukciós feltevésünk szerint mind a $g(x)$, mind a $h(x)$ polinomok már felbonthatók véges sok irreducibilis polinom szorzatára, és így (2.11) miatt $f(x)$ is. A szorzatelőállítás egyértelműségét most is indirekt módon igazolhatjuk. ∎

Tételünk alapján $f(x)$ $(f^\circ \geq 1)$ prímtényezős alakja:

$$f(x) \sim p_1^{\alpha_1}(x)p_2^{\alpha_2}(x)\cdots p_r^{\alpha_r}(x) \quad (\alpha_i \geq 1,\ 1 \leq i \leq r), \tag{2.12}$$

ahol a $p_i(x)$ polinomok prímek (irreducibilisek) $\mathbf{T}[x]$-ben. Szokás (2.12)-t az $f(x)$ kanonikus alakjának is nevezni. Könnyen belátható, hogy $f(x)$ és $g(x)$ prímtényezős alakjából előállíthatók az $\big(f(x), g(x)\big)$ és az $[f(x), g(x)]$ polinomok is. Ugyanis, ha az $f(x)$ és a $g(x)$ polinomokat az alábbi

$$\begin{aligned} f(x) &\sim p_1^{\beta_1}(x)p_2^{\beta_2}(x)\cdots p_k^{\beta_k}(x) \quad (\beta_i \geq 0), \\ g(x) &\sim p_1^{\gamma_1}(x)p_2^{\gamma_2}(x)\cdots p_k^{\gamma_k}(x) \quad (\gamma_i \geq 0) \end{aligned}$$

alakban vesszük fel, akkor

$$\big(f(x), g(x)\big) \sim p_1^{\delta_1}(x)p_2^{\delta_2}(x)\cdots p_k^{\delta_k}(x)$$

és

$$\big[f(x), g(x)\big] \sim p_1^{\eta_1}(x)p_2^{\eta_2}(x)\cdots p_k^{\eta_k}(x),$$

ahol $\delta_i = \min\{\beta_i, \gamma_i\}$ és $\eta_i = \max\{\beta_i, \gamma_i\}$ $(1 \leq i \leq k)$.

A polinomelmélet alaptétele kapcsán felvetődhet a kérdés, hogy $\mathbf{T}[x]$-ben mely polinomok irreducibilisek (prímek). Az nyilvánvaló, hogy az elsőfokú polinomok mindig prímek, de a magasabb fokú polinomoknál — a $\mathbf{T}$ konkrét ismerete nélkül — általában nem válaszolható meg a kérdés. Például az $f(x) = x^2 - 2$ polinom irreducibilis $\mathbf{Q}[x]$-ben, de reducibilis $\mathbf{R}[x]$-ben $\big(x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})\big)$. Megemlítjük, hogy a $\mathbf{C}[x], \mathbf{R}[x]$ és $\mathbf{Q}[x]$ polinomgyűrűk irreducibilis polinomjairól az algebrai egyenletek elméletének segítségével újabb információt nyerhetünk (lásd [7], 286—289. oldal), de ezzel itt nem foglalkozunk.

Euklideszi gyűrűk

Az előzőkeben láttuk, hogy $(\mathbf{Z}, +, \cdot)$-ban és $(\mathbf{T}[x], +, \cdot)$-ban ,,ugyanazt" a számelméletet lehetett kiépíteni. E két struktúra közös tulajdonsága, hogy mindkettő integritástartomány és mindkettőben bizonyítható a maradékos (euklideszi) osztás tétele. Ez utóbbinak $\mathbf{Z}$-beli (lásd 1.1. Tétel) megfogalmazásában fontos szerepet játszik az abszolút érték, míg a $\mathbf{T}[x]$-beli (lásd 2.3. Tétel) alakban a módosított fokszám, amelyek felfoghatók úgy is, mint a gyűrű elemeihez rendelt természetes számok. E tények általánosításaként jutunk el az euklideszi gyűrű fogalmához.

Definíció. A $(\mathbf{K}, +, \cdot)$ integritástartományt euklideszi gyűrűnek nevezzük, ha létezik olyan

$$\delta\colon \mathbf{K} \to \mathbf{N} \quad (a \mapsto \delta(a)) \tag{2.13}$$

leképezés, amelyre igazak az alábbiak:

1. $\delta(a) = 0$ akkor és csak akkor, ha a a $\mathbf{K}$ zéruseleme;
2. $\delta(ab) = \delta(a)\delta(b)$ bármely $a, b \in \mathbf{K}$ esetén;
3. bármely $a, b \in \mathbf{K}$ $(b \neq 0)$ elemhez van olyan $q, r \in \mathbf{K}$, amelyekre

$$a = bq + r, \text{ ahol } 0 \leq \delta(r) < \delta(b). \tag{2.14}$$

A (2.13) alatti δ leképezést euklideszi normának, (2.14)-et maradékos (vagy euklideszi) osztásnak, q-t hányadosnak, míg r-et maradéknak nevezzük.

A definícióból következik, hogy $\mathbf{Z}$-ben az abszolút érték euklideszi norma, mivel

1. $|a| = 0$ akkor és csak akkor, ha $a = 0$;
2. $|ab| = |a|\,|b|$,

és az 1.1. Tétel szerint teljesül a norma 3. feltétele is. $\mathbf{T}[x]$-ben pedig a módosított fokszám euklideszi norma, mivel

1. $f^{\circ\circ} = 0$ akkor és csak akkor, ha $f(x) = 0$;
2. Legyen $f(x)g(x) = h(x)$. Ekkor
(a) ha $f(x) = 0$, akkor $h^{\circ\circ} = 0 = 0g^{\circ\circ} = f^{\circ\circ}g^{\circ\circ}$;
(b) ha $f(x)g(x) \neq 0$, akkor $h^{\circ\circ} = 2^{f^\circ + g^\circ} = 2^{f^\circ}2^{g^\circ} = f^{\circ\circ}g^{\circ\circ}$,
azaz bármely $f(x), g(x) \in \mathbf{T}[x]$ esetén

$$(fg)^{\circ\circ} = f^{\circ\circ}g^{\circ\circ}.$$

A 2.3. Tétel szerint a norma 3. tulajdonsága is teljesül.

Megemlítjük, hogy — az 1.1. Tétel, illetve a 2.3. Tétel szerint — a $\mathbf{Z}$, illetve a $\mathbf{T}[x]$ gyűrűben a maradékos osztásnál fellépő hányados és maradék egyértelműsége is bizonyítható volt, jóllehet ez tetszőleges euklideszi gyűrűben, adott euklideszi norma esetén nem mondható el. Sőt, mint azt az 1.1. Tétel utáni példában láttuk, $\mathbf{Z}$-ben sem bizonyítható a maradékos osztásnál fellépő hányados és maradék egyértelműsége, ha a legkisebb nemnegatív maradék helyett más, például a legkisebb abszolút értékű maradék szerepelne az 1.1. Tételben.

Természetes, hogy minden euklideszi gyűrűben felírható az euklideszi osztások sorozataként kapott

$$\begin{aligned}
a &= bq_0 + r_1, & 0 < \delta(r_1) < \delta(b),\\
b &= r_1q_1 + r_2, & 0 < \delta(r_2) < \delta(r_1),\\
r_1 &= r_2q_2 + r_3, & 0 < \delta(r_3) < \delta(r_2),\\
&\vdots & \vdots\\
r_{n-2} &= r_{n-1}q_{n-1} + r_n, & 0 < \delta(r_n) < \delta(r_{n-1}),\\
r_{n-1} &= r_nq_n + 0,
\end{aligned}$$

euklideszi algoritmus, amely — a $\delta(r_i)$ normák mint természetes számok szigorúan csökkenő sorozata miatt — mindig véges hosszúságú. Mindezek szerint az előzőekben megismert valamennyi számelméleti fogalom definiálható, és valamennyi számelméleti tétel bizonyítható tetszőleges euklideszi gyűrűben is. Ezért igaz az alábbi tétel.

2.17. Tétel. *Minden euklideszi gyűrűben igaz az egyértelmű irreducibilis faktorizáció tétele, azaz a* $(\mathbf{K}, +, \cdot)$ *euklideszi gyűrű bármely zérustól és egységelemének osztóitól (egységektől) különböző eleme a tényezők sorrendjétől és egységtényezőktől (asszociáltaktól) eltekintve egyértelműen írható fel véges sok* $\mathbf{K}$*-beli irreducibilis (prím) elem szorzataként.*

Végül megemlítjük, hogy egy integritástartománynak nem kell szükségképpen euklideszi gyűrűnek lenni ahhoz, hogy benne igaz legyen az egyértelmű irreducibilis faktorizáció tétele. Lásd például a $(\mathbf{Z}[x], +, \cdot)$ gyűrűt [7]-ben a 191—198. oldalon.

Feladatok

1. Legyen $f(x) = 5x^5 + 5x^4 + 3x^2 - 2x - 1$ és $g(x) = x^3 + 2x + 2$. Végezzünk euklideszi osztást az $f(x)$ és $g(x)$ polinomokkal $\mathbf{Q}[x]$-ben.

2. Hajtsuk végre az euklideszi algoritmust az $f(x)$ és $g(x)$ polinomokkal $\mathbf{Q}[x]$-ben, majd az utolsó zérustól különböző maradékot állítsuk elő $f(x)$ és $g(x)$ lineáris kombinációjaként, ha $f(x) = 3x^3 - 2x^2 + x - 1$ és $g(x) = = x^2 - x - 1$.

3. Legyen $f(x), g(x) \in \mathbf{Q}[x]$, $f(x) = 3x^3+4x^2+5x-k$ és $g(x) = -x+1$. Határozzuk meg a k értékét úgy, hogy $g(x) \mid f(x)$ teljesüljön.

4. Legyenek $f(x)$, $g(x)$ $\mathbf{Q}[x]$-beli polinomok, $f(x) = 4x^4-2x^2+kx+l$ és $g(x) = x^2 - x + 1$. Határozzuk meg a k és az l paraméter értékét úgy, hogy $g(x) \mid f(x)$ teljesüljön.

5. Az a és a b racionális együtthatókat hogyan kell megválasztani az n függvényében, hogy $(x-1)^2 \mid (ax^{n+1} + bx^n + 1)$ teljesüljön.

6. Legyen $f(x) = x^m - 1$ és $g(x) = x^n - 1$, ahol $f^\circ, g^\circ \geq 1$. Bizonyítsuk be, hogy $(f(x), g(x)) = x^{(m,n)} - 1$.

7. A legnagyobb közös osztó elemi tulajdonságait használva bizonyítsuk be, hogy $\mathbf{Q}[x]$-ben

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

8. Bontsuk fel az $f(x) = x^4 + 1$ polinomot $\mathbf{R}[x]$-beli irreducibilis polinomok szorzatára.

9. Legyen $f(x) = x^3 + px + q$ és $g(x) = 3x^2 + p$, ahol p és q valós számok. Milyen összefüggésnek kell fennállni a p és q együtthatók között, hogy a $d(x) = \big(f(x), g(x)\big)$ polinom legalább elsőfokú legyen.

10. Határozzuk meg a p, q és r nullától különböző valós számok közötti összefüggést úgy, hogy az $f(x) = x^4 + px^2 + qx + r$ és a $g(x) = 4x^3 + 2px + q$ polinomok relatív prímek legyenek $\mathbf{R}[x]$-ben.

3. Kongruenciák és maradékosztályok Z-ben

Az oszthatósági problémák könnyen kezelhetővé válhatnak a kongruenciák segítségével.

Definíció. Legyen $a, b, m \in \mathbf{Z}$, ahol m rögzített. Az a egész számot kongruensnek nevezzük b-vel az m modulusra nézve, ha $m \mid (a - b)$. A szokásos jelölés:

$$a \equiv b \pmod{m},$$

amelyet „a kongruens b-vel modulo m"-ként olvasunk. Ha $m \nmid (a-b)$, akkor ezt $a \not\equiv b \pmod{m}$-mel jelöljük és „a inkongruens b-vel modulo m"-ként olvassuk.

Mivel $m \mid (a - b)$ esetén $-m \mid (a - b)$ is teljesül, ezért feltehető, hogy $m \geq 0$. Ugyanakkor az $a \equiv b \pmod{0}$ kongruencia, az oszthatóság ismert tulajdonsága miatt, pontosan akkor teljesül, ha $a = b$, míg az $a \equiv b \pmod{1}$ bármely $a, b \in \mathbf{Z}$-re igaz, így e két konkrét modulusra a kongruencia vizsgálata érdektelen. Ezért a továbbiakban csak az $m \geq 2$ modulusú kongruenciákkal foglalkozunk. Felhívjuk az olvasó figyelmét, arra hogy az $a \equiv 0 \pmod{m}$ és az $m \mid a$ kijelentések ekvivalensek.

A kongruencia, hasonlóan az oszthatósághoz, a $(\mathbf{Z}, +, \cdot)$ integritástartományban egy binér reláció, amelyre igazak az alábbi tulajdonságok.

3.1. Tétel. *Bármely a, b, c, d egész számra*

(a) $a \equiv a \pmod{m}$*;*

(b) *ha* $a \equiv b \pmod{m}$, *akkor* $b \equiv a \pmod{m}$*;*

(c) *ha* $a \equiv b \pmod{m}$ *és* $b \equiv c \pmod{m}$, *akkor* $a \equiv c \pmod{m}$*;*

(d) *ha* $a \equiv b \pmod{m}$ *és* $c \equiv d \pmod{m}$, *akkor* $a + c \equiv b + d \pmod{m}$ *és* $ac \equiv bd \pmod{m}$, *azaz a kongruencia, egy — absztrakt algebrai értelemben vett — kongruenciareláció a* $(\mathbf{Z}, +, \cdot)$ *struktúrában.*

Bizonyítás. A kongruencia definíciója alapján a tétel állításai rendre az alábbiakat jelentik:

(a') $m \mid (a - a)$;

(b') ha $m \mid (a - b)$, akkor $m \mid (b - a)$;

(c') ha $m \mid (a - b)$ és $m \mid (b - c)$, akkor $m \mid (a - c)$;

(d') ha $m \mid (a - b)$ és $m \mid (c - d)$, akkor $m \mid ((a + c) - (b + d))$ és $m \mid (ac - bd)$, amelyek igazolása, az oszthatóság ismert tulajdonságai alapján, könnyen elvégezhető.

Foglalkozzunk például a (d') második részének bizonyításával. A feltétel szerint

$$m \mid (a-b) \quad \text{és} \quad m \mid (c-d),$$

amelyből kapjuk, hogy

$$m \mid (a-b)c \quad \text{és} \quad m \mid b(c-d).$$

Ez utóbbiból viszont

$$m \mid ((ac-bc)+(bc-bd)) = ac-bd$$

következik. ∎

Érdemes kiemelni a (d) állítás speciális eseteit:
(d_1) ha $a \equiv b \pmod{m}$, akkor $a \pm c \equiv b \pm c \pmod{m}$;
(d_2) ha $a \equiv b \pmod{m}$, akkor $ac \equiv bc \pmod{m}$;
(d_3) ha $a \equiv b \pmod{m}$ és $n \in \mathbf{N} \setminus \{0\}$, akkor $a^n \equiv b^n \pmod{m}$.

További, a modulussal kapcsolatos tulajdonságokról szól a következő tétel.

3.2. Tétel. *Bármely a, b, c egész számra:*

(a) *ha $a \equiv b \pmod{m}$ és $m_1 \mid m$, akkor $a \equiv b \pmod{m_1}$;*

(b) *ha $ac \equiv bc \pmod{m}$, akkor $a \equiv b \pmod{\frac{m}{(m,c)}}$;*

(c) *ha $a \equiv b \pmod{m_1}$ és $a \equiv b \pmod{m_2}$, akkor*
$a \equiv b \pmod{[m_1, m_2]}$.

Bizonyítás. Az (a) állítás $m_1 \mid m$ és $m \mid (a-b)$ miatt nyilvánvaló. A (b) részben induljunk ki az $m \mid (ac-bc)$ feltételből, amely szerint

$$c(a-b) = mk$$

valamely $k \in \mathbf{Z}$-vel. Ezt (m,c)-vel osztva kapjuk, hogy

$$\frac{c}{(m,c)}(a-b) = \frac{m}{(m,c)}k,$$

amelyből

$$\frac{m}{(m,c)} \;\Big|\; \frac{c}{(m,c)}(a-b)$$

következik. Ugyanakkor az általánosított prímtulajdonság (1.17. Tétel) miatt

$$\frac{m}{(m,c)} \;\Big|\; (a-b), \quad \text{azaz,} \quad a \equiv b \pmod{\frac{m}{(m,c)}}.$$

A (c) állítás a legkisebb közös többszörös definíciójából adódik. ∎

A (b) és (c) állítások speciális eseteit külön is megfogalmazzuk:
(b_1) ha $ac \equiv bc \pmod{m}$ és $(m, c) = 1$, akkor $a \equiv b \pmod{m}$;
(c_1) ha $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$ és $(m_1, m_2) = 1$, akkor $a \equiv b \pmod{m_1 m_2}$.

A kongruencia és a maradékos osztás kapcsolatát mutatja az alábbi tétel.

3.3. Tétel. *Legyen $a, b \in \mathbf{Z}$. $a \equiv b \pmod{m}$ akkor és csak akkor, ha a és b m-mel osztva ugyanazt a legkisebb nemnegatív maradékot adja.*

Bizonyítás. Legyen $a = mq_1 + r_1$ és $b = mq_2 + r_2$, ahol $q_1, q_2, r_1, r_2 \in \mathbf{Z}$ és $0 \le r_i \le m - 1$ $(i = 1, 2)$. Ha $r_1 = r_2$, akkor $a - b = m(q_1 - q_2)$, azaz $a \equiv b \pmod{m}$. Most tegyük fel, hogy $a \equiv b \pmod{m}$, de $r_1 \neq r_2$. Ekkor

$$m \mid (a - b) = m(q_1 - q_2) + r_1 - r_2,$$

amiből $m \mid (r_1 - r_2)$ következik. De ez lehetetlen, mivel $1 \le |r_1 - r_2| \le m - 1$. Az ellentmondás igazolja tételünk elégséges részét. ∎

Absztrakt algebrai tanulmányainkból tudjuk, hogy egy algebrai struktúrán értelmezett kongruenciareláció a struktúra kompatibilis osztályozását szolgáltatja. A 3.1. Tétel szerint a modulo m kongruencia kongruenciareláció, ezért az a $(\mathbf{Z}, +, \cdot)$ integritástartomány kompatibilis osztályozását adja. Egy osztályba tartoznak azok az a és b egészek, amelyekre $a \equiv b \pmod{m}$ igaz, azaz — a 3.3. Tétel szerint — m-mel osztva ugyanazt a legkisebb nemnegatív maradékot adják. Összhangban az absztrakt algebrai elnevezésekkel, az osztályokat modulo m maradékosztályoknak, az osztályok halmazát modulo m faktorhalmaznak nevezzük.

A 3.3. Tétel szerint a maradékosztályok (a szokásos $\overline{x}$ jelöléssel):

$$\begin{aligned}
\overline{0} &= \{n : n = mq + 0,\ q \in \mathbf{Z}\},\\
\overline{1} &= \{n : n = mq + 1,\ q \in \mathbf{Z}\},\\
&\vdots\\
\overline{m-1} &= \{n : n = mq + m - 1,\ q \in \mathbf{Z}\},
\end{aligned}$$

a faktorhalmaz pedig ($\mathbf{Z}/_{(m)}$ jelöléssel)

$$\mathbf{Z}/_{(m)} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}.$$

Definíció. Ha $a \in \overline{a}$, akkor az a egész számot az $\overline{a}$ (osztály) reprezentánsának nevezzük. Ha minden modulo m maradékosztályból pontosan egy

reprezentánst választunk, akkor e reprezentánsok halmazát modulo m teljes reprezentánsrendszernek (vagy maradékrendszernek) nevezzük.

3.4. Tétel. *Az $a_1, a_2, \ldots, a_k$ egész számok akkor és csak akkor alkotnak modulo m teljes reprezentánsrendszert, ha $k = m$ és $a_i \not\equiv a_j \pmod{m}$ minden $1 \leq i < j \leq m$-re.*

Bizonyítás. Az előző definícióból közvetlenül adódik az állítás. ∎

Példák modulo m teljes reprezentánsrendszerre:
A legkisebb nemnegatív maradékok rendszere: $\{0, 1, 2, \ldots, m-1\}$;
A legkisebb pozitív maradékok rendszere: $\{1, 2, \ldots, m\}$;
A legkisebb abszolút értékű maradékok rendszere:
$\left\{0, \pm 1, \pm 2, \ldots, \pm \frac{m-1}{2}\right\}$, ha m páratlan,
$\left\{0, \pm 1, \pm 2, \ldots, \pm \left(\frac{m}{2} - 1\right), \frac{m}{2}\right\}$, ha m páros.

Ha már ismert egy modulo m teljes reprezentánsrendszer, akkor abból az alábbiak szerint újabb teljes reprezentánsrendszerek nyerhetők.

3.5. Tétel. *Legyen $\{a_1, a_2, \ldots, a_m\}$ egy teljes reprezentánsrendszer modulo m. Ha $c, b \in \mathbf{Z}$ és $(c, m) = 1$, akkor*

$$\{ca_1 + b, ca_2 + b, \ldots, ca_m + b\}$$

szintén teljes reprezentánsrendszer modulo m.

Bizonyítás. A $ca_i + b$ $(i = 1, 2, \ldots, m)$ számok száma nyilván m, ezért csak a páronkénti inkongruenciát kell bizonyítani. Tegyük fel, hogy

$$ca_i + b \equiv ca_j + b \pmod{m}$$

valamely $i < j$-re. De ebből a 3.1. Tétel szerint

$$ca_i \equiv ca_j \pmod{m}$$

következik, amelyből $(c, m) = 1$ miatt az

$$a_i \equiv a_j \pmod{m}$$

kongruenciát kapjuk. Ez viszont ellentmond annak, hogy az $a_1, a_2, \ldots, a_m$ egészek teljes reprezentánsrendszert alkottak modulo m. Az ellentmondás bizonyítja a tételt. ∎

A következőkben egy maradékosztály tetszőleges eleme és a modulus legnagyobb közös osztóját vizsgáljuk.

3.6. Tétel. *Legyen* $\overline{a} \in \mathbf{Z}/_{(m)}$. *Bármely* $a_1, a_2 \in \overline{a}$ *egészre*

$$(a_1, m) = (a_2, m).$$

Bizonyítás. Mivel $a_1, a_2 \in \overline{a}$, ezért léteznek olyan q_1, q_2 egész számok, hogy

$$a_1 = mq_1 + a \quad \text{és} \quad a_2 = mq_2 + a.$$

Az 1.13. Tétel (f) pontja alapján

$$(a_1, m) = (mq_1 + a, m) = (a, m) = (mq_2 + a, m) = (a_2, m). \blacksquare$$

Speciálisan, ha $a_1, a_2 \in \overline{a}$ és $(a_1, m) = 1$, akkor $(a_2, m) = 1$. Ez ad lehetőséget a következő definícióra.

Definíció. Azokat a modulo m maradékosztályokat, amelyeknek az elemei m-hez relatív prímek, redukált (vagy prím) maradékosztályoknak nevezzük. Ezen osztályok halmazát $P(m)$-mel jelöljük.

Definíció. Ha minden modulo m redukált maradékosztályból pontosan egy reprezentánst választunk, akkor e reprezentánsok halmazát redukált reprezentánsrendszernek (illetve redukált maradékrendszernek) nevezzük modulo m.

A definíciókhoz kapcsolódva bevezetjük az úgynevezett Euler-féle φ függvényt:

$$\varphi\colon \mathbf{N} \setminus \{0\} \to \mathbf{N}, \quad \varphi(m) = \begin{cases} 1, & \text{ha} \quad m = 1, \\ k, & \text{ha } m \geq 2, \end{cases}$$

ahol k jelöli a modulo m redukált maradékosztályok számát, azaz a 0, 1, …, $m - 1$ teljes reprezentánsrendszerből az m modulushoz relatív prímek számát.

A φ függvény helyettesítési értékeinek kiszámításához szükség van az alábbi tételre.

3.7. Tétel. *Legyen* $a, b \in \mathbf{N} \setminus \{0\}$. *Ha* $(a, b) = 1$, *akkor*

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Bizonyítás. Az $a = 1$, $b \geq 1$ esetekben igaz a tétel, mert

$$\varphi(1b) = \varphi(b) = \varphi(1)\varphi(b).$$

A továbbiakban legyen $a > 1$, $b > 1$ és

$$A = \{ax + by \colon x = 0, 1, 2, \ldots, b-1; \quad y = 0, 1, 2, \ldots, a-1\}.$$

Először megmutatjuk, hogy A teljes maradékrendszer modulo ab. Mivel $|A| = ab$, ezért csak az A elemeinek páronkénti inkongruenciáját kell bizonyítani (lásd 3.4. Tétel). Tegyük fel, hogy az A definíciójában megengedett x és y értékek között léteznek olyan x_1, x_2, y_1, y_2 egészek, amelyekre például $x_1 \neq x_2$ és

$$ax_1 + by_1 \equiv ax_2 + by_2 \pmod{ab}.$$

Ebből a 3.2. Tétel (a) pontja szerint

$$ax_1 + by_1 \equiv ax_2 + by_2 \pmod{a} \quad \text{és} \quad ax_1 + by_1 \equiv ax_2 + by_2 \pmod{b}$$

következik. De ekkor, $(a, b) = 1$ miatt az

$$y_1 \equiv y_2 \pmod{a} \quad \text{és} \quad x_1 \equiv x_2 \pmod{b}$$

kongruenciákat kapjuk. Ez x_1 és x_2 lehetséges értékei miatt csak $x_1 = x_2$ esetben teljesülhet, ami ellentmond a feltevésünknek, azaz A elemei inkongruensek modulo ab.

Így A-ban az ab-hez relatív prímek száma $\varphi(ab)$. Ugyanakkor az 1.16. Tétel szerint $(ax + by, ab) = 1$ akkor és csak akkor, ha

$$(ax + by, a) = 1$$

és

$$(ax + by, b) = 1,$$

amelyekből a legnagyobb közös osztó bizonyított tulajdonságai és $(a, b) = 1$ alapján kapjuk, hogy

$$(ax + by, a) = (by, a) = (y, a) = 1 \quad \text{és} \quad (ax + by, b) = (ax, b) = (x, b) = 1.$$

Ez utóbbiakat kielégítő y-ok száma $\varphi(a)$, az x-ek száma pedig $\varphi(b)$, ezért a lehetséges (y, x) számpárok száma $\varphi(a)\varphi(b)$. Ezzel bebizonyítottuk a tétel állítását, azaz valóban

$$\varphi(ab) = \varphi(a)\varphi(b). \ \blacksquare$$

Igaz az előző tétel általánosítása is.

3.8. Tétel. *Ha $a_1, a_2, \ldots, a_k$ páronként relatív prím pozitív egész számok ($k \geq 2$), akkor*

$$\varphi(a_1 a_2 \cdots a_k) = \varphi(a_1)\varphi(a_2)\cdots\varphi(a_k).$$

Bizonyítás. Alkalmazzunk k szerinti teljes indukciót. ∎

Ha $m(\geq 2)$ kanonikus alakja

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \quad (\alpha_i \geq 1),$$

akkor a 3.8. Tétel alapján

$$\varphi(m) = \varphi\left(p_1^{\alpha_1}\right)\varphi\left(p_2^{\alpha_2}\right)\cdots\varphi\left(p_r^{\alpha_r}\right),$$

ezért $\varphi(m)$ meghatározásához elegendő a $\varphi\left(p_i^{\alpha_i}\right)$ értékeket ismerni.

Foglalkozzunk tehát $\varphi(p^\alpha)$ meghatározásával, ahol p prímszám és $\alpha \geq 1$ egész.

Ha $\alpha = 1$, akkor $\varphi(p) = p - 1$, mivel a $0, 1, 2, \ldots, p-1$ egészek közül egyedül a 0 nem relatív prím p-hez.

Ha $\alpha \geq 2$, akkor $\varphi(p^\alpha)$ jelöli a

$$0, 1, 2, \ldots p, \ldots, 2p, \ldots, p^\alpha - 1 \tag{3.1}$$

számok közül p^α-hoz (azaz p-hez) relatív prímek számát. Sokkal könnyebb meghatározni (3.1)-ből azon elemeket, amelyek nem relatív prímek p-hez. Ezek ugyanis a

$$0, p, 2p, \ldots, (p^{\alpha-1} - 1)p$$

számok és számuk $p^{\alpha-1}$. Ezért

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1 - \frac{1}{p}\right).$$

Ha $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ $(\alpha_i \geq 1)$, akkor

$$\varphi(m) = \prod_{i=1}^{r} \varphi\left(p_i^{\alpha_i}\right) = \prod_{i=1}^{r}\left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right) = \prod_{i=1}^{r} p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right) =$$

$$= m\prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right).$$

Példaként határozzuk meg $\varphi(100)$ értékét:

$$\varphi(100) = \varphi(2^2 5^2) = \varphi(2^2)\varphi(5^2) = \left(2^2 - 2^1\right)\left(5^2 - 5^1\right) = 40.$$

Most térjünk vissza a redukált maradékrendszerek vizsgálatára.

3.9. Tétel. *Az $r_1, r_2, \ldots, r_k$ egész számok akkor és csak akkor alkotnak modulo m redukált reprezentánsrendszert, ha $k = \varphi(m)$, $r_i \not\equiv r_j \pmod{m}$ minden $1 \le i < j \le \varphi(m)$-re és $(r_i, m) = 1$ minden $1 \le i \le \varphi(m)$-re.*

Bizonyítás. A redukált maradékrendszer és a φ függvény definíciója alapján az állítás nyilvánvaló. ∎

Ha már adott egy modulo m redukált reprezentánsrendszer, akkor abból újabb nyerhető a következő tétel szerint.

3.10. Tétel. *Ha $\{r_1, r_2, \ldots, r_{\varphi(m)}\}$ modulo m redukált reprezentánsrendszer és $(c, m) = 1$, akkor*

$$\{cr_1, cr_2, \ldots, cr_{\varphi(m)}\} \tag{3.2}$$

szintén redukált reprezentánsrendszer modulo m.

Bizonyítás. Mivel (3.2)-ben az elemek száma $\varphi(m)$, így a 3.9. Tétel szerint csak azt kell bizonyítani, hogy (3.2) elemei páronként inkongruensek és a modulushoz relatív prímek. Felhasználva, hogy $(c, m) = 1$ és $(r_i, m) = 1$ $(i = 1, \ldots, \varphi(m))$, kapjuk a $(cr_i, m) = 1$ egyenlőséget (lásd 1.16. Tétel). (3.2) elemeinek páronkénti inkongruenciája indirekt módon könnyen bizonyítható. ∎

A számelméleti bizonyításokban és feladatokban nagyon gyakran alkalmazzuk az alábbi, úgynevezett *Euler—Fermat-tételt*.

3.11. Tétel. *Ha $a \in \mathbf{Z}$ és $(a, m) = 1$, akkor*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Bizonyítás. Legyen $\{r_1, r_2, \ldots, r_{\varphi(m)}\}$ modulo m redukált maradékrendszer. Az előző tétel szerint, $(a, m) = 1$ miatt $\{ar_1, ar_2, \ldots, ar_{\varphi(m)}\}$ is modulo m redukált maradékrendszer. Így minden redukált maradékosztályból pontosan két reprezentánsunk van, az egyik az $\{r_1, r_2, \ldots, r_{\varphi(m)}\}$, a másik az $\{ar_1, ar_2, \ldots, ar_{\varphi(m)}\}$ reprezentánsrendszerből. Ezek a reprezentánspárok természetesen kongruensek modulo m, és így

$$ar_1 ar_2 \cdots ar_{\varphi(m)} \equiv r_1 r_2 \cdots r_{\varphi(m)} \pmod{m},$$

amelyből $(r_1 r_2 \cdots r_{\varphi(m)}, m) = 1$ miatt az

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

kongruenciát nyerjük. ∎

Ha $m = p$ prímszám, akkor az Euler—Fermat-tétel speciális esetét kapjuk, melyet *kis Fermat-tételnek* is szokás nevezni.

3.12. Tétel. *Legyen p prímszám. Ha $(a, p) = 1$, akkor*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Külön is érdemes kiemelni, hogy a kis Fermat-tétel a következő alakban is megfogalmazható.

3.13. Tétel. *Bármely a egész és p prímszámra*

$$a^p \equiv a \pmod{p}.$$

Bizonyítás. Ha $(a, p) = 1$, akkor $\varphi(p) = p - 1$ miatt az Euler—Fermat-tétel szerint

$$a^{p-1} \equiv 1 \pmod{p}.$$

E kongruenciát a-val szorozva kapjuk, hogy

$$a^p \equiv a \pmod{p}.$$

Ha $(a, p) \neq 1$, azaz $p \mid a$, akkor $a \equiv 0 \pmod{p}$, így $a^p \equiv 0 \pmod{p}$, ezért az

$$a^p \equiv a \pmod{p}$$

kongruencia most is teljesül. ∎

A továbbiakban tekintsük a $(\mathbf{Z}/_{(m)}, +, \cdot)$ faktorstruktúrát, ahol az összeadás, illetve a szorzás műveletek szokásos definíciója:

$$\overline{a} + \overline{b} = \overline{a + b}, \quad \text{illetve} \quad \overline{a}\overline{b} = \overline{ab},$$

ahol $\overline{a}, \overline{b} \in \mathbf{Z}/_{(m)}$.

3.14. Tétel. *A $(\mathbf{Z}/_{(m)}, +, \cdot)$ struktúra egységelemes kommutatív gyűrű.*

Bizonyítás. Ismeretes, illetve könnyen ellenőrizhető, hogy az

$$f\colon \mathbf{Z} \to \mathbf{Z}/_{(m)}, \quad f(a) = \overline{a}$$

leképezés epimorfizmus a $(\mathbf{Z}, +, \cdot)$ integritástartomány és a $(\mathbf{Z}/_{(m)}, +, \cdot)$ faktorstruktúra között, és így $(\mathbf{Z}/_{(m)}, +, \cdot)$ egységelemes kommutatív gyűrű. ∎

A zérusosztómentesség általában nem igaz, ugyanakkor bizonyos m-ekre $(\mathbf{Z}/_{(m)}, +, \cdot)$ test. Az alábbi művettáblázatokból könnyen leolvasható, hogy például a $(\mathbf{Z}/_{(4)}, +, \cdot)$ gyűrűben a $\overline{2}$ zérusosztó, míg a $(\mathbf{Z}/_{(3)}, +, \cdot)$ test.

$(\mathbf{Z}/_{(4)}, +, \cdot)$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

;

$(\mathbf{Z}/_{(3)}, +, \cdot)$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

.

A redukált maradékosztályok $P(m)$-mel jelölt halmazára igaz az alábbi tétel.

3.15. Tétel. *A $(P(m), \cdot)$ struktúra kommutatív csoport.*

Bizonyítás. Először bebizonyítjuk, hogy ha $\overline{r_1}, \overline{r_2} \in P(m)$, akkor $\overline{r_1} \cdot \overline{r_2} \in P(m)$, azaz a szorzás nem vezet ki $P(m)$-ből. Mivel $(r_1, m) = (r_2, m) = 1$, ezért az 1.16. Tétel szerint $(r_1 r_2, m) = 1$, azaz $\overline{r_1} \cdot \overline{r_2} \in P(m)$. A szorzás kommutativitása, asszociativitása és $\overline{1} \in P(m)$ nyilván teljesül $(m \geq 2)$, ezért már csak azt kell bizonyítani, hogy bármely $\overline{r} \in P(m)$-nek van inverze $P(m)$-ben. Ha $\overline{r} \in P(m)$, azaz $(r, m) = 1$, akkor léteznek olyan x_0, y_0 egész számok, amelyekre

$$rx_0 + my_0 = 1. \tag{3.3}$$

Ebből kapjuk, hogy $rx_0 \equiv 1 \pmod{m}$, azaz $\overline{r} \cdot \overline{x_0} = \overline{1}$. $\overline{x_0} \in P(m)$, mert ellenkező esetben $(x_0, m) = d > 1$, és így (3.3) miatt $d \mid 1$ következne, ami nem lehetséges. ∎

3.16. Tétel. *A $(\mathbf{Z}/_{(m)}, +, \cdot)$ akkor és csak akkor test, ha m prímszám.*

Bizonyítás. A 3.14. Tétel szerint $(\mathbf{Z}/_{(m)}, +, \cdot)$ kommutatív, egységelemes gyűrű. Ha $m = p$ prímszám, akkor $P(p) = \mathbf{Z}/_{(p)} \setminus \{\overline{0}\}$. Ezért az előző tétel szerint $(\mathbf{Z}/_{(p)} \setminus \{\overline{0}\}, \cdot)$ csoport, azaz $(\mathbf{Z}/_{(p)}, +, \cdot)$ test.

Ha m nem prímszám, akkor $m = m_1 m_2$, ahol $2 \leq m_i < m$ $(i = 1, 2)$. Ekkor a $(\mathbf{Z}/_{(m)}, +, \cdot)$ gyűrű nem lehet test, mert például az $\overline{m_1} \in \mathbf{Z}/_{(m)}$-nek

nincs multiplikatív inverze. Ellenkező esetben létezne olyan $\overline{m_3} \in \mathbf{Z}/_{(m)}$, amelyre $\overline{m_1} \cdot \overline{m_3} = \overline{1}$, azaz

$$m_1 m_3 \equiv 1 \pmod{m}, \quad \text{és így} \quad m_1 m_3 + m y_0 = 1 \tag{3.4}$$

valamely $y_0 \in \mathbf{Z}$ esetén. De (3.4)-ből, $m_1 \mid m_1 m_3$ és $m_1 \mid m$ miatt, $m_1 \mid 1$ következne, amely $2 \leq m_1$ miatt lehetetlen. ∎

Eddig, ha azt akartuk eldönteni, hogy az $m \geq 2$ egész szám prímszám-e, akkor az 1.26. Tétel alapján megnéztük, hogy m osztható-e valamely, a $2 \leq p \leq \sqrt{m}$ feltételt kielégítő p prímszámmal. Most egy, a kongruenciák segítségével megfogalmazott prímkritériumot, a Wilson-tételt bizonyítjuk be.

3.17. Tétel. *Az $m \geq 2$ egész szám akkor és csak akkor prímszám, ha*

$$(m-1)! \equiv -1 \pmod{m}.$$

Bizonyítás. Először megmutatjuk, hogy ha m összetett, akkor

$$(m-1)! \not\equiv -1 \pmod{m}.$$

Legyen $m = m_1 m_2$, ahol $2 \leq m_i < m$ $(i = 1, 2)$, és tegyük fel, hogy

$$(m-1)! \equiv -1 \pmod{m}.$$

Ekkor, $m_1 \mid m$ miatt, $(m-1)! \equiv -1 \pmod{m_1}$ is igaz lenne. Ez viszont lehetetlen, mivel $(m-1)! \equiv 0 \pmod{m_1}$.

A második lépésben megmutatjuk, hogy bármely $m = p$ prímszámra

$$(p-1)! \equiv -1 \pmod{p}.$$

Ha $p = 2$ vagy 3, akkor $(2-1)! = 1 \equiv -1 \pmod{2}$, illetve $(3-1)! = 2 \equiv -1 \pmod{3}$ miatt igaz az állítás. Legyen a továbbiakban $p \geq 5$. Mivel a 3.15. Tétel szerint $(P(p), \cdot)$ csoport, ezért bármely $\overline{r} \in P(p)$-nek létezik inverze $P(p)$-ben. Az $\overline{1} \cdot \overline{1} = \overline{1}$, illetve $\overline{(p-1)} \cdot \overline{(p-1)} = \overline{p^2 - 2p + 1} = \overline{1}$ miatt az $\overline{1}$ és $\overline{p-1}$ inverze önmaga. Ugyanakkor bármely $\overline{1}$-től és $\overline{p-1}$-től különböző $\overline{r} \in P(p)$ inverze nem lehet önmaga, mivel ellenkező esetben $\overline{r} \cdot \overline{r} = \overline{1}$, illetve $r^2 \equiv 1 \pmod{p}$, azaz

$$p \mid (r-1)(r+1).$$

De ekkor p prímszám volta miatt $p \mid r-1$ vagy $p \mid r+1$, amely $2 \leq \leq r \leq p-2$ miatt lehetetlen. Ezek alapján — az inverzpárok szorzatát $\overline{1}$-gyel helyettesítve —

$$\overline{(p-1)!} = \overline{1} \cdot \overline{2} \cdot \overline{3} \cdots \overline{(p-1)} = \overline{1} \cdot \overline{1} \cdots \overline{1} \cdot \overline{p-1},$$

azaz

$$(p-1)! \equiv p-1 \equiv -1 \pmod{p}. \quad \blacksquare$$

Valamivel többet mond az alábbi tétel.

3.18. Tétel. *Legyen $m \geq 2$ egész szám. Ekkor*

$$(m-1)! \equiv \begin{cases} 2 \pmod{m}, & \text{ha} \quad m = 4, \\ 0 \pmod{m}, & \text{ha} \quad m \text{ összetett és } m \neq 4, \\ -1 \pmod{m}, & \text{ha} \quad m \text{ prímszám.} \end{cases}$$

Bizonyítás. Ha $m = 4$, akkor $(4-1)! = 6 \equiv 2 \pmod{4}$. Abban az esetben, ha m összetett és $4 < m \neq p^2$ (ahol $p \geq 3$ prímszám), akkor $m = m_1 m_2$ valamely $2 \leq m_1 < m_2 < m$-re és ezért

$$(m-1)! = 1 \cdot 2 \cdots m_1 \cdots m_2 \cdots (m-1) \equiv 0 \pmod{m}.$$

Ha $m = p^2$ és $p \geq 3$ prímszám, akkor $3 \leq p < 2p < p^2 - 1$ miatt

$$(m-1)! = (p^2-1)! = 1 \cdot 2 \cdots p \cdots 2p \cdots (p^2-1) \equiv 0 \pmod{m}.$$

Ha $m = p$ prímszám, akkor a Wilson-tételből adódik az állítás. $\blacksquare$

Feladatok

1. Határozzuk meg x $(0 \leq x \leq 20)$ értékét, ha

$$(850^{70} + 19^{32})^{16} \equiv x \pmod{21}.$$

2. Határozzuk meg x $(0 \leq x \leq 99)$ értékét, ha

$$1311^{1241} \equiv x \pmod{100}.$$

3. Bizonyítsuk be, hogy $n \in \mathbf{N} \setminus \{0\}$ esetén

$$5^n \mid (2^{5^n - 5^{n-1}} - 1).$$

4. Bizonyítsuk be, hogy minden $n \in \mathbf{N}$ esetén

$$320 \mid (81^{(81^{80}-1)n} - 1).$$

5. Igazoljuk, hogy

$$(k_1 + k_2 + \cdots + k_n)^p \equiv k_1^p + k_2^p + \cdots + k_n^p \pmod{p},$$

ahol p prímszám és $k_i \in \mathbf{Z}$ $(1 \leq i \leq n)$.

6. Bizonyítsuk be, hogy ha p és q különböző prímek, akkor

$$pq \mid (n^{pq} - n^p - n^q + n)$$

igaz minden $n \in \mathbf{Z}$-re.

7. Igazoljuk, hogy ha $7 \mid (n^{6k} + n^{6l})$, akkor $7 \mid n$, ahol $k, l, n \in \mathbf{N} \setminus \{0\}$.

8. Bizonyítsuk be, hogy ha n páratlan természetes szám, akkor

$$n \mid (2^{n!} - 1).$$

9. Bizonyítsuk be, hogy $5 \mid (1^n + 2^n + 3^n + 4^n)$ akkor és csak akkor, ha $4 \nmid n$, ahol $n \in \mathbf{N}$.

10. Legyen p kettőtől és öttől különböző prímszám, továbbá jelölje n_p, illetve s_p azt a legkisebb pozitív egész számot, amelyekre

$$10^{n_p} \equiv 1 \pmod{p}, \quad \text{illetve} \quad 10^{s_p} \equiv -1 \pmod{p}.$$

Ezen kongruenciák segítségével igazoljunk oszthatósági szabályokat a tízes számrendszerben felírt pozitív egészek p-vel való oszthatóságára.

11. Legyen A a tízes számrendszerben felírt 4444^{4444} szám számjegyeinek összege, továbbá A számjegyeinek összege B, B számjegyeinek összege C. Határozzuk meg C értékét.

12. Bizonyítsuk be, hogy ha $m \mid b$, akkor

$$(m+1)^b \equiv 1 \pmod{m^2},$$

ahol $m, b \in \mathbf{N}$.

13. Legyen $p > 2$ prímszám. Határozzuk meg x és y értékét, ha

$$\binom{2p}{p} \equiv x \pmod{p} \quad \text{és} \quad \binom{2p}{p} \equiv y \pmod{p^2},$$

ahol $0 \leq x \leq p-1$ és $0 \leq y \leq p-1$.

14. Bizonyítsuk be, hogy $m \geq 2$ esetén

$$\left((m!)^{m!} - 1, (2m)!\right) = \prod_{m<p<2m} p,$$

ahol p prím.

15. Határozzuk meg x $(0 \leq x \leq p-1)$ értékét, ha

$$\frac{(p-1)!}{p-2} \equiv x \pmod{p},$$

ahol $p > 2$ prímszám.

16. Bizonyítsuk be, hogy ha $p > 2$ prímszám, akkor

$$p^2 \mid ((2p-1)! - p).$$

17. Bizonyítsuk be, hogy ha $p > 2$ prímszám, akkor

$$p^p \mid ((p^2-1)! - p^{p-1}).$$

18. Legyen $p > 2$ prímszám. Igazoljuk, hogy

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

19. Legyen $p > 2$ prímszám és a $(1 \leq a \leq p-1)$ egész szám. Bizonyítsuk be, hogy

$$(-1)^{a-1} a \frac{1}{p}\binom{p}{a} \equiv 1 \pmod{p}.$$

20. Bizonyítsuk be, hogy az $m \geq 2$ természetes szám akkor és csak akkor prímszám, ha

$$(m-2)! \equiv 1 \pmod{m}.$$

21. Legyen $\{r_1, r_2, \ldots, r_{\varphi(m)}\}$ egy redukált maradékrendszer modulo m. Bizonyítsuk be, hogy

$$(r_1 r_2 \cdots r_{\varphi(m)})^2 \equiv 1 \pmod{m}.$$

4. Pszeudoprím számok

Mostanában, például kódolási és dekódolási problémákkal kapcsolatban, sokan foglalkoznak prímtesztekkel, azaz olyan eljárásokkal, melyekkel eldönthető egy természetes számról, hogy prím vagy összetett. Az eddigi ismereteink alapján egy n pozitív egészről eldönthetjük, hogy prímszám-e, ha megvizsgáljuk, hogy van-e $\sqrt{n}$-nél nem nagyobb prímosztója. Ha nincs, akkor n prím. Nagy számok esetén azonban ez az eljárás túl hosszú, és néha még számítógép segítségével is kivitelezhetetlen. Sokáig azt gondolták, hogy az Euler—Fermat-, illetve a kis Fermat-tétel megfordítása hatékonyabb módszert szolgáltat.

A kis Fermat-tétel alapján tudjuk, hogy

$$n \mid (2^{n-1}-1), \quad \text{azaz} \quad 2^{n-1} \equiv 1 \pmod{n}, \tag{4.1}$$

ha n egy páratlan prím. Több évszázadon keresztül azt gondolták, hogy a fordítottja is igaz, vagyis hogy ha a (4.1) oszthatóság fennáll, akkor n prímszám. Először Sarrus talált erre egy ellenpéldát 1819-ben, megmutatta, hogy $n = 341 = 11 \cdot 31$ összetett szám, de kielégíti (4.1)-et. Sarrus korában ezt a számot megtalálni nem lehetett könnyű, de az állítás bizonyítása n ismeretében már egyszerű, hiszen

$$2^{341-1} = \left(2^{10}\right)^{34} \equiv 1^{34} = 1 \pmod{11}$$

és

$$2^{341-1} = \left(2^{5}\right)^{68} \equiv 1^{68} = 1 \pmod{31},$$

így valóban igaz, hogy

$$2^{340} \equiv 1 \pmod{341}.$$

Tehát a kis Fermat-tétel nem alkalmas egy egész szám prímvoltának egyértelmű eldöntésére, mert ha (4.1) teljesül, akkor még nem biztos, hogy n prímszám. Sarrus óta már igen sok (4.1)-et kielégítő összetett számot találtak.

Definíció. Ha egy n pozitív egész összetett és kielégíti (4.1)-et, akkor pszeudoprím (majdnem prím) számnak nevezzük.

Felmerül a kérdés, hogy a pszeudoprímek száma véges-e vagy végtelen. A következő tételből és a Sarrus által megtalált pszudoprímből következik ezen számok számának végtelensége.

4.1. Tétel. (Sierpinski, 1947) *Ha n egy pszeudoprím szám, akkor 2^n-1 is pszeudprím.*

Bizonyítás. Legyen n egy pszeudoprím szám és legyen $N = 2^n - 1$. Ekkor

$$2^{N-1} - 1 = 2^{2\left(2^{n-1}-1\right)} - 1.$$

Mivel n pszeudoprím, így $n \mid \left(2^{n-1} - 1\right)$, ezért

$$2^{N-1} - 1 = 2^{nq} - 1 = (2^n - 1)\, Q = NQ,$$

ahol $q, Q > 1$ egészek. Tehát $N \mid \left(2^{N-1} - 1\right)$. Emellett N összetett is. Ugyanis n pszeudoprím, tehát összetett, így $n = rs$-ből

$$N = 2^n - 1 = 2^{rs} - 1 = (2^r - 1)\left(2^{r(s-1)} + 2^{r(s-2)} + \cdots + 1\right)$$

következik. ∎

A tételből már adódik, hogy végtelen sok pszeudoprím létezik. Láttuk, hogy $n_1 = 341$ pszeudoprím. De akkor a tétel alapján $n_2 = 2^{n_1} - 1$ is az, és nyilván $n_2 > n_1$. Folytatva az eljárást, pszeudoprímek egy végtelen, szigorúan monoton növekvő sorozatát kapjuk.

Megjegyezzük, hogy Lehmer ennél többet bizonyított. Megmutatta, hogy az x-nél nem nagyobb pszeudoprímek száma nagyobb, mint $c \log x$, ahol $c > 0$ egy valós szám, hacsak x elég nagy, azaz létezik olyan c és x_0 pozitív valós szám, hogy minden $x > x_0$ valós számra az x-nél nem nagyobb pszeudoprímek száma nagyobb, mint $c \log x$.

A XVII. század első felében Fermat azt állította, hogy az $F_n = 2^{2^n} + 1$ alakú számok, mai elnevezés szerint a Fermat-számok, prímszámok minden $n \geq 0$ esetén. Könnyű ellenőrizni, hogy F_0, F_1, F_2, F_3 és F_4 valóban prímszám. Euler azonban bizonyította, hogy F_5 összetett, vagyis Fermat sejtése nem igaz. Azóta még számítógéppel sem sikerült az első öt Fermat-számon kívül olyat találni, amely prím. Fermatnak azonban annyiban igaza volt, hogy ha F_n nem prím, akkor majdnem prím.

4.2. Tétel. *Ha $n \geq 0$ egy természetes szám és*

$$F_n = 2^{2^n} + 1$$

nem prím, akkor pszeudoprím.

Bizonyítás. Legyen n egy természetes szám. Ekkor

$$2^{F_n-1} - 1 = 2^{2^{2^n}} - 1 = \left(2^{2^n}\right)^{2^{2^n-n}} - 1,$$

ahol $2^n - n \geq 1$ és így 2^{2^n} kitevője páros. Ezért $2^{F_n - 1} - 1$ osztható $2^{2^n} + 1 = F_n$-nel, és így F_n prím, vagy pszeudoprím. ∎

A továbbiakban még fogunk találkozni az $M_n = 2^n - 1$ alakú Mersenne-számokkal. Nyilvánvaló, hogy M_n csak akkor lehet prím, ha n prímszám. A fordítottja azonban nem igaz, ha n egy prímszám, nem biztos, hogy M_n is prím (pl. $M_{11} = 2047 = 23 \cdot 89$ összetett). Igaz viszont a következő tétel.

4.3. Tétel. *Legyen $p > 2$ egy prímszám. Ekkor*

$$M_p = 2^p - 1$$

vagy prím, vagy pszeudoprím.

Bizonyítás. Ha p egy páratlan prím, akkor

$$2^{M_p - 1} - 1 = 2^{2\left(2^{p-1} - 1\right)} - 1,$$

ahol a kis Fermat-tétel miatt $p \mid \left(2^{p-1} - 1\right)$. Ezért $2^{M_p - 1} - 1$ alakja $(2^p)^q - 1$, és így osztható $2^p - 1 = M_p$-vel. Tehát, ha M_p nem prím, úgy pszeudoprím. ∎

A pszeudoprímek számának végtelenségét bizonyítja a következő tétel is.

4.4. Tétel. *Végtelen sok olyan pszeudoprímszám létezik, mely pontosan két különböző páratlan prímszám szorzata.*

Bizonyítás. A bizonyításban felhasználjuk a Mersenne-számok egy tulajdonságát. Ha p egy páratlan prím és $p \mid (2^n - 1)$ $(n > 1)$, de $p \nmid (2^m - 1)$ ha $0 < m < n$, akkor p-t $2^n - 1$ egy primitív prímosztójának nevezzük. Zsigmondi egy 1892-ben bizonyított általánosabb tételéből következik, hogy ha $n > 6$, akkor a $2^n - 1$ Mersenne-számnak van primitív prímosztója.

Ha p egy primitív prímosztója $(2^n - 1)$-nek, akkor $n \mid (p - 1)$. Ugyanis ha $p - 1 = nq + r (0 \leq r < n)$, akkor a kis Fermat-tétel alapján

$$1 \equiv 2^{p-1} \equiv (2^n)^q 2^r \equiv 2^r \pmod{p},$$

ami csak $r = 0$ esetén nem mond ellent annak, hogy p a $2^n - 1$ primitív prímosztója. Hasonlóan látható be, hogy ha q egy prímszám, akkor $2^q - 1$ minden prímosztója primitív.

Legyen $r > 6$ egy prímszám és legyen p egy primitív prímosztója $2^r - 1$-nek. Ekkor az előzőek alapján $r \mid (p - 1)$, továbbá $r < p - 1$ és $p - 1 > 6$ is következik. Legyen q egy olyan prím, mely $2^{p-1} - 1$-nek egy primitív

prímosztója. Zsigmondi előbb említett tétele alapján ilyen q létezik, és q $k\,(p-1)+1$ alakú, ezenkívül $q \neq p$. De ekkor

$$2^{pq-1} = 2^{(p-1)q} 2^{q-1} = 2^{(p-1)q} 2^{k(p-1)}$$

miatt, q definíciója és a kis Fermat-tétel alapján

$$2^{pq-1} \equiv 1 \pmod{p} \quad \text{és} \quad 2^{pq-1} \equiv 1 \pmod{q},$$

vagyis $pq \mid 2^{pq-1}-1$ adódik. Tehát pq pszeudoprím. Különböző $r > 6$ prímek különböző p, q prímeket határoznak meg, így a pq alakú pszeudoprímek száma valóban végtelen. ∎

Megemlítjük, hogy az előző eredménynél több is igaz. Erdős Pál bizonyította 1949-ben, hogy tetszőleges $s > 1$ pozitív egész esetén végtelen sok olyan pszeudoprím létezik, mely pontosan s különböző páratlan prím szorzata.

A pszeudoprím számok természetes általánosítása a következő. Legyen $a \geq 2$ egy természetes szám. Ha n egy összetett pozitív egész és

$$n \mid (a^{n-1} - 1),$$

akkor pszeudoprímnek nevezzük a vonatkozásában. A következő tételből az következik, hogy minden $a \geq 2$ esetén végtelen sok a vonatkozású pszeudoprím létezik.

4.5. Tétel. (Cippola, 1904) *Ha $a \geq 2$ pozitív egész és $p > 2$ egy prím, melyre $p \nmid \left(a^2-1\right)$, akkor*

$$n = \frac{a^{2p}-1}{a^2-1}$$

pszeudoprím a vonatkozásában.

Bizonyítás. Tegyük fel, hogy a és p eleget tesz a tétel feltételeinek. Ekkor

$$a^{n-1} - 1 = a^{\frac{a^{2p}-1}{a^2-1}-1} - 1 = a^{\frac{a^2\left(a^{2(p-1)}-1\right)}{a^2-1}} - 1, \tag{4.2}$$

ahol a kitevő egész, hiszen az $a^{2q}-1$ alakú számok oszthatók $\left(a^2-1\right)$-gyel. Az $a^{2(p-1)}-1$ egész osztható p-vel a kis Fermat-tétel miatt. Továbbá (4.2)-ben az a kitevője páros. Ez nyilvánvaló, ha a páros. Ha pedig a páratlan, akkor

$$\frac{a^2}{a^2-1}\left(a^{2(p-1)}-1\right) = \frac{a^2}{a^2-1}\left(a^2-1\right)\left(\left(a^2\right)^{p-2} + \left(a^2\right)^{p-3} + \cdots + \left(a^2\right)^0\right) =$$
$$= a^2\left(a^{2(p-2)} + a^{2(p-3)} + \cdots + a^{2\cdot 0}\right)$$

miatt páros a kitevő, hiszen a legutolsó zárójelben $p-1$, azaz páros számú páratlan tag összege szerepel. Ezek szerint $a^{n-1}-1$ alakja $a^{2pk}-1$, ahol $q>k$ ezért $a^{n-1}-1$ osztható $a^{2p}-1$-gyel és így $\frac{a^{2p}-1}{a^2-1}$-gyel is. Még azt kell belátni, hogy n összetett. Ez abból következik, hogy az

$$a^{2p}-1=(a^p-1)\,(a^p+1)$$

szorzatban mindkét tényező nagyobb mint a^2-1, ezért n-nek létezik valódi faktorizációja. ∎

A pszeudoprímeknek többféle általánosítása ismert. Például az n összetett természetes számot szuper pszeudoprímnek nevezzük, ha minden osztója prím vagy pszeudoprím. Bizonyítható (Szymiczek, 1966), hogy F_nF_{n+1} szuper pszeudoprím, ahol $n>1$ és F_i az i-edik Fermat-szám.

A pszeudoprímeken alapuló prímteszteknél zavaró, hogy léteznek olyan n összetett számok, melyek minden n-hez relatív prím $a\geq 2$ vonatkozásában pszeudprímek. Ezeket abszolút pszeudoprímeknek vagy Carmichael-számoknak nevezzük, közülük a legkisebb $n=561=3\cdot 11\cdot 17$. A számelmélet egyik legjelentősebb új eredménye ezekre a számokra vonatkozik. Alford, Granville és Pomerance 1994-ben bizonyították, hogy végtelen sok abszolút pszeudoprím létezik. Sőt azt is megmutatták, hogy egy pozitív x valós számnál nem nagyobb abszolút pszeudoprímek száma nagyobb mint $x^{\frac{2}{7}}$, ha x elég nagy.

Feladatok

1. Legyen $n=pq$, ahol p és q különböző páratlan prímek. Legyen továbbá k az a legkisebb pozitív egész, melyre $n\mid(2^k-1)$. Bizonyítsuk be, hogy ha $k\mid(n-1)$, akkor n pszeudoprím, és a $p-1$, $q-1$ számok oszthatók k-val.

2. Bizonyítsuk be, hogy ha p és q különböző prímek, melyekre

$$p\mid(2^{q-1}-1)\quad\text{és}\quad q\mid(2^{p-1}-1),$$

akkor $n=pq$ pszeudoprím.

3. Bizonyítsuk be, hogy ha m és $a\geq 2$ pozitív egészek, m pszeudoprím a vonatkozásában és $(m,a-1)=1$, akkor $\frac{a^m-1}{a-1}$ is pszeudoprím a vonatkozásában.

4. Bizonyítsuk be, hogy ha p egy páratlan prím és $a>2$ egy természetes szám, melyre $p\nmid(a-1)$, akkor $\frac{a^p-1}{a-1}$ pszeudoprím a vonatkozásában.

5. Legyen $F_n = 2^{2^n} + 1$ az n-edik Fermat-szám. Bizonyítsuk be, hogy F_n is és F_nF_{n+1} $(n > 4)$ is szuper pszeudoprím, azaz minden összetett osztójuk pszeudoprím. (Használjuk ki azt az ismert tényt, hogy F_n minden prímosztója, és így minden osztója $k2^{n+2} + 1$ alakú.)

6. Bizonyítsuk be, hogy ha n három különböző páratlan prím szorzata, és minden p prímtényezőjére $(p-1) \mid (n-1)$, akkor n abszolút pszeudoprím.

7. Bizonyítsuk be, hogy 561 abszolút pszeudoprím.

8. Bizonyítsuk be, hogy ha p egy $40k+3$ alakú prím, továbbá $5(p-1)+1$ és $8(p-1)+1$ is prímek, akkor e három prím szorzata abszolút pszeudoprím.

5. Algebrai kongruenciák

Az algebrai egyenletekhez hasonlóan definiáljuk az algebrai kongruenciákat.

DEFINÍCIÓ. Legyen $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbf{Z}[x]$. Az $f(x)$ polinom modulo m foka n, ha $a_n \not\equiv 0 \pmod{m}$. Ha $a_n \equiv a_{n-1} \equiv \equiv \cdots \equiv a_0 \equiv 0 \pmod{m}$, akkor az $f(x)$ polinomnak nem tulajdonítunk modulo m fokot.

DEFINÍCIÓ. Legyen $f(x)$ egy modulo m n-edfokú ($n \geq 1$), egész együtthatós polinom. Az

$$f(x) \equiv 0 \pmod{m} \tag{5.1}$$

kongruenciát n-edfokú egyismeretlenes algebrai kongruenciának nevezzük.

DEFINÍCIÓ. Az x_0 egész számot (5.1) megoldásának nevezzük, ha

$$f(x_0) \equiv 0 \pmod{m}.$$

5.1. TÉTEL. *Ha x_0 megoldása* (5.1)*-nek, akkor az $\overline{x_0}$ maradékosztály minden eleme megoldása* (5.1)*-nek.*

BIZONYÍTÁS. Mivel x_0 megoldás, ezért

$$f(x_0) = a_n x_0^n + a_{n-1}x_0^{n-1} + \cdots + a_1 x_0 + a_0 \equiv 0 \pmod{m}. \tag{5.2}$$

Legyen $x_1 \in \overline{x_0}$. Képezve az $f(x_1) - f(x_0)$ különbséget, az

$$f(x_1) - f(x_0) = a_n(x_1^n - x_0^n) + a_{n-1}(x_1^{n-1} - x_0^{n-1}) + \cdots + a_1(x_1 - x_0)$$

egyenlőséget kapjuk, amelyből $x_1^k \equiv x_0^k \pmod{m}$ $(1 \leq k \leq n)$ miatt

$$f(x_1) - f(x_0) \equiv 0 \pmod{m},$$

azaz (5.2)-vel az

$$f(x_1) \equiv 0 \pmod{m}$$

kongruencia következik. ∎

A fenti tétel alapján bevezetjük a (lényegesen) különböző megoldás fogalmát.

Definíció. Az (5.1) kongruencia x_1 és x_2 megoldását (lényegesen) különbözőnek nevezzük, ha $x_1 \not\equiv x_2 \pmod{m}$. Az (5.1) kongruencia megoldásainak számán az inkongruens megoldások számát értjük.

Az algebrai kongruenciák megoldásánál — hasonlóan az algebrai egyenletekhez — fontos a következő fogalom.

Definíció. Az $f(x) \equiv 0 \pmod{m_1}$ és a $g(x) \equiv 0 \pmod{m_2}$ algebrai kongruenciát ekvivalensnek nevezzük, ha ugyanazon egész számok a megoldásaik (persze ezek a számok más-más maradékosztályba tartozhatnak modulo m_1, illetve modulo m_2 szerint).

Lineáris kongruenciák és lineáris kongruenciarendszerek

Definíció. Az $ax \equiv b \pmod{m}$ algebrai kongruenciát, ahol

$$a \not\equiv 0 \pmod{m},$$

lineáris kongruenciának nevezzük.

A lineáris kongruenciák megoldhatóságáról és a megoldások számáról szól a következő tétel.

5.2. Tétel. *Az $ax \equiv b \pmod{m}$ lineáris kongruencia akkor és csak akkor oldható meg, ha $(a, m) = d \mid b$, továbbá ha megoldható, akkor az inkongruens megoldások száma d. Ha x_0 egy konkrét megoldás, akkor az összes különböző (inkongruens) megoldás:*

$$x_0,\ x_0 + \frac{m}{d},\ x_0 + 2\frac{m}{d}, \ldots,\ x_0 + (d-1)\frac{m}{d}.$$

Bizonyítás. Legyen először $(a, m) = d = 1$. Az Euler—Fermat-tétel alapján behelyettesítéssel ellenőrizhetjük, hogy az

$$x_0 = ba^{\varphi(m)-1}$$

egész szám megoldása az $ax \equiv b \pmod{m}$ kongruenciának, ugyanis

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

miatt

$$ax_0 = aba^{\varphi(m)-1} = ba^{\varphi(m)} \equiv b \pmod{m}.$$

(Az 1.2. és az 1.12. Tétel alapján a megoldhatóság kérdése az $1 = (a, m) = = ax_n + my_n$ lineáris kombinációkénti előállíthatóságból is bizonyítható, mivel ebben az esetben $ax_n \equiv 1 \pmod{m}$, és így $a(bx_n) \equiv b \pmod{m}$. Azaz, $x_0 = bx_n$ egy konkrét megoldás.)

A megoldás egyértelműségét indirekt úton igazoljuk. Tegyük fel, hogy x_1 és x_2 két inkongruens megoldás, azaz

$$ax_1 \equiv b \pmod{m} \quad \text{és} \quad ax_2 \equiv b \pmod{m}, \tag{5.3}$$

ahol $x_1 \not\equiv x_2 \pmod{m}$. (5.3)-ból kapjuk, hogy $ax_1 \equiv ax_2 \pmod{m}$, amelyből $(a, m) = 1$ miatt $x_1 \equiv x_2 \pmod{m}$ következik, ami ellentmond a feltételnek. Ez az ellentmondás bizonyítja a megoldás egyértelműségét.

Legyen a továbbiakban $(a, m) = d > 1$, és foglalkozzunk először a tétel szükséges részének a bizonyításával. Ha x_0 egy megoldás, azaz $ax_0 \equiv b \pmod{m}$, akkor létezik olyan $y_0 \in \mathbf{Z}$, amelyre

$$ax_0 + my_0 = b.$$

De ebből $d \mid a$ és $d \mid m$ miatt $d \mid b$ következik.

A tétel elégséges részének a bizonyításához tegyük fel, hogy $d \mid b$. Megmutatjuk, hogy az

$$ax \equiv b \pmod{m} \tag{5.4}$$

és az

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}} \tag{5.5}$$

kongruenciák ekvivalensek. Legyen például x_0 megoldása (5.4)-nek, azaz $ax_0 \equiv b \pmod{m}$, melyből d-vel osztva kapjuk, hogy

$$\frac{a}{d}x_0 \equiv \frac{b}{d} \pmod{\frac{m}{d}},$$

tehát x_0 megoldása (5.5)-nek. Legyen most x_0' megoldása (5.5)-nek, azaz

$$\frac{a}{d}x_0' \equiv \frac{b}{d} \pmod{\frac{m}{d}}.$$

Ebből akalmas $c \in \mathbf{Z}$-vel az

$$\frac{a}{d}x_0' - \frac{b}{d} = c\frac{m}{d},$$

majd d-vel szorozva az

$$ax_0' - b = cm$$

egyenlőséget kapjuk, amely ekvivalens az $ax_0' \equiv b \pmod{m}$ kongruenciával. Tehát x_0' valóban megoldása (5.4)-nek. Ugyanakkor (5.5)-nek,

$$\left(\frac{a}{d}, \frac{m}{d}\right) = 1$$

miatt, az előzőek alapján pontosan egy inkongruens megoldása van modulo $\frac{m}{d}$, azaz ha x_0 megoldása (5.5)-nek, akkor az (5.5)-öt és az ekvivalencia miatt (5.4)-et is kielégítő összes x egész számra

$$x = x_0 + k\frac{m}{d}, \quad k \in \mathbf{Z}. \tag{5.6}$$

Megmutatjuk, hogy az (5.6)-beli egészek bármelyike kongruens az

$$x_0, x_0 + \frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d} \tag{5.7}$$

egészek valamelyikével az m modulusra nézve. Ehhez k-t maradékosan osztva d-vel kapjuk, hogy $k = dq + r$ $(0 \leq r \leq d-1)$, és így

$$x = x_0 + k\frac{m}{d} = x_0 + (dq + r)\frac{m}{d} = x_0 + r\frac{m}{d} + qm \equiv x_0 + r\frac{m}{d} \pmod{m}.$$

A tétel teljes bizonyításához még meg kell mutatni, hogy az (5.7)-beli egészek páronként inkongruensek modulo m. Tegyük fel, hogy létezik olyan i és j, amelyekre $0 \leq i < j \leq d-1$ és

$$x_0 + i\frac{m}{d} \equiv x_0 + j\frac{m}{d} \pmod{m}.$$

Ebből kapjuk, hogy

$$m \mid \frac{m}{d}(j-i),$$

ami $1 \leq j - i \leq d-1$ miatt lehetetlen. Ezzel tételünk minden állítását bebizonyítottuk. ∎

Megjegyezzük, hogy konkrét lineáris kongruencia megoldásakor is célszerű az előző tétel bizonyításában leírtakat alkalmazni. Példaként oldjuk meg a következő kongruenciát:

$$6x \equiv 9 \pmod{15}. \tag{5.8}$$

Mivel $(6, 15) = 3 \mid 9$, ezért (5.8) megoldható. Az (5.8)-cal ekvivalens kongruencia $2x \equiv 3 \pmod 5$, amelynek egyetlen megoldása $x_0 \equiv 4 \pmod 5$. Így (5.8) inkongruens megoldásai: $x_0 = 4$, $x_1 = 4+5 = 9$, $x_2 = 4+2\cdot 5 = 14$.

A továbbiakban lineáris kongruenciarendszerekkel foglalkozunk.

Definíció. Legyen $n > 1$ és tekintsük az

$$\left.\begin{aligned} a_1 x &\equiv b_1 \pmod{m_1} \\ a_2 x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ a_n x &\equiv b_n \pmod{m_n} \end{aligned}\right\} \tag{5.9}$$

kongruenciákat. A kongruenciák ezen rendszerét lineáris kongruenciarendszernek (illetve szimultán kongruenciáknak) nevezzük. Egy x_0 egész számot a kongruenciarendszer megoldásának nevezzük, ha $a_i x_0 \equiv b_i \pmod{m_i}$ minden $1 \le i \le n$ esetén. A megoldásokat szokás szimultán megoldásoknak nevezni.

E definíció alapján (5.9) megoldhatóságának szükséges feltétele, hogy az $a_i x \equiv b_i \pmod{m_i}$ kongruencia minden $1 \le i \le n$-re megoldható legyen. Ezért, ha egyenként megoldjuk az (5.9)-beli kongruenciákat (feltéve, hogy megoldhatók voltak), akkor mindegyikből $x \equiv c_i \pmod{m_i}$ alakú kongruenciá(ka)t kapunk, és így (5.9) helyett elegendő az

$$\left.\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_n \pmod{m_n} \end{aligned}\right\} \tag{5.10}$$

típusú lineáris kongruenciarendszer szimultán megoldásaival foglalkozni.

5.3. Tétel. *Az*

$$\left.\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \end{aligned}\right\} \tag{5.11}$$

lineáris kongruenciarendszernek akkor és csak akkor létezik szimultán megoldása, ha $d = (m_1, m_2) \mid (c_1 - c_2)$. *Ha* (5.11) *megoldható, akkor a megoldás modulo* $[m_1, m_2]$*-re nézve egyértelmű.*

Bizonyítás. Ha (5.11) megoldható, akkor létezik olyan x_0 egész szám, amelyre

$$m_1 \mid (x_0 - c_1) \quad \text{és} \quad m_2 \mid (x_0 - c_2).$$

De ebből $d = (m_1, m_2) \mid m_i$ $(i = 1, 2)$ miatt

$$d \mid (x_0 - c_1) \quad \text{és} \quad d \mid (x_0 - c_2),$$

amiből pedig $d \mid (c_1 - c_2)$ következik.

A bizonyítás második részében tegyük fel, hogy $d \mid (c_1 - c_2)$. Az $x \equiv c_1 \pmod{m_1}$ kongruencia nyilván megoldható és a megoldások

$$x = c_1 + km_1 \quad (k \in \mathbf{Z})$$

alakúak. Behelyettesítve ezt az $x \equiv c_2 \pmod{m_2}$ kongruenciába, az

$$x = c_1 + km_1 \equiv c_2 \pmod{m_2}, \tag{5.12}$$

majd ezt átrendezve az

$$m_1 k \equiv c_2 - c_1 \pmod{m_2},$$

illetve a vele ekvivalens

$$\frac{m_1}{d} k \equiv \frac{c_2 - c_1}{d} \pmod{\frac{m_2}{d}}$$

kongruenciát kapjuk. Az 5.2. Tétel szerint, $\left(\frac{m_1}{d}, \frac{m_2}{d}\right) = 1$ miatt az utóbbinak egyetlen k_0 inkongruens megoldása van modulo $\frac{m_2}{d}$, ezért minden megoldás

$$k = k_0 + t\frac{m_2}{d} \quad (t \in \mathbf{Z}) \tag{5.13}$$

alakú. Így (5.12)-ből és (5.13)-ból (5.11) szimultán megoldásai:

$$x = c_1 + \left(k_0 + t\frac{m_2}{d}\right) m_1 = c_1 + k_0 m_1 + t\frac{m_1 m_2}{d} \equiv c_1 + k_0 m_1 \mod \big([m_1, m_2]\big).$$

Mivel k_0 egyértelműen meghatározott volt modulo $\frac{m_2}{d}$-re nézve, ezért ezzel a megoldás egyértelműsége is bizonyított. (Természetesen külön, indirekt módon is könnyen igazolható az egyértelműség.) ∎

Az előző tétel $n \geq 2$ esetén is megfogalmazható.

5.4. Tétel. *Az* (5.10) *lineáris kongruenciarendszernek pontosan akkor van szimultán megoldása, ha* $(m_i, m_j) \mid c_i - c_j$ *minden* $1 \leq i < j \leq n$*-re. Ha* (5.10) *megoldható, akkor a megoldás modulo* $[m_1, m_2, \ldots, m_n]$*-re nézve egyértelmű.*

Bizonyítás. A bizonyítást nem részletezzük, teljes indukcióval elvégezhető. ∎

Példaként oldjuk meg az alábbi kongruenciarendszert:

$$\left.\begin{aligned} x &\equiv 3 \pmod 5 \\ x &\equiv 4 \pmod 6 \\ x &\equiv 2 \pmod 4 \end{aligned}\right\}.$$

A megoldhatóság feltétele teljesül, és az első kongruencia összes megoldása $x = 3 + 5t$ $(t \in \mathbf{Z})$. Ezt a másodikba helyettesítve kapjuk, hogy

$$3 + 5t \equiv 4 \pmod 6,$$

amelyet megoldva $t \equiv -1 \pmod 6$, azaz $t = -1 + 6u$ $(u \in \mathbf{Z})$ adódik. Ezért az első két kongruenciából álló rendszer megoldása

$$x = 3 + 5t = 3 + 5(-1 + 6u) = -2 + 30u \quad (u \in \mathbf{Z}).$$

Most ezt behelyettesítve az $x \equiv 2 \pmod 4$ kongruenciába kapjuk, hogy

$$-2 + 30u \equiv 2 \pmod 4,$$

melyet megoldva $u \equiv 0 \pmod 2$, azaz $u = 2j$ $(j \in \mathbf{Z})$. Ezt is felhasználva a keresett megoldás:

$$x = -2 + 30u = -2 + 60j \quad (j \in \mathbf{Z}), \quad \text{vagyis} \quad x \equiv -2 \pmod{60}.$$

Az (5.9) alakú kongruenciarendszer megoldásával kapcsolatos az úgynevezett *kínai maradéktétel.*

5.5. Tétel. *Ha* (5.9)*-ben az* $m_1, m_2, \ldots, m_n$ *modulusok páronként relatív prímek, továbbá* $(a_i, m_i) = 1$ *minden* $1 \leq i \leq n$*-re, akkor* (5.9) *tetszőleges* b_i $(1 \leq i \leq n)$ *egészek esetén megoldható, és a megoldás modulo* $m_1 m_2 \cdots m_n$*-re nézve egyértelmű.*

Bizonyítás. Az itt közölt bizonyítás előnye, hogy szintén algoritmikus jellegű, azaz konkrét feladatok megoldásánál is alkalmazható. (Ez az oka,

hogy nem az 5.4. Tétel speciális eseteként idézzük.) Tekintsük (5.9) helyett az alábbi kongruenciarendszert:

$$\left.\begin{array}{rl} a_1 m_1' y \equiv b_1 & (\mathrm{mod}\ m_1) \\ a_2 m_2' y \equiv b_2 & (\mathrm{mod}\ m_2) \\ \vdots & \\ a_n m_n' y \equiv b_n & (\mathrm{mod}\ m_n) \end{array}\right\}, \tag{5.14}$$

ahol $m_i' = \frac{\prod_{j=1}^{n} m_j}{m_i}$ $(i = 1, 2, \ldots, n)$. Mivel $(a_i m_i', m_i) = 1$ $(i = 1, 2, \ldots, n)$ ezért (5.14) minden kongruenciája megoldható. Legyenek a kongruenciák megoldásai rendre $y_1, y_2, \ldots, y_n$. Megmutatjuk, hogy az

$$x_0 = \sum_{i=1}^{n} m_i' y_i$$

egész szám szimultán megoldása (5.9)-nek. Ehhez helyettesítsük x_0-t (5.9) i-edik $(i = 1, 2, \ldots, n)$ kongruenciájába. Ekkor kapjuk, hogy

$$\begin{aligned} a_i x_0 &= a_i m_1' y_1 + \cdots + a_i m_i' y_i + \cdots + a_i m_n' y_n \equiv \\ &\equiv 0 + \cdots 0 + b_i + 0 + \cdots + 0 = b_i \pmod{m_i}, \end{aligned}$$

hiszen m_k' definíciója miatt $m_i \mid m_k'$ ha $i \neq k$ és (5.14) alapján $a_i m_i' y_i \equiv b_i \pmod{m_i}$. Ebből már következik, hogy x_0 valóban szimultán megoldása (5.9)-nek.

Az egyértelműségre vonatkozó részt indirekt úton bizonyítjuk. Tegyük fel, hogy x_1 és x_2 szimultán megoldása (5.9)-nek, de

$$x_1 \not\equiv x_2 \qquad (\mathrm{mod}\ m_1 m_2 \cdots m_n),$$

azaz

$$\left.\begin{array}{rl} a_1 x_1 \equiv b_1 & (\mathrm{mod}\ m_1) \\ a_2 x_1 \equiv b_2 & (\mathrm{mod}\ m_2) \\ \vdots & \\ a_n x_1 \equiv b_n & (\mathrm{mod}\ m_n) \end{array}\right\} \quad \text{és} \quad \left.\begin{array}{rl} a_1 x_2 \equiv b_1 & (\mathrm{mod}\ m_1) \\ a_2 x_2 \equiv b_2 & (\mathrm{mod}\ m_2) \\ \vdots & \\ a_n x_2 \equiv b_n & (\mathrm{mod}\ m_n) \end{array}\right\}.$$

Az azonos sorokban lévő kongruenciák kivonásával kapjuk, hogy

$$\begin{aligned} a_1(x_1 - x_2) &\equiv 0 \pmod{m_1} \\ a_2(x_1 - x_2) &\equiv 0 \pmod{m_2} \\ &\vdots \\ a_n(x_1 - x_2) &\equiv \pmod{m_n}. \end{aligned}$$

Mivel $(a_i, m_i) = 1$ minden $1 \leq i \leq n$-re, ezért

$$\begin{aligned} x_1 &\equiv x_2 \pmod{m_1} \\ x_1 &\equiv x_2 \pmod{m_2} \\ &\vdots \\ x_1 &\equiv x_2 \pmod{m_n}, \end{aligned}$$

amelyből a 3.2. Tétel (c) pontja és $[m_1, m_2, \ldots, m_n] = m_1 m_2 \cdots m_n$ miatt $x_1 \equiv x_2 \pmod{m_1 m_2 \cdots m_n}$ következik. Ez ellentmond az indirekt feltevésünknek, ezért a tétel állítása igaz. ∎

A tételben leírt megoldási algoritmus illusztrálására oldjuk meg a következő kongruenciarendszert:

$$\left.\begin{aligned} 3x &\equiv 4 \pmod{5} \\ 5x &\equiv 6 \pmod{7} \\ 6x &\equiv 8 \pmod{11} \end{aligned}\right\}. \tag{5.15}$$

A kongruenciarendszer kielégíti a kínai maradéktétel feltételeit, tehát megoldható. A tételbeli jelöléseket használva:

$$m_1' = 7 \cdot 11 = 77, \quad m_2' = 5 \cdot 11 = 55 \quad \text{és} \quad m_3' = 5 \cdot 7 = 35.$$

A külön-külön megoldandó kongruenciák és megoldásaik:

$$\begin{aligned} 3 \cdot 77y &\equiv 4 \pmod{5}, & y_1 &\equiv 2 \pmod{5}, \\ 5 \cdot 55y &\equiv 6 \pmod{7}, & y_2 &\equiv 3 \pmod{7}, \\ 6 \cdot 35y &\equiv 8 \pmod{11}, & y_3 &\equiv 8 \pmod{11}. \end{aligned}$$

Így (5.15) egyetlen szimultán megoldása modulo $5 \cdot 7 \cdot 11 = 385$:

$$x_0 = 77 \cdot 2 + 55 \cdot 3 + 35 \cdot 8 \equiv -17 \pmod{385}.$$

Magasabb fokú kongruenciák

Tekintsük az

$$f(x) \equiv 0 \pmod{m} \tag{5.16}$$

n-edfokú ($n \geq 1$) algebrai kongruenciát. Annak eldöntésére, hogy (5.16) megoldható-e, illetve a megoldások tényleges meghatározására mindig alkalmazható egy véges algoritmus, tudniillik a modulo m egy teljes reprezentánsrendszerének (5.16)-ba való helyettesítése. Persze, nagy n és m esetén ez még számítógéppel is sok munkát igényel. Ezért célszerű olyan eljárást keresni, amellyel csökkenthető a modulus, illetve a kongruencia fokszáma. Ezt az alábbi, úgynevezett redukciós eljárásokkal érjük el.

1. Az együtthatók redukciója. (5.16)-ban valamennyi együtthatót helyettesítjük a vele kongruens legkisebb abszolút értékű egésszel. Ezzel elérhető, hogy az

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod{m}$$

kongruenciában az a_i együtthatóra $|a_i| \leq \frac{m}{2}$ $(0 \leq i \leq n)$. A továbbiakban (5.16) már legyen ilyen alakú.

2. A modulus redukciója. Legyen az $m(\geq 2)$ modulus kanonikus alakja

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r},$$

ahol $1 \leq \alpha_i$ $(1 \leq i \leq r)$. Megmutatjuk, hogy (5.16) és az

$$\left.\begin{aligned} f(x) &\equiv 0 \pmod{p_1^{\alpha_1}} \\ f(x) &\equiv 0 \pmod{p_2^{\alpha_2}} \\ &\vdots \\ f(x) &\equiv 0 \pmod{p_r^{\alpha_r}} \end{aligned}\right\} \tag{5.17}$$

kongruenciarendszer ekvivalens. Ugyanis, ha x_0 megoldása (5.16)-nak, azaz $f(x_0) \equiv 0 \pmod{m}$, akkor $p_i^{\alpha_i} \mid m$ $(1 \leq i \leq r)$ miatt x_0 megoldása (5.17)-nek is. Ha pedig egy x_0' megoldása (5.17)-nek, akkor megoldása az $f(x) \equiv 0 \pmod{m}$ kongruenciának is (lásd: 3.2. Tétel (c) pontja). Ha (5.17)-ben az $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ $(i = 1, 2, \ldots, r)$ kongruenciákat külön-külön megoldjuk (feltéve, hogy megoldhatók), és a megoldásokat c_i-vel jelöljük, akkor

(5.17) egy szimultán megoldását az

$$\left.\begin{aligned} x &\equiv c_1 \pmod{p_1^{\alpha_1}} \\ &\vdots \\ x &\equiv c_r \pmod{p_r^{\alpha_r}} \end{aligned}\right\} \tag{5.18}$$

lineáris kongruenciarendszer szimultán megoldása adja. Természetes, hogy (5.17) összes megoldását megkapjuk, ha megoldjuk az összes, az előbbiek szerint előálló (5.18) típusú lineáris kongruenciarendszert. (Ha az $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ kongruenciának j_i darab megoldása van, akkor összesen $j_1 j_2 \cdots j_r$ darab (5.18) típusú kongruenciarendszert kell megoldani.) De az 5.4. Tétel szerint, az (5.18) típusú kongruenciarendszerek mindig megoldhatók (lévén $(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$ minden $1 \leq i < j \leq r$-re), ezért (5.17) megoldhatósága és a megoldások előállítása attól függ, hogy az

$$f(x) \equiv 0 \pmod{p_i^{\alpha_i}} \tag{5.19}$$

kongruenciák megoldhatók-e, és ha igen, akkor meg tudjuk-e adni az összes megoldását. Ezzel (5.16)-ot visszavezettük olyan kongruenciák megoldhatóságának vizsgálatára és tényleges megoldására, ahol a modulus egyetlen prímszám hatványa.

Foglalkozzunk tehát az

$$f(x) \equiv 0 \pmod{p^\alpha} \tag{5.20}$$

típusú kongruenciákkal, ahol p prímszám és $\alpha \geq 2$ egész szám. (5.20) x' megoldásait a modulus miatt célszerű

$$x' = x_0 + x_1 p + x_2 p^2 + \cdots + x_{\alpha-1} p^{\alpha-1} \tag{5.21}$$

alakban keresni. Feladatunk az $x_0, x_1, \ldots, x_{\alpha-1}$ egészek meghatározása. Ha (5.21) megoldása (5.20)-nak, akkor

$$\begin{aligned} f(x') = a_n(x_0 + x_1 p + \cdots + x_{\alpha-1} p^{\alpha-1})^n + \cdots + \\ + a_1(x_0 + x_1 p + \cdots + x_{\alpha-1} p^{\alpha-1}) + a_0 \equiv 0 \pmod{p^\alpha}, \end{aligned}$$

amelyből $f(x') \equiv a_n x_0^n + a_{n-1} x_0^{n-1} + \cdots + a_1 x_0 + a_0 \equiv 0 \pmod{p}$, azaz

$$f(x_0) \equiv 0 \pmod{p}$$

következik. Így látható, hogy (5.21)-ben x_0 az

$$f(x) \equiv 0 \pmod{p} \tag{5.22}$$

kongruencia megoldása. Vegyük észre, hogy (5.22) már prímmodulusú kongruencia.

Legyen a továbbiakban x_0 egy lehetséges megoldása (5.22)-nek és határozzuk meg ezen x_0 esetén az (5.21)-beli x_1-et. Nyilvánvaló, hogy ebben az esetben $\alpha \geq 2$ és $f(x') \equiv 0 \pmod{p^\alpha}$-ból $f(x') \equiv 0 \pmod{p^2}$ következik. A binomiális tétel alkalmazásával ekkor

$$\begin{aligned} 0 \equiv f(x') &= f(x_0 + x_1 p + \cdots + x_{\alpha-1} p^{\alpha-1}) \equiv \\ &\equiv f(x_0 + x_1 p) = f(x_0) + x_1 p g_1(x_0) \pmod{p^2}, \end{aligned} \tag{5.23}$$

ahol $g_1(x)$ egy alkalmas egész együtthatós polinom, és így $g_1(x_0)$ egy egész szám. Mivel $f(x_0) \equiv 0 \pmod{p}$, azaz $p \mid f(x_0)$, ezért (5.23)-ból kapjuk, hogy

$$\frac{f(x_0)}{p} + g_1(x_0) x_1 \equiv 0 \pmod{p}. \tag{5.24}$$

Ez utóbbi szerint x_1 egy, a levezetésből adódó konkrét prímmodulusú lineáris kongruencia megoldása (feltéve, hogy megoldható).

Legyen a továbbiakban x_1 egy lehetséges megoldása (5.24)-nek és határozzuk meg az eddig ismert x_0 és x_1 egészekhez a (5.21)-beli x_2-t. Nyilvánvaló, hogy ebben az esetben $\alpha \geq 3$ és $f(x') \equiv 0 \pmod{p^\alpha}$-ból $f(x') \equiv 0 \pmod{p^3}$ következik. Ekkor

$$\begin{aligned} 0 \equiv f(x') &= f(x_0 + x_1 p + \cdots + x_{\alpha-1} p^{\alpha-1}) \equiv f(x_0 + x_1 p + x_2 p^2) = \\ &= f(x_0 + x_1 p) + x_2 p^2 g_2(x_0 + x_1 p) \pmod{p^3}, \end{aligned} \tag{5.25}$$

ahol $g_2(x)$ egy alkalmas egész együtthatós polinom. Mivel $f(x_0 + x_1 p) \equiv 0 \pmod{p^2}$, azaz $p^2 \mid f(x_0 + x_1 p)$, ezért (5.25)-ből kapjuk, hogy

$$\frac{f(x_0 + x_1 p)}{p^2} + g_2(x_0 + x_1 p) x_2 \equiv 0 \pmod{p}.$$

Látható tehát, hogy x_2 is egy, a levezetésből adódó konkrét prímmodulusú lineáris kongruencia megoldása (feltéve, hogy létezik megoldás).

Módszerünket hasonlóan folytatva, prímmodulusú lineáris kongruenciák megoldásaiként megkapjuk az $x_3, x_4, \ldots, x_{\alpha-1}$ egészeket is.

Összegezve az eddigieket láthatjuk, hogy az $f(x) \equiv 0 \pmod{p^\alpha}$ kongruencia megoldását visszavezettük az $f(x) \equiv 0 \pmod{p}$, illetve egy sor lineáris kongruencia megoldására. (Természetesen, ha az $f(x) \equiv 0 \pmod{p}$ nem oldható meg, vagy ha az eljárásban szereplő valamely x_i mint megoldás nem létezik, akkor az $f(x) \equiv 0 \pmod{p^\alpha}$ kongruencia nem oldható meg.)

Foglalkozzunk most az $f(x) \equiv 0 \pmod{p}$ típusú kongruenciákkal, ugyanis ekkor a kis Fermat-tétel segítségével a fokszám redukciója is lehetséges.

3. A fokszám redukciója. Legyen p egy prímszám és

$$f(x) \equiv 0 \pmod{p}$$

egy legalább p-edfokú kongruencia, azaz,

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod{p}, \tag{5.26}$$

ahol $a_n \not\equiv 0 \pmod{p}$ és $n \geq p$. Legyen továbbá $i(\geq p)$ egy egész szám. Ekkor a maradékos osztás tétele (lásd 1.1. Tétel) szerint létezik olyan k_i és r_i egész szám, amelyekre $i = k_i p + r_i$, ahol $0 \leq r_i \leq p-1$. Mivel $i \geq p \geq 2$ miatt $k_i \geq 1$, ezért

$$i = k_i p + r_i \geq k_i 2 + r_i > k_i + r_i. \tag{5.27}$$

Tudjuk továbbá, hogy a kis Fermat-tétel szerint $x^p \equiv x \pmod{p}$ bármely $x \in \mathbf{Z}$-re ezért, ha $i \geq p$, akkor

$$x^i = x^{k_i p + r_i} = (x^p)^{k_i} x^{r_i} \equiv x^{k_i + r_i} \pmod{p}.$$

Ez utóbbi szerint az (5.26) kongruenciában x^i $(i \geq p)$ mindig helyettesíthető $x^{k_i + r_i}$-vel, ahol (5.27) szerint $k_i + r_i < i$. Ha $k_i + r_i \geq p$, akkor újabb maradékos osztással — hasonlóan az előbbihez — tovább csökkentjük a kitevőt. Mindaddig alkalmazzuk ezt az eljárást, amíg a kitevő nem lesz kisebb, mint p. Ha ezt az algoritmust alkalmazzuk (5.26) minden olyan $a_i x^i$ tagjára, ahol $i \geq p$, akkor látható, hogy (5.26) ekvivalens az

$$f_1(x) = b_{p-1}x^{p-1} + b_{p-2}x^{p-2} + \cdots + b_1 x + b_0 \equiv 0 \pmod{p} \tag{5.28}$$

legfeljebb $(p-1)$-edfokú, vagy az azonosan nulla ($b_{p-1} \equiv b_{p-2} \equiv \cdots \equiv b_1 \equiv \equiv b_0 \equiv 0 \pmod{p}$) kongruenciával, ahol a b_i $(i = 0, 1, \ldots, p-1)$ együtthatók az előbbi eljárásból és az azonos fokú tagok összevonásából adódnak.

Megjegyezzük, hogy ha az (5.28) kongruenciában $p > 2$ és $b_0 \not\equiv 0 \pmod{p}$, azaz $x \equiv 0 \pmod{p}$ nem megoldása (5.28)-nak, akkor — a kis Fermat-tétel $x^{p-1} \equiv 1 \pmod{p}$ alakja szerint — (5.28) tovább redukálható egy legfeljebb $(p-2)$-edfokú kongruenciára.

Az (5.26)-beli prímmodulusú kongruenciák inkongruens megoldásainak számára vonatkozik az alábbi, úgynevezett fokszámtétel.

5.6. Tétel. *Az $f(x) \equiv 0 \pmod{p}$ prímmodulusú n-edfokú kongruenciának legfeljebb n inkongruens megoldása van (ellenkező esetben $f(x)$ azonosan nulla polinom modulo p).*

Bizonyítás. A bizonyítást a fokszámra nézve teljes indukcióval végezzük. Ha a fokszám egy, akkor (5.26)

$$ax + b \equiv 0 \pmod{p}$$

alakú, ahol $a \not\equiv 0 \pmod{p}$. A lineáris kongruenciáknál tanultak szerint (lásd 5.2. Tétel) ennek pontosan egy inkongruens megoldása van, azaz $n = 1$-re igaz a tétel állítása. Tegyük fel, hogy a legfeljebb $n - 1 (\geq 1)$-edfokú prímmodulusú kongruenciáknak legfeljebb $n - 1$ inkongruens megoldásuk van, és bizonyítsuk az állítást n-re. Azokra az $f(x) \equiv 0 \pmod{p}$ n-edfokú kongruenciákra, amelyek nem oldhatók meg, igaz az állítás. Legyen most az $f(x) \equiv 0 \pmod{p}$ n-edfokú kongruencia megoldható, azaz létezzen olyan $x_1 \in \mathbf{Z}$, amelyre

$$f(x_1) \equiv 0 \pmod{p}. \tag{5.29}$$

Képezve az $f(x) - f(x_1)$ különbséget kapjuk, hogy

$$f(x) - f(x_1) = a_n(x^n - x_1^n) + a_{n-1}(x^{n-1} - x_1^{n-1}) + \cdots + a_1(x - x_1),$$

azaz,

$$f(x) - f(x_1) = (x - x_1)g(x),$$

ahol $g(x)$ egy alkalmas egész együtthatós polinom, melynek foka $n - 1$. Tekintsük az

$$f(x) - f(x_1) \equiv (x - x_1)g(x) \pmod{p}$$

kongruenciát, amely (5.29) miatt

$$f(x) \equiv (x - x_1)g(x) \pmod{p} \tag{5.30}$$

alakban is írható. Ha az $f(x) \equiv 0 \pmod{p}$ kongruenciának lenne $n + 1$ inkongruens megoldása, akkor (5.30) és p prím volta miatt a

$$g(x) \equiv 0 \pmod{p}$$

kongruenciának is lenne n inkongruens megoldása, de a $g(x) \equiv 0 \pmod{p}$ egy $(n-1)$-edfokú kongruencia, és így ellentmondásra jutnánk az indukciós feltevésünkkel. ∎

Megemlítjük, hogy a fokszámtétel következményeként egy újabb bizonyítást adhatunk a Wilson-tétel (lásd 3.17. Tétel) elégséges feltételére.

Definiáljuk az $f(x)$ polinomot a következő módon:

$$f(x) = x^{p-1} - 1 - (x-1)(x-2)\cdots(x-(p-1)),$$

és tekintsük az

$$f(x) \equiv 0 \pmod{p} \tag{5.31}$$

kongruenciát, ahol $p > 2$ prímszám. A kis Fermat-tétel alapján látható, hogy (5.31) inkongruens megoldásai az

$$1, 2, 3, \ldots, p-1$$

számok, holott az (5.31) kongruencia fokszáma $p-2$, mert a szorzások és összevonások elvégzése után x^{p-1} együtthatója 0. Ezért a fokszámtétel szerint (5.31)-nek azonosan nulla kongurenciának kell lennie, azaz (5.31)-ben az $f(x)$ minden együtthatója osztható p-vel. Így pl. $f(x)$ konstans tagja is. De (5.31)-ben $f(x)$ konstans tagja $-1 + (-1)^p(p-1)!$, és ezért

$$-1 + (-1)^p(p-1)! \equiv 0 \pmod{p}.$$

Ebből $p > 2$, azaz p páratlan volta miatt kapjuk, hogy

$$(p-1)! \equiv -1 \pmod{p}.$$

($p = 2$ esetén most is $(2-1)! = 1 \equiv -1 \pmod{2}$ miatt igaz az állítás.)

Az előzőekben láttuk, hogy minden p prímmodulusú kongruencia redukálható egy legfeljebb $(p-1)$-edfokúra, továbbá ha a nulla nem megoldás, akkor egy legfeljebb $(p-2)$-edfokú kongruenciára is. Ha a nulla megoldás, akkor ezt a későbbiekben kizárva, szintén lehetséges egy maximum $(p-2)$-edfokúra való redukció. Ezért elegendő a maximum $(p-2)$-edfokú p prímmodulusú kongruenciák megoldhatóságával foglalkozni. Ezzel kapcsolatos a következő — Kőnig Gyulától és Rados Gusztávtól származó — bizonyítás nélkül közölt tétel.

5.7. Tétel. *Legyen* $f(x) = a_{p-2}x^{p-2} + \cdots + a_1x + a_0 \in \mathbf{Z}[x]$, *ahol* $a_0 \not\equiv 0 \pmod{p}$, $p > 2$ *prímszám és jelölje* M *az alábbi ciklikus mátrixot:*

$$M = \begin{pmatrix} a_{p-2} & a_{p-3} & a_{p-4} & \cdots & a_1 & a_0 \\ a_0 & a_{p-2} & a_{p-3} & \cdots & a_2 & a_1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{p-3} & a_{p-4} & a_{p-5} & \cdots & a_0 & a_{p-2} \end{pmatrix},$$

amelynek rangja legyen r. *Az*

$$f(x) \equiv 0 \pmod{p}$$

kongruencia akkor és csak akkor oldható meg, ha $\det(M) \equiv 0 \pmod{p}$, *és ha megoldható, akkor az inkongruens megoldások száma* $p - 1 - r$.

Ennek a tételnek elsősorban elméleti jelentősége van, ugyanis az M mátrix-szal kapcsolatos determináns és rangszámítás nagyon munkaigényes lehet, ugyanakkor a tényleges megoldásokat e tétel alapján nem lehet meghatározni. Ezért az esetek többségében egyszerűbb a mod p maradékosztályok egy teljes reprezentánsrendszerét behelyettesíteni az $f(x) \equiv 0 \pmod{p}$ kongruenciába, és így meghatározni a konkrét megoldásokat.

Példaként oldjuk meg az

$$f(x) = x^3 + x^2 + 2x - 2 \equiv 0 \pmod{20} \tag{5.32}$$

kongruenciát. A megoldás során a redukciós eljárásban leírtaknak megfelelően járunk el. Mivel $20 = 2^2 \cdot 5$, így (5.32) ekvivalens az

$$\left.\begin{aligned} f(x) &\equiv 0 \pmod{2^2} \\ f(x) &\equiv 0 \pmod{5} \end{aligned}\right\} \tag{5.33}$$

kongruenciarendszerrel. Foglalkozzunk az $f(x) \equiv 0 \pmod{2^2}$ és az $f(x) \equiv \equiv 0 \pmod{5}$ kongruenciák külön-külön történő megoldásával.

Az $f(x) \equiv 0 \pmod{2^2}$ kongruencia megoldását $x = x_0 + 2x_1$ alakban keressük. Az előzőek alapján tudjuk, hogy x_0 megoldása az

$$f(x) \equiv 0 \pmod{2} \tag{5.34}$$

kongruenciának. Az (5.34) $x_{0_1} = 0$ és $x_{0_2} = 1$ megoldásai egyszerű behelyettesítéssel adódnak. Ha az $x = x_0 + 2x_1$-be $x_0 = x_{0_1}$-et helyettesítünk, akkor az

$$f(x) = f(0 + 2x_1) \equiv 0 \pmod{4}$$

kongruenciát kell megoldani, hogy megkapjuk x_1-et. Ekkor

$$f(x) = f(2x_1) = 8x_1^3 + 4x_1^2 + 4x_1 - 2 \equiv 0 \pmod 4,$$

amely $-2 \not\equiv 0 \pmod 4$ miatt nem oldható meg, azaz $x_{0_1} = 0$-hoz nem létezik olyan x_1, amellyel $x = x_{0_1} + 2x_1$ megoldása lenne az $f(x) \equiv 0 \pmod{2^2}$ kongruenciának. Legyen most $x = x_{0_2} + 2x_1$ alakú, és így az

$$f(x) = f(1 + 2x_1) = 8x_1^3 + 16x_1^2 + 14x_1 + 2 \equiv 0 \pmod 4$$

kongruenciát kell megoldani. Ez ekvivalens a

$$2x_1 + 2 \equiv 0 \pmod 4,$$

illetve az

$$x_1 \equiv -1 \pmod 2$$

kongruenciával. Így az $f(x) \equiv 0 \pmod 4$ kongruencia egyetlen megoldása az

$$x = 1 + 2x_1 \equiv -1 \pmod 4.$$

Az $f(x) \equiv 0 \pmod 5$ kongruencia $x \equiv -2 \pmod 5$ egyetlen megoldását a 0, ± 1, ± 2 egészek behelyettesítésével nyerjük. Még meg kell oldani az (5.33)-mal ekvivalens

$$\left.\begin{aligned} x &\equiv -1 \pmod 4 \\ x &\equiv -2 \pmod 5 \end{aligned}\right\} \tag{5.35}$$

lineáris kongruenciarendszert. (5.35) első kongruenciájának

$$x = -1 + 4t \quad (t \in \mathbf{Z}) \tag{5.36}$$

megoldásait az (5.35) második kongruenciájába helyettesítve kapjuk, hogy

$$x = -1 + 4t \equiv -2 \pmod 5,$$

innen pedig $4t \equiv -1 \pmod 5$, azaz $t \equiv 1 \pmod 5$. Ezért $t = 1 + 5u$ $(u \in \mathbf{Z})$ alakú, melyet (5.36)-ba behelyettesítve kapjuk, hogy

$x = -1 + 4(1 + 5u) = -1 + 4 + 20u = 3 + 20u$, azaz $x \equiv 3 \pmod{20}$ az (5.32) kongruencia megoldása.

Binom kongruenciák

Az algebrai egyenletek megoldásánál láttuk, hogy az úgynevezett binom egyenletek megoldhatóságára és a megoldások számára vonatkozó kérdések teljes egészében tisztázhatók. Teljesen hasonló a helyzet az alábbi binom kongruenciák esetén.

Definíció. Az

$$ax^k \equiv b \pmod{m} \tag{5.37}$$

kongruenciát, ahol $a \not\equiv 0 \pmod{m}$ és $k \in \mathbf{N}^+$, k-adfokú binom kongruenciának nevezzük.

Az $y = x^k$ helyettesítéssel (5.37)-ből az $ay \equiv b \pmod{m}$ lineáris kongruenciát kapjuk, amelynek az 5.2. Tétel szerint akkor és csak akkor van megoldása, ha $(a, m) = d \mid b$, és ekkor a megoldások az

$$\frac{a}{d}y \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

kongruencia megoldásaival azonosak. Ez utóbbi y_0 megoldását könnyen felírhatjuk az Euler—Fermat-tétel segítségével, ugyanis $\left(\frac{a}{d}, \frac{m}{d}\right) = 1$ miatt

$$y_0 \equiv \frac{b}{d}\left(\frac{a}{d}\right)^{\varphi\left(\frac{m}{d}\right)-1} \pmod{\frac{m}{d}}.$$

Ebből látható, hogy (5.37) helyett elegendő az

$$x^k \equiv y_0 \pmod{m}, \tag{5.38}$$

típusú kongruenciákkal foglalkozni, amelyek megoldása, mint azt az előző részben láttuk, lényegében prímmodulusú kongruenciák megoldására vezethető vissza. Ezek közül is a legegyszerűbbek az $m = p$ és $y_0 = 1$ esetben kapott

$$x^k \equiv 1 \pmod{p}, \tag{5.39}$$

prímmodulusú binomkongruenciák, ahol feltehető, hogy $1 \leq k \leq p - 1$.

Mivel (5.39) nyilvánvalóan megoldható, azaz létezik olyan $a \in \mathbf{Z}$, amelyre $(a, p) = 1$ és $a^k \equiv 1 \pmod{p}$, például $x = 1$, ezért bevezethetjük a következő fogalmat.

Definíció. Legyen $(a,p)=1$ és p prímszám. Azt a legkisebb pozitív k egész számot, amelyre $a^k \equiv 1 \pmod{p}$, az a egész szám rendjének nevezzük modulo p. (Azt is szokták mondani, hogy a a k kitevőhöz tartozik modulo p.)

5.8. Tétel. *Legyen a rendje k modulo p.*

(a) *Ha* $a^n \equiv 1 \pmod{p}$, *akkor* $k \mid n$ $(n \in \mathbf{N})$;

(b) $k \mid (p-1)$;

(c) *ha* $i,j \in \mathbf{N}$, *úgy* $a^i \equiv a^j \pmod{p}$, *akkor* $i \equiv j \pmod{k}$.

Bizonyítás. Az (a) rész bizonyításában n-et maradékosan osztva k-val kapjuk, hogy

$$n = kq + r, \quad \text{ahol} \quad q, r \in \mathbf{N} \quad \text{és} \quad 0 \le r < k.$$

Ekkor igaz az alábbi kongruenciasor:

$$1 \equiv a^n = a^{kq+r} = (a^k)^q a^r \equiv a^r \pmod{p}.$$

Ha $0 < r < k$, akkor $a^r \equiv 1 \pmod{p}$ ellentmondana k minimális voltának, ezért $r = 0$, azaz $k \mid n$ valóban teljesül.

A (b) és (c) állítás következménye az (a) résznek, ugyanis $(a,p)=1$ esetén a kis Fermat-tétel szerint $a^{p-1} \equiv 1 \pmod{p}$, illetve például $i > j$ esetén $a^i \equiv a^j \pmod{p}$-ből $a^{i-j} \equiv 1 \pmod{p}$ következik, és így (a) miatt $k \mid i-j$. ∎

E tétellel kapcsolatban megjegyezzük, hogy a kis Fermat-tétel szerint bármely a $((a,p)=1)$ egésznek van rendje modulo p, amely nem nagyobb, mint $p-1$, továbbá a rend csak $p-1$ osztói közül kerülhet ki.

Érdemes hangsúlyozni, hogy a rend ugyancsak a maradékosztály és nem az egyes reprezentáns egyedi tulajdonsága. Erről szól az alábbi tétel.

5.9. Tétel. *Ha* $a \equiv b \pmod{p}$ *és a rendje k modulo p, akkor b rendje is k modulo p.*

Bizonyítás. Tegyük fel, hogy b rendje t és $k < t$. De $a \equiv b \pmod{p}$-ből $a^k \equiv b^k \pmod{p}$ következik, és így $a^k \equiv 1 \pmod{p}$ miatt $b^k \equiv 1 \pmod{p}$ is teljesül. Ez utóbbi viszont ellentmond annak, hogy b rendje t. Természetesen a $t < k$ feltételezéssel szintén ellentmondásra jutunk, ezért $k = t$. ∎

5.10. Tétel. *Ha a rendje k modulo p, b rendje t modulo p és $(k,t)=1$, akkor ab rendje kt modulo p.*

Bizonyítás. Az $a^k \equiv 1 \pmod{p}$ és $b^t \equiv 1 \pmod{p}$ kongruenciák miatt

$$(ab)^{tk} = a^{tk}b^{tk} = (a^k)^t(b^t)^k \equiv 1 \pmod{p},$$

azaz, ha ab rendje j modulo p, akkor az 5.8. Tétel szerint $j \mid tk$. Mivel $(k,t) = 1$ és $j \mid tk$, ezért az 1.25. Tétel szerint $j = t_1k_1$, ahol $t_1 \mid t$ és $k_1 \mid k$. Tegyük fel például, hogy $k_1 < k$. Az alábbi kongruenciák szerint

$$1 \equiv \left((ab)^j\right)^{\frac{t}{t_1}} = (ab)^{k_1t_1\frac{t}{t_1}} = a^{k_1t}(b^t)^{k_1} \equiv a^{k_1t} \pmod{p},$$

és ezért (lásd 5.8. Tétel) $k \mid k_1t$, amelyből $(k,t) = 1$ miatt a $k \mid k_1$ ellentmondás következik. Ezzel bizonyítottuk, hogy $k = k_1$. Hasonlóan nyerhető, hogy $t = t_1$, azaz ab rendje kt modulo p. ∎

5.11. Tétel. *Ha az $a_1, a_2, \ldots, a_n$ egészek rendje rendre $k_1, k_2, \ldots, k_n$ modulo p és $(k_i, k_j) = 1$ minden $1 \le i < j \le n$-re, akkor $a_1a_2\cdots a_n$ rendje $k_1k_2\cdots k_n$ modulo p.*

Bizonyítás. Az előző tételt használva, teljes indukcióval bizonyíthatunk. ∎

A továbbiak miatt fontos az alábbi, szintén a renddel kapcsolatos tétel.

5.12. Tétel. *Ha a rendje kt modulo p, akkor a^k rendje t modulo p.*

Bizonyítás. Mivel

$$(a^k)^t = a^{kt} \equiv 1 \pmod{p},$$

ezért elegendő belátni, hogy $1 \le r < t$ esetén $(a^k)^r \not\equiv 1 \pmod{p}$. Ez viszont nyilvánvaló, ellenkező esetben ugyanis

$$a^{kr} = (a^k)^r \equiv 1 \pmod{p},$$

ahol $kr < kt$, amely ellentmond a rendjének. ∎

Az 5.8. Tétel (b) része szerint egy egész szám rendje modulo p csak $p-1$ osztója lehet. Bizonyítható ennek a megfordítása is, azaz, ha $k \mid (p-1)$ $(k \ge 1)$, akkor létezik olyan a egész szám, amelyre $(a,p) = 1$, és a rendje k modulo p. Mi csak a $k = p-1$ speciális eset bizonyításával foglalkozunk.

5.13. Tétel. *Létezik olyan g egész szám, amelyre $(g,p) = 1$, és g rendje $p-1$ modulo p.*

BIZONYÍTÁS. Ha $p = 2$, akkor bármely páratlan egész szám választható g-nek, ugyanis $g = 2l + 1 \equiv 1 \pmod 2$. A továbbiakban feltesszük, hogy $p \geq 3$. Jelölje az $1, 2, \ldots, p-1$ rendjét rendre $\delta_1, \delta_2, \ldots, \delta_{p-1}$. Legyen továbbá

$$\delta = [\delta_1, \delta_2, \ldots, \delta_{p-1}],$$

és δ kanonikus alakja legyen

$$\delta = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \quad (\alpha_i \geq 1, \quad 1 \leq i \leq r).$$

Az 5.8. Tétel szerint $\delta_i \mid (p-1)$ $(1 \leq i \leq p-1)$, ezért nyilvánvaló, hogy

$$\delta = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \mid (p-1).$$

A δ legkisebb közös többszörös prímtényezős alakjából következik, hogy az $1, 2, \ldots, p-1$ egészek között léteznek olyan $b_1, b_2, \ldots, b_r$ egészek, amelyek rendje modulo p rendre $p_1^{\alpha_1} q_1, p_2^{\alpha_2} q_2, \ldots, p_r^{\alpha_r} q_r$ alakúak, ahol $q_i \mid \frac{\delta}{p_i^{\alpha_i}}$ $(1 \leq$ $\leq i \leq r)$. Az 5.12. Tétel szerint, ekkor a $b_1^{q_1}, b_2^{q_2}, \ldots, b_r^{q_r}$ rendje modulo p rendre $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_r^{\alpha_r}$. Az 5.11. Tétel szerint $\left(p_i^{\alpha_i}, p_j^{\alpha_j}\right) = 1$ $(1 \leq i <$ $< j \leq r)$ miatt $b_1^{q_1} b_2^{q_2} \cdots b_r^{q_r}$ rendje $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} = \delta$, azaz, bevezetve a $g = b_1^{q_1} b_2^{q_2} \cdots b_r^{q_r}$ jelölést

$$g^{\delta} \equiv 1 \pmod p.$$

Az 5.8. Tétel (b) része szerint ebből kapjuk, hogy

$$\delta \mid (p-1). \tag{5.40}$$

Mivel i $(1 \leq i \leq p-1)$ rendje δ_i, ezért $i^{\delta_i} \equiv 1 \pmod p$. Mindkét oldalt $\frac{\delta}{\delta_i}$ hatványra emelve kapjuk, hogy

$$\left(i^{\delta_i}\right)^{\frac{\delta}{\delta_i}} = i^{\delta} \equiv 1 \pmod p,$$

azaz $i = 1, 2, \ldots, p-1$ megoldásai az $x^{\delta} \equiv 1 \pmod p$ kongruenciának. A fokszám tétel (lásd 5.6. Tétel) szerint ekkor

$$\delta \geq p-1. \tag{5.41}$$

(5.40)-ből és (5.41)-ből $\delta = p-1$ következik, azaz a fenti g rendje $p-1$ modulo p. ∎

DEFINÍCIÓ. A g egész számot primitív gyöknek nevezzük modulo p, ha $(g, p) = 1$, és g rendje $p-1$ modulo p.

Például $p = 7$ esetén $g = 3$ primitív gyök modulo 7, mivel

$$\begin{aligned} 3^1 &\equiv 3 \pmod 7, & 3^4 &\equiv 4 \pmod 7,\\ 3^2 &\equiv 2 \pmod 7, & 3^5 &\equiv 5 \pmod 7,\\ 3^3 &\equiv 6 \pmod 7, & 3^6 &\equiv 1 \pmod 7. \end{aligned}$$

Megjegyezzük, hogy ha g primitív gyök modulo p és $g \equiv q \pmod p$, akkor az 5.9. Tétel szerint q is primitív gyök modulo p.

A primitív gyökökkel kapcsolatban nagyon fontos az alábbi tétel.

5.14. Tétel. *Ha g primitív gyök modulo p, akkor a*

$$g^0, g^1, \dots, g^{p-2} \tag{5.42}$$

egész számok redukált maradékrendszert alkotnak modulo p.

Bizonyítás. $p = 2$ esetén az állítás triviális, ezért feltesszük, hogy $p \geq 3$. A 3.9. Tétel szerint igaz az állítás, mivel az (5.42)-beli egészek száma $p-1$, relatív prímek p-hez, továbbá páronként inkongruensek modulo p. Ez utóbbit indirekt módon igazoljuk. Tegyük fel, hogy létezik olyan $0 \leq i < j \leq p-2$, amelyre $g^j \equiv g^i \pmod p$. Az 5.8. Tétel (c) része szerint ekkor $j \equiv i \pmod{p-1}$, azaz $(p-1) \mid (j-i)$. De ez ellentmondás, mivel $1 \leq j - i \leq p-2$. ∎

E tétel szerint, ha g primitív gyök modulo p és $(a,p) = 1$, akkor egyértelműen létezik egy i $(0 \leq i \leq p-2)$ természetes szám, amelyre $g^i \equiv a \pmod p$. Ez ad lehetőséget a következő definícióra.

Definíció. Legyen g primitív gyök modulo p és $(a,p) = 1$. Az a egész szám g alapú modulo p indexének nevezzük és $\operatorname{ind}_g a$-val jelöljük azt a legkisebb természetes számot, melyre

$$g^{\operatorname{ind}_g a} \equiv a \pmod p.$$

E definíció emlékezetet a logaritmus definíciójára, és ezért szokás az indexet diszkrét logaritmusnak is nevezni. A logaritmus ismert tulajdonságaihoz hasonlóak az index alábbi tulajdonságai.

5.15. Tétel. *Legyenek g és q primitív gyökök modulo p, továbbá legyen $(a,p) = (b,p) = 1$ és $k \in \mathbf{N}$. Ekkor*

(a) $\operatorname{ind}_g(ab) \equiv \operatorname{ind}_g a + \operatorname{ind}_g b \pmod{p-1}$;

(b) $\operatorname{ind}_g a^k \equiv k \operatorname{ind}_g a \pmod{p-1}$;

(c) $\operatorname{ind}_g a \equiv (\operatorname{ind}_q a)(\operatorname{ind}_g q) \pmod{p-1}$.

Bizonyítás. A bizonyítás az index definíciója alapján könnyen elvégezhető. Álljon itt például a (c) rész igazolása.

Legyen $A = \operatorname{ind}_g a$, $B = \operatorname{ind}_q a$ és $C = \operatorname{ind}_g q$. Az index definíciója szerint ekkor

$$g^A \equiv a \pmod{p}, \quad q^B \equiv a \pmod{p} \quad \text{és} \quad g^C \equiv q \pmod{p},$$

amelyből kapjuk, hogy

$$g^A \equiv a \equiv q^B \equiv g^{BC} \pmod{p}.$$

Ebből az 5.8. Tétel (c) állítása szerint $A \equiv BC \pmod{p-1}$ következik, amely a bizonyítandó állítást adja. ∎

E fejezet végén konkrét indextáblázatok találhatók, míg itt előállítjuk a $p = 7$ és $g = 3$ esetnek megfelelő táblázatot. A

$$\begin{aligned} 3^0 &\equiv 1 \pmod{7}, & 3^3 &\equiv 6 \pmod{7}, \\ 3^1 &\equiv 3 \pmod{7}, & 3^4 &\equiv 4 \pmod{7}, \\ 3^2 &\equiv 2 \pmod{7}, & 3^5 &\equiv 5 \pmod{7}, \\ & & 3^6 &\equiv 1 \pmod{7} \end{aligned}$$

kongruenciákból látható, hogy $g = 3$ valóban primitív gyök modulo 7, és az indexek is leolvashatók:

számok	1	2	3	4	5	6
indexek	0	2	1	4	5	3

indexek	0	1	2	3	4	5
számok	1	3	2	6	4	5

Adott p modulus esetén természetesen annyi indextáblázat készíthető, ahány inkongruens primitív gyök létezik modulo p. Az egyes táblázatok között az 5.15. Tétel (c) része alapján találunk kapcsolatot, ezért általában csak a legkisebb pozitív primitív gyökkel mint indexalappal szokás elkészíteni az indextáblázatokat.

Az inkongruens primitív gyökök számára vonatkozik az alábbi tétel.

5.16. Tétel. *A modulo p inkongruens primitív gyökök száma $\varphi(p-1)$.*

BIZONYÍTÁS. Legyen g primitív gyök modulo p, és tekintsük a

$$g^0, g^1, \dots, g^{p-2}$$

redukált maradékrendszert modulo p. Megmutatjuk, hogy g^i $(0 \le i \le p-2)$ akkor és csak akkor primitív gyök modulo p, ha $(i, p-1) = 1$, és így az inkongruens primitív gyökök száma valóban $\varphi(p-1)$.

Legyen először $(i, p-1) = d \ge 2$. Ekkor léteznek olyan k és t természetes számok, amelyekre $i = kd$, $p - 1 = dt$ $\quad (0 \le k \le i$ és $0 < t < p-1)$. Mivel

$$(g^i)^t = g^{kd\frac{p-1}{d}} = (g^{p-1})^k \equiv 1 \pmod{p},$$

így a t lehetséges értékei miatt g^i nem lehet primitív gyök modulo p.

Ha viszont $(i, p-1) = 1$ és

$$(g^i)^h \equiv 1 \pmod{p}$$

valamely $1 \le h \le p-2$-re, akkor g primitív gyök volta miatt $(p-1) \mid ih$. De $(i, p-1) = 1$ miatt, ebből $(p-1) \mid h$ következik, amely ellentmond az $1 \le h \le p-2$ feltételezésnek. Ezért $h \ge p-1$ és $(g^i)^{p-1} \equiv 1 \pmod{p}$ miatt g^i valóban primitív gyök modulo p. ∎

Most térjünk vissza az $x^k \equiv a \pmod{p}$ típusú kongruenciák megoldhatóságának vizsgálatára, ahol $a \in \mathbf{Z}$, $k \in \mathbf{N}^+$ és p prímszám.

5.17. TÉTEL. *Az $x^k \equiv a \pmod{p}$ $(p \nmid a)$ kongruencia akkor és csak akkor oldható meg, ha*

$$(k, p-1) \mid \operatorname{ind}_g a, \tag{5.43}$$

vagy ami ezzel ekvivalens, ha

$$a^{\frac{p-1}{(k,p-1)}} \equiv 1 \pmod{p}. \tag{5.44}$$

Ha megoldható, akkor az inkongruens megoldások száma $(k, p-1)$.

BIZONYÍTÁS. Az index definíciója szerint az $x^k \equiv a \pmod{p}$ kongruencia

$$\left(g^{\operatorname{ind}_g x}\right)^k \equiv g^{\operatorname{ind}_g a} \pmod{p}$$

alakban is írható, amelyből az 5.8. Tétel (c) része alapján kapjuk, hogy

$$k \operatorname{ind}_g x \equiv \operatorname{ind}_g a \pmod{p-1}.$$

Ez utóbbi $\operatorname{ind}_g x$-szel mint ismeretlennel egy lineáris kongruencia, amely az 5.2. Tétel szerint akkor és csak akkor oldható meg, ha $(k, p-1) \mid \operatorname{ind}_g a$, és az inkongruens megoldások száma $(k, p-1)$.

A továbbiakban elegendő megmutatni, hogy az (5.43) és az (5.44) állítások ekvivalensek. Az index és a primitív gyök definíciója miatt (5.43)-ból következik (5.44), ugyanis

$$a^{\frac{p-1}{(k,p-1)}} \equiv \left(g^{\operatorname{ind}_g a}\right)^{\frac{p-1}{(k,p-1)}} = \left(g^{p-1}\right)^{\frac{\operatorname{ind}_g a}{(k,p-1)}} \equiv 1 \pmod{p}.$$

Ha (5.44)-ből indulunk, akkor

$$1 \equiv a^{\frac{p-1}{(k,p-1)}} \equiv \left(g^{\operatorname{ind}_g a}\right)^{\frac{p-1}{(k,p-1)}} = g^{\frac{(p-1)\operatorname{ind}_g a}{(k,p-1)}} \pmod{p}.$$

Mivel g primitív gyök modulo p, ezért

$$(p-1) \;\Big|\; \frac{(p-1)\operatorname{ind}_g a}{(k,p-1)},$$

amelyből (5.43) következik. ∎

Definíció. Az a egész számot k-adik hatványmaradéknak nevezzük modulo p, ha az $x^k \equiv a \pmod{p}$ kongruencia megoldható. Ellenkező esetben nem k-adik hatványmaradéknak nevezzük modulo p.

Ezzel a definícióval az előző tétel így is megfogalmazható.

5.18. Tétel. *Legyen $p \nmid a$. Az a egész szám akkor és csak akkor k-adik hatványmaradék modulo p, ha*

$$(k, p-1) \mid \operatorname{ind}_g a,$$

vagy ami ezzel ekvivalens

$$a^{\frac{p-1}{(k,p-1)}} \equiv 1 \pmod{p}.$$

A k-adik hatványmaradékok számáról szól a következő tétel.

5.19. Tétel. *Az inkongruens k-adik hatványmaradékok száma modulo p*

$$\frac{p-1}{(k,p-1)}.$$

Bizonyítás. Az előző tétel szerint a akkor és csak akkor k-adik hatványmaradék modulo p, ha

$$a^{\frac{p-1}{(k,p-1)}} \equiv 1 \pmod{p},$$

azaz a megoldása az

$$x^{\frac{p-1}{(k,p-1)}} \equiv 1 \pmod{p}$$

kongruenciának. De ennek az 5.17. Tétel szerint

$$\left(\frac{p-1}{(k,p-1)}, p-1\right) = \frac{p-1}{(k,p-1)}$$

számú inkongruens megoldása van, azaz a k-adik hatványmaradékok száma valóban $\frac{p-1}{(k,p-1)}$. ∎

Példaként oldjuk meg az $x^{10} \equiv 9 \pmod{13}$ binom kongruenciát. Könnyen ellenőrizhető, hogy $p = 13$ esetén $g = 2$ primitív gyök, és az indextáblázat a következő:

a	1	2	3	4	5	6	7	8	9	10	11	12
$\operatorname{ind}_g a$	0	1	4	2	9	5	11	3	8	10	7	6

A kongruencia megoldható, mivel $(10, 12) \mid \operatorname{ind}_2 9 = 8$. Így a megoldandó lineáris kongruencia: $10 \operatorname{ind}_2 x \equiv 8 \pmod{12}$. Ezt megoldva kapjuk, hogy $\operatorname{ind}_2 x \equiv 2 \pmod{12}$ és $\operatorname{ind}_2 x \equiv 8 \pmod{12}$. Az indextáblázatból látjuk, hogy a megoldások: $x_1 \equiv 4 \pmod{13}$ és $x_2 \equiv 9 \pmod{13}$.

Az eddigiekben az algebrai kongruenciák megoldásához szükséges prímmodulusú kongruenciákkal foglalkoztunk, és ezért csak prímmodulusok esetére definiáltuk a rend, a primitív gyök és az index fogalmát. Természetesen mindez megtehető tetszőleges $m(\geq 2)$ modulus esetén is.

Definíció. Legyen $m \in \mathbf{N} \setminus \{0, 1\}$, $a \in \mathbf{Z}$ és $(a, m) = 1$. Azt a legkisebb k pozitív egész számot, amelyre $a^k \equiv 1 \pmod{m}$, az a szám rendjének nevezzük modulo m. (Szokás azt is mondani, hogy az a szám a k kitevőhöz tartozik modulo m.)

5.20. Tétel. *Legyen az a egész szám rendje k modulo m.*

(a) *Ha $a^n \equiv 1 \pmod{m}$, akkor $k \mid n$ ($n \in \mathbf{N}$);*

(b) *$k \mid \varphi(m)$;*

(c) *ha $i, j \in \mathbf{N}$, akkor $a^i \equiv a^j \pmod{m}$, akkor $i \equiv j \pmod{k}$.*

Bizonyítás. A tétel az 5.8. Tétel általánosítása, így a bizonyítása hasonló módon elvégezhető. (Természetesen a (b) rész bizonyításában a kis Fermat-tétel helyett az általánosabb Euler—Fermat-tételt használjuk.) ∎

Definíció. Ha az a egész szám rendje $\varphi(m)$ modulo m (azaz az a szám a $\varphi(m)$ kitevőhöz tartozik modulo m), akkor a-t primitív gyöknek nevezzük modulo m.

Az 5.13. Tétel szerint minden p prímmodulus esetén létezik primitív gyök modulo p. Most megvizsgáljuk, hogy mely összetett m modulusok esetén van primitív gyök modulo m.

5.21. Tétel. *Legyen $m \geq 4$ összetett egész szám. Akkor és csak akkor létezik primitív gyök modulo m, ha $m = p^e$ $(e \geq 2)$ vagy $m = 2p^e$ $(e \geq 1)$, ahol p páratlan prímszám, vagy ha $m = 4$.*

Bizonyítás. Legyen $m = 2^t p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ alakú, ahol a p_i egészek különböző páratlan prímek, $t \geq 0$, $e_i \geq 1$ és $k \geq 1$ (azaz $m \neq 2^t$). Ha a egy egész és $(a, m) = 1$, akkor

$$(a, p_1^{e_1}) = 1 \text{ és } \left(a, \frac{m}{p_1^{e_1}}\right) = 1,$$

és így az Euler—Fermat-tétel szerint

$$a^{\varphi(p_1^{e_1})} \equiv 1 \pmod{p_1^{e_1}} \text{ és } a^{\varphi\left(\frac{m}{p_1^{e_1}}\right)} \equiv 1 \pmod{\frac{m}{p_1^{e_1}}}. \tag{5.45}$$

Ha $k \geq 2$ vagy $k = 1$ és $t \geq 2$, akkor

$$\varphi(p_1^{e_1}) \text{ és } \varphi\left(\frac{m}{p_1^{e_1}}\right)$$

páros természetes számok, azaz

$$\frac{1}{2}\varphi\left(p_1^{e_1}\right) \in \mathbf{N} \text{ és } \frac{1}{2}\varphi\left(\frac{m}{p_1^{e_1}}\right) \in \mathbf{N}.$$

Ekkor (5.45)-ből hatványozással kapjuk, hogy

$$a^{\frac{1}{2}\varphi(p_1^{e_1})\varphi\left(\frac{m}{p_1^{e_1}}\right)} \equiv 1 \pmod{p_1^{e_1}} \text{ és } a^{\frac{1}{2}\varphi\left(\frac{m}{p_1^{e_1}}\right)\varphi(p_1^{e_1})} \equiv 1 \pmod{\frac{m}{p_1^{e_1}}},$$

amelyből az

$$a^{\frac{1}{2}\varphi(m)} = a^{\frac{1}{2}\varphi(p_1^{e_1})\varphi\left(\frac{m}{p_1^{e_1}}\right)} \equiv 1 \pmod{m}$$

kongruencia következik. Ezért nem létezik primitív gyök, ha $k \geq 2$ vagy ha $k = 1$ és $t \geq 2$, azaz a vizsgált m-ekből csak az $m = p^e$ $(t = 0, k = 1, e \geq 2)$ és $m = 2p^e$ $(t = 1, k = 1, e \geq 1)$ összetett egészek esetén lehet primitív gyök modulo m.

Ha m kettőhatvány, azaz $m = 2^t$, akkor $t \geq 3$ esetén szintén nem létezik primitív gyök modulo 2^t. Ugyanis minden $a \in \mathbf{Z}$, $(a, m) = 1$ esetén a páratlan, de az $a = 2j + 1$ páratlan egészre igaz, hogy

$$a^2 = 4j(j+1) + 1 = 1 + 8j_1,$$
$$a^4 = (1 + 8j_1)^2 = 1 + 16j_2,$$
$$a^8 = (1 + 16j)^2 = 1 + 32j_3,$$

ahol j_1, j_2, j_3 egész számok. Teljes indukcióval könnyen bizonyítható, hogy $t \geq 3$ esetén

$$a^{2^{t-2}} = 1 + 2^t j_{t-2},$$

azaz

$$a^{2^{t-2}} \equiv 1 \pmod{2^t}.$$

Mivel $\varphi(2^t) = 2^{t-1} > 2^{t-2}$, ezért ha $t \geq 3$, akkor bármely a páratlan egész szám modulo m rendje kisebb, mint $\varphi(m)$, vagyis nem létezik primitív gyök modulo 2^t. Tehát az $m = 2^t$ alakú összetett egészekből legfeljebb $m = 4$ esetén lehet primitív gyök modulo m.

A továbbiakban belátjuk, hogy a tételben szereplő modulusok esetén valóban létezik primitív gyök.

1. Vizsgáljuk először az $m = p^e$ esetet, ahol p páratlan prímszám és $e \geq 2$. Legyen g primitív gyök modulo p és $g^p - g = vp$. ($g^p \equiv g \pmod{p}$ miatt létezik ilyen v.) Megmutatjuk, hogy az $r = g + (v-1)p$ egész szám primitív gyök modulo p^e minden $e \geq 2$ esetén.

Jelölje δ az r rendjét modulo p^e. Ekkor

$$\delta \mid \varphi(p^e) = p^{e-1}(p-1), \tag{5.46}$$

továbbá $r^\delta \equiv 1 \pmod{p^e}$ és $r \equiv g \pmod{p}$ miatt $g^\delta \equiv r^\delta \equiv 1 \pmod{p}$, és ezért

$$(p-1) \mid \delta. \tag{5.47}$$

Így (5.46)-ból és (5.47)-ből kapjuk, hogy δ

$$\delta = p^s(p-1)$$

alakú, ahol $0 \leq s \leq e-1$. Foglalkozzunk most ezekkel a számokkal.

Mivel a binomiális tétel szerint (alkalmas egész A-val)

$$r^p = (g + (v-1)p)^p = g^p + pg^{p-1}(v-1)p + p^2 A,$$

ezért

$$r^p \equiv g^p \pmod{p^2},$$

amellyel

$$\begin{aligned} r(r^{p-1}-1) = r^p - r \equiv g^p - g - (v-1)p = (g^p - g) - (v-1)p = \\ = vp - vp + p = p \pmod{p^2}. \end{aligned}$$

Ez utóbbiból kapjuk, hogy

$$p^2 \nmid r^{p-1} - 1. \tag{5.48}$$

Tudjuk viszont, hogy $r \equiv g \pmod{p}$ miatt

$$p \mid r^{p-1} - 1. \tag{5.49}$$

(5.48)-ból és (5.49)-ből következik, hogy létezik olyan b_0 egész szám, amelyre

$$r^{p-1} = 1 + b_0 p \quad \text{és} \quad p \nmid b_0.$$

Ezt felhasználva a binomiális tétel alapján

$$r^{p(p-1)} = \left(r^{p-1}\right)^p = (1 + b_0 p)^p \equiv 1 + b_0 p^2 \pmod{p^3},$$

adódik, azaz létezik olyan b_1 egész szám, amelyre

$$r^{p(p-1)} = 1 + b_1 p^2 \quad \text{és} \quad p \nmid b_1.$$

Teljesen hasonlóan nyerhető, hogy

$$r^{p^2(p-1)} = (1 + b_1 p^2)^p \equiv 1 + b_1 p^3 \pmod{p^4},$$

azaz létezik olyan b_2 egész szám, amelyre

$$r^{p^2(p-1)} = 1 + b_2 p^3 \quad \text{és} \quad p \nmid b_2.$$

A továbbiakban teljes indukcióval könnyen bizonyítható, hogy bármely $s \geq 0$ egész esetén

$$r^{p^s(p-1)} \equiv 1 + b_{s-1} p^{s+1} \pmod{p^{s+2}} \text{ és } p \nmid b_{s-1},$$

azaz

$$p^{s+1} \mid (r^{p^s(p-1)} - 1), \quad \text{de} \quad p^{s+2} \nmid (r^{p^s(p-1)} - 1).$$

Ezt $e = s + 1$ esetben alkalmazva kapjuk, hogy

$$p^e \mid (r^{p^{e-1}(p-1)} - 1) \quad \text{de} \quad p^e \nmid (r^{p^s(p-1)} - 1), \quad \text{ha} \quad 0 \leq s \leq e-2.$$

Ezzel beláttuk, hogy r primitív gyök modulo p^e mivel, mint láttuk, rendje csak $\delta = p^s(p-1)$ alakú lehet.

2. Vizsgáljuk meg most az $m = 2p^e$ alakú számokat, ahol p páratlan prímszám és $e \geq 1$. Legyen g_1 primitív gyök modulo p^e, és jelölje g a g_1 és $g_1 + p^e$ közül a páratlan egész számot. Egyrészt $g \equiv 1 \pmod 2$ miatt

$$g^{\varphi(2p^e)} \equiv 1 \pmod 2 \tag{5.50}$$

nyilvánvalóan teljesül, másrészt $g \equiv g_1 \equiv g_1 + p^e \pmod{p^e}$ miatt g és g_1 rendje modulo p^e azonos. Ezért $\varphi(p^e)$ a legkisebb pozitív egész kitevő, amelyre

$$g^{\varphi(2p^e)} = g^{\varphi(p^e)} \equiv 1 \pmod{p^e}.$$

Ez utóbbiból és (5.50)-ből kapjuk, hogy $\varphi(2p^e)$ a legkisebb pozitív egész kitevő, amelyre

$$g^{\varphi(2p^e)} \equiv 1 \pmod{2p^e}.$$

Ezzel beláttuk, hogy $m = 2p^e$ (p páratlan prím és $e \geq 1$) esetben van primitív gyök modulo m.

3. Az $m = 4$ esetben közvetlenül belátható, hogy $g = 3$ primitív gyök modulo 4, azaz 3 rendje $\varphi(4) = 2$ modulo 4.

Ezzel tételünk bizonyítását befejeztük. ∎

A következő tétel az 5.14. Tétel általánosítása.

5.22. Tétel. *Legyen g primitív gyök modulo m. A*

$$g^0, g^1, \ldots, g^{\varphi(m)-1}$$

egész számok redukált maradékrendszert alkotnak modulo m.

Bizonyítás. A 3.9. Tétel alapján a bizonyítás könnyen elvégezhető. ∎

E tétel alapján most is lehetőség van az index definíciójára, de ezek már kevésbé hasznosak, mint prímmodulus esetén voltak, ezért ettől eltekintünk, és visszatérünk a prímmodulusú másodfokú kongruenciák megoldásainak vizsgálatára.

Kvadratikus kongruenciák

Legyenek c, d és e egész számok, és tekintsük a

$$cx^2 + dx + e \equiv 0 \pmod{p} \tag{5.51}$$

prímmodulusú kongruenciát, ahol $p \nmid c$. (5.51)-et $4c$-vel szorozva kapjuk, hogy

$$4c^2x^2 + 4cdx + 4ce \equiv 0 \pmod{p},$$

amely

$$(2cx + d)^2 \equiv d^2 - 4ce \pmod{p}$$

alakban is írható. Ebből az

$$y = 2cx + d \quad \text{és} \quad b = d^2 - 4ce$$

jelöléssel adódik az

$$y^2 \equiv b \pmod{p}$$

kongruencia. Látható tehát, hogy az (5.51) kongruencia mindig visszavezethető egy másodfokú binom kongruenciára és egy lineáris kongruenciára. Ezért a továbbiakban elegendő az

$$x^2 \equiv a \pmod{p} \tag{5.52}$$

alakú kongruenciák megoldásával foglalkozni.

Definíció. Az (5.52) alatti kongruenciát (prímmodulusú) kvadratikus kongruenciának nevezzük. Továbbá, ha (5.52) megoldható, akkor a-t kvadratikus maradéknak nevezzük modulo p, ellekező esetben a nem kvadratikus maradék modulo p.

Mivel $p = 2$ esetén az (5.52) kongruencia nagyon könnyen kezelhető, ezért a továbbiakban feltételezzük, hogy $p > 2$.

5.23. Tétel. *Az* $x^2 \equiv a \pmod{p}$ $(p \nmid a,\ p > 2)$ *kongruencia akkor és csak akkor oldható meg, azaz, a akkor és csak akkor kvadratikus maradék modulo p, ha*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

vagy ami ezzel ekvivalens, ha

$$2 \mid \operatorname{ind}_g a,$$

ahol g primitív gyök modulo p. Ha megoldható, akkor az inkongruens megoldások száma 2.

Bizonyítás. Tételünk állítása az 5.17. Tétel speciális eseteként ($k = 2$ helyettesítéssel) adódik. ∎

Az a egész szám kvadratikus karakteréről szól az *Euler-lemma* néven ismert következő tétel.

5.24. Tétel. *Legyen $p > 2$ és $p \nmid a$. Ekkor*

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 \pmod p, & \text{ha } a \text{ kvadratikus maradék modulo } p, \\ -1 \pmod p, & \text{ha } a \text{ nem kvadratikus maradék modulo } p. \end{cases}$$

Bizonyítás. Tudjuk, hogy az

$$x^{p-1} \equiv 1 \pmod p$$

kongruenciának $p-1$ inkongruens megoldása van, amelyek

$$x^{p-1} - 1 = \left(x^{\frac{p-1}{2}} - 1\right)\left(x^{\frac{p-1}{2}} + 1\right)$$

miatt, vagy az

$$x^{\frac{p-1}{2}} \equiv 1 \pmod p, \tag{5.53}$$

vagy az

$$x^{\frac{p-1}{2}} \equiv -1 \pmod p \tag{5.54}$$

kongruencia megoldásai. Az 5.23. Tétel szerint (5.53)-at pontosan a kvadratikus maradékok elégítik ki, azaz amely a egész nem kvadratikus maradék, az szükségképpen az (5.54) kongruencia megoldása. Bizonyításunkból az is adódik, hogy a kvadratikus, illetve a nem kvadratikus maradékok száma is $\frac{p-1}{2}$, hiszen (5.53) inkongruens megoldásainak száma $\left(\frac{p-1}{2}, p-1\right) = \frac{p-1}{2}$. ∎

Az Euler-lemma alapján bevezetjük az $\left(\frac{a}{p}\right)$ úgynevezett *Legendre-szimbólum* fogalmát.

Definíció. Legyen $p > 2$ prím és $p \nmid a$. Ekkor az

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ha } a \text{ kvadratikus maradék modulo } p, \\ -1, & \text{ha } a \text{ nem kvadratikus maradék modulo } p \end{cases}$$

egyenlőséggel definiált $\left(\frac{a}{p}\right)$ számot Legendre-szimbólumnak nevezzük.

Az 5.24. Tétel és a definíció miatt nyilvánvaló, hogy

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

minden páratlan p prím esetén.

A Legendre-szimbólum tulajdonságaival foglalkozik a következő tétel.

4.25. Tétel. *Legyen $p > 2$, $p \nmid a$ és $p \nmid b$.*

(a) *Ha $a \equiv b \pmod{p}$, akkor $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*

(b) $\left(\frac{a^2}{p}\right) = 1$ *(így $\left(\frac{1}{p}\right) = 1$).*

(c) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(d) $\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{ha } p \equiv 1 \pmod{4}, \\ -1, & \text{ha } p \equiv -1 \pmod{4}. \end{cases}$

Bizonyítás. (a) Ha $a \equiv b \pmod{p}$, akkor az

$$a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \pmod{p}$$

kongruencia is teljesül, azaz az Euler-lemma szerint a és b kvadratikus karaktere azonos, és így $(\frac{a}{p}) = (\frac{b}{p})$.

(b) Mivel az $x^2 \equiv a^2 \pmod{p}$ kongruencia nyilvánvalóan megoldható, így a^2 kvadratikus maradék modulo p, azaz $(\frac{a^2}{p}) = 1$.

(c) Az Euler-lemma és a Legendre-szimbólum definíciója alapján igaz az

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$$

kongruencia, amelyből

$$\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv 0 \pmod{p} \tag{5.55}$$

adódik. A Legendre-szimbólum jelentése alapján (5.55) bal oldala csak 0 és ± 2 értékeket vehet fel. De $p > 2$ miatt $p \nmid \pm 2$, és így

$$\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 0.$$

(d) $p = 4k \pm 1$ helyettesítéssel az Euler-lemmából adódik az állítás. ∎

A Legendre-szimbólummal való konkrét számoláshoz hasznosak a következő tulajdonságok.

5.26. Tétel. *Legyen $p > 2$ és $p \nmid a_i$ $(i = 1, 2, \ldots, k)$.*

(a) $\left(\dfrac{\prod_{i=1}^{k} a_i}{p}\right) = \prod_{i=1}^{k} \left(\frac{a_i}{p}\right)$.

(b) *Ha $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, $\alpha_i \geq 1$ és $\alpha_i = 2k_i + \delta_i$, ahol*

$$\delta_i = \begin{cases} 1, & \text{ha } \alpha_i \equiv 1 \pmod 2, \\ 0, & \text{ha } \alpha_i \equiv 0 \pmod 2, \end{cases}$$

akkor

$$\left(\frac{a}{p}\right) = \prod_{i=1}^{r} \left(\frac{p_i^{\delta_i}}{p}\right) \quad \text{és} \quad \left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right) \prod_{i=1}^{r} \left(\frac{p_i^{\delta_i}}{p}\right).$$

Bizonyítás. Az állítás (a) része az előző tétel (c) pontja alapján teljes indukcióval bizonyítható, míg a (b) állítás az (a) részből és az előző tétel (b) pontjából következik. ∎

Érdemes kiemelni, hogy az $(\frac{a}{p})$ Legendre-szimbólum értékének kiszámításához — a fenti tétel (b) pontja szerint — elegendő ismerni az a kanonikus alakjában páratlan kitevővel szereplő p_i prímekre a $(\frac{p_i}{p})$ értékeket, valamint negatív a esetén $(\frac{-1}{p})$ értékét.

Az a egész szám kvadratikus karakterének eldöntésére szolgál az alábbi, *Gauss-lemma* néven ismert tétel is.

5.27. Tétel. *Legyen $p > 2$ és $p \nmid a$. Tekintsük az*

$$a,\ 2a,\ 3a,\ \ldots,\ \frac{p-1}{2}a \tag{5.56}$$

számok modulo p vett legkisebb pozitív maradékait. Legyen ezek között m darab, amely nagyobb, mint $\frac{p}{2}$. Ekkor

$$\left(\frac{a}{p}\right) = (-1)^m,$$

azaz m paritása már meghatározza az a kvadratikus karakterét.

Bizonyítás. Mivel $p \nmid a$, ezért az (5.56)-beli egész számok páronként inkongruensek modulo p, hiszen $ia \equiv ja \pmod{p}$ $\left(1 \le i < j \le \frac{p-1}{2}\right)$ esetén $p \mid (i-j)$ következne, ami lehetetlen. Jelöljük az (5.56)-beli egészek modulo p vett legkisebb pozitív maradékait $c_1, c_2, \ldots, c_n$-nel, ha $0 < c_i < \frac{p}{2}$ $(i = 1, 2, \ldots, n)$, illetve $b_1, b_2, \ldots, b_m$-mel, ha $\frac{p}{2} < b_i \le p-1$ $(i = 1, 2, \ldots, m)$, ahol $n + m = \frac{p-1}{2}$. Ekkor

$$1a2a \cdots \frac{p-1}{2}a \equiv c_1 c_2 \cdots c_n b_1 b_2 \cdots b_m \pmod{p},$$

amelyből kapjuk, hogy

$$a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv c_2 c_2 \cdots c_n b_1 b_2 \cdots b_m \pmod{p}. \tag{5.57}$$

Ugyanakkor a b_i számokra tett $\frac{p}{2} < b_i \le p-1$ feltevésből következik, hogy

$$\frac{p}{2} > p - b_i \ge 1 \quad (i = 1, 2, \ldots, m). \tag{5.58}$$

Az természetes, hogy $p - b_i \not\equiv p - b_j \pmod{p}$, ha $1 \le i < j \le m$. Megmutatjuk, hogy $p - b_i \not\equiv c_j \pmod{p}$ is igaz, ha $1 \le i \le m$ és $1 \le j \le n$. Ugyanis ellenkező esetben létezne olyan t és q egész, amelyekre

$$p - ta \equiv qa \pmod{p}, \quad 1 \le t \le \frac{p-1}{2} \quad \text{és} \quad 1 \le q \le \frac{p-1}{2}.$$

De ebből

$$a(q+t) \equiv 0 \pmod{p},$$

azaz $p \mid (q+t)$ következne, amely $2 \le t + q \le p-1$ miatt lehetetlen. Így tehát a $c_1, c_2, \ldots, c_n$ és az (5.58)-beli $p - b_1, p - b_2, \ldots, p - b_m$ számok $\frac{p}{2}$-nél kisebb pozitív egészek, és páronként inkongruensek modulo p, ezért

$$\{c_1, c_2, \ldots, c_n, p - b_1, p - b_2, \ldots, p - b_m\} = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}.$$

Ezt felhasználva (5.57)-ből

$$a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv c_1 \cdots c_n b_1 \cdots b_m \equiv c_1 \cdots c_n (p - b_1) \cdots (p - b_m)(-1)^m \equiv$$
$$\equiv (-1)^m \left(\frac{p-1}{2}\right)! \pmod{p},$$

adódik, amely ekvivalens az

$$a^{\frac{p-1}{2}} \equiv (-1)^m \pmod{p}$$

kongruenciával. Így valóban $\left(\frac{a}{p}\right) = (-1)^m$. ∎

A Gauss-lemma alábbi alkalmazásával meghatározzuk a $\left(\frac{2}{p}\right)$ $(p > 2)$ Legendre-szimbólum értékét.

5.28. Tétel. *Legyen p egy páratlan prím. Ekkor*

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{ha } p \equiv \pm 1 \pmod 8, \\ -1, & \text{ha } p \equiv \pm 3 \pmod 8. \end{cases}$$

Bizonyítás. Ebben az esetben a

$$2,\ 2\cdot 2,\ 3\cdot 2,\ \cdots,\ \frac{p-1}{2}\cdot 2$$

számok az első $\frac{p-1}{2}$ pozitív páros számot adják, ahol a legnagyobb is kisebb, mint p. Ezért a Gauss-lemmában szereplő m értékét megkapjuk, ha a p-nél kisebb pozitív páros számok számából kivonjuk a $\frac{p}{2}$-nél kisebb pozitív páros számok számát, azaz

$$m = \left[\frac{p}{2}\right] - \left[\frac{p}{4}\right], \tag{5.59}$$

ahol $[x]$ az x egész részét jelöli. A p prímszám $8k \pm 1$ és $8k \pm 3$ alakjait (5.59)-be helyettesítve láthatjuk, hogy m páros, ha $p = 8k \pm 1$ alakú, míg m páratlan, ha $p = 8k \pm 3$, azaz

$$\left(\frac{2}{p}\right) = (-1)^m = \begin{cases} 1, & \text{ha } p \equiv \pm 1 \pmod 8, \\ -1, & \text{ha } p \equiv \pm 3 \pmod 8. \end{cases}$$

Például, ha p alakja $p = 8k - 1$, akkor

$$\left[\frac{p}{2}\right] = \left[\frac{8k-1}{2}\right] = \left[\frac{8(k-1)+7}{2}\right] = 4(k-1) + 3$$

és

$$\left[\frac{p}{4}\right] = \left[\frac{8(k-1+7}{4}\right] = 2(k-1) + 1,$$

így

$$m = \left[\frac{p}{2}\right] - \left[\frac{p}{4}\right] = 2(k-1) + 2.$$

Tehát m páros és $\left(\frac{2}{p}\right) = (-1)^m = 1$. ∎

A továbbiakban egy, a Gauss-lemmához hasonló tételt bizonyítunk.

5.29. Tétel. *Legyen $p > 2$ prímszám, a egy páratlan egész, $p \nmid a$ és $t = \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right]$. Ekkor*

$$\left(\frac{a}{p}\right) = (-1)^t.$$

Bizonyítás. A ja ($j = 1, 2, \ldots, \frac{p-1}{2}$) egészeket p-vel maradékosan osztva kapjuk, hogy

$$ja = p\left[\frac{ja}{p}\right] + r_j, \quad \text{ahol} \quad 0 < r_j \leq p-1, \tag{5.60}$$

amelyből

$$ja \equiv r_j \pmod{p}, \quad 0 < r_j \leq p-1$$

következik. (5.60)-at és a Gauss-lemma bizonyításában bevezetett c_i és b_i jelöléseket használva

$$a\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{\frac{p-1}{2}} ja = p\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] + \sum_{j=1}^{\frac{p-1}{2}} r_j = p\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] + \sum_{i=1}^{m} b_i + \sum_{i=1}^{n} c_i, \tag{5.61}$$

következik, ahol $m + n = \frac{p-1}{2}$, illetve

$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{i=1}^{m}(p - b_i) + \sum_{i=1}^{n} c_i = mp - \sum_{i=1}^{m} b_i + \sum_{i=1}^{n} c_i. \tag{5.62}$$

(5.61) és (5.62) megfelelő oldalait kivonva az

$$(a-1)\sum_{j=1}^{\frac{p-1}{2}} j = p\left(\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] - m\right) + 2\sum_{i=1}^{m} b_i \tag{5.63}$$

egyenlőséget kapjuk. Mivel a feltétel szerint $a-1$ páros szám és p páratlan prímszám, ezért (5.63)-ból következik, hogy

$$t=\sum_{j=1}^{\frac{p-1}{2}}\left[\frac{ja}{p}\right]\equiv m \pmod 2,$$

azaz t és m paritása azonos, és így a Gauss-lemma alapján valóban

$$\left(\frac{a}{p}\right)=(-1)^m=(-1)^t. \ \blacksquare$$

E fejezet zárásaként bizonyítjuk a szintén Gausstól származó, úgynevezett *kvadratikus reciprocitás tételét.*

5.30. Tétel. *Legyen p és q két különböző páratlan prímszám. Ekkor*

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

azaz

$$\left(\frac{p}{q}\right)=\begin{cases}\left(\frac{q}{p}\right), & \text{ha } p\equiv 1 \pmod 4 \text{ vagy } q\equiv 1 \pmod 4,\\ -\left(\frac{q}{p}\right), & \text{ha } p\equiv q\equiv -1 \pmod 4.\end{cases}$$

Bizonyítás. Definiáljuk a H, H_1 és H_2 egész számpárokból álló halmazokat az alábbi módon:

$$H=\left\{(i,j)\colon 1\le i\le\frac{p-1}{2},\ \ 1\le j\le\frac{q-1}{2}\right\},$$
$$H_1=\left\{(i,j)\colon 1\le i\le\frac{p-1}{2},\ \ 1\le j\le\frac{q-1}{2},\ \ pj<qi\right\},$$
$$H_2=\left\{(i,j)\colon 1\le i\le\frac{p-1}{2},\ \ 1\le j\le\frac{q-1}{2},\ \ qi<pj\right\}.$$

A definíciókból világos, hogy $|H|=\frac{p-1}{2}\frac{q-1}{2}$, $H=H_1\cup H_2$, $H_1\neq\emptyset$, $H_2\neq\emptyset$ és $H_1\cap H_2=\emptyset$. Ezért

$$\frac{p-1}{2}\frac{q-1}{2}=|H|=|H_1|+|H_2|. \tag{5.64}$$

A H_1 és H_2 halmazok számosságát úgy is meghatározhatjuk, hogy rögzítjük az i (illetve j) értékét, és meghatározzuk a hozzá tartozó lehetséges j (illetve i) értékek számát, majd mindezt összegezzük $i = 1$-től $i = \frac{p-1}{2}$-ig (illetve $j = 1$-től $j = \frac{q-1}{2}$-ig). Mivel H_1 esetén adott i-hez $1 \leq j < \frac{qi}{p}$ számú j érték tartozhat, ezért

$$|H_1| = \sum_{i=1}^{\frac{p-1}{2}} \left[\frac{qi}{p}\right]. \tag{5.65}$$

Hasonlóan a H_2 halmaz esetén adott j-hez $1 \leq i < \frac{pj}{q}$ számú i érték választható, ezért

$$|H_2| = \sum_{j=1}^{\frac{q-1}{2}} \left[\frac{pj}{q}\right]. \tag{5.66}$$

Így (5.64), (5.65) és (5.66) alapján

$$\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{qi}{p}\right] + \sum_{j=1}^{\frac{q-1}{2}} \left[\frac{pj}{q}\right] = \frac{p-1}{2}\frac{q-1}{2},$$

amelyből

$$(-1)^{\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{qi}{p}\right]} (-1)^{\sum_{j=1}^{\frac{q-1}{2}} \left[\frac{pj}{q}\right]} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

következik. Ez utóbbi viszont — az előző tétel szerint — ekvivalens a

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

egyenlőséggel. Ebből viszont $\left(\frac{p}{q}\right) = \pm\left(\frac{q}{p}\right)$ miatt az következik, hogy $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ akkor és csak akkor teljesül, ha $\frac{p-1}{2}$ és $\frac{q-1}{2}$ egyike páros, vagyis p és q közül legalább az egyik $4k+1$ alakú. Ezzel a tétel minden állítását bizonyítottuk. ∎

Megjegyezzük, hogy az $\left(\frac{a}{p}\right)$ Legendre-szimbólum általánosításaként kapható az alábbi $\left(\frac{a}{m}\right)$ *Jacobi-szimbólum.*

Definíció. Legyen $(a,m)=1$ és $m\geq 3$ páratlan egész szám, melynek kanonikus alakja $m=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$. Az

$$\left(\frac{a}{m}\right)=\prod_{i=1}^{r}\left(\frac{a}{p_i}\right)^{\alpha_i},$$

szorzattal definiált $+1$ vagy -1 értékeket felvevő szimbólumot Jacobi-szimbólumnak nevezzük. (A szorzatban $\left(\frac{a}{p_i}\right)$ a Legendre-szimbólumot jelenti, és ha $m=p$ páratlan prím, akkor a két szimbólum azonos.)

A Jacobi-szimbólum tulajdonságaival és alkalmazásával nem foglalkozunk.

Példaként vizsgáljuk meg, hogy megoldható-e az

$$x^2\equiv 990 \pmod{3719}$$

prímmodulusú kongruencia. Ehhez meghatározzuk $\left(\frac{990}{3719}\right)$ értékét. Mivel $990=3^2\cdot 11\cdot 2\cdot 5$, így

$$\left(\frac{990}{3719}\right)=\left(\frac{3^2}{3719}\right)\left(\frac{11}{3719}\right)\left(\frac{2}{3719}\right)\left(\frac{5}{3719}\right).$$

A Legendre-szimbólum tulajdonságai és a kvadratikus reciprocitási tétel szerint $\left(\frac{3^2}{3719}\right)=1$; $\left(\frac{11}{3719}\right)=-\left(\frac{3719}{11}\right)=-\left(\frac{11\cdot 338+1}{11}\right)=-\left(\frac{1}{11}\right)=-1$; $\left(\frac{2}{3719}\right)=\left(\frac{2}{465\cdot 8-1}\right)=1$; $\left(\frac{5}{3719}\right)=\left(\frac{3719}{5}\right)=\left(\frac{5\cdot 744-1}{5}\right)=\left(\frac{-1}{5}\right)=1$. Így

$$\left(\frac{990}{3719}\right)=1\cdot(-1)\cdot 1\cdot 1=-1,$$

azaz a fenti kongruencia nem oldható meg.

Feladatok

1. Oldjuk meg az alábbi lineáris kongruenciákat:

(a) $21x\equiv 18 \pmod{30}$;

(b) $110x\equiv 170 \pmod{230}$.

2. Igazoljuk, hogy ha $(a,p)=1$ és b tetszőleges egész, akkor az $ax\equiv b \pmod{p}$ kongruencia egyetlen inkongruens megoldása

$$x_0\equiv(-1)^{a-1}\frac{1}{p}\binom{p}{a}b \pmod{p},$$

ahol $1 \leq a \leq p-1$ és $p > 2$ prímszám.

3. Oldjuk meg az alábbi lineáris kongruenciarendszereket:

(a)

$$\left.\begin{aligned} 3x &\equiv 4 \pmod 7 \\ 8x &\equiv 9 \pmod{11} \\ 7x &\equiv 10 \pmod{12} \end{aligned}\right\},$$

(b)

$$\left.\begin{aligned} x &\equiv 5 \pmod{11} \\ x &\equiv 7 \pmod{13} \\ x &\equiv 3 \pmod 7 \end{aligned}\right\}.$$

4. Oldjuk meg az alábbi kongruenciákat:

(a) $x^3 + 22x + 28 \equiv 0 \pmod{225}$;

(b) $x^3 + x^2 + 3 \equiv 0 \pmod{225}$;

(c) $x^3 + x^2 + x + 1 \equiv 0 \pmod{1125}$;

(d) $x^3 + 2x^2 + 9 \equiv 0 \pmod{154}$.

5. Határozzuk meg 4 rendjét modulo 47.

6. Legyen p prímszám, továbbá a és a' olyan egészek, amelyekre $aa' \equiv 1 \pmod p$. Bizonyítsuk be, hogy a és a' modulo p rendje egyenlő.

7. Legyen $p > 2$ prímszám és $(a, p) = 1$. Bizonyítsuk be, hogy ha a modulo p rendje páratlan szám, akkor nem létezik olyan $n \in \mathbf{N}$, amelyre $a^n \equiv -1 \pmod p$.

8. Bizonyítsuk be, hogy 10 primitív gyök modulo 17.

9. Bizonyítsuk be a primitív gyök segítségével, hogy ha p prím, akkor $(p-1)! \equiv -1 \pmod p$.

10. Legyen $p > 2$ prímszám és $k \in \mathbf{N}^+$. Határozzuk meg x ($0 \leq x \leq p-1$) értékét, ha $\sum_{i=1}^{p-1} i^k \equiv x \pmod p$.

11. Keressük meg a legkisebb pozitív primitív gyököt modulo 17, majd készítsük el az indextáblázatot.

12. Oldjuk meg indextáblázat segítségével az alábbi binom kongruenciákat:

(a) $x^{11} \equiv 6 \pmod{17}$;

(b) $11 \cdot x^{10} \equiv 5 \pmod{17}$.

13. Az Euler-lemma segítségével állapítsuk meg, hogy az $x^2 \equiv 26 \pmod{29}$ kongruencia megoldható-e.

14. A Gauss-lemma segítségével állapítsuk meg, hogy az

$$x^2 \equiv 5 \pmod{19}$$

kongruencia megoldható-e.

15. Határozzuk meg az alábbi Legendre-szimbólumok értékét:

(a) $\left(\frac{-4}{41}\right)$;

(b) $\left(\frac{94}{109}\right)$;

(c) $\left(\frac{77}{103}\right)$;

(d) $\left(\frac{-131}{191}\right)$.

16. Oldjuk meg az alábbi kongruenciákat:

(a) $x^2 - 3x - 3 \equiv 0 \pmod{17}$;

(b) $x^{10} - x^5 - 5 \equiv 0 \pmod{17}$.

17. Határozzuk meg a $\left(\frac{3}{p}\right)$ és $\left(\frac{5}{p}\right)$ Legendre-szimbólumok p alakjától függő értékét.

Az 1000-nél kisebb prímszámok és ezek legkisebb primitív gyökei

p	g	p	g	p	p	p	g	p	g
2	1	151	6	353	3	577	5	811	3
3	2	157	5	359	7	587	2	821	2
5	2	163	2	367	6	593	3	823	3
7	3	167	5	373	2	599	7	827	2
11	2	173	2	379	2	601	7	829	2
13	2	179	2	383	5	607	3	839	11
17	3	181	2	389	2	613	2	853	2
19	2	191	19	397	5	617	3	857	3
23	5	193	5	401	3	619	2	859	2
29	2	197	2	409	21	631	3	863	5
31	3	199	3	419	2	641	3	877	2
37	2	211	2	421	2	643	11	881	3
41	6	223	3	431	7	647	5	883	2
43	3	227	2	433	5	653	2	887	5
47	5	229	6	439	15	659	2	907	2
53	2	233	3	443	2	661	2	911	17
59	2	239	7	449	3	673	5	919	7
61	2	241	7	457	13	677	2	929	3
67	2	251	6	461	2	683	5	937	5
71	7	257	3	463	3	691	3	941	2
73	5	263	5	467	2	701	2	947	2
79	3	269	2	479	13	709	2	953	3
83	2	271	6	487	3	719	11	967	5
89	3	277	5	491	2	727	5	971	6
97	5	281	3	499	7	733	6	977	3
101	2	283	3	503	5	739	3	983	5
103	5	293	2	509	2	743	5	991	6
107	2	307	5	521	3	751	3	997	7
109	6	311	17	523	2	757	2		
113	3	313	10	541	2	761	6		
127	3	317	2	547	2	769	11		
131	2	331	3	557	2	773	2		
137	3	337	10	563	2	787	2		
139	2	347	2	569	3	797	2		
149	2	349	2	571	3	809	3		

Indextáblázatok

$p = 3, g = 2$

számok	1	2
indexek	0	1

$p = 5, g = 2$

számok	1	2	3	4
indexek	0	1	3	2

$p = 7, \quad g = 2$

számok	1	2	3	4	5	6
indexek	0	2	1	4	5	3

$p = 11, \quad g = 2$

számok	1	2	3	4	5	6	7	8	9	10
indexek	0	1	8	2	4	9	7	3	6	5

$p = 13, \quad g = 2$

számok	1	2	3	4	5	6	7	8	9	10	11	12
indexek	0	1	4	2	9	5	11	3	8	10	7	6

$p = 17, \quad g = 3$

számok	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
indexek	0	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

$p = 19, \quad g = 2$

számok	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
indexek	0	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

$p = 23, \quad g = 5$

számok	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
indexek	0	2	16	4	1	18	19	6	10	3	9	20	14	21	17	8	7	12	15	5	13	11

6. Számelméleti függvények

DEFINÍCIÓ. Egy $f\colon \mathbf{N}^+ \to \mathbf{R}$ függvényt számelméleti függvénynek nevezzük.

Analízisbeli tanulmányokban a fenti függvényeket sorozatoknak nevezik. Ott elsősorban a sorozatok analitikus tulajdonságaival foglalkoznak, míg jelen esetben a fenti függvények számelméleti tulajdonságait vizsgáljuk. Megemlítjük, hogy az Euler—Fermat-tétel kapcsán megismert φ függvény is egy speciális számelméleti függvény. Természetesen a számelméleti függvények is nagyon változatosak lehetnek, amelyek között különösen fontosak a multiplikatív és az additív függvények.

DEFINÍCIÓ. Az f számelméleti függvényt multiplikatívnak nevezzük, ha bármely $a, b \in \mathbf{N}^+$ és $(a, b) = 1$ esetén $f(ab) = f(a)f(b)$. Ha az $(a, b) = 1$ feltétel elhagyható, akkor az f függvényt totálisan multiplikatívnak nevezzük.

DEFINÍCIÓ. Az f számelméleti függvényt additívnak nevezzük, ha bármely $a, b \in \mathbf{N}^+$, $(a, b) = 1$ esetén $f(ab) = f(a) + f(b)$. Ha az $(a, b) = 1$ feltétel elhagyható, akkor az f-et totálisan additív függvénynek nevezzük.

Így például totálisan multiplikatív az $f(n) = n^k$ $(k \in \mathbf{Z})$, illetve totálisan additív az $f(n) = \log n$ hozzárendeléssel megadott f számelméleti függvény, ahol log a természetes alapú logaritmus függvényt jelöli. Ugyanakkor az azonosan zérus függvény ($f(n) = 0$ minden n-re) totálisan additív is és totálisan multiplikatív is. Az ismert φ függvény is multiplikatív.

Azt, hogy a számelméleti függvények „többsége" se nem multiplikatív, se nem additív, jól mutatja a multiplikativitás, illetve az additivitás alábbi szükséges feltétele.

6.1. TÉTEL. *Ha az f számelméleti függvény multiplikatív és $f(n) \not\equiv 0$, akkor $f(1) = 1$. Ha pedig az f számelméleti függvény additív, akkor*

$$f(1) = 0.$$

BIZONYÍTÁS. Legyen f multiplikatív. Mivel $f(n) \not\equiv 0$, ezért létezik olyan $n \in \mathbf{N}^+$, amelyre $f(n) \neq 0$, továbbá f multiplikativitása miatt

$$f(n) = f(n1) = f(n)f(1),$$

amelyből $f(1) = 1$ adódik. Ha pedig f additív, akkor

$$f(n) = f(n1) = f(n) + f(1),$$

amiből $f(1) = 0$ következik. ∎

Felvetődhet a kérdés, hogy adott multiplikatív, illetve additív számelméleti függvényekből a szorzás és az összeadás segítségével lehet-e újabb multiplikatív, illetve additív függvényeket nyerni. Erről szól az alábbi tétel.

6.2. Tétel. *Multiplikatív függvények szorzata is multiplikatív, additív függvények összege is additív, ahol fg, illetve $f + g$ az alábbi módon értelmezett:*

$$(fg)(n) = f(n)g(n),$$
$$(f + g)(n) = f(n) + g(n).$$

Bizonyítás. Legyenek f és g multiplikatív számelméleti függvények, továbbá $a, b \in \mathbf{N}^+$ és $(a, b) = 1$. Ekkor

$$(fg)(ab) = f(ab)g(ab) = \big(f(a)f(b)\big)\big(g(a)g(b)\big) =$$
$$= \big(f(a)g(a)\big)\big(f(b)g(b)\big) = (fg)(a)(fg)(b),$$

azaz fg is multiplikatív.

Additív esetben a bizonyítás teljesen hasonló. ∎

Megjegyezzük, hogy az f és g nem azonosan zérus multiplikatív függvények összege soha sem lehet multiplikatív, mivel $(f+g)(1) = f(1)+g(1) = 2$. Ugyanakkor konkrét additív számelméleti függvényekkel igazolható, hogy additív függvények szorzata lehet additív és nem additív is.

Ugyancsak felvetődhet, hogy lehet-e multiplikatív függvényből additívet, illetve additívből multiplikatívet előállítani. Erről szól a következő tétel.

6.3. Tétel. *Ha f multiplikatív számelméleti függvény, és minden n pozitív egészre $f(n) \in \mathbf{R}^+$, akkor a*

$$g\colon \mathbf{N}^+ \to \mathbf{R}, \quad g(n) = \log f(n)$$

számelméleti függvény additív. Ha pedig f additív, akkor a

$$g\colon \mathbf{N}^+ \to \mathbf{R}, \quad g(n) = e^{f(n)}$$

számelméleti függvény multiplikatív.

Bizonyítás. A tétel első állítása az alábbiakból adódik. Legyenek a, b pozitív egészek, és $(a, b) = 1$. Ekkor

$$g(ab) = \log f(ab) = \log\big(f(a)f(b)\big) = \log f(a) + \log f(b) =$$
$$= g(a) + g(b).$$

A második állítás a hatványozás egyik azonosságából következik. ∎

Tételünk bizonyításából látható, hogy ha az f totálisan multiplikatív (illetve additív), akkor g is totálisan additív (illetve multiplikatív).

A multiplikatív, illetve az additív tulajdonság alapján könnyen igazolható az alábbi tétel.

6.4. Tétel. *Legyenek az $a_1, a_2, \ldots, a_k$ $(k \geq 2)$ pozitív egész számok páronként relatív prímek. Ha az f számelméleti függvény multiplikatív, akkor*

$$f(a_1 a_2 \cdots a_k) = \prod_{i=1}^{k} f(a_i).$$

Ha az f számelméleti függvény additív, akkor

$$f(a_1 a_2 \cdots a_k) = \sum_{i=1}^{k} f(a_i).$$

Bizonyítás. Az állítás k szerinti teljes indukcióval igazolható. ∎

E tétel fontos következménye, hogy multiplikatív, illetve additív számelméleti függvények helyettesítési értékeinek meghatározáshoz elegendő ismerni a prímhatvány helyeken felvett helyettesítési értékeket, illetve totálisan multiplikatív vagy additív esetben elegendő ismerni a prím helyeken felvett helyettesítési értékeket. Legyen a kanonikus alakja az alábbi:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \quad (\alpha_i \geq 1,\ 1 \leq i \leq r,\ p_i \neq p_j, \quad \text{ha} \quad i \neq j).$$

Így a 6.4. Tétel szerint, ha f multiplikatív, akkor

$$f(a) = \prod_{i=1}^{r} f(p_i^{\alpha_i}),$$

míg abban az esetben, ha f additív, akkor

$$f(a) = \sum_{i=1}^{r} f(p_i^{\alpha_i}).$$

Totálisan multiplikatív, illetve totálisan additív esetben pedig

$$f(a) = \prod_{i=1}^{r} f^{\alpha_i}(p_i), \quad \text{illetve} \quad f(a) = \sum_{i=1}^{r} \alpha_i f(p_i).$$

A számelméleti függvények bizonyos feltételeknek megfelelő csoportjának jellemzése általában nehéz számelméleti probléma. E témakörből álljon itt — e jegyzet írásának évében (1996) elhunyt — Erdős Pál egyik tétele.

6.5. Tétel. *Ha f totálisan additív és szigorúan monoton növekvő számelméleti függvény, akkor $f(n) = c \log n$, ahol c egy konstans.*

Bizonyítás. Mivel f additív, ezért $f(1) = 0 (= c \log 1)$ így az f szigorúan monoton növekvő volta miatt $f(n) > 0$, ha $n > 1$. A továbbiakban indirekt módon bizonyítunk. Tegyük fel, hogy $\frac{f(n)}{\log n}$ nem állandó, azaz léteznek olyan $a, b \in \mathbf{N}^+ \setminus \{1\}$, amelyekre például

$$\frac{f(a)}{\log a} < \frac{f(b)}{\log b}. \tag{6.1}$$

Definiáljuk a g függvényt az alábbi módon:

$$g\colon \mathbf{N}^+ \setminus \{1\} \to \mathbf{R}, \quad g(n) = f(n) - \frac{f(a)}{\log a} \log n.$$

Először bizonyítjuk, hogy g felülről korlátos, majd megmutatjuk, hogy g felülről nem korlátos. Ebből természetesen adódik az indirekt állításnak a cáfolata. Mivel $a \geq 2$, ezért bármely $n \in \mathbf{N}^+ \setminus \{1\}$-hez létezik olyan $k \in \mathbf{N}$, hogy

$$a^k \leq n < a^{k+1},$$

amelyből az f és a log függvények szigorúan monoton növekvő volta és $\frac{f(a)}{\log a} > 0$ miatt

$$f(a^k) \leq f(n) < f(a^{k+1}),$$
$$\log a^k \leq \log n < \log a^{k+1}$$

és

$$\frac{f(a)}{\log a} \log a^k \leq \frac{f(a)}{\log a} \log n < \frac{f(a)}{\log a} \log a^{k+1}$$

következik. Ezen egyenlőtlenségeket és f totálisan additív tulajdonságát felhasználva kapjuk, hogy

$$g(n) = f(n) - \frac{f(a)}{\log a} \log n < f(a^{k+1}) - \frac{f(a)}{\log a} \log a^k =$$
$$= (k+1) f(a) - k \frac{f(a)}{\log a} \log a = f(a).$$

Ezzel beláttuk, hogy a g függvény felülről korlátos.

Mivel $b \geq 2$, ezért bármely $n \in \mathbf{N}^+ \setminus \{1\}$ egészhez létezik olyan $l \in \mathbf{N}$, hogy

$$b^l \leq n < b^{l+1}, \tag{6.2}$$

amelyből az f és a log függvények szigorúan növekvő volta és az $\frac{f(a)}{\log a} > 0$ miatt

$$f(b^l) \leq f(n) < f(b^{l+1}),$$
$$\log b^l \leq \log n < \log b^{l+1}$$

és

$$\frac{f(a)}{\log a} \log b^l \leq \frac{f(a)}{\log a} \log n < \frac{f(a)}{\log a} \log b^{l+1}$$

következik. Ezeket az egyenlőtlenségeket, továbbá az f totális additivitását felhasználva adódik, hogy

$$\begin{aligned} g(n) = f(n) - \frac{f(a)}{\log a} \log n > f(b^l) - \frac{f(a)}{\log a} \log b^{l+1} = l f(b) - \\ - (l+1) \frac{f(a)}{\log a} \log b = l \left(f(b) - \frac{f(a)}{\log a} \log b \right) - \frac{f(a)}{\log a} \log b = \\ = l \log b \left(\frac{f(b)}{\log b} - \frac{f(a)}{\log a} \right) - \frac{f(a)}{\log a} \log b. \end{aligned} \tag{6.3}$$

A (6.1) egyenlőtlenség alapján

$$\frac{f(b)}{\log b} - \frac{f(a)}{\log a} > 0,$$

továbbá $\log b > 0$ és (6.2) miatt, $l \to \infty$, ha $n \to \infty$. Ezért (6.3)-ból következik, hogy a g függvény felülről nem korlátos.

A g függvény korlátosságára bizonyított ellentmondó állításokból adódik a tétel állítása. ∎

Nevezetes számelméleti függvények

A továbbiakban a számelméleti bizonyításokban és feladatokban gyakran használt nevezetes számelméleti függvényekkel foglalkozunk.

Definíció. Az e, i és u számelméleti függvényeket az alábbi egyenlőségekkel definiáljuk:

$$e(n) = 1, \quad i(n) = \begin{cases} 1, & \text{ha } n = 1, \\ 0, & \text{egyébként} \end{cases} \qquad \text{és} \quad u(n) = n.$$

6.6. Tétel. *Az e, i és u számelméleti függvények totálisan multiplikatív függvények.*

Bizonyítás. Az állítás nyilvánvaló. ∎

Definíció. A d és σ számelméleti függvények esetén $d(n)$ jelöli az n pozitív osztóinak a számát, azaz $d(n) = \sum\limits_{\substack{d|n \\ d>0}} 1$, míg $\sigma(n)$ jelöli az n pozitív osztóinak az összegét, azaz $\sigma(n) = \sum\limits_{\substack{d|n \\ d>0}} d$.

6.7. Tétel. *A d és σ számelméleti függvények multiplikatív, de nem totálisan multiplikatív függvények.*

Bizonyítás. Azt, hogy d és σ nem totálisan multiplikatív konkrét példákkal igazolhatjuk. Például $d(2\cdot 2) = 3$, de $d(2)d(2) = 4$, illetve $\sigma(2\cdot 2) = 7$, de $\sigma(2)\sigma(2) = 9$.

Legyen $a, b \in \mathbf{N}^+$ és $(a, b) = 1$. Jelölje továbbá a pozitív osztóit

$$d_1, d_2, \ldots, d_{d(a)},$$

míg b pozitív osztóit

$$\delta_1, \delta_2, \ldots, \delta_{d(b)}.$$

Az 1.25. Tétel szerint ab pozitív osztói az a és b pozitív osztóinak szorzataként állnak elő, azaz ab összes pozitív osztója:

$$\begin{array}{cccc} d_1\delta_1, & d_1\delta_2, & \ldots, & d_1\delta_{d(b)}, \\ d_2\delta_1, & d_2\delta_2, & \ldots, & d_2\delta_{d(b)}, \\ \vdots & \vdots & \ddots & \vdots \\ d_{d(a)}\delta_1, & d_{d(a)}\delta_2, & \ldots, & d_{d(a)}\delta_{d(b)}. \end{array}$$

Ebből látható, hogy $d(ab) = d(a)d(b)$, továbbá soronként végezve az összegzést: $\sigma(ab) = d_1\sigma(b) + d_2\sigma(b) + \cdots + d_{d(a)}\sigma(b) = (d_1 + d_2 + \cdots + d_{d(a)})\sigma(b) = \\ = \sigma(a)\sigma(b)$, azaz valóban multiplikatív függvények. ∎

A multiplikatív tulajdonság felhasználásával előállítjuk a d és a σ függvény explicit alakját.

6.8. Tétel. *Ha n kanonikus alakja*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \quad (\alpha_i \geq 1,\ 1 \leq i \leq r,\ p_i \neq p_j \quad \text{ha} \quad i \neq j),$$

akkor

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1) = \prod_{i=1}^{r} (\alpha_i + 1),$$

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{\alpha_r+1} - 1}{p_r - 1} = \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1},$$

és természetesen $d(1) = \sigma(1) = 1$.

Bizonyítás. Tudjuk, hogy mindkét függvény multiplikatív, ezért

$$d(n) = \prod_{i=1}^{r} d(p_i^{\alpha_i}), \quad \text{illetve} \quad \sigma(n) = \prod_{i=1}^{r} \sigma(p_i^{\alpha_i}). \tag{6.4}$$

Mivel $p_i^{\alpha_i}$ pozitív osztói az $1, p_i, p_i^2, \ldots, p_i^{\alpha_i}$ egészek, ezért nyilvánvaló, hogy

$$d(p_i^{\alpha_i}) = \alpha_i + 1$$

és

$$\sigma(p_i^{\alpha_i}) = 1 + p_i + p_i^2 + \cdots + p_i^{\alpha_i} = \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

Ezt (4)-be helyettesítve adódik az állítás. ∎

Külön is érdemes kiemelni, hogy ha p prímszám, akkor $d(p) = 2$ és $\sigma(p) = p + 1$.

A σ számelméleti függvénnyel kapcsolatos a számelmélet egyik, részben máig is megoldatlan problémája. Ez a *tökéletes* számok problémaköre.

Definíció. Az n pozitív egész számot tökéletes számnak nevezzük, ha $\sigma(n) = 2n$. Ha $\sigma(n) > 2n$, illetve $\sigma(n) < 2n$ akkor az n számot osztókban bővelkedő, illetve szűkölködő számnak nevezzük.

A definíció szerint tehát egy pozitív egész akkor tökéletes, ha az önmagánál kisebb pozitív osztóinak összege az illető számmal egyenlő. Ilyen például a 6, mert $1 + 2 + 3 = 6$.

Már Euklidész bizonyította, hogy bizonyos páros számok tökéletesek, míg Euler bizonyította Euklidész állításának a megfordítását. Ezt foglaltuk össze az alábbi tételben.

6.9. Tétel. *Az n páros pozitív egész szám akkor és csak akkor tökéletes, ha*

$$n = 2^{p-1}(2^p - 1)$$

alakú, ahol p és $2^p - 1$ is prímszám.

Bizonyítás. Legyen n a tételben leírt alakú. Mivel $(2^{p-1}, 2^p - 1) = 1$ és $2^p - 1$ prím, ezért

$$\sigma(n) = \sigma\left(2^{p-1}(2^p - 1)\right) = \sigma(2^{p-1})\sigma(2^p - 1) = \frac{2^p - 1}{2 - 1}(1 + 2^p - 1) =$$
$$= 2^p(2^p - 1) = 2\left(2^{p-1}(2^p - 1)\right) = 2n,$$

azaz n valóban tökéletes szám.

Legyen most $n = 2^\alpha m$, ahol $(2, m) = 1$ és $\alpha \geq 1$. Tegyük fel, hogy n tökéletes szám, azaz $2n = \sigma(n)$. Ezt az egyenlőséget részletezve kapjuk, hogy

$$2^{\alpha+1}m = 2 \cdot 2^\alpha m = \sigma(2^\alpha)\sigma(m) = (2^{\alpha+1} - 1)\sigma(m),$$

amelyből a

$$\frac{2^{\alpha+1}}{2^{\alpha+1} - 1} = \frac{\sigma(m)}{m}$$

egyenlőség következik. Mivel $(2^{\alpha+1}, 2^{\alpha+1} - 1) = 1$, ezért létezik olyan k pozitív egész, hogy

$$\sigma(m) = k2^{\alpha+1} \quad \text{és} \quad m = k(2^{\alpha+1} - 1) = k2^{\alpha+1} - k. \tag{6.5}$$

Ebből látható, hogy $\sigma(m) = m + k$ és $k \mid m$. Tehát $\sigma(m)$ az m két pozitív osztójának összegével egyenlő. Ez csak akkor fordulhat elő, ha m prím és $k = 1$. Így (6.5)-ből kapjuk, hogy $m = 2^{\alpha+1} - 1$, azaz $\alpha + 1 = p$ jelöléssel

$$n = 2^{p-1}(2^p - 1),$$

ahol $m = 2^p - 1$ prím. $2^p - 1$ viszont csak akkor lehet prím, ha p prím. Ugyanis ha $p = qr$ $(q, r \geq 2)$, akkor $2^p - 1 = (2^q)^r - 1^r$ osztható $2^q - 1$-gyel és így $2^p - 1$ összetett. ∎

Tételünkből adódik, hogy pontosan annyi páros tökéletes szám van, mint Merssenne-féle prímszám. Máig nyitott az a kérdés, hogy számuk végtelen vagy csak véges. Még kevesebbet tudunk a páratlan tökéletes számokról. Pontosabban, azt sem tudjuk, hogy léteznek-e, vagy sem. Egyelőre annyit tudunk, hogy ha egyáltalán létezik páratlan tökéletes szám, akkor az nagyon nagy, és nagyon sok különböző prímtényezővel rendelkezik.

Ugyancsak a σ függvény segítségével definiálható az úgynevezett *barátságos számpár*.

Definíció. Az n és m pozitív egészeket barátságos számpárnak nevezzük, ha

$$\sigma(n) = \sigma(m) = n + m.$$

Tehát a barátságos számpár egyik tagjának önmagánál kisebb pozitív osztóinak összege a pár másik tagjával egyenlő és viszont.

A tökéletes számokhoz hasonlóan a barátságos számpárok száma sem tisztázott, ma is alig lehet többet mondani e témakörben, mint azt az alábbi, a IX. századból származó *Abdul-Hassan Thabit ben Korrach-tétel* állít.

6.10. Tétel. *Legyen* $p_n = 3 \cdot 2^n - 1$ *és* $q_n = 9 \cdot 2^{2n-1} - 1$, *ahol* $n \in \mathbf{N}^+$. *Ha* p_{n-1}, p_n *és* q_n *egyszerre prímek, akkor az*

$$a = 2^n p_{n-1} p_n \quad \text{és} \quad b = 2^n q_n$$

számok barátságos számpárt alkotnak.

Bizonyítás. $\sigma(a)$ és $\sigma(b)$ meghatározásával könnyen ellenőrizhető, hogy $\sigma(a) = \sigma(b) = a + b$. ∎

Érdemes megjegyezni, hogy a fenti tétel feltételei kielégíthetők. Például $n = 2$ esetben: $a = 220 = 2^2 \cdot 5 \cdot 11$ és $b = 284 = 2^2 \cdot 71$ barátságos számok. Ugyanakkor az is igaz, hogy nem minden barátságos számpár a fenti alakú. Erre példa az 1966-ban, Niedo Paganini által talált $a = 1184 = 2^5 \cdot 37$ és $b = 1210 = 2 \cdot 5 \cdot 112$ barátságos számpár.

A későbbiekben nagyon fontos szerepet játszik a következő, úgynevezett Moebius-féle μ függvény, melyet minden pozitív egészre a következőképpen definiáljuk:

$$\mu(n) = \begin{cases} 1, & \text{ha } n = 1, \\ (-1)^r, & \text{ha } n = p_1 p_2 \cdots p_r, \text{ ahol a } p_i\text{-k különböző prímek}, \\ 0, & \text{ha van olyan } p \text{ prím, melyre } p^2 \mid n. \end{cases}$$

6.11. Tétel. *A* μ *számelméleti függvény multiplikatív.*

Bizonyítás. Ha $n = 1$ és $m \geq 1$, akkor

$$\mu(m1) = \mu(m) = \mu(m)1 = \mu(m)\mu(1).$$

Ha $n > 1$, $m > 1$ és létezik olyan p prím, hogy $p^2 \mid m$, akkor $p^2 \mid mn$ miatt

$$\mu(mn) = 0 = 0\mu(n) = \mu(m)\mu(n).$$

Ha $n > 1$, $m > 1$, $(m, n) = 1$ és m, n egyikének sincs prímnégyzet osztója, akkor $m = p_1 p_2 \cdots p_r$ és $n = q_1 q_2 \cdots q_t$ miatt

$$\mu(mn) = (-1)^{r+t} = (-1)^r (-1)^t = \mu(m)\mu(n).$$

Mivel m és n minden lehetséges értékére bebizonyítottuk, hogy ha $(m, n) = 1$, akkor $\mu(mn) = \mu(m)\mu(n)$, ezért a μ függvény valóban multiplikatív. ∎

A továbbiakban két additív számelméleti függvénnyel ismerkedünk meg.

Definíció. A ν, illetve a χ olyan számelméleti függvények, melyek értékét a

$$\nu(n) = \begin{cases} 0, & \text{ha } n = 1, \\ r, & \text{ha } n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}, \end{cases}$$

illetve a

$$\chi(n) = \begin{cases} 0, & \text{ha } n = 1, \\ \sum\limits_{i=1}^{r} \alpha_i, & \text{ha } n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \end{cases}$$

egyenlőségek határozzák meg, ahol a definícióban az n kanonikus alakja szerepel.

6.12. Tétel. *A ν számelméleti függvény additív, míg a χ függvény totálisan additív.*

Bizonyítás. Legyen $m > 1$, $n > 1$, $(n, m) = 1$ és n, illetve m kanonikus alakja

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}, \quad \text{illetve} \quad n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_t^{\beta_t}.$$

Ekkor — felhasználva, hogy $p_i \neq q_j$ minden i-re és j-re —

$$\nu(mn) = \nu(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} \cdots q_t^{\beta_t}) = r + t = \nu(m) + \nu(n).$$

Ha $m = 1$ és $n \geq 1$, akkor

$$\nu(1n) = \nu(n) = 0 + \nu(n) = \nu(1) + \nu(n),$$

azaz a ν függvény valóban additív.

Legyen most $m > 1$, $n > 1$ továbbá az m és n nem feltétlenül relatív prím egészek prímtényezős alakja

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \quad \text{és} \quad n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r} \quad (\alpha_i \geq 0, \quad \beta_j \geq 0).$$

Ekkor

$$\chi(mn) = \chi\left(\prod_{i=1}^{r} p_i^{\alpha_i+\beta_i}\right) = \sum_{i=1}^{r}(\alpha_i+\beta_i) = \sum_{i=1}^{r}\alpha_i + \sum_{i=1}^{r}\beta_i = \chi(m)+\chi(n).$$

Ha $m = 1$ és $n \geq 1$, akkor

$$\chi(1n) = \chi(n) = 0 + \chi(n) = \chi(1) + \chi(n),$$

azaz a χ számelméleti függvény valóban totálisan additív. ∎

Megjegyezzük, hogy a számelméletben a fenti két függvény jelölése nem egységes, egyes esetekben az itt használt ν és χ függvényeket pontosan fordítva definiálják.

Definíció. A Liouville-féle λ, illetve a Mangoldt-féle Λ számelméleti függvényeket a következő egyenlőségekkel definiáljuk:

$$\lambda(n) = (-1)^{\chi(n)}, \quad \text{illetve} \quad \Lambda(n) = \begin{cases} \log p, & \text{ha } n = p^\alpha \ (p \text{ prím és } \alpha \geq 1), \\ 0, & \text{egyébként.} \end{cases}$$

6.13. Tétel. *A λ függvény totálisan multiplikatív, míg a Λ függvény se nem multiplikatív, se nem additív.*

Bizonyítás. Legyen $m, n \in \mathbf{N}^+$. Ekkor χ totálisan additív volta miatt

$$\lambda(mn) = (-1)^{\chi(mn)} = (-1)^{\chi(m)+\chi(n)} = (-1)^{\chi(m)}(-1)^{\chi(n)} = \lambda(m)\lambda(n),$$

azaz a λ függvény valóban totálisan multiplikatív.

A Λ függvényre vonatkozó állítás konkrét példával is igazolható. Például

$$\Lambda(2\cdot 3) = 0 \quad \text{de,} \quad \Lambda(2)\Lambda(3) = \log 2 \cdot \log 3 \neq 0,$$

azaz Λ nem lehet multiplikatív. (Természetesen $\Lambda(1) = 0 \neq 1$ már kizárja a multiplikativitást.) Ugyanakkor

$$\Lambda(2) + \Lambda(3) = \log 2 + \log 3 \neq 0$$

miatt Λ nem nem lehet additív sem. ∎

A Dirichlet-féle konvolúciós szorzás

Korábban már foglalkoztunk számelméleti függvények szorzatával, ahol az f és a g függvény szorzatát az $(fg)(n) = f(n)g(n)$ egyenlőséggel definiáltuk. Most egy, a számelméletben hasznosabb szorzással, az úgynevezett *Dirichlet-féle konvolúcióval* foglalkozunk.

Vezessük be a következő jelölést:

$$D = \{f : f \text{ számelméleti függvény}\}$$

Definíció. Legyen $f, g \in D$. Az f és g Dirichlet-féle konvulúcióján értjük és $f \star g$-vel jelöljük az

$$(f \star g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \sum_{d_1 d_2 = n} f(d_1) g(d_2)$$

egyenlőséggel meghatározott számelméleti függvényt, ahol az összegzés n összes pozitív osztójára értendő.

6.14. Tétel. *A $(D, \star)$ struktúra kommutatív egységelemes félcsoport, amelynek az i számelméleti függvény az egységeleme.*

Bizonyítás. A D halmaz nyilvánvalóan zárt a $\star$ műveletre. A kommutatív tulajdonság, azaz $f \star g = g \star f$ szintén teljesül, mivel a konvolúció definíciója szerint mindkét oldal ugyanaz az összeg bármely $n \in \mathbf{N}^+$ esetén. A $\star$ művelet asszociativitását például az alábbi módon igazolhatjuk. Legyen $f, g, h \in D$, ekkor

$$\big((f \star g) \star h\big)(n) = \sum_{d_1 d_2 d_3 = n} \big(f(d_1) g(d_2)\big) h(d_3) = \\ = \sum_{d_1 d_2 d_3 = n} f(d_1) \big(g(d_2) h(d_3)\big) = \big(f \star (g \star h)\big)(n).$$

Az i egységelem voltához az $i \star f = f$ egyenlőséget kell igazolni bármely f számelméleti függvényre.

$$(i \star f)(n) = \sum_{d|n} i(d) f\left(\frac{n}{d}\right) = i(1) f(n) + \sum_{\substack{d|n \\ d>1}} i(d) f\left(\frac{n}{d}\right) = \\ = 1 f(n) + \sum_{\substack{d|n \\ d>1}} 0 \cdot f\left(\frac{n}{d}\right) = f(n) \quad \text{minden } n\text{-re.}$$

Mivel asszociatív struktúrában legfeljebb egy egységelem lehet, ezért i az egyetlen egységelem a $(D, \star)$ struktúrában. ∎

Felvetődhet a kérdés, hogy D elemei közül melyeknek létezik inverze a $\star$ műveletre nézve. Erről szól az alábbi tétel.

6.15. Tétel. *Az f számelméleti függvénynek akkor és csak akkor létezik inverze a $\star$ műveletre nézve, ha $f(1) \neq 0$.*

Bizonyítás. Ha f-nek van inverze, melyet jelöljünk f^{-1}-gyel, akkor $(f \star f^{-1})(n) = i(n)$ teljesül minden $n \in \mathbf{N}^+$ esetén, így

$$(f \star f^{-1})(1) = i(1).$$

Ebből kapjuk, hogy

$$(f \star f^{-1})(1) = f(1)f^{-1}(1) = i(1) = 1$$

miatt $f(1) \neq 0$.

Legyen most $f(1) \neq 0$. Az f inverzének létezését oly módon bizonyítjuk, hogy megkonstruáljuk az f^{-1} függvényt. A keresett f^{-1} függvénynek minden $n \in \mathbf{N}^+$ esetén teljesítenie kell az

$$(f \star f^{-1})(n) = i(n)$$

egyenlőséget. $(f \star f^{-1})(1) = f(1)f^{-1}(1) = 1$-ből kapjuk, hogy

$$f^{-1}(1) = \frac{1}{f(1)}.$$

$f^{-1}(2)$ meghatározható az

$$(f \star f^{-1})(2) = f(1)f^{-1}(2) + f(2)f^{-1}(1) = i(2) = 0$$

egyenlőségből, azaz

$$f^{-1}(2) = -\frac{f(2)f^{-1}(1)}{f(1)}.$$

Teljes indukcióval belátható, hogy $f^{-1}(n)$ értéke mindig meghatározható az $f(k)$ és $f^{-1}(l)$ értékek ismeretében, ahol $1 \leq k \leq n$ és $1 \leq l \leq n-1$. Az f^{-1} egyértelműsége szintén a $\star$ művelet asszociatív tulajdonságából következik. ∎

E tétel egyszerű következménye, hogy minden multiplikatív számelméleti függvénynek van inverze a $\star$ műveletre nézve. Továbbá az is bizonyítható, hogy multiplikatív függvény inverze is multiplikatív.

Az f és f^{-1} számelméleti függvényekkel érdekes, úgynevezett inverziós formulák nyerhetők az alábbi tétel szerint.

6.16. Tétel. *Legyen $f, g, h \in D$ és létezzen az f^{-1} számelméleti függvény. $f \star g = h$ akkor és csak akkor, ha $g = f^{-1} \star h$.*

Bizonyítás. Kiindulva az $f \star g = h$ egyenlőségből, melyet f^{-1}-gyel szorozva kapjuk, hogy

$$f^{-1} \star (f \star g) = f^{-1} \star h.$$

Ebből, az asszociativitás és $f^{-1} \star f = i$ alapján $g = f^{-1} \star h$ adódik.

Teljesen hasonlóan nyerhető a $g = f^{-1} \star h$ egyenlőségből az $f \star g = h$ egyenlőség. ∎

Konkrét inverziós formulákat nyerhetünk az f és az f^{-1} függvény konkretizálásával. Ilyenek például az e és a μ számelméleti függvények.

6.17. Tétel. *Az e és a μ számelméleti függvény egymás inverze a konvolúciós szorzásra nézve.*

Bizonyítás. Igazolni kell, hogy $(e \star \mu)(n) = i(n)$ minden $n \in \mathbf{N}^+$ egészre. Mivel

$$(e \star \mu)(n) = \sum_{d|n} e(d)\mu\left(\frac{n}{d}\right) = \sum_{d|n} 1 \cdot \mu\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d), \tag{6.6}$$

ezért ha $n = 1$, akkor

$$(e \star \mu)(1) = \sum_{d|1} \mu(1) = 1 = i(1).$$

Legyen $n > 1$ és n kanonikus alakja $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$. Ekkor (6.6) szerint

$$\begin{aligned}(e \star \mu)(n) = \sum_{d|n} \mu(d) = \mu(1) + \mu(p_1) + \mu(p_2) + \cdots + \mu(p_r) + \\ + \mu(p_1p_2) + \mu(p_1p_3) + \cdots + \mu(p_{r-1}p_r) + \\ + \mu(p_1p_2p_3) + \mu(p_1p_2p_4) + \cdots + \mu(p_{r-2}p_{r-1}p_r) + \\ + \cdots + \mu(p_1p_2\cdots p_r) + \sum_{\substack{d|n \\ p_i^2|d}} \mu(d).\end{aligned}$$

Ebből, a μ definíciója és a binomiális együtthatók ismert tulajdonsága alapján kapjuk, hogy

$$(e\star\mu)(n) = 1+\binom{r}{1}(-1)+\binom{r}{2}1+\binom{r}{3}(-1)+\cdots+\binom{r}{r}(-1)^r+0 = 0 = i(n).$$

Ezzel beláttuk, hogy e és μ valóban egymás inverzei. ∎

A tételből, illetve a bizonyításából közvetlen adódik a μ függvény egy tulajdonsága, de ezt érdemes külön is kiemelni.

Minden $n \geq 2$ egész szám esetén

$$\sum_{d|n} \mu(d) = 0.$$

A 6.16. Tétel és a 6.17. Tétel következményeként nyerhető az alábbi, úgynevezett *Moebius-féle inverziós formula.* Legyen $f, g \in D$. $e\star f = g$ akkor és csak akkor, ha

$$f = \mu \star g.$$

Ezt részletesebben kifejtve kapjuk, hogy

$$(6.7) \quad g(n) = \sum_{d|n} f(d) \text{ akkor és csak akkor, ha } f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right).$$

Definíció. Ha $g(n) = \sum\limits_{d|n} f(d)$, akkor a g számelméleti függvényt az f számelméleti függvény összegezési függvényének nevezzük. Ha pedig $f(n) = \sum\limits_{d|n} \mu(d) g\left(\frac{n}{d}\right)$, akkor f-et a g függvény Moebius-transzformáltjának nevezzük.

E definíciókkal (6.7) így is megfogalmazható: *Az f függvény összegezési függvénye akkor és csak akkor a g függvény, ha g Moebius-féle transzformáltja f.*

Tudjuk, hogy multiplikatív számelméleti függvények esetén a helyettesítési értékek meghatározásához elegendő a prímhatvány helyeken felvett értékeket ismerni. Ezért érdemes megvizsgálni, hogy multiplikatív függvények konvolúciós szorzata multiplikatív-e vagy nem.

6.18. Tétel. *Ha f és g multiplikatív, akkor $f \star g$ is az.*

Bizonyítás. Igazolni kell, hogy minden $(m, n) = 1$ esetén

$$(6.8) \qquad (f \star g)(mn) = (f \star g)(m)(f \star g)(n).$$

Induljunk ki (6.8) bal oldalából, majd alkalmazzuk az 1.25. Tétel állítását.

$$(f\star g)(mn)=\sum_{d|mn}f(d)g\left(\frac{mn}{d}\right)=\sum_{d_1|m}\sum_{d_2|n}f(d_1d_2)g\left(\frac{mn}{d_1d_2}\right)=$$
$$=\sum_{d_1|m}\sum_{d_2|n}f(d_1)f(d_2)g\left(\frac{m}{d_1}\right)g\left(\frac{n}{d_2}\right)=$$
$$=\left(\sum_{d_1|m}f(d_1)g\left(\frac{m}{d_1}\right)\right)\left(\sum_{d_2|n}f(d_2)g\left(\frac{n}{d_2}\right)\right)=(f\star g)(m)(f\star g)(n),$$

tehát $f\star g$ valóban multiplikatív. ∎

Az e és a μ multiplikativitása miatt tételünk nyilvánvaló következménye, hogy multiplikatív függvény összegezési függvénye, illetve Moebius-féle transzformáltja is multiplikatív. Ezért, ha f multiplikatív és g az összegezési függvénye, akkor $g(1)=1$, míg $n>1$ esetén, ha n kanonikus alakja $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$, úgy

$$g(n)=\prod_{i=1}^{r}g\left(p_i^{\alpha_i}\right)=\prod_{i=1}^{r}\sum_{d|p_i^{\alpha_i}}f(d)=\prod_{i=1}^{r}\sum_{\beta_i=0}^{\alpha_i}f\left(p_i^{\beta_i}\right).$$

Hasonlóan nyerhető a g multiplikatív függvény f Moebius-féle transzformáltjára, hogy $f(1)=1$, míg $n>1$ esetén, ha n kanonikus alakja $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$, akkor

$$f(n)=\prod_{i=1}^{r}f\left(p_i^{\alpha_i}\right)=\prod_{i=1}^{r}\sum_{d|p_i^{\alpha_i}}\mu(d)g\left(\frac{p_i^{\alpha_i}}{d}\right)=$$
$$=\prod_{i=1}^{r}\sum_{\beta_i=0}^{\alpha_i}\mu\left(p_i^{\beta_i}\right)g\left(p_i^{\alpha_i-\beta_i}\right)=$$
$$=\prod_{i=1}^{r}\left(\mu(1)g\left(p_i^{\alpha_i}\right)+\mu(p_i)g\left(p_i^{\alpha_i-1}\right)+0\right)=$$
$$=\prod_{i=1}^{r}\left(g\left(p_i^{\alpha_i}\right)-g\left(p_i^{\alpha_i-1}\right)\right).$$

A fentiek alkalmazásával szép összefüggések nyerhetők különböző számelméleti függvények között. Példaként határozzuk meg az u számelméleti

függvény f Moebius-féle transzformáltját. Mivel az u függvény multiplikatív, ezért $f(1) = 1$, míg $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ esetben az előzőek szerint

$$f(n) = \prod_{i=1}^{r} \left(u\left(p_i^{\alpha_i}\right) - u\left(p_i^{\alpha_i - 1}\right) \right) =$$

$$= \prod_{i=1}^{r} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1} \right) = \varphi(n).$$

Azt kaptuk tehát, hogy az u függvény Moebius-féle transzformáltja az Euler-féle φ függvény. Ebből adódik a következő összefüggés:

$$\varphi(n) = \sum_{d|n} \mu(d) u\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \frac{n}{d} =$$

$$= n \sum_{d|n} \frac{\mu(d)}{d}.$$

Számelméleti függvények értékeinek eloszlása, átlagérték függvények

Az eddigiekben megvizsgáltuk a számelméleti függvények egyes tulajdonságait (multiplikativitás, additivitás stb.), a továbbiakban a függvények értékkészletének vizsgálatával foglalkozunk. Felvetődhet az igény, hogy egy konkrét számelméleti függvény értékkészletét vizsgálva szerezzünk újabb ismereteket a függvényről. Egyszerűbb esetekben az értékkészlet könnyen megadható, például a μ függvény esetében $\{0, 1, -1\}$, vagy a ν esetén az $\mathbf{N}$, ugyanakkor más esetekben nehéz matematikai probléma lehet az értékkészlet meghatározása.

Kérdés lehet, hogy egy adott számelméleti függvény értékei nagy ingadozást mutatnak-e, hogy a felvett értékek milyen nagyok lehetnek az n függvényében. Például a φ függvényre $n > 1$ esetén nyilván $\varphi(n) \leq n - 1$, és ez nem is javítható, mivel ha n prímszám, akkor $\varphi(n) = n - 1$.

A továbbiakban a d számelméleti függvény értékkészletét vizsgáljuk.

6.19. Tétel. *$d(n) = 1$ akkor és csak akkor ha $n = 1$, és minden $m > 1$ egész számhoz végtelen sok $n \in \mathbf{N}^+$ létezik, amelyekre $d(n) = m$.*

Bizonyítás. Mivel $n = 1$ az egyetlen pozitív egész, melynek egyetlen pozitív osztója van, ezért az első állítás triviális. Adott $m > 1$ esetén tekintsük például az $n = p^{m-1}$ egész számokat, ahol p prímszám. Ekkor

$$d(n) = d(p^{m-1}) = m,$$

és mivel végtelen sok prímszám van, ezért az állítás második része is igaz. ∎

Ha meghatározzuk a $d(n)$ értékeket, akkor jelentős ingadozásokat figyelhetünk meg. Például $d(36) = 9$, $d(37) = 2$ és $d(38) = 6$. Vajon lehet-e tetszőlegesen nagy ,,ugrás" valamely két szomszédos egész szám helyen? Ennél lényegesen többet állít az alábbi tétel.

6.20. Tétel. *Tetszőleges $\omega \in \mathbf{N}^+$ esetén végtelen sok szomszédos pozitív egész számokból álló $a-1$, a, $a+1$ számhármas létezik, melyekre*

$$d(a-1) - d(a) \geq \omega \quad \text{és} \quad d(a+1) - d(a) \geq \omega, \tag{6.9}$$

(azaz a d függvény grafikonjában végtelen sok, legalább ω ,,mélységű völgyet" találunk.)

Bizonyítás. Tételünk bizonyításához szükségünk lesz Dirichlet egy tételére, amelyet speciális esetekben a 7. fejezetben bizonyítunk. A tétel a következőt mondja ki. Legyen $a, b \in \mathbf{N}^+$ és $(a, b) = 1$. Az

$$a,\ a+b,\ a+2b,\ a+3b, \ldots$$

számtani sorozatban végtelen sok prímszám van.

Válasszunk 2ω számú különböző prímszámot, melyeket

$$p_1, p_2, \ldots, p_\omega \quad \text{és} \quad q_1, q_2, \ldots, q_\omega$$

jelöl, továbbá legyen

$$P = \prod_{i=1}^{\omega} p_i \quad \text{és} \quad Q = \prod_{i=1}^{\omega} q_i.$$

Tekintsük az

$$\left.\begin{aligned} x &\equiv 1 \pmod{P} \\ x &\equiv -1 \pmod{Q} \end{aligned}\right\} \tag{6.10}$$

szimultán kongruenciarendszert. Az 5.3. Tétel (vagy az 5.5. Tétel) szerint (6.10) megoldható és egyetlen x_0 megoldása van modulo PQ. Ezért a (6.10)-et kielégítő x egész számok

$$x = x_0 + PQk$$

alakúak, ahol $k \in \mathbf{Z}$. Nyilvánvaló, hogy $(x_0, PQ) = 1$, továbbá feltehető, hogy $x_0 > 0$. Dirichlet tétele szerint így az

$$\{x : x = x_0 + PQk,\ k \in \mathbf{N}\}$$

halmazban (illetve a megfelelő számtani sorozatban) végtelen sok prímszám van. Megmutatjuk, hogy ha az $a = p$ prímszám ezen prímek közé tartozik, akkor (6.9) teljesül. p nyilvánvalóan megoldása (6.10)-nek, azaz

$$p \equiv 1 \pmod{P} \quad \text{és} \quad p \equiv -1 \pmod{Q}.$$

Ebből kapjuk, hogy

$$p_i \mid (p-1) \quad \text{és} \quad q_i \mid (p+1)$$

minden i $(1 \le i \le \omega)$ indexre. Ezért $p-1$-nek és $p+1$-nek legalább annyi pozitív osztója van, mint amennyit az ω darab különböző prímből elő lehet állítani. A $d = 1$ osztóval együtt ezek száma nyilván 2^ω. Ezek alapján

$$d(p-1) \ge 2^\omega, \quad d(p) = 2, \quad d(p+1) \ge 2^\omega,$$

amelyből a kívánt

$$d(p-1) - d(p) \ge 2^\omega - 2 \ge \omega \quad \text{és} \quad d(p+1) - d(p) \ge 2^\omega - 2 \ge \omega$$

egyenlőtlenségek adódnak, ha $\omega \ge 2$. ∎

A $d(n)$ értékeknek az n-hez hasonlított nagyságrendjéről szól a következő tétel.

6.21. Tétel. *Tetszőleges $\varepsilon > 0$ valós számhoz létezik olyan ε-tól függő c pozitív konstans, hogy bármely n pozitív egészre*

$$d(n) < cn^\varepsilon.$$

Bizonyítás. Legyen $n > 1$ és kanonikus alakja $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, továbbá igazoljuk állításunkat

$$\frac{d(n)}{n^\varepsilon} < c \tag{6.11}$$

alakban, ahol feltehető, hogy $0 < \varepsilon < 1$. $d(n)$ explicit alakját használva kapjuk, hogy

$$\frac{d(n)}{n^\varepsilon} = \frac{(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_r+1)}{p_1^{\varepsilon\alpha_1} p_2^{\varepsilon\alpha_2} \cdots p_r^{\varepsilon\alpha_r}} = \prod_{i=1}^{r} \frac{\alpha_i+1}{p_i^{\varepsilon\alpha_i}}. \tag{6.12}$$

Ahhoz, hogy a (6.11)-ben szereplő egyenlőtlenséghez jussunk, a (6.12)-ban szereplő

$$\frac{\alpha_i+1}{p_i^{\varepsilon\alpha_i}}$$

tényezőket kell felülről becsülni. Kezdjük ezt a $p_i^{\varepsilon\alpha_i}$ alsó becslésével:

$$p_i^{\varepsilon\alpha_i} \geq 2^{\varepsilon\alpha_i} = e^{\varepsilon\alpha_i \log 2} > \varepsilon\alpha_i \log 2 = \varepsilon\frac{\alpha_i+\alpha_i}{2}\log 2 \geq \varepsilon\frac{\alpha_i+1}{2}\log 2, \tag{6.13}$$

ahol felhasználtuk, hogy $p_i \geq 2$, $e^x > x$ és $\alpha_i \geq 1$. Azon $p_i^{\varepsilon\alpha_i}$-re, ahol $p_i^{\varepsilon} \geq 2$, a (6.13)-ban szereplő alsó becslésnél jobbat is adhatunk, ugyanis $\alpha_i \geq 1$ miatt

$$p_i^{\varepsilon\alpha_i} \geq 2^{\alpha_i} \geq \alpha_i + 1. \tag{6.14}$$

A (6.13) és a (6.14) becslések segítségével (6.12)-ből az alábbi egyenlőtlenségek adódnak:

$$\frac{d(n)}{n^\varepsilon} = \prod_{i=1}^{r}\frac{\alpha_i+1}{p_i^{\varepsilon\alpha_i}} = \prod_{\substack{p_i\mid n\\ p_i^\varepsilon<2}}\frac{\alpha_i+1}{p_i^{\varepsilon\alpha_i}}\prod_{\substack{p_j\mid n\\ p_j^\varepsilon\geq 2}}\frac{\alpha_j+1}{p_j^{\varepsilon\alpha_j}} \leq$$

$$\leq \prod_{\substack{p_i\mid n\\ p_i^\varepsilon<2}}\frac{\alpha_i+1}{\frac{\varepsilon}{2}(\alpha_i+1)\log 2}\prod_{\substack{p_j\mid n\\ p_j^\varepsilon\geq 2}}\frac{\alpha_j+1}{\alpha_j+1} = \prod_{\substack{p_i\mid n\\ p_i^\varepsilon<2}}\frac{2}{\varepsilon\log 2} \leq \prod_{p^\varepsilon<2}\frac{2}{\varepsilon\log 2},$$

ahol az utolsó szorzást minden olyan p prímre el kell végezni, amelyekre $p^\varepsilon < 2$. Látható, hogy

$$c = \prod_{p^\varepsilon<2}\frac{2}{\varepsilon\log 2} > 1$$

független n-től, és így egyedül ε-tól függő konstans. Mivel $c > 1$, így (6.11) $n = 1$ esetén is teljesül. ∎

Tételünkből egyszerűen következik, hogy

$$\lim_{n\to\infty}\frac{\log d(n)}{\log n} = 0, \tag{6.15}$$

ugyanis a $d(n) < cn^\varepsilon$ egyenlőtlenségből mindkét oldal logaritmusát véve kapjuk, hogy $\log d(n) < \log c + \varepsilon \log n$, vagyis $n > 1$ esetben

$$0 < \frac{\log d(n)}{\log n} < \frac{\log c}{\log n} + \varepsilon.$$

Mivel ez utóbbi minden $\varepsilon > 0$-ra teljesül, és $\lim_{n\to\infty} \frac{\log c}{\log n} = 0$, ezért igaz (6.15).

A számelméleti függvények értékkészlete, mint azt az előzőekben a d függvénynél is láttuk, alig-alig mutatnak valami szabályosságot, inkább jellemző rájuk a nagyfokú ingadozás. Ezért is merült fel, hogy a számelméleti függvények átlagérték függvényeit vizsgáljuk, reménykedve abban, hogy ezek már közelíthetők — legalábbis nagy n-ek esetén — ismert valós függvényekkel.

Definíció. Legyen f számelméleti függvény és

$$F(n) = f(1) + f(2) + \cdots + f(n).$$

Az $\overline{F}(n) = \frac{F(n)}{n}$ hozzárendeléssel értelmezett $\overline{F}$ számelméleti függvényt az f átlagérték függvényének nevezzük.

E témakör fontos definíciója a következő.

Definíció. Legyen f és g két valós függvény. Ha

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1,$$

akkor azt mondjuk, hogy f aszimptotikusan egyenlő g-vel és ezt az $f \sim g$ szimbólummal jelöljük.

Vezessük be a következő jelöléseket:

$$S(n) = \sum_{i=1}^{n} \sigma(i), \qquad \overline{S}(n) = \frac{S(n)}{n};$$
$$\Phi(n) = \sum_{i=1}^{n} \varphi(i), \qquad \overline{\Phi}(n) = \frac{\Phi(n)}{n};$$
$$V(n) = \sum_{i=1}^{n} \nu(i), \qquad \overline{V}(n) = \frac{V(n)}{n};$$
$$D(n) = \sum_{i=1}^{n} d(i), \qquad \overline{D}(n) = \frac{D(n)}{n}.$$

Ismertek a fentiekre vonatkozó alábbi aszimptotikus egyenlőségek.

$$\overline{S} \sim f, \quad \text{ahol} \quad f(n) = \frac{\pi^2}{6} n;$$
$$\overline{\Phi} \sim g, \quad \text{ahol} \quad g(n) = \frac{3}{\pi^2} n;$$
$$\overline{V} \sim h, \quad \text{ahol} \quad h(n) = \log\log n \quad (n > 1);$$
$$\overline{D} \sim t, \quad \text{ahol} \quad t(n) = \log n.$$

Ezek közül csak az utolsót részletezzük.

6.22. Tétel. *A d számelméleti függvény átlagérték függvénye aszimptotikusan egyenlő a* log *függvénnyel, azaz*

$$\frac{1}{n}\sum_{i=1}^{n} d(i) \sim \log n.$$

Bizonyítás. Tételünk bizonyításához szükségünk van a számelméleti bizonyításokban gyakran használt

$$\log(n+1) < \sum_{m=1}^{n} \frac{1}{m} < 1 + \log n \tag{6.16}$$

egyenlőtlenségre, amelyet szokás integrállal, illetve az analízisből ismert

$$\left(1+\frac{1}{m}\right)^{m} < e < \left(1+\frac{1}{m}\right)^{m+1} \quad (m \in \mathbf{N}^{+}) \tag{6.17}$$

egyenlőtlenség segítségével igazolni. Az integrálos bizonyítások inkább a prímszámelméletben elterjedtek (lásd a 7. fejezetet), ezért (6.16)-ot itt a (6.17) alapján bizonyítjuk.

A (6.17)-beli egyenlőtlenségek mindkét oldalát logaritmálva kapjuk, hogy

$$m \log \frac{m+1}{m} < 1 < (m+1) \log \frac{m+1}{m},$$

amelyből log $\frac{m+1}{m}$-mel osztva, majd az egyenlőtlenség reciprokát véve az

$$\frac{1}{m+1} < \log \frac{m+1}{m} < \frac{1}{m} \tag{6.18}$$

egyenlőtlenséghez jutunk. (6.18)-ból adódik, hogy

$$\sum_{m=1}^{n} \log \frac{m+1}{m} < \sum_{m=1}^{n} \frac{1}{m},$$

azaz, a logaritmus ismert azonossága miatt

$$\log(n+1) = \log\left(2 \cdot \frac{3}{2} \cdot \frac{4}{3} \cdots \frac{n+1}{n}\right) = \sum_{m=1}^{n} \log \frac{m+1}{m} < \sum_{m=1}^{n} \frac{1}{m}.$$

Ugyancsak (6.18)-ból kapjuk, hogy

$$1+\sum_{m=1}^{n-1}\frac{1}{m+1}<1+\sum_{m=1}^{n-1}\log\frac{m+1}{m},$$

amelyből

$$\sum_{m=1}^{n}\frac{1}{m}<1+\log\left(2\cdot\frac{3}{2}\cdot\ldots\cdot\frac{n}{n-1}\right)=1+\log n$$

következik. Ezzel a (6.16) egyenlőtlenséget igazoltuk.

A tételünk bizonyításához szintén felhasználjuk a

$$D(n)=d(1)+d(2)+\cdots+d(n)=\sum_{m=1}^{n}\left[\frac{n}{m}\right] \tag{6.19}$$

összefüggést, amely pedig azért igaz, mert az osztók számának a meghatározása nem függhet az összeszámlálási módtól. Ugyanis a jobb oldali összegzéskor azt vizsgáljuk, hogy egy adott m az $1,2,\ldots,n$ számok közül hánynak osztója, míg a másik esetben az $1,2,\ldots,n$ számok osztóinak a számát összegezzük. ($[x]$ az x egész részét jelöli.)

A továbbiakban $D(n)$-re adunk egy alsó és egy felső becslést (6.16) és (6.19) segítségével.

$$\begin{aligned}D(n)=\sum_{m=1}^{n}\left[\frac{n}{m}\right]\geq\sum_{m=1}^{n}(\frac{n}{m}-1)=-n+n\sum_{m=1}^{n}\frac{1}{m}>\\ >n\log(n+1)-n>n\log n-n\end{aligned}$$

és

$$D(n)=\sum_{m=1}^{n}\left[\frac{n}{m}\right]\leq\sum_{m=1}^{n}\frac{n}{m}=n\sum_{m=1}^{n}\frac{1}{m}<n(1+\log n).$$

Ezen egyenlőtlenségekből kapjuk, hogy

$$-1<\frac{D(n)}{n}-\log n<1. \tag{6.20}$$

Legyen

$$r(n)=\frac{D(n)}{n}-\log n, \tag{6.21}$$

ahol (6.20) miatt $|r(n)| < 1$. (6.21)-ből következik, hogy

$$\frac{\overline{D}(n)}{\log n} = \frac{D(n)}{n \log n} = 1 + \frac{r(n)}{\log n},$$

amelyből $|r(n)| < 1$ miatt

$$\lim_{n \to \infty} \frac{\overline{D}(n)}{\log n} = 1,$$

azaz $\overline{D} \sim \log$. ∎

E témakör befejezéseként megemlítjük, hogy általában nem igaz az, hogy $f(n)$ leggyakrabban az $\overline{F}(n)$-hez közeli érték, jóllehet van ilyen számelméleti függvény is.

Feladatok

1. Mi a szükséges és elégséges feltétele annak, hogy $d(n)$ értéke páratlan legyen?

2. Legyen $P(n) = \prod_{d|n} d$. Bizonyítsuk be, hogy $P(n) = n^{\frac{d(n)}{2}}$.

3. Melyik az a minimális n, amelyre $d(n) = 23$.

4. Bizonyítsuk be, hogy

(a) minden prímszámhatvány osztókban hiányos (szűkölködő);

(b) három páratlan prímszám szorzata osztókban hiányos (szűkölködő).

5. Bizonyítsuk be, hogy ha n tökéletes szám, akkor $\sum_{d|n} \frac{1}{d} = 2$.

6. Bizonyítsuk be, hogy $\varphi(n)$ páros szám, ha $n \geq 3$.

7. Odjuk meg a $\varphi(x) = 24$ egyenletet.

8. Bizonyítsuk be, hogy bármely $n \in \mathbf{N}^+$-ra

(a) $d(n) + \varphi(n) \leq n + 1$;

(b) $\sigma(n)\varphi(n) \leq n^2$.

9. Bizonyítsuk be, hogy bármely $m, n \in \mathbf{N}^+$-ra

(a) ha $m \mid n$, akkor $\varphi(m) \mid \varphi(n)$;

(b) $2^{\nu(n)} \leq d(n) \leq 2^{\chi(n)}$.

10. Bizonyítsuk be, hogy

(a) az u függvény ($u(n) = n$) összegezési függvénye a σ függvény;

(b) a φ függvény összegezési függvénye az u függvény;

(c) $\sum_{d|n} |\mu(d)| = 2^k$, ha $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$.

(d) ha $f(n) = (-1)^{n+1}$ és $g(n) = (1-k)d(m)$, ahol $n = 2^k m$ ($k \geq 0$, $(2, m) = 1$), akkor f összegezési függvénye g;

(e) ha $f(n) = \frac{1}{n}$ és $g(n) = \frac{\sigma(n)}{n}$, akkor f összegezési függvénye g;

(f) $\sum_{d|n} \lambda(d) = \begin{cases} 1, & \text{ha } n \text{ négyzetszám,} \\ 0, & \text{egyébként.} \end{cases}$

11. Bizonyítsuk be, hogy

(a) $\sum_{d|n} \Lambda(d) = \log n$;

(b) $\Lambda(n) = -\sum_{d|n} \mu(d) \log d$.

12. Igazoljuk, hogy bármely $n \in \mathbf{N}^+$ esetén

(a) $(\varphi \star d)(n) = \sigma(n)$;

(b) $\frac{1}{n}(\varphi \star \sigma)(n) = d(n)$;

(c) $(\Lambda \star d)(n) = \frac{1}{2} d(n) \log n$.

13. Bizonyítsuk be, hogy $\chi(n) \log 2 \leq \log n$, ha $n \in \mathbf{N}^+$.

14. Bizonyítsuk be, hogy bármely $m \in \mathbf{N}^+$ esetén

$$\frac{\sigma(m!)}{m!} \geq \sum_{d=1}^{m} \frac{1}{d}.$$

15. Bizonyítsuk be, hogy $n \geq 9$ esetén $d(n) \leq n - 5$.

16. Milyen n pozitív egész számokra igaz, hogy

$$2d(n^2) - 3d(n) = 0?$$

7. A prímszámelmélet elemei

Az előzőekben már foglalkoztunk prímszámokkal és a prímszámok jelentőségével a számelméleti problémák tárgyalása során. Most a prímszámok mélyebb tulajdonságait és a velük kapcsolatban felvetődő eloszlási problémákat fogjuk megvizsgálni.

Korábban említettük (1.28. Tétel), hogy a prímek száma végtelen. Ezt már Euklidész is tudta, de a prímek végtelensége a fejezetünk legtöbb tételéből is következik. Bevezetésként azonban megmutatunk erre egy másik elemi bizonyítást.

7.1. Tétel. *A prímszámok száma végtelen.*

Bizonyítás. Bebizonyítjuk, hogy az

$$F_n = 2^{2^n} + 1 \quad (n = 0, 1, 2, \ldots)$$

alakú Fermat-számok páronként relatív prímek. Legyenek $k \geq 1$ és $n \geq 0$ pozitív egészek és legyen $d = (F_{n+k}, F_n)$. Mivel

$$F_{n+k} = 2^{2^n 2^k} + 1 = (F_n - 1)^{2^k} + 1,$$

ezért a binomiális tétel alkalmazásával vagy más elemi módszerrel könnyű belátni, hogy F_{n+k} alakja

$$F_{n+k} = F_n t + 2,$$

ahol t egy pozitív egész. De $d \mid F_n$ és $d \mid F_{n+k}$, ezért $d \mid 2$ és így $d = 1$, mivel a Fermat-számok páratlanok.

(A $d = 1$ állítás kongruenciák alkalmazásával is bizonyítható. Mivel $d \mid F_n$ és $d \mid F_{n+k}$, ezért $2^{2^n} \equiv -1 \pmod{d}$ és

$$\begin{aligned} 0 \equiv F_{n+k} - F_n = 2^{2^{n+k}} - 2^{2^n} = 2^{2^n}\left(2^{2^{n+k}-2^n} - 1\right) \equiv \\ \equiv -\left(2^{2^{n+k}-2^n} - 1\right) = 1 - \left(2^{2^n}\right)^{2^k-1} \equiv \\ \equiv 1 - (-1)^{2^k-1} = 2 \pmod{d}. \end{aligned}$$

Ebből $d \mid 2$ és d páratlan volta miatt $d = 1$ következik.)

Tehát a Fermat-számok valóban páronként relatív prímek. Mindegyik Fermat-szám tartalmaz legalább egy prímtényezőt, ami a relatív prímség

miatt különbözik a többi Fermat-szám prímtényezőitől, így legalább annyi prímszám van, mint ahány Fermat-szám, vagyis végtelen sok. ∎

Az egymást követő $p_1 = 2$, $p_2 = 3$, $p_3, p_4, \ldots$ prímszámok sorozatát szemlélve nehéz közöttük valami szabályosságot találni. Egy durva felső korlát viszont könnyen adható az n-edik prímszámra.

7.2. Tétel. *Legyen p_n az n-edik prímszám. Ekkor*

$$p_n < 2^{2^{n-1}},$$

ha $n > 1$.

Bizonyítás. Megjegyezzük, hogy az $n > 1$ feltétel azért szükséges, mert $n = 1$ esetén $p_1 = 2 = 2^{2^{1-1}}$ és így a tételbeli szigorú egyenlőtlenség helyett egyenlőség teljesül. A tételt teljes indukcióval bizonyítjuk. Az állítás $n = 2$ és $n = 3$ esetén igaz, mert $p_2 = 3 < 2^{2^1} = 4$ és $p_3 = 5 < 2^{2^2} = 16$. Tegyük fel, hogy igaz az állítás $n = 2, 3, \ldots, k-1$ esetén, ahol $k > 2$. Ekkor az $N = p_1 p_2 \cdots p_{k-1} + 1$ egészre

$$\begin{aligned} N = \prod_{i=1}^{k-1} p_i + 1 < 2^1 2^2 2^{2^2} \cdots 2^{2^{k-2}} + 1 = \\ = 2^{1+2+2^2+\cdots+2^{k-2}} + 1 = 2^{2^{k-1}-1} + 1 < \\ < 2 \cdot 2^{2^{k-1}-1} = 2^{2^{k-1}} \end{aligned}$$

felső becslés adható. Legyen p_j az N egy prímosztója, amelyre nyilvánvalóan $p_j \le N$. De $j \ge k$, mert $p_i \nmid N$, ha $1 \le i \le k-1$, ezért

$$p_k \le p_j \le N < 2^{2^{k-1}}.$$

Tehát az állítás $n = k$ esetén is igaz, és így igaz minden n természetes számra. ∎

A következőkben egész számok számtani sorozataiban előforduló prímszámokkal foglalkozunk. Tekintsünk egy $a \neq 0$ differenciájú, $b \neq 0$ kezdőelemű $ax + b$ $(x = 0, 1, 2, \ldots)$ végtelen számtani sorozatot. A sorozat tagjai között nyilván csak akkor fordulhat elő végtelen sok különböző prím, ha a és b relatív prímek, ugyanis $(a, b) \mid (ax + b)$ minden egész x esetén. Dirichlet bizonyította, hogy az $(a, b) = 1$ feltétel ehhez nemcsak szükséges, hanem elégséges is.

7.3. Tétel. (Dirichlet) *Legyenek a és b zérustól különböző relatív prím természetes számok. Ekkor az*

$$ak + b \quad (k = 0, 1, 2, \ldots)$$

végtelen számtani sorozat tagjai között végtelen sok prímszám van.

A tétel bizonyítása túl messzire vezetne, ezért csak néhány speciális esetét bizonyítjuk be ($a = 4,\ b = \pm 1$ esetek).

7.4. Tétel. *Végtelen sok $4k-1$ alakú prímszám van.*

Bizonyítás. Az állítást indirekt úton bizonyítjuk. Tegyük fel, hogy véges számú $4k-1$ alakú prímszám létezik és ezek $p_1, p_2, \ldots, p_n$. Tekintsük az

$$N = 4p_1p_2 \cdots p_n - 1$$

egész számot. Az N szintén $4k-1$ alakú, ezért kell hogy legyen egy $4k-1$ alakú p prímosztója, mivel minden páratlan prím $4k+1$ vagy $4k-1$ alakú és a $4k+1$ alakú számok szorzatának alakja is $4k+1$. De p különbözik a felsorolt prímektől, hiszen $p \mid N$ és $p_i \nmid N$ $(i = 1, 2, \ldots, n)$. Ez ellentmond annak, hogy az összes $4k-1$ alakú prímet felsoroltuk. ∎

7.5. Tétel. *Végtelen sok $4k+1$ alakú prímszám van.*

Bizonyítás. Az előző gondolatmenet itt nem használható, mivel egy $4k+1$ alakú szám nem biztos, hogy tartalmaz tényezői között $4k+1$ alakú prímeket, hiszen páros számú $4k-1$ alakú prím szorzatának alakja $4k+1$. Ezért más módszert alkalmazunk.

Legyen $N > 1$ egy tetszőleges pozitív egész. Bebizonyítjuk, hogy létezik egy N-nél nagyobb $4k+1$ alakú prím. Tekintsük az $(N!)^2 + 1$ egész egy p prímosztóját. Erre nyilván $(N!, p) = 1$ és $p > N$, hiszen $N!$ minden N-nél nem nagyobb pozitív egésszel osztható, 1 pedig csak 1-gyel. A $p \mid \left((N!)^2 + 1\right)$ oszthatóságból

$$(N!)^2 \equiv -1 \pmod{p}$$

következik. A kongruencia mindkét oldalát $(p-1)/2$ hatványra emelve, és alkalmazva az Euler—Fermat-tételt,

$$1 \equiv (N!)^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

adódik és így $p \neq 2$ miatt $(-1)^{\frac{p-1}{2}} = 1$. Ebből azonban az következik, hogy p alakja $4k+1$, mert $p = 4k-1$ esetén $(p-1)/2$ páratlan lenne.

Tehát tetszőleges pozitív számnál nagyobb $4k+1$ alakú prím létezik, amiből az ilyen alakú prímek végtelen száma következik. ∎

Dirichlet tételének egy alkalmazásaként megmutatjuk, hogy végtelen sok úgynevezett izolált prím létezik. Ezalatt azt értjük, hogy léteznek olyan

prímszámok, melyek előtt és után tetszőlegesen előírt számú összetett szám ,,sorakozik", vagyis összetett számokkal van elválasztva az előtte és utána következő prímektől. Pontosabban a következőt bizonyítjuk.

7.6. Tétel. *Minden $Q > 1$ egész szám esetén található egy p prím úgy, hogy a $[p - Q, p + Q]$ intervallumban csak p a prím.*

Bizonyítás. Legyen q egy prímszám, melyre $q > Q + 2$ és tekintsük az

$$s = 2 \cdot 3 \cdots (q-1)\,(q+1)\,(q+2) \cdots (2q-2)$$

egyenlőséggel definiált s egész számot. Mivel $q \nmid s$, ezért $(q, s) = 1$, így a 7.3. Tétel következtében van olyan $k > 0$ természetes szám, melyre

$$p = sk + q$$

prím. De

$$p + i = 2 \cdots (q-2)\,(q-1)\,(q+1)\,(q+2) \cdots \big(q + (q-2)\big)k + (q+i)$$

osztható $(q+i)$-vel minden $i = 1, 2, \ldots q-2$ esetén, és hasonlóan a $p - i$ számok oszthatók $(q-i)$-vel, ezért $p+i$ és $p-i$ összetett, ha $1 \le i \le q-2$. Ebből már következik az állítás, mivel $q - 2 > Q$. ∎

A $\pi(x)$ becslése

Azt már láttuk (több előző tételből is következik), hogy a prímszámok száma végtelen. Jó lenne azonban tudni, hogy a természetes számok között milyen sok a prímek száma. A probléma ilyen felvetése nyilván értelmetlen, hiszen a természetes számok halmaza is és a prímek halmaza is megszámlálhatóan végtelen. Érdekes azonban azt keresni, hogy egy korlátnál nem nagyobb prímszámok és természetes számok száma hogy viszonyul egymáshoz.

Legyen x egy pozitív valós szám. A következőkben $\pi(x)$-szel jelöljük az x-nél nem nagyobb prímszámok számát. Például $\pi\left(\sqrt{2}\right) = 0$, mert minden prím legalább 2, és $\pi(7) = 4$, mert 2, 3, 5 és 7 a 7-nél nem nagyobb prímek. A matematikusok régóta foglalkoznak azzal, hogy $\pi(x)$ értékét minél pontosabban meghatározzák. Az nyilvánvaló, hogy egy $n > 1$ természetes szám esetén $\pi(n) < n$, hiszen nem minden természetes szám prím. A 7.2 Tétel alapján adódó $\pi\left(2^{2^{i-1}}\right) \ge i$ becslésből pedig, $n = 2^{2^{i-1}}$ helyettesítéssel, $\pi(n) \ge \log_2(\log_2 n) + 1$ alsó korlát adható. Ezek a triviális korlátok

azonban lényegesen javíthatók. Hadamard és de la Vallée Poussin 1896-ban bebizonyították a következő, úgynevezett *nagy prímszámtételt*.

7.7. Tétel. *Legyen $\pi(x)$ az $x > 1$ valós számnál nem nagyobb prímszámok száma. Ekkor*

$$\pi(x) \sim \frac{x}{\log x},$$

ahol $\log x$ az x természetes alapú logaritmusát jelöli és az aszimptotikus egyenlőség azt jelenti, hogy

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1.$$

A tétel alapján tehát tetszőleges $\varepsilon > 0$ esetén

$$(1-\varepsilon)\frac{x}{\log x} < \pi(x) < (1+\varepsilon)\frac{x}{\log x},$$

ha x az ε-től függően elég nagy.

A nagy prímszámtételt nem bizonyítjuk, csak annak egy gyengébb változatát.

7.8. Tétel. *Minden $n \geq 2$ természetes szám esetén igaz az*

$$\frac{1}{6}\frac{n}{\log n} < \pi(n) < 6\frac{n}{\log n}$$

egyenlőtlenség.

A tétel bizonyításában felhasználunk néhány segéderedményt a faktoriális függvénnyel, illetve a binomiális együtthatókkal kapcsolatban.

I. Segédtétel. (Legendre-formula) *Minden $n > 1$ természetes szám esetén*

$$n! = \prod_{p\leq n} p^{\alpha},$$

ahol a szorzást az összes n-nél nem nagyobb p prímre terjesztettük ki és

$$\alpha = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right].$$

Bizonyítás. Legyen $p \leq n$ egy prímszám. Ez a prím az

$$n! = 1 \cdot 2 \cdot 3 \cdots n$$

szorzatban a p, $2p, \ldots$ tényezők osztója, melyek darabszáma $\left[\frac{n}{p}\right]$. De a p^2, $2p^2, \ldots$ tényezők p^2-tel is oszthatók, ezért a szorzatban p kitevőjét ezek $\left[\frac{n}{p^2}\right]$ értékkel növelik. Folytatva a gondolatmenetet,

$$\alpha = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$$

adódik, ahol a tagok száma véges, mert $p^i > n$ esetén $\left[\frac{n}{p^i}\right]$ nulla. ∎

II. Segédtétel. *Legyen*

$$\prod_{n<p\leq 2n} p$$

az n-nél nagyobb, de $2n$-nél nem nagyobb prímek szorzata. Ekkor

$$\left(\prod_{n<p\leq 2n} p\right) \Bigg| \binom{2n}{n}$$

minden $n \geq 1$ esetén.

Bizonyítás. Mivel

$$\binom{2n}{n} = \frac{2n\,(2n-1)\,(2n-2)\cdots(n+1)}{n!}$$

ezért minden $n < p \leq 2n$ feltételt kielégítő p prím szerepel a tört számlálójában tényezőként, a nevezőnek viszont nem osztója. Így ezen prímek szorzatával az egyszerűsítés után is osztható a $\binom{2n}{n}$ binomiális együttható. ∎

III. Segédtétel. *Legyen*

$$\prod_{p^r\leq 2n<p^{r+1}} p^r$$

a különböző, $2n$-nél nem nagyobb prímek azon hatványainak szorzata, melyekre az előírt egyenlőtlenség teljesül. Ekkor

$$\binom{2n}{n} \Bigg| \left(\prod_{p^r\leq 2n<p^{r+1}} p^r\right)$$

minden $n \geq 1$ esetén.

Bizonyítás. A Legendre-formula (I. Segédtétel) alapján

$$\binom{2n}{n} = \frac{(2n)!}{n!n!} = \prod_{p \leq 2n} p^{\beta},$$

ahol $p^r \leq 2n < p^{r+1}$ feltételezéssel

$$\beta = \sum_{i=1}^{r} \left(\left[\frac{2n}{p^i} \right] - 2 \left[\frac{n}{p^i} \right] \right).$$

Belátjuk, hogy $\left[\frac{2n}{q}\right] - 2\left[\frac{n}{q}\right] = 0$ vagy 1 minden pozitív egész q esetén. Legyen $n = qt + s$, ahol t, s nemnegatív egészek és $0 \leq s < q$. Ekkor valóban

$$\left[\frac{2n}{q} \right] - 2 \left[\frac{n}{q} \right] = 2t + \left[\frac{2s}{q} \right] - 2t = \left[\frac{2s}{q} \right] = 0 \,\text{vagy}\, 1,$$

mivel $0 \leq 2s < 2q$. Ebből már következik, hogy $\beta \leq r$. Így a tételbeli oszthatóság bal oldalán szereplő prímek kitevői nem nagyobbak, mint a jobb oldaliak, ezért az oszthatóság valóban fennáll. ∎

IV. Segédtétel.

$$2^n < \binom{2n}{n} < 2^{2n}$$

minden $n > 1$ természetes szám esetén.

Bizonyítás. Mivel

$$\binom{2n}{n} < (1+1)^{2n} = 2^{2n},$$

ezért a jobb oldali egyenlőtlenség valóban igaz. Másrészt azonban

$$\begin{aligned}
\binom{2n}{n} &= \frac{2n\,(2n-1)\cdots(2n-(n-1))}{n\,(n-1)\cdots 2\cdot 1} = \\
&= \frac{2n}{n}\left(\frac{2\,(n-1)+1}{n-1}\right)\cdots\left(\frac{2\,(n-k)+k}{n-k}\right)\cdots\left(\frac{2\cdot 1+n-1}{1}\right) = \\
&= 2\left(2+\frac{1}{n-1}\right)\cdots\left(2+\frac{k}{n-k}\right)\cdots\left(2+\frac{n-1}{1}\right) > 2^n,
\end{aligned}$$

ezért a bal oldali egyenlőtlenség is igaz. ∎

Most már rátérhetünk a tételük bizonyítására.

A 7.8. Tétel bizonyítása. Legyen $n \geq 2$ egy természetes szám. Mivel a pozitív egészek körében az $a \mid b$ relációból $a \leq b$ következik, ezért a II. és a IV. Segédtétel alapján

$$\prod_{n<p\leq 2n} p \leq \binom{2n}{n} < 2^{2n}.$$

A bal oldali szorzatban minden prímtényező n-nél nagyobb ezért $\pi(x)$ definíciója miatt

$$\prod_{n<p\leq 2n} p > n^{\pi(2n)-\pi(n)},$$

és így

$$n^{\pi(2n)-\pi(n)} < 2^{2n}. \tag{7.1}$$

Hasonló gondolatmenettel a III. és a IV. Segédtétel alapján

$$\prod_{p^r\leq 2n<p^{r+1}} p^r \geq \binom{2n}{n} > 2^n,$$

illetve a $\pi(x)$ definíciójából

$$\prod_{p^r\leq 2n<p^{r+1}} p^r \leq (2n)^{\pi(2n)}$$

adódik, és így

$$(2n)^{\pi(2n)} > 2^n. \tag{7.2}$$

Legyen az n pozitív egész $n = 2^k$ alakú, ahol $k \geq 0$. Ekkor (7.1) alapján

$$2^{k\left(\pi\left(2^{k+1}\right)-\pi\left(2^k\right)\right)} < 2^{2^{k+1}},$$

vagyis

$$k\Big(\pi\left(2^{k+1}\right) - \pi\left(2^k\right)\Big) < 2^{k+1},$$

Ebből, felhasználva a $\pi(n) \leq \frac{n}{2}$ triviális becslést,

$$(k+1)\,\pi\left(2^{k+1}\right) - k\pi\left(2^k\right) < 2^{k+1} + \pi\left(2^{k+1}\right) \leq 2^{k+1} + 2^k = 3\cdot 2^k$$

következik, amiből $k = 0, 1, 2, \ldots, (k-1)$ helyettesítéssel a

$$\begin{aligned} \pi(2) - 0 &< 3 \cdot 2^0 \\ 2\pi\left(2^2\right) - \pi(2) &< 3 \cdot 2^1 \\ 3\pi\left(2^3\right) - 2\pi\left(2^2\right) &< 3 \cdot 2^2 \\ &\vdots \\ k\pi\left(2^k\right) - (k-1)\,\pi\left(2^{k-1}\right) &< 3 \cdot 2^{k-1} \end{aligned}$$

egyenlőtlenségek következnek. Az egyenlőtlenségek megfelelő oldalait összeadva azt kapjuk, hogy

$$k\pi\left(2^k\right) < 3\left(1 + 2 + 2^2 + \cdots + 2^{k-1}\right) < 3 \cdot 2^k,$$

és így

$$\pi\left(2^k\right) < 3 \cdot \frac{2^k}{k}.$$

Hasonlóan következik (7.2)-ből a

$$2^{(k+1)\pi\left(2^{k+1}\right)} > 2^{2^k},$$

illetve $k+1$ helyett k-t írva a

$$\pi\left(2^k\right) > \frac{2^{k-1}}{k} = \frac{1}{2} \cdot \frac{2^k}{k}$$

egyenlőtlenség. Azt kaptuk tehát, hogy

$$\frac{1}{2} \cdot \frac{2^k}{k} < \pi\left(2^k\right) < 3 \cdot \frac{2^k}{k}. \tag{7.3}$$

Legyen $n > 1$ egy pozitív egész, melyre a

$$2^k \le n < 2^{k+1}$$

egyenlőtlenség teljesül valamely $k \ge 1$ mellett. Ekkor (7.3) alapján

$$\begin{aligned} \pi(n) \ge \pi\left(2^k\right) > \frac{1}{2}\frac{2^k}{k} = \frac{1}{4}\frac{2^{k+1}}{k} > \\ > \frac{1}{4}\frac{n}{k} \ge \frac{1}{4}\frac{n}{\frac{\log n}{\log 2}} > \frac{1}{6}\frac{n}{\log n} \end{aligned}$$

és

$$\pi(n) < \pi\left(2^{k+1}\right) < 3\frac{2^{k+1}}{k+1} = 6\frac{2^k}{k+1} \leq$$
$$\leq 6\frac{n}{k+1} < 6\frac{n}{\frac{\log n}{\log 2}} < 6\frac{n}{\log n}$$

következik, tehát a tételünk állítása minden $n \geq 2$ esetén igaz. ∎

Az n-edik prímszám becslése

A p_n-nel jelölt n-edik prímszámra a 7.2. Tétel ad egy felső korlátot, és $p_n > n$ is nyilván igaz, hiszen az $1, 2, \ldots, n$ számok között nem mindegyik prím. Az előző tételünk alapján azonban lényegesen jobb becslést adhatunk az n-edik prímszámra.

7.9. Tétel. *Ha p_n az n-edik prímszám és $n > 1$, akkor*

$$\frac{1}{6} n \log n < p_n < 12 n \log n.$$

Bizonyítás. Mivel $\pi(p_n) = n$, hiszen az n-edik prímszámig pontosan n prímszám található, ezért a 7.8. Tétel alapján

$$\pi(p_n) = n < 6\frac{p_n}{\log p_n},$$

és így $p_n > n$ felhasználásával

$$p_n > \frac{1}{6} n \log p_n > \frac{1}{6} n \log n. \tag{7.4}$$

Másrészt, szintén a 7.8. Tétel alapján

$$\pi(p_n) = n > \frac{1}{6}\frac{p_n}{\log p_n},$$

amiből

$$p_n < 6 n \log p_n \tag{7.5}$$

következik. A 7.8. Tétel miatt

$$\pi\left(n^2\right) > \frac{1}{6}\frac{n^2}{\log n^2} = n\frac{n}{12 \log n} > n = \pi(p_n)$$

ha $n \geq 47$, ezért

$$p_n < n^2,$$

és (7.5) alapján

$$p_n < 6n \log n^2 = 12n \log n,$$

ami (7.4)-gyel együtt a tételt bizonyítja $n \geq 47$ esetén. Az $n = 2, 3, \ldots, 46$ esetek közvetlenül beláthatók. ∎

Megjegyezzük, hogy a 7.7. Tétel alapján az is igazolható, hogy

$$p_n \sim n \log n, \quad \text{azaz} \quad \lim_{n\to\infty} \frac{p_n}{n \log n} = 1.$$

A prímszámok eloszlása

A következőkben megmutatjuk, hogy a prímszámok az egész számok sorozatában viszonylag sűrűn helyezkednek el. Ismert, hogy a négyzetszámok reciprokösszegének végtelen sora konvergens. A következő tételből azonban következik, hogy a prímek reciprokösszegének sora viszont divergens.

7.10. Tétel. *Megadható két c_1, c_2 pozitív valós szám úgy, hogy az n-nél nem nagyobb prímszámok reciprokösszegére*

$$c_1 \log(\log n) < \sum_{p \leq n} \frac{1}{p} < c_2 \log(\log n),$$

ha n elég nagy.

Bizonyítás. A bizonyításban szükségünk lesz az n-nél nem nagyobb természetes számok reciprokösszegének becslésére. A 6.22. Tétel bizonyításában már láttunk az összegre egy egyenlőtlenséget, most azonban más módszerrel adunk a reciprokösszegre alsó, illetve felső korlátot. A reciprokfüggvény $[1, n]$ intervallumra való leszűkítésének az $\{1, 2, \ldots, n\}$ beosztáshoz tartozó alsó és felső integrálközelítő összegét tekintve — felhasználva, hogy a függvény szigorúan monoton csökkenő — az

$$\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} < \int_1^n \frac{dx}{x} = \log n < 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n-1}$$

egyenlőtlenséget kapjuk. Ebből viszont az következik, hogy

$$\log n < \sum_{k=1}^{n} \frac{1}{k} < 1 + \log n. \tag{7.6}$$

A tételünk bizonyítása céljából tekintsük az n-nél nem nagyobb természetes számok reciprokösszegét. Erre nyilván

$$\sum_{k=1}^{n} \frac{1}{k} < \prod_{p \le n} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right),$$

hiszen minden $k \le n$ egész n-nél nem nagyobb prímek hatványainak szorzata. Ennek alapján, (7.6) felhasználásával,

$$\log n < \prod_{p \le n} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) = \prod_{p \le n} \frac{1}{1 - \frac{1}{p}}$$

adódik. Mindkét oldal logaritmusát véve azt kapjuk, hogy

$$\log (\log n) < -\sum_{p \le n} \log \left(1 - \frac{1}{p}\right). \tag{7.7}$$

De $-\log (1 - \delta) < 2\delta$, ha $0 < \delta \le \frac{1}{2}$, ezért (7.7) következtében

$$\log (\log n) < 2 \sum_{p \le n} \frac{1}{p},$$

amiből a tétel bal oldali egyenlőtlensége következik $c_1 = \frac{1}{2}$ konstanssal.

Most rátérünk az összegünk felső becslésére. Mivel az n-nél nem nagyobb prímek száma n-nél kisebb, és a 7.9. Tétel alapján $p_n > \frac{1}{6} n \log n$, ezért

$$\sum_{p \le n} \frac{1}{p} = \sum_{r=1}^{\pi(n)} \frac{1}{p_r} < \frac{1}{2} + \frac{1}{3} + \sum_{r=3}^{n} \frac{6}{r \log r}.$$

De könnyű belátni, hogy

$$\frac{1}{r \log r} < \int_{r-1}^{r} \frac{dx}{x \log x},$$

ha $r \geq 3$, ezért

$$\sum_{p \leq n} \frac{1}{p} < \frac{5}{6} + 6 \sum_{r=3}^{n} \int_{r-1}^{r} \frac{dx}{x \log x} =$$

$$= \frac{5}{6} + 6 \int_{2}^{n} \frac{dx}{x \log x} = \frac{5}{6} + 6 \left[\log(\log x)\right]_2^n =$$

$$= 6 \log (\log n) + \left(\frac{5}{6} - 6 \log(\log 2) \right),$$

ami a tételünk hiányzó állítását bizonyítja tetszőleges $c_2 > 6$ konstanssal, ha n elég nagy. ∎

Megemlítjük, hogy a prímszámok reciprokösszegére vonatkozó

$$\sum_{p \leq n} \frac{1}{p} \sim \log (\log n)$$

aszimptotikus egyenlőség is igaz.

A 7.6. Tételből következik, hogy tetszőlegesen nagy olyan intervallum található a számegyenesen, melyben minden egész összetett. Ez közvetlenül is igazolható. Legyen ugyanis N egy tetszőleges pozitív egész ekkor az

$$(N+1)! + 2,\ (N+1)! + 3,\ \ldots,\ (N+1)! + (N+1)$$

egészek N darab egymást követő összetett számok, mivel rendre 2-vel, 3-mal, $\ldots, (N+1)$-gyel oszthatók. Nem igaz tehát az, hogy ha egy intervallum elég nagy, akkor található benne legalább egy prím. Érdemes azonban azt vizsgálni, hogy egy intervallum alsó végpontjához viszonyítva mekkora felső végpont esetén garantálható egy prím létezése az intervallumban. Bertrand sejtette és Csebisev bizonyította a következő eredményt.

7.11. Tétel. (Bertrand-posztulátum, illetve Csebisev-tétel) *Ha $n > 1$ egész szám, akkor az $(n, 2n)$ nyílt intervallum tartalmaz legalább egy prímet.*

A tétel bizonyításának előkészítéseként belátunk néhány segédtételt. Korábban a $\binom{2n}{n}$ binomiális együtthatóra már adtunk alsó, és felső korlátot, de most pontosabb korlátokra lesz szükségünk.

I. Segédtétel. *Ha $n > 1$, akkor*

$$\binom{2n}{n} > \frac{4^n}{2n}.$$

Bizonyítás. Mivel

$$2n\binom{2n}{n} = \frac{1\cdot 2\cdot 3\cdots(2n-1)2n2n}{(1\cdot 2\cdots n)(1\cdot 2\cdots n)} = \\ = \frac{2}{1}\frac{3}{1}\frac{4}{2}\frac{5}{2}\cdots\frac{2k}{k}\frac{2k+1}{k}\cdots\frac{2n}{n}\frac{2n}{n} > 2^{2n} = 4^n,$$

ezért igaz az állítás. ∎

II. Segédtétel. *Ha $n \geq 5$, akkor*

$$\binom{2n}{n} < 4^{n-1}.$$

Bizonyítás. $n = 5$ esetén igaz az állítás, mivel

$$\binom{10}{5} = 252 < 256 = 4^4.$$

Tegyük fel, hogy valamely $n \geq 5$ esetén teljesül az egyenlőtlenség. Akkor $n+1$-re is, mert

$$\binom{2(n+1)}{n+1} = \frac{(2n+2)!}{(n+1)!(n+1)!} = \frac{(2n)!}{n!n!}\frac{(2n+1)(2n+2)}{(n+1)(n+1)} = \\ = \binom{2n}{n}\left(1+\frac{n}{n+1}\right)2 < 4^{n-1}\cdot 2\cdot 2 = 4^{(n+1)-1}.$$

Ezért a teljes indukciós gondolatmenet alapján minden $n \geq 5$ természetes számra fennáll az egyenlőtlenség. ∎

III. Segédtétel. *Ha $n \geq 2$, akkor az n-nél nem nagyobb prímek szorzatára fennáll a*

$$\prod_{p\leq n} p < 4^n$$

egyenlőtlenség.

Bizonyítás. Teljes indukcióval bizonyítjuk az állítást. Az egyenlőtlenség $2 \leq n \leq 10$ esetén közvetlenül belátható. Tegyük fel, hogy $2, 3, \ldots, n$ esetén igaz az állítás. Ha n alakja $n = 2k$, ahol $k \geq 2$, akkor

$$\prod_{p\leq n+1} p = \prod_{p\leq 2k+1} p = \left(\prod_{p\leq k+1} p\right)\left(\prod_{\substack{k+1<p\\ p\leq 2k+1}} p\right).$$

De, mint ahogy a 7.8. Tétel II. Segédtételében láttuk, $\binom{2k+2}{k+1}$ binomiális együttható osztható a $k+1$-nél nagyobb és $2k+1$-nél nem nagyobb prímek szorzatával, így $\binom{2k+2}{k+1}$ nem kisebb a szorzatnál, ezért az indukciós feltétel és a II. Segédtétel miatt

$$\prod_{p\le n+1} p < 4^{k+1}\binom{2k+2}{k+1} < 4^{k+1}4^k = 4^{n+1}.$$

Ha viszont n alakja $n = 2k-1$, akkor

$$\prod_{p\le n+1} p = \prod_{p\le 2k} p = \prod_{p\le 2k-1} p = \prod_{p\le n} p < 4^n < 4^{n+1}.$$

Tehát a feltételek mellett páros és páratlan n esetén egyaránt igaz az állítás $n+1$-re is, ezért az állításunk minden $n \ge 2$ esetén igaz. ∎

IV. Segédtétel. *Legyen $n \ge 5$ egy természetes szám. Ekkor $\binom{2n}{n}$ prímtényezős felbontásában a $\sqrt{2n} < p \le 2n$ feltételnek eleget tevő prímek legfeljebb az első hatványon szerepelnek, míg a $\frac{2}{3}n < p \le n$ feltételt kielégítő prímek egyáltalán nem szerepelnek.*

Bizonyítás. A Legendre-formula (a 7.8. Tétel I. Segédtétele) miatt

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2} = \prod_{p\le 2n} p^{\gamma},$$

ahol

$$\gamma = \sum_{i=1}^{\infty}\left(\left[\frac{2n}{p^i}\right] - 2\left[\frac{n}{p^i}\right]\right).$$

Azt már korábban láttuk (a 7.8. Tétel III. Segédtételének bizonyításában), hogy $\left[\frac{2n}{q}\right] - 2\left[\frac{n}{q}\right] = 0$ vagy 1, bármely $q \ge 1$ egész esetén. Ezért ha egy p prímre $\sqrt{2n} < p \le 2n$, akkor a hozzá tartozó γ kitevő valóban 0 vagy 1, hiszen a γ-ban szereplő összeg tagjai $p^2 > 2n$ miatt mind zérus, ha $i > 1$.

Legyen most p egy olyan prím, melyre $\frac{2}{3}n < p \le n$. A γ-t meghatározó összeg most is csak egytagú, mivel $n \ge 5$ és a p-re adott korlátok miatt $p^i > 2n$, ha $i > 1$. Az $i = 1$ esetben

$$2 = \left[\frac{2n}{n}\right] \le \left[\frac{2n}{p}\right] \le \left[\frac{2n}{\frac{2}{3}n}\right] = 3$$

és

$$1 = \left[\frac{n}{n}\right] \le \left[\frac{n}{p}\right] \le \left[\frac{n}{\frac{2}{3}n}\right] = \left[\frac{3n}{2n}\right] = 1$$

adódik, azaz $2 \le \left[\frac{2n}{p}\right] \le 3$ és $\left[\frac{n}{p}\right] = 1$. De $p > \frac{2}{3}n$ miatt $\frac{2n}{p} < 2n/(\frac{2}{3}n) = 3$, ezért $\left[\frac{2n}{p}\right] = 2$, és így valóban

$$\gamma = \left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right] = 2 - 2 \cdot 1 = 0. \ \blacksquare$$

V. Segédtétel. *Legyen a* $\binom{2n}{n}$ *binomiális együttható prímhatványtényezős felbontása*

$$\binom{2n}{n} = \prod_{p \le 2n} p^{\alpha}.$$

Ekkor minden prímhatványtényezőre $p^{\alpha} \le 2n$.

Bizonyítás. Legyen p egy prímszám $p \le 2n$ feltétellel és legyen k az a pozitív egész, melyre $p^k \le 2n < p^{k+1}$. Ekkor a Legendre-formula alapján

$$\alpha = \left(\left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right]\right) + \left(\left[\frac{2n}{p^2}\right] - 2\left[\frac{n}{p^2}\right]\right) + \cdots + \left(\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right]\right) \le k,$$

mivel, mint ahogy korábban is láttuk, minden zárójelben lévő érték 0 vagy 1. Így valóban

$$p^{\alpha} \le p^k \le 2n. \ \blacksquare$$

A segédtételek alapján a tételünk bizonyítása már nem okoz sok nehézséget.

A 7.11. Tétel bizonyítása. Legyen $n \ge 5$. Ekkor a IV. Segédtétel alapján $\binom{2n}{n}$ prímhatványtényezős felbontása

$$\binom{2n}{n} = \left(\prod_{p \le \sqrt{2n}} p^{\alpha}\right)\left(\prod_{\sqrt{2n} < p \le \frac{2}{3}n} p\right)\left(\prod_{n < p < 2n} p\right) \tag{7.8}$$

alakban írható fel. A $\sqrt{2n}$-nél nem nagyobb prímek száma nyilván kisebb, mint $\sqrt{2n}$, ezért az V. Segédtétel alapján (7.8)-ban

$$\prod_{p \le \sqrt{2n}} p^{\alpha} \le (2n)^{\sqrt{2n}},$$

a III. Segédtétel miatt pedig

$$\prod_{\sqrt{2n}<p\le\frac{2}{3}n} p < \prod_{p\le\frac{2}{3}n} p < 4^{\frac{2}{3}n}$$

adódik. Ezek alapján, alkalmazva az I. Segédtételt, (7.8)-ból

$$\prod_{n<p<2n} p > \frac{\binom{2n}{n}}{(2n)^{\sqrt{2n}}4^{\frac{2}{3}n}} > \frac{4^n}{2n(2n)^{\sqrt{2n}}4^{\frac{2}{3}n}} = \\ = \frac{4^{\frac{1}{3}n}}{(2n)^{\sqrt{2n}+1}}$$

következik. Ellenőrizhető, hogy

$$\frac{4^{\frac{1}{3}n}}{(2n)^{\sqrt{2n}+1}} > 1$$

ha $n > 2000$, így a tételünk valóban igaz a kétezernél nagyobb n-ekre, mert az $(n, 2n)$ intervallumban lévő prímek szorzata 1-nél nagyobb, tehát van prím az intervallumban. Az $n \le 2000$ esetekben számítógéppel könnyen ellenőrizhető az állítás. ∎

A 7.11. Tétellel kapcsolatban felvetődik a kérdés, hogy az $(n, 2n)$ intervallumnál kisebb intervallumban tudjuk-e garantálni prímek létezését? Bizonyítható, hogy tetszőleges $\delta > 0$ valós szám esetén van olyan $n_0 > 0$ természetes szám úgy, hogy az $(n, (1+\delta)\, n)$ intervallum tartalmaz legalább egy prímet, ha $n > n_0$.

Régi és máig sem megoldott probléma, hogy két szomszédos négyzetszám, n^2 és $(n+1)^2$ között van-e mindig prím? Ez a probléma a következőképpen fogalmazható át. Legyen $n^2 = x$, és így $(n+1)^2$ alakja

$$(n+1)^2 = n^2 + 2n + 1 = x + \sqrt{x}\left(2 + \frac{1}{\sqrt{x}}\right) = x + x^{\frac{1}{2}+\varepsilon},$$

ahol

$$\varepsilon = \frac{\log\left(2 + x^{\frac{-1}{2}}\right)}{\log x} \to 0, \quad \text{ha} \quad x \to \infty.$$

Ennek alapján az eredeti problémánk a következővel ekvivalens. Igaz-e, hogy tetszőleges $\varepsilon > 0$ mellett az $\left(x, x + x^{\frac{1}{2}+\varepsilon}\right)$ intervallum tartalmaz legalább

egy prímet, ha x az ε-tól függően elég nagy? Manapság a probléma következő változatával foglalkoznak. Adjuk meg $\delta > 0$ értékét úgy, hogy az $\left(x, x + x^{\delta+\varepsilon}\right)$ intervallum tartalmazzon prímet minden δ-tól és ε-től függően elég nagy x esetén. A cél természetesen $\delta = \frac{1}{2}$ bizonyítása. A 7.11. Tételünkből következik, hogy $\delta = 1$ kielégíti a követelményeket minden $x > 2$ esetén, de bizonyították, hogy $\delta = \frac{16}{31}$ is megfelelő. A $\frac{16}{31}$ közel van ugyan $\frac{1}{2}$-hez, de $\delta = \frac{1}{2}$ értékre még nem sikerült bizonyítani az állítást.

Befejezésül megemlítünk néhány prímszámokkal kapcsolatos megoldatlan problémát.

Még nem sikerült sem bizonyítani, sem cáfolni Goldbach azon sejtését, mely szerint minden 4-nél nagyobb páros szám felírható két páratlan prím összegeként. Csak részeredmények ismertek ezzel kapcsolatban. Ma még csak az ismert, hogy a páros számok felírhatók $2n = p + Q$ alakban, ahol p egy páratlan prím és Q legfeljebb két prímtényező szorzata. Az úgynevezett páratlan Goldbach-sejtés szerint minden 7-nél nagyobb páratlan szám felírható három páratlan prím összegeként. Könnyű belátni, hogy a páros esetből a páratlan már következik, de ennek fordítottja nem igaz. A páratlan Goldbach-sejtés megoldásához közel állunk, mivel Vinogradov bebizonyította a sejtést, minden elég nagy páratlan számra, de a korlát még nem érhető el, a hiányzó számokra nem igazolható a sejtés közvetlenül még modern számítógépekkel sem.

A kis Fermat-tétel alapján $p \mid \left(2^{p-1} - 1\right)$ minden p páratlan prím esetén. De vannak-e olyan prímek, melyekre $p^2 \mid \left(2^{p-1} - 1\right)$? Az ilyen tulajdonságú prímeket Wieferich-prímeknek nevezzük. Eddig két Wieferich-prímet ismerünk, ezek 1093 és 3511. Problémaként merül fel, hogy van-e több Wieferich-prím, illetve ezen prímek száma véges-e vagy végtelen? A probléma eldöntése azért is fontos lenne, mert bizonyítható, hogy elősegítené az $x^p + y^p = z^p$ Fermat-egyenlet megoldhatatlanságának bizonyítását is.

Az $M_n = 2^n - 1$ alakú számokat Mersenne-számoknak nevezzük. Egy M_n Mersenne-szám csak akkor lehet prím, ha n is prím. Ugyanis ha $n = rs$ és $r, s \geq 2$, akkor

$$M_n = 2^{rs} - 1 = (2^r)^s - 1^s,$$

és így $2^r - 1$ egy valódi osztója M_n-nek. Itt is nyilvánvalóan felvetődik az a probléma, hogy a Mersenne-számok között a prímek száma véges-e vagy végtelen. Ez a kérdés is eldöntetlen. A viszonylag könnyű kezelhetőség miatt számítógépekkel általában a Mersenne-számok között keresnek nagy prímszámokat, 1994-ig 33 Mersenne-prím volt ismert, ezek közül a két legnagyobb $2^{756839} - 1$ és $2^{859433} - 1$. Korábban már láttuk, hogy a Mersenne-prímek létezése összefügg a páros tökéletes számok létezésével is.

Feladatok

1. $\varphi(n)$ explicit alakját használva bizonyítsuk be, hogy végtelen sok prímszám van.

2. Bizonyítsuk be, hogy végtelen sok $3k \pm 1$ és $6k \pm 1$ alakú prímszám létezik.

3. Bizonyítsuk be, hogy $n > 2$ egész esetén $2^n - 1$ és $2^n + 1$ nem ikerprím.

4. Bizonyítsuk be, hogy $p_k \leq 2^k$, ahol p_k a k-adik prímszám.

5. Bizonyítsuk be, hogy $n \geq 2$ akkor és csak akkor prímszám, ha

$$\frac{\pi(n-1)}{n-1} < \frac{\pi(n)}{n}.$$

6. Melyek azok a p és q prímszámok, amelyekre $p^q + q^p$ is prímszám.

7. Bizonyítsuk be, hogy $(3k+2)^2 \neq n^2 + p$, ha $k, n \in \mathbf{N}$ és p prímszám.

8. Határozzuk meg a nem feltétlenül különböző $p_1, p_2, \ldots, p_{10}$ prímszámokat, amelyekre

$$984 + \sum_{i=1}^{10} p_i^2 = \prod_{i=1}^{10} p_i.$$

9. Bizonyítsuk be, hogy a $k! + 1$, $2k! + 1, \ldots, k \cdot k! + 1$ ($k \in \mathbf{N}$) egészek páronként relatív prímek.

10. Bizonyítsuk be, hogy az $n \geq 2$ egész szám akkor és csak akkor prím, ha $\varphi(n) \,|(n-1)$ és $(n+1) \,|\sigma(n)$.

8. Diofantikus egyenletek

Nemcsak a matematikában, hanem a gyakorlati életben is gyakran találkozunk olyan problémákkal, melyek megoldásait az egész számok körében keressük. Az ilyen problémákat Diophantosz, a csaknem kétezer évvel ezelőtt élt alexandriai matematikus úttörő munkásságának tiszteletére diofantikus (vagy diofantoszi) problémáknak nevezzük. Ezen problémák klasszikus esetei a diofantikus egyenletek, melyek

$$f(x_1, x_2, \ldots, x_k) = c$$

alakúak, ahol f egy $k(\geq 2)$-változós racionális egész együtthatójú polinomfüggvény, c egy rögzített egész szám, és az egyenlet $x_1, \ldots, x_k$ egész megoldásait keressük.

A diofantikus egyenletekkel kapcsolatban természetesen vetődnek fel a következő problémák. Egy adott diofantikus egyenlet megoldható-e, vagyis léteznek-e olyan $x_1, \ldots, x_k$ egész számok, melyek kielégítik az egyenletet? Megoldhatóság esetén a megoldásokat szolgáltató $(x_1, \ldots, x_k)$ szám k-asok száma véges vagy végtelen? Ha megoldható egy egyenlet, akkor megadható-e az összes megoldás? 1900-ban David Hilbert többek között a következő problémát vetette fel (Hilbert 10. problémája). Létezik-e olyan algoritmus, mellyel véges számú lépésben minden diofantikus egyenletről eldönthető, hogy megoldható-e vagy nem? Hilbert problémáját 1970-ben egy fiatal, 22 éves orosz matematikus, Jurij Matijasevics válaszolta meg: bebizonyította, hogy ilyen algoritmus nem létezik. Így továbbra is fontosak azok az eredmények, melyek konkrét diofantikus egyenleteknek vagy az egyenletek egy osztályának a megoldhatóságára, illetve a megoldások meghatározására vonatkoznak.

Elsőfokú egyenletek

A legegyszerűbb eset az

$$ax + by = c \tag{8.1}$$

kétváltozós lineáris diofantikus egyenlet, ahol $a(\neq 0)$, $b(\neq 0)$, c adott egészek és az x, y megoldásokat az egész számok körében keressük. A megoldhatóság szükséges feltétele nyilvánvalóan az, hogy a és b legnagyobb közös osztója osztója legyen c-nek. Hiszen ha $ax_0 + by_0 = c$ valamely x_0, y_0 egészek esetén és $d = (a, b)$, akkor $d \mid (ax_0 + by_0)$ és így $d \mid c$. Az is nyilvánvaló, hogy

ha $d \mid c$ és x_0, y_0 megoldása (8.1)-nek, akkor megoldása az $\frac{a}{d}x + \frac{b}{d}y = \frac{c}{d}$ egyenletnek is, és viszont. Ezek alapján ha $d \nmid c$, akkor az egyenlet nem oldható meg. Ha pedig $d \mid c$, akkor mindkét oldalát d-vel osztva, (8.1)-gyel ekvivalens egyenlethez jutunk, melyben x és y együtthatói relatív prímek. Elég tehát azon egyenletekkel foglalkozni, melyekben $(a, b) = 1$.

8.1. Tétel. *Legyenek a és b zérustól különböző egészek $(a, b) = 1$ feltétellel, és legyen c egy tetszőleges egész szám. Ekkor az*

$$ax + by = c$$

egyenletnek végtelen sok x, y egész megoldása van. Továbbá ha x_0, y_0 egy megoldása az egyenletnek, akkor az összes megoldást az

$$x = x_0 + bt, \quad y = y_0 - at$$

alakú egészek szolgáltatják, ahol t végigfut az egészek halmazán.

Bizonyítás. Először az egyenlet megoldhatóságát bizonyítjuk. Mivel a és b relatív prímek, ezért az 1.2. és 1.12. Tételek alapján léteznek olyan x', y' egész számok, melyekre

$$ax' + by' = 1.$$

Mindkét oldalt c-vel szorozva

$$a\,(cx') + b\,(cy') = c$$

adódik, amiből az egyenletünk megoldhatósága következik, hiszen $x = cx'$, $y = cy'$ egy megoldás.

Tegyük fel most, hogy x_0, y_0 egy megoldás, vagyis

$$ax_0 + by_0 = c. \tag{8.2.}$$

Ha x, y is egy megoldás, azaz

$$ax + by = c, \tag{8.3}$$

akkor a (8.2) és a (8.3) egyenlőségek különbségéből

$$a\,(x - x_0) = -b\,(y - y_0) \tag{8.4}$$

következik. Ennek alapján $b \mid a\,(x - x_0)$. De $(a, b) = 1$, ezért $b \mid (x - x_0)$, vagyis van egy olyan t egész, melyre $x - x_0 = bt$, és így x alakja $x = x_0 + bt$. Az $x - x_0 = bt$ értéket (8.4)-be helyettesítve

$$abt = -b(y - y_0)$$

adódik, amiből viszont $y = y_0 - at$ következik. Tehát, ha az x_0, y_0 megoldáson kívül x, y is megoldása az egyenletnek, akkor ez csak $x = x_0 + bt$, $y = y_0 - at$ alakú lehet. Azonban (8.2) alapján

$$a(x_0 + bt) + b(y_0 - at) = ax_0 + by_0 = c,$$

tehát az $x = x_0 + bt$, $y = y_0 - at$ számpár bármely t egész mellett megoldása az egyenletünknek. Ezzel a tétel minden állítását bebizonyítottuk. ∎

Ha egy konkrét kétismeretlenes lineáris diofantikus egyenlet megoldásait meg akarjuk határozni, akkor az előző tétel alapján elég egy megoldást megkeresni. Követve a tétel bizonyításának gondolatmenetét, ez a következőképpen történhet. Végrehajtjuk az a, b egészeken az euklideszi algoritmust. Az utolsó zérustól különböző maradék nyilván 1, hiszen $(a, b) = 1$. Ezt az 1-et az 1.2 Tétel bizonyításában látott módon felírjuk $1 = ax' + by'$ alakban, amiből már következik, hogy $x = cx'$, $y = cy'$ megoldása az $ax + by = c$ egyenletnek.

A megoldások megkeresésére megmutatunk egy másik módszert is, aminek hátterében szintén az euklideszi algoritmus húzódik meg, de gyakorlatilag talán könnyebben alkalmazható. A módszer lényege az, hogy az eredeti egyenletet visszavezetjük diofantikus egyenletek sorozatára, melyekben az ismeretlenek együtthatóinak abszolút értéke egyre csökken. Példaként oldjuk meg a

$$7x + 19y = 24 \tag{8.5}$$

egyenletet. Az egyenlet megoldható, hiszen $(7, 19) = 1$. Tegyük fel, hogy egy x, y egész számpár kielégíti az egyenletünket. Fejezzük ki (8.5)-ből x és y közül azt, melynek együtthatójának abszolút értéke kisebb, vagyis x-et. Így

$$x = \frac{24 - 19y}{7} = 3 - 2y + \frac{3 - 5y}{7} \tag{8.6}$$

adódik, ahol

$$u = \frac{3 - 5y}{7}$$

egész szám, mivel x is és y is egész. Ebből az

$$5y + 7u = 3$$

diofantikus egyenlethez jutunk, melyben az ismeretlenek együtthatói abszolút értékének maximuma kisebb, mint az eredeti egyenletben. Folytatva az eljárást azt kapjuk, hogy

$$y = \frac{3 - 7u}{5} = -u + \frac{3 - 2u}{5},$$

ahol

$$v = \frac{3 - 2u}{5}$$

egész szám és u, v kielégíti a

$$2u + 5v = 3$$

egyenletet. Ebből

$$u = \frac{3 - 5v}{2} = 1 - 2v + \frac{1 - v}{2},$$

ahol $t = \frac{1-v}{2}$ egész, és így v alakja

$$v = 1 - 2t.$$

De ekkor

$$u = 1 - 2v + t = 1 - 2(1 - 2t) + t = 5t - 1,$$
$$y = -u + v = -(5t - 1) + 1 - 2t = 2 - 7t$$

és

$$x = 3 - 2y + u = 3 - 2(2 - 7t) + 5t - 1 = -2 + 19t$$

következik. Tehát, ha van megoldása az egyenletünknek, akkor az $x = -2+$ $+19t$, $y = 2 - 7t$ alakú. Behelyettesítéssel ellenőrizhető, hogy minden ilyen alakú számpár megoldás.

Megjegyezzük, hogy ha (8.6)-ban a $19 = 2 \cdot 7 + 5$ felbontás helyett a $19 = 3 \cdot 7 - 2$ egyenlőséget használjuk, akkor $x = 3 - 3y + q$ következik, ahol $q = \frac{3+2y}{7}$, amiből $y = -1 + 3q + \frac{-1+q}{2} = -1 + 3q + k$, így q alakja $q = 2k+1$, y alakja $y = 2+7k$ és x alakja $x = -2-19k$. Tehát az eljárás egy lépéssel rövidebb. Érdemes tehát arra törekedni, hogy az adódó törtekben a számlálóbeli együtthatók abszolút értéke minimális legyen. A most kapott

$x = -2 - 19k$, $y = 2 + 7k$ megoldások csak formailag különböznek az előzőekben kapottaktól, $k = -t$ helyettesítéssel azonos alakúak lesznek.

A kettőnél több ismeretlent tartalmazó lineáris diofantikus egyenletekre az előzőekhez hasonlóak érvényesek.

8.2. Tétel. *Legyenek $a_1, a_2, \ldots, a_n$ ($n \geq 2$) nem zérus egészek és legyen c egy tetszőleges egész szám. Az*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$$

diofantikus egyenletnek akkor és csak akkor van $x_1, \ldots, x_n$ egész megoldása, ha

$$(a_1, a_2, \ldots, a_n) \mid c. \tag{8.7}$$

Ha megoldható, akkor végtelen sok megoldás van, melyek $n-1$ paraméterrel állíthatók elő.

A tételt hosszadalmas volta miatt nem bizonyítjuk be teljes egészében. A (8.7) feltétel szükségessége nyilvánvaló, hasonlóan látható be, mint az $n = 2$ esetben. Az ismeretlenek együtthatóinak legnagyobb közös osztójával osztva az egyenletet, az $n > 2$ esetben is elég olyan egyenletekkel foglalkozni, melyekben az együtthatók relatív prímek. Ilyen esetben könnyű egy megoldást találni, hiszen az 1.14 Tétel szerint a legnagyobb közös osztó előállítható

$$(a_1, \ldots, a_n) = 1 = a_1x_1' + \cdots + a_nx_n'$$

alakban, aminek alapján $x_1 = cx_1', \ldots, x_n = cx_n'$ megoldása az egyenletünknek. Végtelen sok megoldás létezését egy konkrét egyenleten mutatjuk be, módszerünk a (8.5) egyenlet megoldásánál alkalmazott eljáráshoz hasonló. Példaként oldjuk meg a

$$7x + 10y + 16z = 500 \tag{8.8}$$

diofantikus egyenletet. Tegyük fel, hogy egy x, y, z egész számhármas kielégíti (8.8)-at. Ekkor

$$x = \frac{500 - 10y - 16z}{7} = 71 - y - 2z + \frac{3 - 3y - 2z}{7} = \\ = 71 - y - 2z + u,$$

ahol $u = \frac{3-3y-2z}{7}$ egy egész szám. Ebből a

$$2z + 3y + 7u = 3$$

egyenlethez jutunk, amiből

$$z = \frac{3 - 3y - 7u}{2} = 1 - 2y - 3u + \frac{1 + y - u}{2} = \\ = 1 - 2y - 3u + v,$$

ahol $v = \frac{1+y-u}{2}$ egész. Innen már következik, hogy ha x, y, z megoldásai (8.8)-nak, akkor alakjuk

$$y = u + 2v - 1,$$
$$z = 1 - 2(u + 2v - 1) - 3u + v = -5u - 3v + 3,$$
$$x = 71 - (u + 2v - 1) - 2(-5u - 3v + 3) + u = 10u + 4v + 66.$$

Az ilyen alakú számok megoldásai (8.8)-nak minden egész u, v esetén mivel

$$7(10u + 4v + 66) + 10(u + 2v - 1) + 16(-5u - 3v + 3) = 500$$

u és v értékétől függetlenül.

Magasabb fokú egyenletek

A következőkben néhány magasabb fokú diofantikus egyenlettel foglalkozunk. Elsőként a jól ismert

$$x^2 + y^2 = z^2,$$

úgynevezett pitagoraszi egyenlet megoldásait keressük meg. Az egyenletnek $x = 0$, $y = \pm z$, illetve $y = 0$, $x = \pm z$ nyilván megoldásai, de ezektől a triviális megoldásoktól a továbbiakban eltekintünk. Az is nyilvánvaló, hogy ha x, y, z egy megoldása az egyenletnek, akkor a $\pm x$, $\pm y$, $\pm z$ számhármas is az tetszőleges előjelválasztás mellett. Így csak a zérustól különböző pozitív megoldások meghatározására törekszünk. Ha egy x, y, z számhármas megoldása a pitagoraszi egyenletnek, akkor cx, cy, cz is megoldás minden c egész esetén, hiszen ekkor

$$(cx)^2 + (cy)^2 = c^2 \left(x^2 + y^2\right) = c^2 z^2 = (cz)^2 .$$

Hasonlóan, ha $(x, y, z) = d$ és x, y, z egy megoldás, akkor

$$\left(\frac{x}{d}\right)^2 + \left(\frac{y}{d}\right)^2 = \frac{x^2 + y^2}{d^2} = \left(\frac{z}{d}\right)^2$$

miatt az $\frac{x}{d}$, $\frac{y}{d}$, $\frac{z}{d}$ számhármas is megoldás. Ezek alapján elég az egyenlet olyan megoldásait meghatározni, melyekben x, y és z relatív prímek, hiszen ezeket pozitív egészekkel szorozva megkapjuk az összes pozitív megoldást. Azokat a triviálistól különböző pozitív megoldásokat, melyekben $(x, y, z) = 1$, primitív megoldásoknak nevezzük.

8.3. Tétel. *Az*

$$x^2 + y^2 = z^2 \tag{8.9}$$

egyenlet összes primitív megoldását szolgáltatják (x *és* y *felcserélésétől eltekintve*) *az*

$$\begin{aligned} x &= 2uv, \\ y &= u^2 - v^2, \\ z &= u^2 + v^2 \end{aligned}$$

alakú számhármasok, ahol u *és* v *pozitív egészek,* $(u, v) = 1$, $u > v$ *és* u, v *paritása különböző.*

Bizonyítás. A (8.9) egyenlet megoldható, hiszen $(x, y, z) = (3, 4, 5)$ egy megoldás. Tegyük fel, hogy (x, y, z) egy nem triviális primitív megoldás. Ekkor x, y és z páronként is relatív prímek, hiszen ha p egy közös prímosztója közülük bármely kettőnek, akkor (8.9) miatt p osztója a harmadiknak is, és így nem lennének relatív prímek. x, y, z mindegyike nyilván nem lehet páros, hiszen relatív prímek. De nem lehet mindegyik páratlan sem, mert akkor (8.9) két oldalának paritása különböző, és nem állhat fenn az egyenlőség. Paritásvizsgálattal hasonlóan látható be, hogy x, y, z között nem lehet két páros és egy páratlan szám. Tehát a három pozitív egész közül egy páros és kettő páratlan. z nem lehet páros, mert ha z páros és x, y páratlanok, vagyis $2k+1$ alakúak, akkor x és y négyzete $4k+1$, négyzetük összege pedig $4k + 2$ alakú, és így (8.9) jobb oldala 4-gyel lenne osztható, míg a bal oldal csak 2-vel. Tehát x és y közül az egyik páros, a másik pedig z-vel együtt páratlan. Szimmetria okok miatt feltehetjük, hogy x páros, y és z páratlan. Ekkor (8.9)-ből

$$\left(\frac{x}{2}\right)^2 = \frac{z^2 - y^2}{4} = \frac{z+y}{2} \cdot \frac{z-y}{2} \tag{8.10}$$

következik, ahol $\frac{x}{2}$, $\frac{z+y}{2}$ és $\frac{z-y}{2}$ egész számok. Belátjuk, hogy a két utóbbi egész relatív prím. Legyen

$$d = \left(\frac{z+y}{2}, \frac{z-y}{2}\right).$$

Ekkor

$$d \mid \left(\frac{z+y}{2} + \frac{z-y}{2} \right) = z$$

és

$$d \mid \left(\frac{z+y}{2} - \frac{z-y}{2} \right) = y.$$

ezért $d = 1$, hiszen y és z relatív prímek. Tehát $\frac{z+y}{2}$ és $\frac{z-y}{2}$ relatív prímek, és ezért az 1.26 Tétel alapján (8.10)-ből

$$\frac{z+y}{2} = u^2, \quad \frac{z-y}{2} = v^2$$

adódik, ahol u és v pozitív egészek. Ebből azonban

$$z = \frac{z+y}{2} + \frac{z-y}{2} = u^2 + v^2$$

és

$$y = \frac{z+y}{2} - \frac{z-y}{2} = u^2 - v^2,$$

(8.10) alapján pedig

$$x = 2\sqrt{\frac{z+y}{2} \cdot \frac{z-y}{2}} = 2uv$$

következik.

Tehát (8.9) primitív megoldásai csak a tételbeli alakúak lehetnek. Az adott alakú számhármasok bármely u, v egészek esetén megoldásai (8.9)-nek, mert

$$(2uv)^2 + (u^2 - v^2)^2 = (u^2 + v^2)^2.$$

Ha (x, y, z) egy primitív megoldás, akkor nyilván $u > v$, mert y pozitív, továbbá $(u, v) = 1$ és u, v paritása különböző, mert másként x, y, z nem lennének relatív prímek. Ez fordítva is igaz, vagyis ha u, v egészekre az előbbi feltételek teljesülnek, akkor az általuk meghatározott (x, y, z) páronként relatív prím megoldása (8.9)-nek. Ehhez elegendő azt belátni, hogy $(z, y) = d = 1$. z és y alakja alapján $d \mid (z + y) = 2u^2$ és $d \mid (z - y) = 2v^2$, ezért $d = 1$ vagy $d = 2$, mert $(u, v) = 1$. De $d \neq 2$, mert u és v paritásának különbözősége miatt z is és y is páratlan. Így $d = 1$, és ezzel a tétel minden állítását igazoltuk. ∎

Következmény. A tételből és a tétel kimondása előtti meggondolásokból következik, hogy a (8.9) egyenlet összes pozitív megoldását az

$$x = duv, \; y = d(u^2 - v^2), \quad z = d(u^2 + v^2)$$

alakú számhármasok szolgáltatják, ahol u és v eleget tesz a tételben leírt feltételeknek, d pedig tetszőleges pozitív egész.

A 8.3. Tétel alapján természetesen vetődik fel az a probléma, hogy az

$$x^n + y^n = z^n \tag{8.11}$$

diofantikus egyenletnek van-e az $x = 0$, $y = z$, illetve $y = 0$, $x = z$ triviális megoldásoktól eltekintve pozitív egész megoldása, ha $n > 2$? A XVII. század első felében Pierre Fermat azt állította, hogy (8.11)-nek $n > 2$ esetén nincs pozitív egész megoldása. Egy könyvben tett kézírásos megjegyzése szerint erre egy szép bizonyítást talált, de a bizonyítás nem maradt fenn utána. Valószínűleg hibás volt a bizonyítása, mert azóta már napjainkig igen sokan próbálkoztak sikertelenül az állítás bizonyításával. Csak részeredményeket értek el, és csak bizonyos n-re sikerült a bizonyítás, például az $n = 3$ esetet Euler bizonyította. Fermat nyomán az állítást *Fermat-sejtésnek*, *nagy Fermat-tételnek*, illetve *Fermat utolsó tételének* nevezték el. Sok jelentős és matematikailag igen mély részeredmény után 1993-ban Andrew Wiles amerikai matematikus egy előadásán bejelentette, hogy megoldott egy problémát az úgynevezett elliptikus görbékkel kapcsolatban, amiből már következik Fermat közel 350 éves híres állítása.

A Fermat-sejtés bizonyításához elég csak az $n = 4$ és $n = p$, ahol p páratlan prím, esetekkel foglalkozni. Legyen ugyanis n alakja $n = pq$, ahol p egy páratlan prím és $q > 1$ egy pozitív egész. Ha ezen n mellett (8.11)-nek van egy x_1, y_1, z_1 megoldása, akkor

$$(x_1^q)^p + (y_1^q)^p = (z_1^q)^p$$

miatt (8.11) az $n = p$ esetben is megoldható. Ha pedig n összetett és nincs páratlan prímtényezője, akkor n 2-nek hatványa, vagyis $n = 2^\alpha$ alakú, ahol $\alpha \geq 2$. De ha ekkor (8.11)-nek van egy x_2, y_2, z_2 megoldása, akkor $q = 2^{\alpha-2}$ jelöléssel,

$$(x_2^q)^4 + (y_2^q)^4 = (z_2^q)^4$$

miatt (8.11) $n = 4$ esetén is megoldható. Ezek alapján, ha a Fermat-sejtés igaz az $n = 4$ és $n = p$ (páratlan prím) esetekben, akkor igaz minden $n > 2$ esetén.

Fermat az állítását csak az $n = 4$ esetben bizonyította. Gondolatmenete a következő volt. Ha az $x^4 + y^4 = z^4$ diofantikus egyenlet megoldható, akkor $z^4 = (z^2)^2$ miatt az $x^4 + y^4 = z^2$ egyenlet is. Elég tehát azt belátni, hogy az utóbbi egyenletnek nem lehet pozitív egész megoldása. Ennek bizonyításában az úgynevezett *végtelen leszállás* (*descente infinie*) elvét alkalmazta. Ezt az elvet mutatjuk be a következő bizonyításban.

8.4. Tétel. *Az*

$$x^4 + y^4 = z^2 \tag{8.12}$$

diofantikus egyenletnek nincs x, y, z pozitív egész megoldása.

Bizonyítás. Tegyük fel, hogy (8.12)-nek van triviálistól különböző (x, y, z egyike sem zérus) megoldása. Ekkor van olyan x, y, z pozitív egész megoldás, melynél z minimális. Ezen megoldásra $(x, y, z) = 1$, mert egyébként, ha egy p prím mindhárom számnak osztója lenne, akkor a (8.12)-ből adódó

$$\left(\frac{x}{p}\right)^4 + \left(\frac{y}{p}\right)^4 = \left(\frac{z}{p^2}\right)^2$$

egyenlőség alapján az $\frac{x}{p}$, $\frac{y}{p}$, $\frac{z}{p^2}$ pozitív egészek is egy megoldást adnának, ami $\frac{z}{p^2} < z$ következtében ellentmondana z minimális voltának.

Mivel a (8.12) egyenlőség

$$(x^2)^2 + (y^2)^2 = z^2$$

alakba is írható, és mint az előbb láttuk x^2, y^2, z relatív prímek, ezért x^2, y^2, z a pitagoraszi egyenletnek egy primitív megoldása. Így alakjuk a 8.3. Tétel alapján

$$x^2 = 2uv, \quad y^2 = u^2 - v^2, \quad z = u^2 + v^2 \tag{8.13}$$

ahol u és v különböző paritású, relatív prím pozitív egészek $u > v$ feltétellel. (8.13) alapján a

$$v^2 + y^2 = u^2$$

egyenlőség is fennáll, ahol $(u, v) = 1$ miatt $(u, v, y) = 1$ és u, v közül v a páros, mert y páratlan. Így a 8.3. Tétel alapján

$$v = 2mn, \quad y = m^2 - n^2, \quad u = m^2 + n^2 \tag{8.14}$$

valamely m és n különböző paritású, relatív prím pozitív egészekkel. De ekkor (8.13) és (8.14) felhasználásával

$$x^2 = 2uv = 4umn,$$

illetve

$$\left(\frac{x}{2}\right)^2 = umn$$

adódik. De $(m, n) = 1$, ezért $u = m^2 + n^2$ miatt u, m és n páronként relatív prímek, így az 1.26 Tétel következtében u, m, n mindegyike teljes négyzet, vagyis

$$m = a^2, \quad n = b^2, \quad u = c^2, \tag{8.15}$$

ahol a, b, c pozitív egészek. Ezeket a (8.14)-ben szereplő $u = m^2 + n^2$ egyenlőségbe írva

$$a^4 + b^4 = c^2$$

következik, tehát az a, b, c pozitív egész számhármas is megoldása a (8.12) egyenletnek. De (8.15) és (8.13) miatt $c < u < z$, ami ellentmond z minimalitásának. Ezek szerint (8.12) minden pozitív megoldása esetén található egy olyan pozitív megoldás, melyben z értéke kisebb. Ez a végtelen leszállás ellentmond a természetes számok tulajdonságainak, ezért a (8.12) egyenletnek nem lehet triviálistól különböző pozitív megoldása. ∎

A Waring-probléma

A következőkben az úgynevezett Waring-féle problémakörrel fogunk foglalkozni. A Waring által 1770-ben felvetett probléma a következő. Megadható-e minden $k \geq 2$ természetes szám esetén egy k-tól függő g pozitív egész úgy, hogy minden természetes szám előállítható legyen g darab k-adik hatvány összegeként, megengedve a $0 = 0^k$ tagokat is?

Először a probléma $k = 2$ esetével foglalkozunk. Belátjuk, hogy két négyzetszám összegeként nem írható fel minden természetes szám.

8.5. Tétel. *Legyen n egy természetes szám. Az*

$$x^2 + y^2 = n \tag{8.16}$$

diofantikus egyenlet nem oldható meg, ha n alakja

$$n = 2^q(4k + 3),$$

ahol q és k természetes számok.

Bizonyítás. A tételt q-ra teljes indukcióval bizonyítjuk. Felhasználjuk, hogy minden c természetes szám esetén

$$c^2 \equiv 0 \quad \text{vagy} \quad 1 \pmod 4, \tag{8.17}$$

aszerint, hogy c páros vagy páratlan. Ha $q = 0$, akkor

$$n = 4k + 3 \equiv 3 \pmod 4.$$

De (8.17) alapján

$$x^2 + y^2 \equiv 0, \quad 1 \quad \text{vagy} \quad 2 \pmod 4$$

bármely x, y egészek esetén, így (8.16) valóban nem oldható meg.

Legyen most $q = 1$. Ekkor $n = 8k + 6$ és (8.16) megoldásaként csak azonos paritású x, y jöhet szóba. Páratlan x, y nem lehet megoldása (8.16)-nak. Ugyanis egy páratlan $c = 2t + 1$ egész esetén $c^2 = 4t(t + 1) + 1 \equiv 1 \pmod 8$, hiszen t vagy $t + 1$ páros, így ha x és y páratlan, akkor

$$x^2 + y^2 \equiv 2 \pmod 8,$$

azonban

$$n \equiv 6 \pmod 8.$$

Ha pedig x, y mindkettője páros, akkor (8.16) bal oldala osztható 4-gyel, a jobb oldal pedig $n = 8k + 6$ miatt nem. Tehát (8.16) ebben az esetben sem oldható meg.

Tegyük fel, hogy a tétel igaz $q = s - 1$ és $q = s$ esetén, ahol $s \geq 1$, és tegyük fel, hogy az

$$x^2 + y^2 = 2^{s+1}(4k + 3) \tag{8.18}$$

egyenlet megoldható. Legyen x, y egy megoldás, ahol x és y paritása nyilván megegyezik. Ekkor x és y nem lehet páratlan, hiszen ekkor $x^2 + y^2 \equiv 2 \pmod 4$ adódna, ami $s \geq 1$ miatt lehetetlen. Ha x, y páros egészek, akkor a (8.18)-ból következő

$$\left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2 = 2^{s-1}(4k + 3)$$

egyenlőség miatt (8.16) megoldható lenne $q = s - 1$ esetén. Ez ellentmond a feltételünknek, így az állítás igaz minden $q \geq 0$-ra. ∎

Bizonyítás nélkül megemlítjük, hogy azok és csak azok a természetes számok bonthatók fel két négyzetszám összegére, melyek nem tartalmaznak $4k + 3$ alakú prímeket páratlan hatványon.

Megmutatjuk, hogy három négyzetszám összegeként sem állítható elő minden természetes szám.

8.6. Tétel. *Legyen $q, k \in \mathbf{N}$. Ha n $4^q(8k+7)$ alakú, akkor az*

$$x^2 + y^2 + z^2 = n \tag{8.19}$$

egyenletnek nincs egész megoldása.

Bizonyítás. Legyen először $q = 0$, vagyis $n = 8k + 7 \equiv 7 \pmod 8$. Mivel minden c egész szám $c = 4t$, $c = 4t + 1$, $c = 4t + 2$ vagy $c = 4t + 3$ alakú, ezért $c^2 \equiv 0, 1$ vagy $4 \pmod 8$. Így tetszőleges x, y, z egészekre

$$x^2 + y^2 + z^2 \equiv 0, 1, 2, 3, 4, 5, \text{ vagy } 6 \not\equiv 7 \pmod 8,$$

ezért (8.19)-nek nincs x, y, z egész megoldása.

Tegyük fel, hogy valamely $q \geq 0$ esetén (8.19) nem megoldható. Ekkor ha

$$x^2 + y^2 + z^2 = 4^{q+1}(8k + 7)$$

fennáll valamely x, y, z egészekre, akkor x, y, z mindegyike páros, mert

$$x^2 + y^2 + z^2 \equiv 0, 1, 2 \text{ vagy } 3 \pmod 4$$

aszerint, hogy 0, 1, 2, vagy 3 páratlan szám van közöttük. De ha x, y és z páros, akkor

$$\left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2 + \left(\frac{z}{2}\right)^2 = 4^q(8k + 7),$$

ami ellentmond a feltevésünknek. Így az állítás tetszőleges $q \geq 0$-ra igaz. ∎

A tétellel kapcsolatban bizonyítás nélkül megemlítjük, hogy csak a tételbeli $n = 4^q(8k + 7)$ alakú számok nem írhatók fel három négyzetszám összegeként.

Az eddigiekből következik, hogy legalább négy négyzetszám szükséges ahhoz, hogy minden természetes szám előállítható legyen négyzetszámok összegeként. Négy azonban elég is.

8.7. Tétel. *Minden pozitív egész szám felírható négy négyzetszám összegeként.*

Bizonyítás. Először bizonyítjuk, hogy minden p páratlan prím esetén létezik egy m pozitív egész, melyre $1 \leq m < p$ és mp előállítható

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2 \tag{8.20}$$

alakban, ahol x_i $(1 \le i \le 4)$ egész szám. Tekintsük az

$$S_1 = \left\{ 0^2, 1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2 \right\}$$

és

$$S_2 = \left\{ -0^2 - 1, -1^2 - 1, -2^2 - 1, \ldots, -\left(\frac{p-1}{2}\right)^2 - 1 \right\}$$

halmazokat. Mivel az $x^2 \equiv y^2 \pmod{p}$ kongruenciából

$$p \mid (x-y) \quad \text{vagy} \quad p \mid (x+y)$$

következik, S_1 bármely két s_1', s_1'' különböző elemére $s_1' \not\equiv s_1'' \pmod{p}$, hiszen $0 < \left|\sqrt{s_1'} - \sqrt{s_1''}\right| < p$ és $0 < \left|\sqrt{s_1'} + \sqrt{s_1''}\right| < p$. Hasonlóan látható be, hogy az S_2 halmaz bármely két különböző eleme is inkongruens modulo p. De S_1 és S_2 összesen $p+1$ elemet tartalmaz, ezért a skatulya elv alapján van S_1-nek olyan eleme, mely kongruens S_2 valamely elemével, vagyis

$$x^2 \equiv -y^2 - 1 \pmod{p}$$

valamely x, y egészekre $0 \le x, y \le \frac{p-1}{2}$ feltétellel. De ebből az következik, hogy van egy m pozitív egész szám, melyre

$$mp = x^2 + y^2 + 1 = x^2 + y^2 + 1^2 + 0^2$$

és

$$1 \le m = \frac{x^2 + y^2 + 1}{p} \le \frac{1}{p}\left(2\left(\frac{p-1}{2}\right)^2 + 1\right) < p.$$

Ezzel az állítást bizonyítottuk.

Most belátjuk, hogy ha m a legkisebb olyan pozitív egész, melyre (8.20) fenáll valamely x_1, x_2, x_3, x_4 mellett, akkor $m = 1$. Ha a (8.20)-beli m páros, akkor az x_i számok között a páratlanok száma 0, 2 vagy 4. Ha a páratlanok száma nem nulla, akkor jelölhetjük az x_i-ket úgy, hogy x_1 és x_2 páratlanok legyenek. Így elérhetjük, hogy az $x_1 \pm x_2$ és $x_3 \pm x_4$ számok minden esetben párosak. Ekkor azonban (8.20)-ból

$$\frac{m}{2}p = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2$$

következik, és m nem lenne minimális. Ha $m \neq 1$ páratlan, akkor nyilván $3 \leq m < p$, és találhatók olyan y_i egészek, melyekre a (8.20)-ban lévő x_i számokkal

$$y_i \equiv x_i \pmod{m} \quad \text{és} \quad -\frac{m-1}{2} \leq y_i \leq \frac{m-1}{2} \tag{8.21}$$

minden $1 \leq i \leq 4$ esetén. Ezekre az y_i egészekre (8.20) alapján

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{m},$$

és így létezik egy n egész szám úgy, hogy

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = mn \tag{8.22}$$

és

$$0 \leq n = \frac{1}{m}\left(y_1^2 + y_2^2 + y_3^2 + y_4^2\right) \leq \frac{4}{m}\left(\frac{m-1}{2}\right)^2 < m.$$

Ha n értéke nulla, akkor $y_i = 0$ és $x_i \equiv 0 \pmod{m}$ lenne minden $1 \leq i \leq 4$-re, amiből $x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{m^2}$, illetve $m^2 \mid mp$ és $m \mid p$ következne, ami $3 \leq m < p$ miatt lehetetlen. Tehát $0 < n < m$. Egy Euler által talált formula alapján

$$\left(x_1^2 + x_2^2 + x_3^2 + x_4^2\right)\left(y_1^2 + y_2^2 + y_3^2 + y_4^2\right) = t_1^2 + t_2^2 + t_3^2 + t_4^2, \tag{8.23}$$

ahol

$$\begin{aligned} t_1 &= x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4, \\ t_2 &= x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3, \\ t_3 &= x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4 \end{aligned}$$

és

$$t_4 = x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2.$$

Az azonosságot a műveletek és az összevonások elvégzésével elemi úton, csak kicsit hosszadalmasan igazolhatjuk. Euler formulájában (8.20) és (8.21) miatt minden t_i osztható m-mel. Így (8.20), (8.22) és (8.23) alapján

$$m^2np = t_1^2 + t_2^2 + t_3^2 + t_4^2,$$

azaz

$$np = \left(\frac{t_1}{m}\right)^2 + \left(\frac{t_2}{m}\right)^2 + \left(\frac{t_3}{m}\right)^2 + \left(\frac{t_4}{m}\right)^2$$

következik, ahol a $\frac{t_i}{m}$ számok egészek és $0 < n < m$.

Az előzőek alapján tehát a (8.20)-beli m csak akkor lehet minimális, ha $m = 1$. Ennek alapján minden p páratlan prímszám felírható

$$p = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

alakban, vagyis négy négyzetszám összegeként. De $p = 2$ is, hiszen $2 = 1^2 + 1^2 + 0^2 + 0^2$. A számelmélet alaptétele szerint minden $n > 1$ természetes szám felírható prímszámok szorzataként. De mint láttuk minden prímszám előállítható négy négyzetszám összegeként, ezért Euler (8.23)-beli formulája alapján minden pozitív egész felírható, mint négy négyzetszám összege. ∎

Ha a természetes számokat negyedik hatványok összegeként akarjuk felírni, akkor legalább 16 hatványra van szükségünk, amit egy konkrét példa,

$$31 = 2^4 + 1^4 + \cdots + 1^4 \quad (16 \text{ tag})$$

is igazol. De nemcsak 31 az egyedüli ilyen szám.

8.8. Tétel. *Az $n = 31 \cdot 16^q$ alakú számok, ahol $q \geq 0$ egy egész, nem állíthatók elő 16-nál kevesebb negyedik hatvány összegeként.*

Bizonyítás. $q = 0$, vagyis $n = 31$ esetén láttuk, hogy $31 \cdot 16^0$ nem írható fel 15 negyedik hatvány összegeként. Tegyük fel, hogy a tétel állítása igaz valamely $q \geq 0$ esetén, vagyis a

$$31 \cdot 16^q = x_1^4 + x_2^4 + \cdots + x_{15}^4 \tag{8.24}$$

diofantikus egyenlet nem oldható meg. Ha az állítással ellentétben a

$$31 \cdot 16^{q+1} = x_1^4 + x_2^4 + \cdots + x_{15}^4 \tag{8.25}$$

egyenlet megoldható lenne, akkor az $x_1, \ldots, x_{15}$ megoldásban minden x_i csak páros lehet. Ugyanis

$$x_i^4 \equiv \begin{cases} 0 \pmod{16}, & \text{ha } x_i \text{ páros,} \\ 1 \pmod{16}, & \text{ha } x_i \text{ páratlan,} \end{cases}$$

ezért

$$x_1^4 + \cdots + x_{15}^4 \equiv r \pmod{16},$$

ahol $0 \leq r \leq 15$. De (8.25) bal oldala osztható 16-tal, így $r = 0$, vagyis (8.25) megoldhatósága esetén valóban minden x_i $(i = 1, \ldots, 15)$ páros. Ekkor azonban

$$31 \cdot 16^q = \left(\frac{x_1}{2}\right)^4 + \cdots + \left(\frac{x_{15}}{2}\right)^4$$

következne, ahol az $\frac{x_i}{2}$ számok egészek, ami elletmond a feltételünknek, miszerint a (8.24) egyenletnek nincs egész megoldása. Ezen ellentmondásból, teljes indukciós gondolatmenettel a tétel állítása minden $q \geq 0$-ra következik. ∎

Visszatérve Waring említett problémájára, egy $k \geq 2$ természetes szám esetén jelöljük $g(k)$-val azt a pozitív egészet, melyre igaz, hogy minden természetes szám felírható legfeljebb $g(k)$ darab k-adik hatvány összegeként, de van olyan pozitív egész, mely $g(k)$-nál kevesebb k-adik hatvány összegeként nem állítható elő. 1909-ben Hilbert igazolta, hogy minden $k \geq 2$ esetén létezik ilyen $g(k)$. Az előző tételeinkből következik, hogy $g(2) = 4$ és $g(4) \geq 16$. Bizonyítható még, hogy $g(3) = 9$ és $g(4) = 19$. Tetszőleges k esetén a következő alsó becslést bizonyítjuk $g(k)$-ra.

8.9. Tétel. *Minden $k \geq 2$ pozitív egész esetén*

$$g(k) \geq 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2, \tag{8.26}$$

ahol $[\ \ ]$ *az egészrész-függvényt jelöli.*

Bizonyítás. Legyen $k \geq 2$, és tekintsük az

$$n = 2^k \left[\left(\frac{3}{2}\right)^k\right] - 1$$

pozitív egészet. Mivel

$$n < 2^k \left(\frac{3}{2}\right)^k - 1 = 3^k - 1 < 3^k,$$

ezért az n egész $n = \sum i^k$ alakú előállításában csak $i = 1$ vagy $i = 2$ fordulhat elő. De 2^k tagokból is legfeljebb $\left[\left(\frac{3}{2}\right)^k\right] - 1$ számú szerepelhet, mert

$$\left[\left(\frac{3}{2}\right)^k\right] 2^k > n.$$

Így

$$n = \left(\left[\left(\frac{3}{2}\right)^k\right] - 1\right) 2^k + \left(2^k - 1\right) 1^k$$

miatt n előállítható

$$\left(\left[\left(\frac{3}{2}\right)^k\right]-1\right)+\left(2^k-1\right)=2^k+\left[\left(\frac{3}{2}\right)^k\right]-2$$

darab k-adik hatvány összegeként, de ennél kevesebb hatvány összegeként már nem. ∎

1957-ben Mahler bebizonyította, hogy a (8.26)-ban az egyenlőség érvényes, ha k elég nagy. Minden k-ra azonban még nem ismerjük $g(k)$ pontos értékét.

A továbbiakban (9.6., 9.7., 9.9. és 10.11. Tétel) még foglalkozunk diofantikus egyenletekkel, de azok tárgyalásához további ismeretek szükségesek.

Feladatok

1. Megoldható-e az egész számok körében az $x^2+1=7y^3$ egyenlet.

2. Határozzuk meg azt a tízes számrendszerben felírt négyjegyű pozitív egész számot, amely 132-vel osztva 98 maradékot, míg 131-gyel osztva 112 maradékot ad.

3. Határozzuk meg az alábbi lineáris diofantikus egyenletek megoldásait:

(a) $62x+46y=182$;

(b) $98x-77y=14$;

(c) $273x+210y-165x=18$;

(d) $100x+101y+102z=103$.

4. Legyen $p>2$ prímszám. Határozzuk meg az

$$\frac{1}{x}+\frac{1}{y}=\frac{2}{p}$$

egyenlet pozitív egész megoldásait.

5. Bizonyítsuk be, hogy ha n nem $4k+2$ ($k\in\mathbf{Z}$) alakú, akkor az $x^2-y^2=n$ diofantikus egyenlet megoldható.

6. Határozzuk meg az $x^2 - 4y^2 = 116$ diofantikus egyenlet pozitív egész megoldásait.

7. Melyek azok a tízes számrendszerben felírt pozitív egész számok, amelyeknek négyzete ugyanarra a két számjegyre végződik, mint maga a szám.

8. Melyik az a tízes számrendszerben felírt négyjegyű négyzetszám, amely $aabb_{10}$ alakú.

9. Mely pitagoraszi számhármasok lehetnek számtani sorozat szomszédos tagjai.

10. Mely pitagoraszi számhármasok lehetnek mértani sorozat szomszédos tagjai.

11. Oldjuk meg az $\left(x^2 + y^2\right)^4 = z^2 + t^2$ diofantikus egyenletet.

12. Legyenek x, y és z páronként relatív prím egész számok. Az

$$x = a + 2b, \quad y = a - b \ (a, b \in \mathbf{Z})$$

helyettesítések alkalmazásával oldjuk meg az $x^2 + 2y^2 = 3z^2$ diofantikus egyenletet.

13. Oldjuk meg a $3x^2 + 3y^2 - z^2 = 10xy$ diofantikus egyenletet.

14. Oldjuk meg a $4x^2 + y^2 - z^2 = 2xy + 2xz - 24x - 36$ diofantikus egyenletet.

15. Határozzuk meg az $x! + y! = z!$ egyenlet pozitív egész megoldásait.

9. Diofantikus approximáció és alkalmazásai

A gyakorlatban sokszor szükséges a valós számok racionális számokkal való közelítése vagy más szóval approximálása. Például a körrel kapcsolatos numerikus számolás esetén π értékét általában 3,14-dal közelítjük. Adott α arányú fogaskerék-áttétel esetén pedig úgy kell meghatározni a kerekek p, illetve q fogszámát, hogy p/q minél jobban approximálja α-t. Tetszőleges α valós szám és $\varepsilon > 0$ esetén végtelen sok olyan p, q egész szám található úgy, hogy $|\alpha - p/q| < \varepsilon$, mivel a racionális számok a számegyenesen mindenütt sűrűn helyezkednek el. Ezért az a kérdés érdektelen, hogy egy valós α közelíthető-e racionális számokkal tetszőleges pontossággal. Érdekes viszont azt vizsgálni, hogy az approximációnál elkövetett hiba mekkora az approximáló tört nevezőjéhez viszonyítva. Hogy a következőkben pontosan beszélhessünk az approximáció minőségéről, bevezetjük az approximáció rendjének fogalmát.

A továbbiakban az approximáló p/q törtekről feltesszük, hogy $q > 0$, hiszen $q < 0$ esetén a tört -1-gyel bővíthetjük.

Definíció. Legyen $k > 0$ egy valós szám. Akkor mondjuk, hogy egy α valós szám k-ad rendben approximálható, ha létezik egy $c = c(\alpha) > 0$ csak α-tól függő konstans úgy, hogy az

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{c}{q^k}$$

egyenlőtlenség végtelen sok p, q egész szám esetén fennáll.

Már az ókori görögök is tudták, hogy π értéke, azaz a kör kerületének és átmérőjének aránya a $3\frac{1}{7} = \frac{22}{7}$ racionális számmal közelíthető. Ez az előző definíció értelmében, az elkövetett hibát a közelítő tört nevezőjéhez viszonyítva, π-nek jobb approximációját adja, mint a manapság használt $3{,}14 = \frac{157}{50}$. Ugyanis rövid numerikus számítással

$$\left|\pi - \frac{22}{7}\right| < 0{,}00127 < \frac{1}{7^2}\,(= 0{,}0204\ldots)$$

adódik, míg

$$\left|\pi - \frac{157}{50}\right| > 0{,}00159 > \frac{1}{50^2}\,(= 0{,}0004)\,.$$

Egy a/b racionális szám esetén a legjobban approximáló tört nyilván önmaga. De ekkor sem érdektelen az approximáció kérdése, hiszen nagy nevező esetén célszerű a törtet kisebb nevezőjű, de őt jól approximáló racionális számmal helyettesíteni. Racionális számokra a következő tételt bizonyítjuk.

9.1. Tétel. *A racionális számok első rendben approximálhatók, de magasabb rendben nem.*

Bizonyítás. Legyen a/b egy racionális szám, melyre $(a, b) = 1$. Ekkor az

$$ax - by = 1$$

diofantikus egyenlet megoldható, és végtelen sok x, y egész megoldása van. Tehát végtelen sok q, p egész szám esetén fennáll az

$$aq - bp = 1$$

egyenlőség. Ebből, mindkét oldalt bq-val osztva

$$\left|\frac{a}{b} - \frac{p}{q}\right| = \frac{1}{|bq|} \leq \frac{1}{|q|}$$

adódik. Feltehetjük, hogy $q > 0$, mert ellenkező esetben a (p, q) számpárt $(-p, -q)$-val helyettesíthetjük, így

$$\left|\frac{a}{b} - \frac{p}{q}\right| \leq \frac{1}{q} < \frac{2}{q}$$

végtelen sok p, q egész számpár esetén, vagyis a/b első rendben approximálható.

A tétel második részét indirekt úton bizonyítjuk. Tegyük fel, hogy egy a/b racionális szám $k > 1$ rendben approximálható, vagyis valamely $c > 0$ konstans mellett

$$0 < \left|\frac{a}{b} - \frac{p}{q}\right| < \frac{c}{q^k}$$

végtelen sok p, q egész esetén. Ekkor azonban

$$0 < |aq - bp| \leq \frac{c\,|b|\,q}{q^k} = \frac{c\,|b|}{q^{k-1}},$$

ami nem teljesülhet végtelen sok q esetén, hiszen $|aq - bp|$ pozitív egész, és $k - 1 > 0$ miatt

$$\frac{c\,|b|}{q^{k-1}} \to 0 \quad \text{ha} \quad q \to \infty,$$

így 0 és $c\,|b|/q^{k-1}$ közé nem eshet egész szám, ha q elég nagy. Ez az ellentmondás bizonyítja a tételünk második felét. ∎

Az irracionális számok jobban approximálhatók. Dirichlet következő tétele értelmében minden irracionális szám legalább másodrendben approximálható.

9.2.Tétel. *Minden irracionális α esetén létezik egy $c = c(\alpha) \leq 1$ pozitív konstans úgy, hogy*

$$\left|\alpha - \frac{p}{q}\right| < \frac{c}{q^2}$$

végtelen sok p, q egész esetén.

Bizonyítás. Legyen Q egy tetszőlegesen nagy pozitív egész, és tekintsük az

$$\alpha - [\alpha], 2\alpha - [2\alpha], 3\alpha - [3\alpha], \ldots, (Q+1)\alpha - [(Q+1)\alpha]$$

számokat, ahol [ ] az egészrész-függvény. Ezek a számok az egészrész-függvény tulajdonságai és α irracionalitása miatt a $(0,1)$ nyílt intervallumban helyezkednek el, különböznek egymástól és számuk $Q+1$. Osszuk fel a [0,1] intervallumot a $0, {}^{1}\!/_{Q}, {}^{2}\!/_{Q}, \ldots, {}^{Q}\!/_{Q} = 1$ pontokkal Q darab ${}^{1}\!/_{Q}$ hosszúságú intervallumra. A számaink nem esnek intervallum végpontba, mivel α irracionális, és számuk $Q+1$, ezért van olyan intervallum, amely két számot tartalmaz, azaz van olyan i és j $(1 \leq i < j \leq Q+1)$ úgy, hogy $i\alpha - [i\alpha]$ és $j\alpha - [j\alpha]$ ugyanabban az intervallumban van. Ezekre a számokra

$$\big|\big(j\alpha - [j\alpha]\big) - \big(i\alpha - [i\alpha]\big)\big| = \big|\big(j-i\big)\alpha - \big([j\alpha] - [i\alpha]\big)\big| < \frac{1}{Q}. \tag{9.1}$$

Legyen $j - i = q$ és $[j\alpha] - [i\alpha] = p$. Az így meghatározott p, q számok egészek, $0 < q \leq Q$ és (9.1)-ből

$$|q\alpha - p| < \frac{1}{Q},$$

azaz

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{qQ} \leq \frac{1}{q^2}$$

következik. Tehát van olyan ${}^{p}\!/_{q}$ racionális szám, amely másodrendben approximálja α-t $c = 1$ konstanssal. $\left|\alpha - \frac{p}{q}\right| > 0$ miatt megadható egy $Q' > 0$ egész úgy, hogy

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{qQ'}.$$

Ezzel a Q'-vel megismételve az előző eljárást, meg tudunk adni olyan p', q' egész számokat, melyekre

$$\left|\alpha - \frac{p'}{q'}\right| < \frac{1}{q'Q'} \leq \frac{1}{q'^2},$$

és p', q' nyilván különbözik a p, q egészektől.

Folytatva az eljárást, végtelen sok különböző p/q racionális szám adható meg, melyek másodrendben approximálják α-t $c = 1$ konstanssal. ∎

A tételünkből és annak bizonyításából következik, hogy minden irracionális valós szám esetén végtelen sok másodrendben approximáló tört létezik $c = 1$ approximációs konstans mellett. Felvetődik a kérdés, hogy c-re mi a legjobb lehetőség. Hurwitz bizonyította, hogy ez $c = 1/\sqrt{5}$, vagyis minden α irracionális szám esetén végtelen sok p/q tört található úgy, hogy

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2},$$

de van olyan irracionális szám, melyre az

$$\left|\alpha - \frac{p}{q}\right| < \frac{c}{q^2}$$

egyenlőtlenség csak véges számú p/q törtre teljesülhet, ha $c < 1/\sqrt{5}$. Ilyen például $\alpha = \frac{1-\sqrt{5}}{2}$.

Az irracionális számok között vannak olyanok, melyek másodrendnél nem approximálhatók jobban, ilyenek például az irracionális algebrai számok. Mielőtt rátérünk az erre vonatkozó eredményekre, felelevenítünk néhány korábbi ismeretet.

Egy α valós vagy komplex számot algebrai számnak nevezzük, ha van olyan

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \quad (n \geq 1)$$

racionális együtthatós polinom, melynek α zérushelye. Ha α zérushelye $f(x)$-nek, de nem zérushelye egyetlen n-nél alacsonyabb fokú racionális együtthatós polinomnak, akkor α-t n-edfokú algebrai számnak nevezzük, az $f(x)$ polinomot pedig α definiáló polinomjának. Az $f(x)$ definiáló polinom nyilván irreducibilis a racionális számtest felett, hiszen másként α foka n-nél kisebb lenne. $f(x)$ minden zérushelye egyszeres, hiszen többszörös zérushelyek esetén $f(x)$ és deriált polinomja nem lennének relatív prímek, így $f(x)$ nem lenne irreducibilis. Továbbá ha α egy legalább másodfokú algebrai szám, akkor a definiáló polinomjának nincs racionális zérushelye, hiszen ellenkező esetben a racionális gyöktényező leválasztásával α egy $n-1$-edfokú

racionális együtthatós polinomnak lenne a zérushelye. Az algebrai számok definiáló polinomjairól feltételezhetjük, hogy egész együtthatósak, mert az együtthatók nevezőinek legkisebb közös többszörösével szorozva a polinomot, a zérushelyek nem változnak. Megemlítjük még, hogy bizonyítható, miszerint az algebrai számok definiáló polinomjai konstans szorzótól eltekintve egyértelműek. A nem algebrai számokat transzcendens számoknak nevezzük.

Visszatérve az approximációs problémáinkhoz, a 9.1. Tétel alapján az elsőfokú algebrai számok (azaz a racionális számok) pontosan első rendben, a 9.2. Tétel szerint pedig az irracionális algebrai számok (amelyek legalább másodfokúak) legalább másodrendben approximálhatók. Bebizonyítható, hogy az említetteknél jobb approximáció nem érthető el. Bizonyítás nélkül idézzük az alábbi eredményt.

9.3. Tétel. *Legyen α egy valós algebrai szám és $\varepsilon > 0$ egy tetszőleges rögzített valós szám. Ekkor bármely $c > 0$ mellett az*

$$\left|\alpha - \frac{p}{q}\right| < \frac{c}{q^{2+\varepsilon}}$$

egyenlőtlenséget kielégítő p/q racionális számok száma véges.

A fenti tétel egy nyilvánvaló következményét a későbbiekben fel fogjuk használni.

Következmény. Legyen α egy n-edfokú valós algebrai szám $n \geq 3$ feltétellel. Ekkor bármely $c > 0$ mellett az

$$\left|\alpha - \frac{p}{q}\right| < \frac{c}{q^{n}}$$

egyenlőtlenséget kielégítő p/q racionális számok száma véges (vagyis egy n-edfokú ($n \geq 3$) valós algebrai szám csak n-nél alacsonyabb rendben approximálható).

A 9.3. Tétel és következményének bizonyítása messzire vezetne, ezért nem bizonyítjuk. A következmény egy gyengébb formája azonban könyebben igazolható.

9.4. Tétel. *Legyen α egy n-edrendű valós algebrai szám, k pedig egy pozitív valós szám $k > n$ feltétellel. Ekkor bármely $c > 0$ esetén az*

$$\left|\alpha - \frac{p}{q}\right| < \frac{c}{q^{k}}$$

egyenlőtlenséget kielégítő p/q racionális számok száma véges (*azaz α nem approximálható a fokánál magasabb rendben*).

Bizonyítás. Feltehetjük, hogy $n \geq 2$, mert az $n = 1$ eset következik a 9.1. Tételünkből. Legyen α definiáló polinomja

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0,$$

ahol $a_0, \ldots, a_n$ egész számok és $a_n \neq 0$. Legyenek $k > n$ és $c > 0$ valós számok és tegyük fel, hogy

$$\left| \alpha - \frac{p}{q} \right| < \frac{c}{q^k} \tag{9.2}$$

valamely $p/q \neq 0$ racionális számra. Tekintsük a

$$q^n f\left(\frac{p}{q}\right) = q^n \left(a_n \left(\frac{p}{q}\right)^n + \cdots + a_0 \right) = a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_0 q^n$$

számot ami nyilván egész és nem nulla, mert α definiáló polinomjának nincs racionális gyöke. Legyenek $f(x)$ zérushelyei $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$, ahol $|\alpha_i - \alpha| > 0$ minden $2 \leq i \leq n$ esetén, mert a definiáló polinom zérushelyei különbözőek. Mivel a zérushelyek nem racionálisak és

$$f(x) = a_n (x - \alpha)(x - \alpha_2) \cdots (x - \alpha_n),$$

ezért (9.2) alapján

$$0 < \left| q^n f\left(\frac{p}{q}\right) \right| = \left| q^n a_n \left(\frac{p}{q} - \alpha\right) \prod_{i=2}^{n} \left(\frac{p}{q} - \alpha_i\right) \right| =$$

$$= \left| q^n a_n \left(\alpha - \frac{p}{q}\right) \right| \left| \prod_{i=2}^{n} \left(\alpha - \frac{p}{q} + \alpha_i - \alpha\right) \right| <$$

$$< q^n \frac{|a_n|\, c}{q^k} \prod_{i=2}^{n} \left(\left| \alpha - \frac{p}{q} \right| + |\alpha_i - \alpha| \right)$$

egyenlőtlenség adódik. De (9.2) miatt feltehetjük, hogy $\left| \alpha - \frac{p}{q} \right| < 1$, ezért létezik egy $c' > 0$ valós szám, melyre

$$\prod_{i=2}^{n} \left(\left| \alpha - \frac{p}{q} \right| + |\alpha_i - \alpha| \right) < c'$$

és így

$$0 < \left| q^n f\left(\frac{p}{q}\right)\right| < \frac{|a_n|\, cc'}{q^{k-n}}.$$

Ez az egyenlőtlenség azonban csak véges sok p/q esetén teljesülhet, mert $q^n f\left(\frac{p}{q}\right)$ egész és $k-n>0$ miatt $q^{k-n}\to\infty$, ha $q\to\infty$. ∎

A korábbi tanulmányainkból tudjuk, Cantor munkássága nyomán, hogy végtelen sok transzcendens szám létezik. Sőt a valós algebrai számok halmazának számossága megszámlálhatóan végtelen, míg a transzcendens számoké kontinuum. Régebben a transzcendens számok létezésének bizonyítása is nehézségekbe ütközött. Először Liouville bizonyította 1851-ben transzcendens szám létezését a következő szellemes konstrukcióval.

9.5. Tétel. *A*

$$\gamma = \sum_{n=1}^{\infty} \frac{1}{2^{n!}}$$

konvergens sor összegével definiált γ valós szám transzcendens.

Bizonyítás. Könnyen belátható, hogy a sor valóban konvergens, és így valóban definiál egy valós számot.

Megmutatjuk, hogy a fenti γ tetszőleges rendben approximálható. Legyen t egynél nagyobb pozitív egész, és tekintsük a

$$\frac{p}{q} = \sum_{n=1}^{t-1} \frac{1}{2^{n!}}$$

racionális számot, ahol nyilván $q = 2^{(t-1)!}$. Ekkor

$$\left|\gamma - \frac{p}{q}\right| = \sum_{n=t}^{\infty} \frac{1}{2^{n!}} = \frac{1}{2^{t!}}\left(1 + \sum_{n=t+1}^{\infty} \frac{1}{2^{n!-t!}}\right) <$$
$$< \frac{1}{2^{t!}}\left(1 + \sum_{i=1}^{\infty} \frac{1}{2^i}\right) = \frac{2}{2^{t!}},$$

mert $(t+i)! - t! > i$ minden $i \geq 1$ esetén és

$$\sum_{n=0}^{\infty} \frac{1}{2^n} = 2.$$

Ebből $q = 2^{(t-1)!}$ miatt $t = k$ helyettesítéssel

$$\left|\gamma - \frac{p}{q}\right| < \frac{2}{2^{(t-1)!t}} = \frac{2}{q^t} = \frac{2}{q^k}$$

következik, $t = k + i$ esetén pedig

$$\left|\gamma - \frac{p_i}{q_i}\right| < \frac{2}{q_i^t} = \frac{2}{q_i^{k+i}} \leq \frac{2}{q_i^k}$$

minden $i \geq 0$-ra, ahol $p_0/q_0 = p/q$, $p_1/q_2, \ldots$ közelítő törtek különbözőek, mivel a $q_i = 2^{(t-1)!} = 2^{(k+i-1)!}$ nevezők különböző hatványai 2-nek, a számlálók pedig páratlanok.

Tehát γ tetszőleges rendben approximálható $c = 2$ approximációs konstanssal, ezért a 9.3., illetve a 9.4. Tétel értelmében nem lehet algebrai. ∎

A Pell-egyenlet megoldása

A diofantikus approximáció eredményei jól használhatók a diofantikus egyenletekkel kapcsolatos problémáknál is. Ezzel kapcsolatban bemutatunk néhány példát.

Tekintsük először a Pell-egyenletként ismert

$$x^2 - Dy^2 = 1$$

egyenletet, ahol D egész szám és az egyenlet x, y egész megoldásait keressük. $x = \pm 1$, $y = 0$ nyilván megoldás, ezért a következőkben ezen triviális megoldástól eltekintünk. Szintén feltehetjük, hogy $D \neq 0$, hiszen ha D=0, akkor csak az $x = \pm 1$, $y =$ tetszőleges megoldások adódnak. $D < 0$ esetén két pozitív egész összege 1, így $|x| = 1$ és $y = 0$, illetve $x = 0$ és $|y| = 1$ szolgáltathatják a megoldásokat, az utóbbi csak $D = -1$ esetén. Ha D teljes négyzet, vagyis $D = d^2$, ahol d egész, akkor az egyenlet

$$(x + dy)\,(x - dy) = 1$$

alakú és visszavezethető az $|x + dy| = 1$, $|x - dy| = 1$ egyenletrendszerre, aminek konkrét esetben véges számú összes megoldása könnyen megadható. Tehát végtelen sok megoldás csak akkor várható, ha $D > 0$ és D nem egy egész szám négyzete.

9.6. Tétel. *Ha $D > 0$ és D nem teljes négyzet, akkor az*

$$x^2 - Dy^2 = 1$$

Pell-egyenletnek van nem triviális megoldása.

Bizonyítás. A feltételek miatt $\sqrt{D}$ irracionális, ezért a 9.2. Tétel alapján végtelen sok olyan p, q relatív prím egész számpár található, melyekre

$$\left|\sqrt{D} - \frac{p}{q}\right| < \frac{1}{q^2}. \tag{9.3}$$

Ezen számpárokra (9.3) kétszeri felhasználásával az

$$\begin{aligned}\left|p^2 - Dq^2\right| &= \left|p - \sqrt{D}q\right| \left|p + \sqrt{D}q\right| = \\ &= q^2 \left|\sqrt{D} - \frac{p}{q}\right| \left|\sqrt{D} + \frac{p}{q}\right| < \left|\sqrt{D} + \frac{p}{q}\right| = \\ &= \left|\frac{p}{q} - \sqrt{D} + 2\sqrt{D}\right| < \frac{1}{q^2} + 2\sqrt{D} \leq 1 + 2\sqrt{D}\end{aligned}$$

egyenlőtlenség adódik, amiből

$$-\left(1 + 2\sqrt{D}\right) < p^2 - Dq^2 < 1 + 2\sqrt{D}$$

következik. De a $p^2 - Dq^2$ számok egészek és egyik sem zérus, mert D nem teljes négyzet, továbbá csak véges számú értéket vehetnek fel, ezért a skatulya elv alapján van olyan $t \neq 0$ egész szám, melyre

$$-\left(1 + 2\sqrt{D}\right) < t < 1 + 2\sqrt{D}$$

és

$$p^2 - Dq^2 = t \tag{9.4}$$

végtelen sok különböző p, q egész számra. Redukáljuk ezen (p, q) számpárokat modulo $|t|$, azaz tekintsük helyettük azon (p', q') párokat, melyekre $p \equiv p'$, illetve $q \equiv q' \pmod{|t|}$ és $0 \leq p', q' < |t|$. A különböző (p', q') számpárok száma véges, maximum $|t|^2$, ezért a (9.4)-et kielégítő végtelen sok (p, q) pár között van két (p_1, q_1) és (p_2, q_2) számpár úgy, hogy $p_1 \equiv p_2$ és $q_1 \equiv q_2 \pmod{|t|}$. Ezek segítségével definiáljuk az

$$x = \frac{p_1 p_2 - D q_1 q_2}{|t|}, \quad y = \frac{p_1 q_2 - p_2 q_1}{|t|} \tag{9.5}$$

számokat. x és y egész számok, mert (9.4) alapján

$$p_1 p_2 - D q_1 q_2 \equiv p_1^2 - D q_1^2 = t \equiv 0 \pmod{|t|}$$

és

$$p_1q_2 - p_2q_1 \equiv p_1q_1 - p_1q_1 = 0 \pmod{|t|}.$$

Ezekre az x, y egészekre azonban, szintén (9.4) alapján

$$x^2 - Dy^2 = \frac{(p_1p_2 - Dq_1q_2)^2 - D(p_1q_2 - p_2q_1)^2}{t^2} =$$
$$= \frac{(p_1^2 - Dq_1^2)(p_2^2 - Dq_2^2)}{t^2} = \frac{tt}{t^2} = 1,$$

tehát (x, y) megoldása a tételbeli egyenletnek. Ez a megoldás nem triviális, mert (9.5) alapján $y = 0$-ból $p_1/q_1 = p_2/q_2$ következne és így (p_1, q_1) és (p_2, q_2) nem lennének különböző megoldásai (9.4)-nek. ∎

A Pell-egyenlet megoldhatóságát tehát bebizonyítottuk. Hátra van még annak az eldöntése, hogy van-e végtelen sok megoldás és ha igen, ezek meghatározhatók-e. Mielőtt ezekre a kérdésekre válaszolnánk bevezetjük az egyenlet alapmegoldásának fogalmát. Tekintsük az egyenlet pozitív megoldásait, vagyis azokat, melyekre $x \geq 1$, $y \geq 1$. Ilyenek vannak az előző tétel alapján (legalább egy), mert (x, y)-nal együtt $(\pm x, \pm y)$ is megoldás. Ezek között alapmegoldásnak nevezzük azt a (u, v) megoldást, melyre $u + \sqrt{D}v$ értéke minimális. Tehát (u, v) alapmegoldás, ha u, v pozitív egészek,

$$u^2 - Dv^2 = 1$$

és minden (x, y) pozitív megoldás esetén $x + \sqrt{D}y \geq u + \sqrt{D}v$. Ilyen alapmegoldás nyilván létezik és egyértelműen meghatározott.

Most már rátérhetünk a fenti kérdések megválaszolására.

9.7. Tétel. *Legyen $D > 0$ egy nem teljes négyzet természetes szám. Ekkor az*

$$x^2 - Dy^2 = 1$$

Pell-egyenletnek végtelen sok (x, y) egész megoldása van. Ha (u, v) az egyenlet alapmegoldása, akkor az összes megoldásai azon (x, y) számpárok, melyeket az

$$x + \sqrt{D}y = \pm\left(u \pm \sqrt{D}v\right)^n \tag{9.6}$$

egyenlőség definiál, ahol $n = 0, 1, 2, \ldots$.

Bizonyítás. Először megmutatjuk, hogy a (9.6) által definiált (x, y) párok megoldásai az egyenletnek, ami végtelen sok megoldás létezését bizonyítja. Legyen (x, y) egy számpár, melyre

$$x + \sqrt{D}y = \left(u + \sqrt{D}v\right)^n,$$

ahol n egy rögzített egész. Feltehetjük, hogy $n > 0$, mert $n = 0$-ra triviális az állítás. A binomiális tétel alapján könnyen belátható, hogy ekkor

$$x - \sqrt{D}y = \left(u - \sqrt{D}v\right)^n,$$

és így

$$\begin{aligned} x^2 - Dy^2 &= \left(x + \sqrt{D}y\right)\left(x - \sqrt{D}y\right) = \left(u + \sqrt{D}v\right)^n \left(u - \sqrt{D}v\right)^n = \\ &= \left(u^2 - Dv^2\right)^n = 1, \end{aligned}$$

tehát (x, y) valóban megoldás. Hasonlóan látható be az állítás, ha (9.6)-ban az előjeleket változtatjuk.

Most bizonyítjuk, hogy minden megoldást a (9.6) egyenlőség generál. Tegyük fel az állításunkkal ellentétben, hogy (x', y') egy megoldása az egyenletnek, de nem elégíti ki (9.6)-ot. Feltehetjük, hogy $x', y' > 0$, mert ha egy (x, y) pár kielégíti a (9.6) egyenlőséget, akkor a $(\pm x, \pm y)$ párok is, a jobb oldalon alkalmasan megválasztva az előjeleket. A feltételünk és az alapmegoldás definíciója következtében van olyan k pozitív egész, melyre

$$\left(u + \sqrt{D}v\right)^k < x' + \sqrt{D}y' < \left(u + \sqrt{D}v\right)^{k+1},$$

vagy ami ezzel azonos

$$1 < \left(x' + \sqrt{D}y'\right)\left(u + \sqrt{D}v\right)^{-k} < u + \sqrt{D}v. \tag{9.7}$$

Mivel $u^2 - Dv^2 = 1$ és így

$$\frac{1}{u + \sqrt{D}v} = \frac{u - \sqrt{D}v}{u^2 - Dv^2} = u - \sqrt{D}v,$$

ezért definiálhatunk (a, b) és (α, β) egész számpárokat az

$$\alpha + \sqrt{D}\beta = \left(x' + \sqrt{D}y'\right)\left(u - \sqrt{D}v\right)^k = \left(x' + \sqrt{D}y'\right)\left(a - \sqrt{D}b\right) \tag{9.8}$$

egyenlőségekkel. Az előzők alapján (a, b) megoldása az egyenletünknek. De az (α, β) számpár is megoldás, mert

$$\alpha - \sqrt{D}\beta = \left(x' - \sqrt{D}y'\right)\left(a + \sqrt{D}b\right) \tag{9.9}$$

és így (9.8) és (9.9) alapján

$$\alpha^2 - D\beta^2 = \left(\alpha + \sqrt{D}\beta\right)\left(\alpha - \sqrt{D}\beta\right) = \left(x'^2 - Dy'^2\right)\left(a^2 - Db^2\right) = 1 \cdot 1 = 1.$$

(9.8)-ból adódik, hogy

$$\alpha = ax' - Dby' \quad \text{és} \quad \beta = ay' - bx'.$$

(x', y') és (a, b) az egyenletünk pozitív megoldásai, ezért $x' > \sqrt{D}y'$ és $a > \sqrt{D}b$, így

$$\alpha = ax' - \left(\sqrt{D}b\right)\left(\sqrt{D}y'\right) > ax' - ax' = 0,$$

tehát α pozitív. (9.7) és (9.8) miatt

$$\alpha + \sqrt{D}\beta > 1 \text{ is igaz, mert } (u + \sqrt{D}v)^{-k} = (u - \sqrt{D}v)^k.$$

De β sem lehet negatív, mert ha $\beta < 0$ lenne, akkor $\alpha + \sqrt{D}\beta > 1$ következtében, felhasználva, hogy $\left(\alpha + \sqrt{D}\beta\right)\left(\alpha - \sqrt{D}\beta\right) = 1$,

$$\alpha - \sqrt{D}\beta = |\alpha| + \sqrt{D}\,|\beta| = \frac{1}{\alpha + \sqrt{D}\beta} < 1$$

adódna, ami lehetetlen, mert (α, β) nem triviális megoldás. Így (α, β) egy pozitív megoldás, ami szintén lehetetlen, mert a (9.7)-ből adódó

$$1 < \alpha + \sqrt{D}\beta < u + \sqrt{D}v$$

egyenlőtlenség ellentmondana annak, hogy (u, v) alapmegoldás.

Tehát az egyenlet minden megoldása kielégíti (9.6)-ot. Ezzel a tétel minden állítását bebizonyítottuk. ∎

A matematikában egy probléma megoldása gyakran új problémákat vet fel. Most is a Pell-egyenlet megoldása után felvetődik, hogy az egyenlet (u, v) alapmegoldása hogy határozható meg. Adható-e D-től függő felső korlát az u, v egészekre? A kérdés megválaszolása azért fontos, mert ha ismerünk egy ilyan korlátot, akkor számítógép segítségével kiszámítható idő alatt meghatározható az alapmegoldás, mely az összes megoldást generálja. A problémával kapcsolatban több eredmény is ismert, ezek közül egy a következő. Legyen (u, v) az $x^2 - Dy^2 = 1$ Pell-egyenlet alapmegoldása és

vezessük be a $q = \left[\sqrt{D}\,\right]$ és $E = 2\,(q+1)\left(\frac{2}{3}q+1\right)^{2q}$ jelöléseket. Ekkor $u < (q+1)\,E$ és $v < E$.

A Pell-egyenlet természetes általánosítása az

$$x^2 - Dy^2 = N$$

másodfokú diofantikus egyenlet, ahol N egy rögzített zérustól különböző egész szám, $D > 0$ és D nem teljes négyzet. Ez az egyenlet azonban nem minden N-re oldható meg, még $N = -1$ esetén is van olyan D, hogy nincs egész megoldása az egyenletnek. Például az $x^2 - 3y^2 = -1$ egyenletet egyetlen (x, y) egész értékpár sem elégíti ki. Igaz viszont a következő.

9.8. Tétel. *Legyenek D és N rögzített egész számok $D > 0$, D nem teljes négyzet és $N \neq 0$ feltétellel. Ekkor ha az*

$$x^2 - Dy^2 = N$$

egyenletnek van egész x, y megoldása, akkor végtelen sok megoldása van.

Bizonyítás. Legyen x_0, y_0 megoldása az egyenletnek és legyen (u, v) az $x^2 - Dy^2 = 1$ egyenlet alapmegoldása. Definiáljunk egy (x_n, y_n) egész számpárt az

$$x_n + \sqrt{D}y_n = \left(u + \sqrt{D}v\right)^n \left(x_0 + \sqrt{D}y_0\right)$$

egyenlőséggel. Ekkor (x_n, y_n) megoldása a tételbeli egyenletnek minden $n \geq 0$ természetes szám esetén, mert

$$\begin{aligned} x_n^2 - Dy_n^2 &= \left(x_n + \sqrt{D}y_n\right)\left(x_n - \sqrt{D}y_n\right) = \\ &= \left(u + \sqrt{D}v\right)^n \left(x_0 + \sqrt{D}y_0\right)\left(u - \sqrt{D}v\right)^n \left(x_0 - \sqrt{D}y_0\right) = \\ &= \left(u^2 - Dv^2\right)^n \left(x_0^2 - Dy_0^2\right) = 1N = N \end{aligned}$$

és különböző n értékek különböző (x_n, y_n) számpárokat határoznak meg. Tehát valóban végtelen sok megoldása van. ∎

A Thue—Siegel-tétel

A diofantikus approximációra vonatkozó eredmények egy másik alkalmazását mutatjuk be kétváltozós diofantikus egyenletekkel kapcsolatban.

9.9. Tétel. (Thue—Siegel-tétel) *Legyen* $n \geq 3$ *és*

$$f(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_0$$

egy n*-edfokú racionális együtthatós polinom, mely irreducibilis a racionális számtest felett. Legyen továbbá* N *egy racionális egész szám. Ekkor a*

$$g(x,y) = a_n x^n + a_{n-1} x^{n-1} y + \cdots + a_1 x y^{n-1} + a_0 y^n = N \tag{9.10}$$

diofantikus egyenletnek csak véges sok (x,y) *egész megoldása lehet.*

Bizonyítás. $z = x/y$ helyettesítéssel a $g(x,y)$ polinom

$$g(x,y) = y^n g\left(\frac{x}{y}, 1\right) = y^n g(z,1) = y^n f(z)$$

alakba is írható.

Először feltesszük, hogy az $f(z)$ polinomnak nincs valós zérushelye. Ebben az esetben analízisbeli eszközökkel igazolható, hogy van olyan $c > 0$ valós szám úgy, hogy

$$|f(z)| \geq c$$

minden valós z esetén ($a_n > 0$ esetén c az f (polinom)függvény minimuma, $a_n < 0$ esetén pedig a maximum abszolút értéke). Tegyük fel, hogy (x,y) egy megoldása a (9.10) egyenletnek. Ekkor

$$|N| = \left| y^n g\left(\frac{x}{y}, 1\right) \right| = \left| y^n f\left(\frac{x}{y}\right) \right| \geq c\,|y|^n,$$

vagyis

$$|y|^n \leq \frac{|N|}{c}.$$

Ez csak véges sok y egész számra állhat fenn, és ezeket (9.10)-be helyettesítve mindegyikhez legfeljebb n darab egész x található úgy, hogy (x,y) megoldása legyen az egyenletnek. Így valóban csak véges lehet a megoldások száma.

Tegyük fel, hogy $f(z)$-nek van valós zérushelye és legyen ez α_1. Az α_1 különbözik a többi zérushelytől, mert $f(z)$ nem lehetne irreducibilis többszörös gyökök mellett. Írjuk fel $f(z)$-t az

$$f(z) = a_n \prod_{i=1}^{n} (z - \alpha_i)$$

gyöktényezős alakban. Ekkor

$$g(x,y) = y^n a_n \prod_{i=1}^{n} \left(\frac{x}{y} - \alpha_i \right),$$

és így (x,y) csak akkor lehet megoldása (9.10)-nek, ha

$$|N| = |g(x,y)| = |y|^n |a_n| \prod_{i=1}^{n} \left| \frac{x}{y} - \alpha_i \right|, \tag{9.11}$$

vagyis ha

$$\left| \frac{x}{y} - \alpha_1 \right| = \frac{|N|}{|a_n| \prod\limits_{i=2}^{n} \left| \frac{x}{y} - \alpha_i \right|} \cdot \frac{1}{|y|^n}. \tag{9.12}$$

Ha (9.10)-nek végtelen sok $(x,y) = (x_j, y_j)$ megoldása lenne, akkor

$$\lim_{j \to \infty} y_j = \infty,$$

és ezért (9.11) ezen megoldásokra csak akkor lehet igaz, ha az $\frac{x_j}{y_j}$ sorozat, vagy ennek egy részsorozata konvergál valamely α_i-hez. α_i nem lehet komplex, mert komplex α_i esetén $|r - \alpha_i| \geq |\mathrm{Im}(\alpha_i)|$ minden r valós számra. Tehát α_i valós, feltehetjük, hogy $\alpha_i = \alpha_1$. De ha $x_j/y_j \to \alpha_1$ ha $j \to +\infty$, akkor

$$\lim_{j \to \infty} \prod_{i=2}^{n} \left| \frac{x_j}{y_j} - \alpha_i \right| = \prod_{i=2}^{n} |\alpha_1 - \alpha_i| = c',$$

ahol $c' > 0$ egy konstans. Így végtelen sok megoldás feltételezése esetén (9.12) alapján létezne egy $c_1 > 0$ pozitív valós szám úgy, hogy az

$$\left| \frac{x}{y} - \alpha_1 \right| < \frac{c_1}{|y|^n}$$

egyenlőtlenségnek végtelen sok (x,y) egész megoldása lenne. Ez azonban ellentmond a 9.3. Tételből adódó következménynek. ∎

Feladatok

1. Legyen α adott valós szám. Bizonyítsuk be, hogy ha tetszőleges ε pozitív valós számhoz található p egész szám és q természetes szám, melyekre

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{\varepsilon}{q}$$

teljesül, akkor α irracionális szám.

2. Bizonyítsuk be, hogy az

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!} + \cdots$$

szám irracionális.

3. Bizonyítsuk be, hogy

$$\left|\sqrt{2} - \frac{p}{q}\right| > \frac{1}{3q^2}$$

bármely p, q pozitív egész esetén.

4. Legyen $D > 0$ és D nem teljes négyzet egész szám. Bizonyítsuk be, hogy ha az x_0, y_0 pozitív egészek megoldásai az $x^2 - Dy^2 = 1$ Pell-egyenletnek, akkor

$$\left|\sqrt{D} - \frac{x_0}{y_0}\right| < \frac{1}{\sqrt{D}y_0^2}.$$

5. Bizonyítsuk be, hogy az

$$x^2 - 8y^2 = 4 \quad \text{és} \quad x^2 - 2x = -1$$

egyenleteknek végtelen sok x, y egész megoldása van, de az

$$x^2 - 8y^2 = 2 \quad \text{és} \quad x^2 - 3x = -1$$

egyenletek nem oldhatók meg az egész számok körében.

6. Adjuk meg az

$$x^2 - 2y^2 = 1$$

Pell-egyenlet összes olyan megoldását, melyekre $0 < x < 50$.

7. Bizonyítsuk be, hogy ha az $x^2 - 2y^2 = N_1$ és $x^2 - 2y^2 = N_2$ Pell-egyenletek megoldhatók, akkor az $x^2 - 2y^2 = N_1N_2$ egyenlet is megoldható.

10. Másodrendű lineáris rekurzív sorozatok

Fibonacci vagy más néven Leonardo Pisano olasz matematikus 1202-ben megjelent könyvében szerepelt a következő feladat. A nyulak két hónapos korukban érik el az ivarérettséget, és ettől kezdve minden nyúlpár havonta egy újszülött nyúlpárnak ad életet. Hány pár nyulunk lesz egy év múlva, ha jelenleg egy újszülött nyúlpárunk van, és közben egy nyúl sem pusztul el? A probléma megoldása nem nehéz. Jelöljük az n-edik hónapban rendelkezésünkre álló nyúlpárok számát F_n-nel. Nyilván $F_1 = F_2 = 1$ és $F_3 = 2$, hiszen a kezdő nyúlpárunk a harmadik hónapban produkál egy új párt. Ha $n > 2$, akkor az n-edik hónapban megvannak az $n-1$-edik hónapban élők és még annyi újszülött pár ahány legalább kéthónapos nyúlpárunk van. A legalább kéthónapos párok száma annyi, ahány párunk volt az $n-2$-edik hónapban, vagyis F_{n-2}. Tehát az n-edik hónapban a nyúlpárok száma $F_n = F_{n-1} + F_{n-2}$. Ezek alapján már könnyű felírni a nyúlpárok számának sorozatát az első 12 hónapban:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144,$$

vagyis egy év múlva $F_{12} = 144$ nyúlpárunk lesz.

A Fibonacci-sorozat

A fenti probléma az egész számoknak egy érdekes sorozatához vezet, mely a feladat szerzőjének a nevét viseli. A sorozatot mostanában a következőképpen definiálják.

Definíció. Az egész számokból álló F_n $(n = 0, 1, 2, \ldots)$ végtelen sorozatot Fibonacci-sorozatnak nevezzük, ha kezdő elemei $F_0 = 0$, $F_1 = 1$ és minden további tag kielégíti az

$$F_n = F_{n-1} + F_{n-2} \quad (n > 1)$$

lineáris rekurzív képletet. A sorozat tagjait Fibonacci-számoknak nevezzük.

1202 óta már igen sokan foglalkoztak a Fibonacci-sorozattal, sok érdekes feladat és összefüggés ismert a Fibonacci-számokkal kapcsolatban. Fibonacci-számokhoz vezet például a következő probléma is. Hányféleképpen tudunk felmenni egy n fokú lépcsőn, ha egyszerre 1 vagy 2 lépcsőfokot léphetünk? Hasonlóan, mint a bevezető problémánknál, a k-adik $(k > 1)$ lépcsőfokra vagy a $k-1$-edik, vagy pedig a $k-2$-edik lépcsőről léphetünk

fel. A k-adik lépcsőre való lépés lehetőségeinek száma tehát annyi, amennyi a $k-1$-edik fokra jutások száma, hozzáadva a $k-2$-edik lépcsőre jutás számát. Az első lépcsőre $1 = F_2$, a másodikra pedig $2 = F_3$ féle képpen juthatunk fel, így könnyű utánagondolni, hogy az n-edik lépcsőre F_{n+1} különböző úton juthatunk el.

A jól ismert Pascal-háromszög

$$\begin{array}{ccccccc} 1 & & & & & & \\ 1 & 1 & & & & & \\ 1 & 2 & 1 & & & & \\ 1 & 3 & 3 & 1 & & & \\ 1 & 4 & 6 & 4 & 1 & & \\ \vdots & & & & & & \end{array}$$

alakú elrendezéséből kiindulva érdekes dolgot tapasztalhatunk. Az első oszlop egyeseiből kiinduló, felfelé vezető átlókban lévő számok összegei Fibonacci-számok: $1 = F_1$, $1 = F_2$, $1 + 1 = F_3$, $1 + 2 = F_4$, $1 + 3 + 1 = F_5, \ldots$. Ez általánosan is igaz.

10.1. Tétel. *Ha $n \geq 1$, akkor*

$$F_n = \binom{n-1}{0} + \binom{n-2}{1} + \binom{n-3}{2} + \cdots,$$

ahol $\binom{k}{t} = 0$, ha $t > k$.

Bizonyítás. Az állítást n-re vonatkozó teljes indukcióval bizonyítjuk. $n = 1$ és $n = 2$ esetén már láttuk, hogy a tétel igaz. Legyen $n \geq 2$ és tegyük fel, hogy az egyenlőség igaz az $1, 2, \ldots, n$ számokra. Ekkor, felhasználva a binomiális együtthatókra vonatkozó ismert

$$\binom{k}{t} + \binom{k}{t+1} = \binom{k+1}{t+1}$$

és $\binom{k}{0} = 1$ egyenlőségeket,

$$\begin{aligned} F_{n+1} = F_n + F_{n-1} = \binom{n-1}{0} + \binom{n-2}{1} + \binom{n-3}{2} + \cdots + \\ + \binom{n-2}{0} + \binom{n-3}{1} + \binom{n-4}{2} + \cdots = \\ = \binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \cdots \end{aligned}$$

adódik, vagyis a tétel $n+1$-re is igaz. ∎

A Fibonacci-számoknak sokféle előállítása ismert, ezek közül az alábbiakban az úgynevezett Binet-formulát ismertetjük. Az

$$x^2 - x - 1 = 0$$

egyenletet a Fibonacci-sorozat definiáló, vagy karakterisztikus egyenletének nevezzük. Az egyenlet gyökei

$$\alpha = \frac{1+\sqrt{5}}{2} \quad \text{és} \quad \beta = \frac{1-\sqrt{5}}{2},$$

melyekre nyilván $\alpha + \beta = 1$, $\alpha\beta = -1$ és $\alpha - \beta = \sqrt{5}$. Ezen gyökök segítségével a sorozattagokra explicit képlet is adható.

10.2. Tétel. (Binet-formula) *Minden n természetes szám esetén*

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \frac{\alpha^n - \beta^n}{\sqrt{5}}. \tag{10.1}$$

Bizonyítás. Mivel

$$\frac{\alpha^0 - \beta^0}{\sqrt{5}} = 0 = F_0 \quad \text{és} \quad \frac{\alpha - \beta}{\sqrt{5}} = \frac{\sqrt{5}}{\sqrt{5}} = 1 = F_1,$$

ezért az állítás igaz, ha $n = 0$ vagy 1. Tegyük fel, hogy $n \geq 1$, és a tétel igaz n és $n-1$ esetén. Ekkor

$$F_{n+1} = F_n + F_{n-1} = \frac{\alpha^n - \beta^n}{\sqrt{5}} + \frac{\alpha^{n-1} - \beta^{n-1}}{\sqrt{5}} = \\ = \frac{\alpha^{n-1}(\alpha+1) - \beta^{n-1}(\beta+1)}{\sqrt{5}}.$$

Mivel α a karakterisztikus egyenlet gyöke, és így $\alpha + 1 = \alpha^2$, és hasonlóan $\beta + 1 = \beta^2$, ezért

$$F_{n+1} = \frac{\alpha^{n-1}\alpha^2 - \beta^{n-1}\beta^2}{\sqrt{5}} = \frac{\alpha^{n+1} - \beta^{n+1}}{\sqrt{5}}.$$

Tehát az állítás $n+1$ esetén is igaz, ami a teljes indukciós gondolatmenet alapján bizonyítja a tételt. ∎

A továbbiakban szükségünk lesz egy összefüggésre.

10.3. Tétel. *Minden n, m pozitív egész esetén*

$$F_{n+m} = F_{n-1}F_m + F_nF_{m+1}.$$

Bizonyítás. m-re teljes indukcióval bizonyítunk. Ha $m = 1$, akkor $F_1 = F_2 = 1$ miatt

$$F_{n-1}F_1 + F_nF_2 = F_{n-1} + F_n = F_{n+1},$$

ha pedig $m = 2$, akkor

$$\begin{aligned} F_{n-1}F_2 + F_nF_3 &= F_{n-1} + 2F_n = \\ &= F_{n-1} + F_n + F_n = F_{n+1} + F_n = F_{n+2}. \end{aligned}$$

Tehát az állítás igaz, ha $m = 1$ vagy 2. Tegyük fel, hogy $m > 2$ és az állítás igaz $m - 1$ és $m - 2$ esetén. Ekkor

$$\begin{aligned} F_{n+m} &= F_{n+(m-1)} + F_{n+(m-2)} = \\ &= (F_{n-1}F_{m-1} + F_nF_m) + (F_{n-1}F_{m-2} + F_nF_{m-1}) = \\ &= F_{n-1}(F_{m-1} + F_{m-2}) + F_n(F_m + F_{m-1}) = \\ &= F_{n-1}F_m + F_nF_{m+1}, \end{aligned}$$

amiből következik a tétel minden pozitív egész m-re. ∎

Két szomszédos Fibonacci-szám nyilván relatív prím. Hiszen ha $n > 1$ és $(F_n, F_{n+1}) = d$, akkor a rekurzív definícióból adódó $F_{n-1} = F_{n+1} - F_n$ miatt $d \mid F_{n-1}$ következik. De ha $d \mid F_n$ és $d \mid F_{n-1}$ akkor az előzőekhez hasonlóan $d \mid F_{n-2}$ adódik. Folytatva az eljárást, végül azt kapjuk, hogy $d \mid F_1 = 1$, tehát valóban $d = 1$. Két nem szomszédos Fibonacci-szám már nem mindig relatív prím, ezt mutatja a következő tétel.

10.4. Tétel. *Ha m és n pozitív egész számok és $m \mid n$, akkor $F_m \mid F_n$.*

Bizonyítás. Legyen $n = m \cdot m_1$, ahol $m_1 \geq 1$. Ha $m_1 = 1$, akkor az állítás triviálisan igaz. Tegyük fel, hogy a tétel igaz valamely pozitív egész m_1-re, vagyis $F_m \mid F_{mm_1}$. Ekkor a 10.3. Tételből adódó

$$F_{m(m_1+1)} = F_{mm_1+m} = F_{mm_1-1}F_m + F_{mm_1}F_{m+1}$$

egyenlőségből $F_m \mid F_{m(m_1+1)}$ következik, vagyis a tétel $m_1 + 1$-re is igaz. Tehát, teljes indukciós gondolatmenettel, igaz a tétel minden m_1-re, azaz minden m-mel osztható n-re. ∎

Az előző tételünk egy erősebb formában is igaz.

10.5. Tétel. *Minden m, n pozitív egész esetén*

$$(F_m, F_n) = F_{(m,n)}.$$

Bizonyítás. Feltehetjük, hogy $m < n$ és $m \nmid n$, mert egyébként az állítás következik a 10.4. Tételből. Végezzük el az euklideszi algoritmust az m, n számokon:

$$\begin{aligned}
n &= mq_0 + r_1, \quad \text{ahol} \quad 0 < r_1 < m,\\
m &= r_1q_1 + r_2, \quad \text{ahol} \quad 0 < r_2 < r_1,\\
r_1 &= r_2q_2 + r_3, \quad \text{ahol} \quad 0 < r_3 < r_2,\\
&\vdots\\
r_{t-2} &= r_{t-1}q_{t-1} + r_t, \quad \text{ahol} \quad 0 < r_t < r_{t-1},\\
r_{t-1} &= r_tq_t,
\end{aligned}$$

ahol q_0, q_i és r_i pozitív egészek minden $1 \le i \le t$ esetén. A 10.3. Tétel alapján

$$F_n = F_{mq_0+r_1} = F_{mq_0-1}F_{r_1} + F_{mq_0}F_{r_1+1}$$

adódik. Az F_{mq_0-1} és F_{mq_0} Fibonacci-számok szomszédosak, tehát relatív prímek, ezért egyenlőségünkből a 10.4. Tétel és a legnagyobb közös osztó tulajdonságai alapján $(F_m, F_n) \mid (F_{r_1}, F_m)$ és $(F_{r_1}, F_m) \mid (F_m, F_n)$ és így $(F_m, F_n) = (F_{r_1}, F_m)$. Folytatva az eljárást, az utolsó lépésben $r_t \mid r_{t-1}$ felhasználásával

$$(F_m, F_n) = (F_{r_1}, F_m) = (F_{r_2}, F_{r_1}) = \cdots = (F_{r_t}, F_{r_{t-1}}) = F_{r_t}$$

következik. Az euklideszi algoritmus ismert tulajdonsága alapján azonban $r_t = (m, n)$. ∎

Megjegyezzük, hogy a 10.4., illetve a 10.5. Tételbeli tulajdonságokkal rendelkező egész számsorozatokat oszthatósági, illetve erős oszthatósági sorozatoknak nevezzük.

A Fibonacci-számok oszthatósági tulajdonságait vizsgálva felmerül a kérdés, hogy melyek azok a pozitív egészek, amelyek osztói valamely F_0-tól különböző Fibonacci-számnak.

10.6. Tétel. *Minden pozitív egész m esetén az első m^2 Fibonacci-szám között van pozitív indexű m-mel osztható.*

Bizonyítás. Feltehetjük, hogy $m > 2$, hiszen egyébként az állítás nyilvánvaló. Jelöljük $\overline{F}_i$-vel az F_i Fibonacci-szám m-mel való osztásánál fellépő legkisebb nemnegatív maradékát. Tehát $F_i \equiv \overline{F}_i \pmod{m}$, ahol $0 \leq \overline{F}_i < m$. Tekintsük a szomszédos maradékpárok

$$\langle \overline{F}_1, \overline{F}_2 \rangle, \langle \overline{F}_2, \overline{F}_3 \rangle, \langle \overline{F}_3, \overline{F}_4 \rangle, \ldots$$

végtelen sorozatát. Mivel m különböző $\overline{F}_i$ érték fordulhat elő, ezért a különböző maradékpárok száma legfeljebb m^2. Ebből a skatulya elv alapján az következik, hogy az első $m^2 + 1$ pár között van két megegyező, vagyis

$$\langle \overline{F}_k, \overline{F}_{k+1} \rangle = \langle \overline{F}_t, \overline{F}_{t+1} \rangle$$

valamely k, t pozitív egészekkel melyekre $1 \leq k < t \leq m^2 + 1$. De ekkor

$$\begin{aligned} \overline{F}_{k-1} \equiv F_{k-1} = F_{k+1} - F_k \equiv \overline{F}_{k+1} - \overline{F}_k = \overline{F}_{t+1} - \overline{F}_t \equiv \\ \equiv F_{t+1} - F_t = F_{t-1} \equiv \overline{F}_{t-1} \pmod{m}, \end{aligned}$$

amiből $\overline{F}_{k-1} = \overline{F}_{t-1}$ következik. Így ha a k-adik és a t-edik számpárok egyenlőek, akkor a $k-1$-edik és $t-1$-edik párok is. Folytatva az eljárást azt kapjuk, hogy már az első számpár megegyezik egy másikkal. Feltehetjük tehát, hogy $k = 1$, azaz

$$\langle 1, 1 \rangle = \langle \overline{F}_t, \overline{F}_{t+1} \rangle,$$

ahol $2 \leq t \leq m^2 + 1$. Ebből következik, hogy

$$F_{t-1} = F_{t+1} - F_t \equiv \overline{F}_{t+1} - \overline{F}_t = 1 - 1 = 0 \pmod{m},$$

vagyis $m \mid F_{t-1}$, ahol $1 \leq t - 1 \leq m^2$. ∎

A tételünkből az is következik, hogy végtelen sok m-mel osztható Fibonacci-szám létezik. Hiszen ha $m \mid F_n$, akkor a 10.4. Tétel miatt minden n-nel osztható indexű sorozattag osztható m-mel. Az első m-mel osztható sorozattag indexére adott m^2 felső korlátnál lényegesen jobb is adható. Például egy későbbi tételből (10.8. Tétel) következik, hogy ha p egy prímszám, akkor az első p-vel osztható nemzérus sorozattag indexe nem nagyobb mint $p + 1$.

Általános másodrendű sorozatok

A Fibonacci-sorozat a következőképpen általánosítható.

Definíció. Legyenek A és B zérustól különböző egészek. Az egész számok G_n $(n = 0, 1, 2, \ldots)$ végtelen sorozatát A, B paraméterekkel és G_0, G_1 nem mindkettő zérus kezdőelemekkel megadott másodrendű lineáris rekurzív sorozatnak nevezzük, ha

$$G_n = AG_{n-1} + BG_{n-2}$$

minden $n > 1$ esetén.

A sorozat $A = B = 1$, $G_0 = 0$, $G_1 = 1$ speciális esete a Fibonacci-sorozat. Az általános sorozat tagjai, a Fibonacci-számokhoz hasonlóan, megadhatók explicit alakban is.

Tekintsük az

$$x^2 - Ax - B = 0$$

egyenletet, melyet a sorozat karakterisztikus egyenletének nevezzük. Az egyenlet gyökei

$$\gamma = \frac{A + \sqrt{A^2 + 4B}}{2} \quad \text{és} \quad \delta = \frac{A - \sqrt{A^2 + 4B}}{2},$$

melyekre nyilván $\gamma+\delta = A$, $\gamma\delta = -B$, és ha $D = A^2+4B$, akkor $\gamma-\delta = \sqrt{D}$.

10.7. Tétel. *Ha $D \neq 0$ (és így $\gamma \neq \delta$), akkor*

$$G_n = \frac{(G_1 - \delta G_0)\gamma^n - (G_1 - \gamma G_0)\delta^n}{\gamma - \delta} \tag{10.2}$$

minden $n \geq 0$ esetén.

Bizonyítás. A tétel a 10.2. Tétel bizonyításához hasonlóan teljes indukcióval is belátható, azonban most egy másik bizonyítást mutatunk be. Legyen k egy tetszőleges valós vagy komplex szám. A sorozat definíciója alapján, feltéve, hogy $n > 0$,

$$\begin{aligned} G_{n+1} - kG_n &= AG_n + BG_{n-1} - kG_n = \\ &= (A - k)(G_n - kG_{n-1}) - (k^2 - Ak - B)G_{n-1}. \end{aligned}$$

Ha $k = \gamma$ vagy δ, akkor $k^2 - Ak - B = 0$, ezért $\gamma + \delta = A$ felhasználásával és $k = \gamma$ helyettesítéssel

$$G_{n+1} - \gamma G_n = \delta(G_n - \gamma G_{n-1})$$

adódik. Ha $n-1>0$, akkor a jobb oldalon újra felhasználhatjuk a kapott egyenlőséget $n+1$ helyett n-nel. Folytatva ezt az eljárást, végül

$$G_{n+1}-\gamma G_n=\delta^n(G_1-G_0)$$

következik. $k=\delta$ helyettesítésével hasonlóan adódik, hogy

$$G_{n+1}-\delta G_n=\gamma^n(G_1-\delta G_0).$$

Az utóbbi két egyenlőség különbségéből (10.2) már következik minden $n>0$ esetén. Az $n=0$ esetben az állítás közvetlenül belátható. ∎

Bizonyítás nélkül megemlítjük, hogy a $D=0$ (azaz $\delta=\gamma$) esetben

$$G_n=(nG_1-(n-1)\gamma G_0)\gamma^{n-1}$$

minden $n\geq 0$-ra, de ezzel az esettel a továbbiakban nem foglalkozunk.

Az általános másodrendű sorozat fontos speciális esete a 0 és 1 kezdőtagú sorozat, ezt a következőkben R-rel fogjuk jelölni. Tehát R_n ($n=0$, $1,2,\ldots$) egy olyan másodrendű lineáris rekurzív sorozat, melynek elemei kielégítik az

$$R_n=AR_{n-1}+BR_{n-2}\quad (n>1) \tag{10.3}$$

rekurziót, ahol A és B nem zérus egészek, a kezdőelemek pedig $R_0=0$ és $R_1=1$. Ezen sorozat tagjai (10.2) alapján

$$R_n=\frac{\gamma^n-\delta^n}{\gamma-\delta}=\frac{\gamma^n-\delta^n}{\sqrt{D}} \tag{10.4}$$

alakúak.

Az R sorozat a Fibonacci-sorozathoz hasonló tulajdonságokkal rendelkezik. Minden n,m pozitív egész szám esetén

$$R_{n+m}=BR_{n-1}R_m+R_nR_{m+1}, \tag{10.5}$$

mely a 10.3. Tételhez hasonlóan bizonyítható. Ennek felhasználásával belátható a 10.4. és 10.5. Tétel megfelelője, miszerint ha $(A,B)=1$, akkor

$$R_m \mid R_n \tag{10.6}$$

akkor és csak akkor, ha $m \mid n$, továbbá

$$(R_m,R_n)=R_{(m,n)}. \tag{10.7}$$

A 10.6. Tétel megfelelője is igazolható, bizonyos kikötéseket róva m-re, de helyette pontosabb tételeket fogunk bizonyítani.

Az R sorozat oszthatósági tulajdonságait vizsgálva érdemes kikötni, hogy $(A, B) = 1$, ugyanis (10.3) miatt $(A, B) = d > 1$ esetén minden 1-nél nagyobb indexű tag osztható d-vel. Ez nem nehezítené, de bonyolítaná az általános tételek megfogalmazását. Az $m \mid R_n$ típusú oszthatóságok feltételeit keresve mindig kikötjük, hogy $(m, B) = 1$. Ennek indoka a következő. Legyen p egy prímszám, melyre $p \mid B$, de $(A, B) = 1$ miatt $p \nmid A$. Ekkor nyilván $p \nmid R_1 = 1$ és $p \nmid R_2 = A$. De ha $p \nmid R_{n-1}$ és $p \nmid R_{n-2}$ akkor (10.3) miatt $p \nmid R_n$. Ezekből következik, hogy ha $(A, B) = 1$ és $p \mid B$, akkor nincs a sorozatnak p-vel osztható tagja, így $m \nmid R_n$ minden $n > 0$ indexű tagra, ha $(m, B) > 1$.

Először a sorozattagok prímszámokkal való oszthatóságát vizsgáljuk.

10.8. Tétel. *Ha $(A, B) = 1$, p egy prímszám és $p \nmid B$, akkor*

$$p \mid R_{p-(D/p)},$$

ahol $D = A^2 + 4B$, (D/p) a Legendre-szimbólum, ha p páratlan és $p \nmid D$; $(D/p) = 0$, ha $p \mid D$; továbbá $(D/p) = -1$, ha $p = 2$ és A páratlan.

Bizonyítás. Legyen p egy páratlan prím $p \nmid B$ feltétellel. (10.4) alapján, felhasználva a binomiális tételt,

$$\begin{aligned}
R_p &= \frac{1}{\sqrt{D}}\left[\left(\frac{A+\sqrt{D}}{2}\right)^p - \left(\frac{A-\sqrt{D}}{2}\right)^p\right] = \\
&= \frac{1}{2^p\sqrt{D}}\left[\binom{p}{0}A^p + \binom{p}{1}A^{p-1}\sqrt{D} + \cdots + \binom{p}{p}\sqrt{D}^p - \right. \\
&\qquad \left. - \binom{p}{0}A^p + \binom{p}{1}A^{p-1}\sqrt{D} - \cdots + \binom{p}{p}\sqrt{D}^p\right] = \\
&= \frac{1}{2^p\sqrt{D}}\left[2\binom{p}{1}A^{p-1}\sqrt{D} + 2\binom{p}{3}A^{p-3}\sqrt{D}^3 + \cdots + 2\binom{p}{p}\sqrt{D}^p\right] = \\
&= \frac{1}{2^{p-1}}\left[\binom{p}{1}A^{p-1} + \binom{p}{3}A^{p-3}D + \cdots + D^{\frac{p-1}{2}}\right].
\end{aligned}$$

Ebből, felhasználva a kis Fermat-tételt és a binomiális együtthatók ismert tulajdonságát, miszerint $p \mid \binom{p}{k}$ ha $0 < k < p$,

$$R_p \equiv 2^{p-1}R_p \equiv D^{\frac{p-1}{2}} \pmod{p} \tag{10.8}$$

következik. Hasonlóan adódik, hogy

$$R_{p+1} = \frac{1}{2^p}\left[\binom{p+1}{1}A^p + \binom{p+1}{3}A^{p-2}D + \cdots + \binom{p+1}{p}AD^{\frac{p-1}{2}}\right].$$

De $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$, ha $0 < k \le n$, ezért

$$2^p R_{p+1} = \left[\binom{p}{0} + \binom{p}{1}\right]A^p + \left[\binom{p}{2} + \binom{p}{3}\right]A^{p-2}D + \cdots + \\ + \left[\binom{p}{p-1} + \binom{p}{p}\right]AD^{\frac{p-1}{2}},$$

amiből, ismét a kis Fermat-tétel és az említett $p \mid \binom{p}{k}$ oszthatóság alapján

$$2R_{p+1} \equiv A^p + AD^{\frac{p-1}{2}} \equiv A + AD^{\frac{p-1}{2}} = A(1 + D^{\frac{p-1}{2}}) \pmod{p}. \tag{10.9}$$

Ezek után ha $p \mid D$, akkor (10.8) miatt $R_p \equiv 0 \pmod{p}$, vagyis $p \mid R_p$, illetve $p \mid R_{p-(D/p)}$, mert most $(D/p) = 0$ a definíció miatt.

Ha $(D/p) = -1$, vagyis $D^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, akkor (10.9)-ből

$$2R_{p+1} \equiv 0 \pmod{p}, \quad \text{azaz} \quad p \mid R_{p+1} = R_{p-(D/p)}$$

következik.

Ha pedig $(D/p) = 1$, azaz $D^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, akkor az $R_{p+1} = AR_p + BR_{p-1}$ egyenlőségből és a (10.8), (10.9) kongruenciákból

$$2BR_{p-1} = 2R_{p+1} - 2AR_p \equiv 2A - 2A = 0 \pmod{p},$$

illetve $(p, 2B) = 1$ miatt $R_{p-1} \equiv 0 \pmod{p}$ adódik. Tehát ebben az esetben $p \mid R_{p-1} = R_{p-(D/p)}$.

Legyen most $p = 2$. A sorozat rekurzív definíciója alapján a sorozattagok $R_0 = 0$, $R_1 = 1$, $R_2 = A$, $R_3 = A^2 + B, \ldots$ Ha $2 \mid D = A^2 + 4B$, akkor A páros és $2 \mid R_2 = A$. Ha pedig $2 \nmid D$, akkor A páratlan és $2 \nmid B$ miatt B is páratlan, így $2 \mid R_3 = A^2 + B$. Tehát, (D/p) definíciója miatt a tétel $p = 2$ esetén is igaz.

Ezzel a tétel minden állítását bebizonyítottuk. ∎

A következő tétel a prímhatványokkal osztható sorozattagok meghatározását teszi lehetővé.

10.9. Tétel. *Ha p egy prímszám, $p \nmid B$ és $p^s \mid R_n$ valamely s, n pozitív egészek esetén, akkor*

$$p^{s+1} \mid R_{np}.$$

Bizonyítás. Legyen először p egy páratlan prímszám. Ekkor $\sqrt{D}^{p-1}R_n$ egész szám minden $n > 0$ természetes szám mellett. (10.4) alapján, felhasználva hogy $\gamma\delta = -B$ és $\binom{p}{k} = \binom{p}{p-k}$,

$$\begin{aligned}
&\sqrt{D}^{p-1}R_n^p = \frac{1}{\sqrt{D}}(\gamma^n - \delta^n)^p = \\
&= \frac{1}{\sqrt{D}}\left[\gamma^{np} - \delta^{np} + \sum_{k=1}^{p-1}(-1)^k\binom{p}{k}\gamma^{n(p-k)}\delta^{nk}\right] = \\
&= \frac{1}{\sqrt{D}}\left[\gamma^{np} - \delta^{np} + \sum_{k=1}^{\frac{p-1}{2}}(-1)^k\binom{p}{k}(\gamma\delta)^{nk}\left(\gamma^{n(p-2k)} - \delta^{n(p-2k)}\right)\right] = \\
&= R_{np} + \sum_{k=1}^{\frac{p-1}{2}}(-1)^k(-B)^{nk}\binom{p}{k}R_{n(p-2k)} = R_{np} + S.
\end{aligned}$$

Tegyük fel, hogy $p^s \mid R_n$. Ekkor nyilván $p^{s+1} \mid R_n^p$. De az S összegben $p \mid \binom{p}{k}$ és (10.6)-ból adódó $R_n \mid R_{n(p-2k)}$ miatt minden tag osztható p^{s+1}-gyel, ezért $p^{s+1} \mid R_{np}$ is igaz.

Legyen most $p = 2$. (10.5) alapján

$$\begin{aligned}
R_{2n} = R_{n+n} &= BR_{n-1}R_n + R_nR_{n+1} = \\
&= R_n(BR_{n-1} + R_{n+1}).
\end{aligned}$$

Ha $2^s \mid R_n$, és így R_n páros, akkor (10.7) miatt R_{n-1} és R_{n+1} páratlan. De a $p \nmid B$ feltétel miatt B is páratlan, ezért $2 \mid (BR_{n-1} + R_{n+1})$ és így $2^{s+1} \mid R_{2n}$. Tehát a tétel $p = 2$ esetén is igaz. ∎

Az előző két tételből adódik, hogy $(m, B) = 1$ feltétel mellett végtelen sok m-mel osztható tagja van a sorozatunknak.

10.10. Tétel. *Legyen az $m > 1$ pozitív egész szám kanonikus alakja*

$$m = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_t^{\alpha_t}$$

és legyen

$$n = \prod_{i=1}^{t} p_i^{\alpha_i - 1}(p_i - (D/p_i)),$$

ahol (D/p_i) a 10.8. Tételben definiált szimbólum. Ha $(m, B) = 1$, akkor

$$m \mid R_{nk}$$

minden k természetes szám esetén.

Bizonyítás. (10.6) miatt elég azt bizonyítani, hogy $m \mid R_n$. Ehhez pedig, szintén (10.6) miatt, elég a $p_i^{\alpha_i} \mid R_{p_i^{\alpha_i-1}(p_i-(D/p_i))}$ oszthatóságot belátni, ami viszont következik a 10.8. és 10.9. Tételből. ∎

Megemlítjük, hogy a sorozatokban nem mindig a $p-(D/p)$ indexű tag az első p-vel osztható. Legyen $r(p)$ a legkisebb pozitív egész, melyre $p \mid R_{r(p)}$ (vagyis $p \mid R_{r(p)}$, de $p \nmid R_n$, ha $0 < n < r(p)$). (10.7)-ből következik, hogy $r(p) \mid (p-(D/p))$. Bebizonyítható, hogy a $(p-(D/p))/r(p)$ hányados tetszőlegesen nagy is lehet.

Eddig még nem ismert, hogy egy sorozat esetén melyek azok a p prímszámok, melyek esetén az első p-vel osztható tag p^2-tel is osztható? Vagy ami ezzel egyenértékű, melyek azok a prímek, melyekre $p^2 \mid R_{p-(D/p)}$? Az $A=3$, $B=-2$ paraméterekkel megadott R sorozat (vagyis a Mersenne-számok $R_n = 2^n - 1$ sorozata) esetén eddig csak két ilyen prímszámot találtak, ezek $p=1093$ és $p=3511$, a Fibonacci-sorozat esetében pedig egyet sem.

A Fibonacci-sorozatra a 10.8. Tétel a következőket mondja ki. Mivel $A=B=1$ miatt most $D=A^2+4B=5$, ezért $(5/p)=0$ akkor és csak akkor, ha $p=5$. Így valóban $5 \mid F_5 = 5$. $p=2$ esetén a tételbeli definíció szerint $(5/2)=-1$ és $2 \mid F_3 = 2$. Ha p páratlan prím, $p \neq 5$ és p alakja $10k \pm 1$, akkor a kvadratikus reciprocitási tétel alapján

$$(5/p) = \left(\frac{5}{p}\right) = \left(\frac{5}{10k\pm 1}\right) = \left(\frac{10k\pm 1}{5}\right) = \left(\frac{\pm 1}{5}\right) = 1.$$

A $p = 10k \pm 3$ alakú prímeknél pedig hasonlóan

$$(5/p) = \left(\frac{\pm 3}{5}\right) = -1$$

adódik. Így a 10.8. Tétel alapján

$$p \mid F_{p-1}, \quad \text{ha} \quad p = 10k \pm 1$$

és

$$p \mid F_{p+1} \quad \text{ha} \quad p = 10k \pm 3.$$

Egy diofantikus egyenlet megoldása

A rekurzív sorozatok jól használhatók diofantikus egyenletek megoldása során is. Mielőtt ezt egy példával szemléltetnénk, definiáljuk a G sorozat egyik speciális esetét.

Definíció. Legyen L_n $(n = 0, 1, 2, \ldots)$ az egész számok azon végtelen sorozata, melynek kezdő elemei $L_0 = 2$, $L_1 = 1$ és

$$L_n = L_{n-1} + L_{n-2},$$

ha $n > 1$. Ezt a sorozatot Lucas-sorozatnak, tagjait pedig Lucas-számoknak nevezzük.

A 10.7. Tétel alapján a Lucas-számok

$$\begin{aligned} L_n &= \frac{(1-2\beta)\alpha^n - (1-2\alpha)\beta^n}{\alpha-\beta} = \\ &= \frac{((\alpha+\beta)-2\beta)\alpha^n - ((\alpha+\beta)-2\alpha)\beta^n}{\alpha-\beta} = \alpha^n + \beta^n \end{aligned} \tag{10.10}$$

alakúak, ahol α és β az $x^2 - x - 1 = 0$ karakterisztikus egyenlet gyökei. A Fibonacci- és a Lucas-számokra fennáll az

$$L_n^2 - 5F_n^2 = 4 \cdot (-1)^n \tag{10.11}$$

egyenlőség, ugyanis (10.1) és (10.10) miatt, felhasználva, hogy $\alpha\beta = -1$,

$$(\alpha^n + \beta^n)^2 - 5 \cdot \left(\frac{\alpha^n - \beta^n}{\sqrt{5}}\right)^2 = 4(\alpha\beta)^n = 4 \cdot (-1)^n.$$

Ebből következik, hogy az $x^2 - 5y^2 = \pm 4$ Pell-típusú egyenleteknek végtelen sok megoldása van, minden $(x, y) = (L_n, F_n)$ számpár megoldás. Bebizonyítjuk, hogy lényegében ezen számpárok szolgáltatják az összes megoldást.

10.11. Tétel. *Az*

$$x^2 - 5y^2 = \pm 4$$

egyenlet összes nemnegatív megoldása $(x, y) = (L_n, F_n)$, $n = 0, 1, 2, \ldots$, *ahol* L_n, *illetve* F_n *az* n*-edik Lucas-, illetve Fibonacci-szám.*

Bizonyítás. Nyilván elég az egyenlet nemnegatív megoldásait keresni, hiszen ha (x, y) egy megoldás, akkor $(\pm x, \pm y)$ is az. Azt már láttuk, hogy az (L_n, F_n) alakú számpárok megoldásai az egyenletnek, ezért csak azt kell

bizonyítani, hogy minden megoldás ilyen alakú. Tegyük fel az állítással ellentétben, hogy van olyan megoldás, mely nem (L_n, F_n) alakú. Legyen (x_0, y_0) egy olyan megoldás, melyben y_0 minimális és nem Fibonacci-szám. Könnyen ellenőrizhető, hogy ekkor $y_0 > 4$. Mivel

$$x_0 = \sqrt{5y_0^2 \pm 4} = 2y_0\sqrt{\frac{5}{4} \pm \frac{4}{4y_0^2}},$$

ezért $2y_0 < x_0 < 3y_0$, továbbá x_0, y_0 paritása megegyező, így van olyan $0 < t < y_0$, melyre

$$x_0 = y_0 + 2t.$$

Az egyenletünkbe visszahelyettesítve

$$(y_0 + 2t)^2 - 5y_0^2 = \pm 4,$$

azaz

$$4y_0^2 - 4ty_0 - 4t^2 \pm 4 = 0$$

adódik. Ebből

$$2y_0 = t \pm \sqrt{5t^2 \pm 4}. \tag{10.12}$$

De y_0 és t egész számok, ezért $5t^2 \pm 4$ teljes négyzet, vagyis

$$5t^2 \pm 4 = s^2,$$

ahol s nemnegatív egész. Így $(x, y) = (s, t)$ a tételbeli egyenlet egy olyan megoldása, melyre $0 < t < y_0$. Tehát t az y_0-nál kisebb megoldás, ezért a feltételünk miatt $t = F_n$ valamely $n > 0$-ra. Belátjuk, hogy s pedig az n-edik Lucas-szám. Mivel

$$s^2 - 5F_n^2 = \pm 4$$

és (10.11) következtében

$$L_n^2 - 5F_n^2 = \pm 4,$$

ezért

$$s^2 - L_n^2 = 0 \quad \text{vagy} \quad \pm 8.$$

Két négyzetszám különbsége csak akkor lehet 8, ha az egyik 9 a másik pedig 1, vagyis ha $s \leq 3$. Könnyű ellenőrizni, hogy ekkor a megoldásokat csak az (L_n, F_n) alakú párok adják, így valóban $s = L_n$. Tehát (10.12) alapján

$$2y_0 = t \pm s = F_n \pm L_n.$$

De (10.1) és (10.10) segítségével belátható, hogy $F_n < L_n$ és $F_n + L_n = 2F_{n+1}$, ha $n > 1$, ezért

$$2y_0 = F_n + L_n = 2F_{n+1},$$

vagyis y_0 csak Fibonacci-szám lehet, x_0 pedig, mint előbb is láttuk, a hozzá tartozó Lucas-szám. Ez ellentmond a feltevésünknek, tehát minden megoldás $(x, y) = (L_n, F_n)$ alakú. ∎

Feladatok

1. Egy $2 \times n$-es ($n \geq 1$) téglalapot hányféleképpen tudunk lefedni 1×2-es téglalapokkal?

2. Határozzuk meg az első n Fibonacci-szám összegét.

3. Határozzuk meg az első n Fibonacci-szám négyzetének összegét

4. Legyen F_i, illetve L_i az i-edik Fibonacci-, illetve Lucas-szám. Bizonyítsuk be az alábbi azonosságokat:

(a) $F_{n+1}^2 = F_n F_{n+2} + (-1)^n$,

(b) $nF_1 + (n-1)F_2 + (n-2)F_3 + \cdots + 2F_{n-1} + F_n = F_{n+4} - (n+3)$,

(c) $L_{n+1} = 5F_n - L_{n-1}$,

(d) $L_{2n} = 5F_n^2 + 4(-1)^n$.

5. Legyenek a és b pozitív egész számok és jelölje F_i az i-edik Fibonacci-számot. Bizonyítsuk be, hogy ha $F_{n-1} \leq b < F_n$, akkor az a és b egészeken végrehajtott euklideszi algoritmus hosssza legfeljebb $2n$.

6. Az előző feladat segítségével bizonyítsuk be, hogy az $a, b \geq 2$ egész számokon végrehajtott euklideszi algoritmus hossza legfeljebb $c \log b$, ahol $c > 0$ egy a és b-től nem függő konstans.

7. Legyen R_n ($n = 0, 1, 2, \ldots$) egy $R_0 = 0$, $R_1 = 1$ kezdőelemekkel és az $R_{n+1} = AR_n + BR_{n-1}$ rekurzióval definiált sorozat, ahol A, B zérustól különböző konstansok. Bizonyítsuk be, hogy

$$R_{3n} = DR_n^3 + 3(-B)^n R_n,$$

ahol $D = A^2 + 4B$.

8. Legyen R_n az előző feladatban definiált sorozat. Bizonyítsuk be, hogy ha $D > 0$ és α az $x^2 - Ax - B = 0$ egyenlet nagyobb abszolút értékű gyöke, akkor

$$\lim_{n\to\infty} \frac{R_{n+1}}{R_n} = \alpha.$$

9. Bizonyítsuk be, hogy az előző feladat feltételei mellett

$$\left|\alpha - \frac{R_{n+1}}{R_n}\right| < \frac{1}{cR_n^2}$$

akkor és csak akkor teljesül végtelen sok n esetén, ha $|B| = 1$ és $c \leq \sqrt{D}$.

Irodalom

[1] Erdős Pál—Surányi János: *Válogatott fejezetek a számelméletből.* Tankönyvkiadó, Budapest, 1960.

[2] Gyarmati Edit—Turán Pál: *Számelmélet.* Nemzeti Tankönyvkiadó, Budapest, 1994.

[3] Hua Loo Keng: *Introductiun to Number Theory.* Springer-Verlag, Berlin 1982.

[4] J. Niven—H. S. Zuckerman: *Bevezetés a számelméletbe.* Műszaki Kiadó, Budapest, 1978.

[5] Sárközi András: *Számelmélet.* Műszaki Kiadó, Budapest, 1976.

[6] Sárközi András—Surányi János: *Számelmélet feladatgyűjtemény.* Tankönyvkiadó, Budapest, 1985.

[7] Szendrei János: *Algebra és számelmélet.* Nemzeti Tankönyvkiadó, Budapest, 1996.

[8] Szendrei János: *Matematikai feladatgyűjtemény I.* Tankönyvkiadó, Budapest, 1990.