

BEVEZETÉS AZ ALGEBRÁBA ÉS A SZÁMELMÉLETBE I.

Dr. TÓTH LÁSZLÓ egyetemi docens

Pécsi Tudományegyetem, 2007

Bevezetés

Ez az anyag tartalmazza a „Bevezetés az algebra és a számelméletbe I.” tárgy kötelező elméleti anyagának a nagy részét. Tartalmaz továbbá olyan kiegészítő részeket is, amelyek nem kötelezőek, ezek „★ ★” jelek között szerepelnek. Az anyagban feladatok is vannak, amelyek egy része a gyakorlaton feldolgozásra kerül. A feladatok előtt ▼ jel áll.

A tételek, állítások és bizonyítások végét a □ jel mutatja.

Felhívom a figyelmet

- a definíciók pontos ismeretére (a fogalmak nevei **kövér betűkkel** szedettek),
- az egyes fogalmakra adott példákra (ezek általában • jel után szerepelnek); adjanak, keressenek további példákat az anyag jobb megértése érdekében,
- a Tételek pontos megfogalmazására és a bizonyításokra,
- a feladatok megoldására.

További irodalom

1. Szendrei János, Algebra és számelmélet, Nemzeti Tankönyvkiadó, Budapest, 1996.
2. Szendrei Ágnes, Diszkrét matematika, Polygon, Szeged, 2000.
3. Freud R., Gyarmati E., Számelmélet, Nemzeti Tankönyvkiadó, Budapest, 2000.
4. Megyesi L., Bevezetés a számelméletbe, Polygon, Szeged, 1997.
5. Erdős P., Surányi J., Válogatott fejezetek a számelméletből, Polygon, Szeged, 1996.
6. I. Niven, H. S. Zuckerman, Bevezetés a számelméletbe, Műszaki Könyvkiadó, Budapest, 1978.
7. Sárközy A., Számelmélet – példatár, Műszaki Könyvkiadó, Budapest, 1976.
8. Sárközy A., Surányi J., Számelmélet – feladatgyűjtemény, Tankönyvkiadó, Budapest, 1979.
9. P. Bundschuh, Einführung in die Zahlentheorie, Springer Verlag, Berlin Heidelberg New York, 1996.
10. G. H. Hardy, E. M. Wright, An Introduction to the Theory of Numbers, Clarendon Press, Oxford, Fifth Edition, 1979.

1. Halmazok, relációk, függvények

1.1. Halmazok

A **halmaz** bizonyos jól meghatározott dolgok (tárgyak, fogalmak), a halmaz **elemei**-nek az összessége. Azt, hogy az a elem **hozzátartozik** az A halmazhoz így jelöljük: $a \in A$ (a eleme A -nak); $b \notin A$ jelentése: b nem eleme A -nak.

Egy halmazt egyértelműen meghatároznak az elemei. Egy halmazt megadhatunk úgy, hogy felsoroljuk az elemeit, pl. $A = \{1, 2, 3, 4\}$, $B = \{x, y, z\}$ vagy úgy, hogy megadunk egy, a halmaz x elemeire jellemző $T(x)$ tulajdonságot: $A = \{x | T(x)\} = \{x : T(x)\}$, pl. $A = \{x | x \in \mathbb{R} \text{ és } 0 \leq x \leq 3\}$.

Itt és a továbbiakban a számhalmazokra az alábbi jelöléseket használjuk:

$\mathbb{N} = \{0, 1, 2, 3, \dots\}$ a természetes számok halmaza, $\mathbb{N}^* = \{1, 2, 3, \dots\} = \mathbb{N} \setminus \{0\}$ a nullától különböző természetes számok halmaza, $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ az egész számok halmaza, $\mathbb{Q} = \{\frac{a}{b} | a, b \in \mathbb{Z}, b \neq 0\}$ a racionális számok halmaza, $\mathbb{R}$ a valós számok halmaza, $\mathbb{C}$ a komplex számok halmaza. Továbbá $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$, $2\mathbb{Z}$ a páros egészek halmaza, $2\mathbb{Z} + 1$ a páratlan egészek halmaza.

Az üres halmaz (egyetlen eleme sincs) jele: $\emptyset$. Az A és B halmazokat egyenlőknek nevezzük, ha ugyanazok az elemei, azaz $\forall x : x \in A \Leftrightarrow x \in B$, jel. $A = B$.

Az A halmaz **részhalmaza** a B halmaznak, ha A minden eleme B -nek is eleme, azaz $\forall x : x \in A \Rightarrow x \in B$, jel. $A \subseteq B$.

Jegyezzük meg, hogy $A = B$ akkor és csak akkor teljesül, ha $A \subseteq B$ és $B \subseteq A$.

Műveletek halmazokkal. Az A és B halmazok **metszete** a közös elemek összessége: $A \cap B = \{x | x \in A \wedge x \in B\}$. Ha $A \cap B = \emptyset$, akkor azt mondjuk, hogy A és B **diszjunkt** vagy **idegen halmazok**.

Az A és B halmazok **egyesítése** vagy **uniója** azoknak az elemeknek az összessége, melyek hozzátartoznak legalább az egyik halmazhoz: $A \cup B = \{x | x \in A \vee x \in B\}$.

Itt $\vee$ a "logikai vagy" művelet, $\wedge$ pedig a "logikai és" művelet.

Az $A \setminus B$ **különbség**halmaz az A olyan elemeinek a halmaza, melyek nem tartoznak a B -hez: $A \setminus B = \{x | x \in A \wedge x \notin B\}$.

Ha $A \subseteq E$, akkor $E \setminus A$ -t az A halmaz E -re vonatkozó **kiegészítő** vagy **komplement** halmazának nevezzük, jelölés: $\mathbb{C}_E(A)$. Ha E , neve **alaphalmaz**, rögzített, akkor a $\mathbb{C}(A)$ vagy $\overline{A}$ jelöléseket is használjuk.

Tétel. Ha $A, B, C \subseteq E$ tetszőleges halmazok, akkor

- 1) $(A \cap B) \cap C = A \cap (B \cap C)$, $(A \cup B) \cup C = A \cup (B \cup C)$ (asszociativitás),
- 2) $A \cap B = B \cap A$, $A \cup B = B \cup A$ (kommutativitás),
- 3) $A \cap (A \cup B) = A$, $A \cup (A \cap B) = A$ (abszorbcio),
- 4) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (disztributivitas),
- 5) $A \cup \mathbb{C}_E(A) = E$, $A \cap \mathbb{C}_E(A) = \emptyset$,
- 6) $\mathbb{C}(A \cap B) = \mathbb{C}(A) \cup \mathbb{C}(B)$, $\mathbb{C}(A \cup B) = \mathbb{C}(A) \cap \mathbb{C}(B)$ (de Morgan képletek),
- 7) $A \cap A = A$, $A \cup A = A$,
- 8) $\mathbb{C}(\mathbb{C}(A)) = A$, $A \setminus B = A \cap \mathbb{C}(B)$, $\square$

Az A és B halmazok **Descartes-szorzatának** nevezzük az $A \times B = \{(x, y) : x \in A \wedge y \in B\}$ halmazt. Itt (x, y) **rendezett elempárt** jelöl, ahol lényeges az elemek sorrendje: $(x, y) = (z, t)$ akkor és csak akkor, ha $x = z$ és $y = t$.

Ha A és B elemeinek a száma m , illetve n ($m, n \in \mathbb{N}^*$), akkor $A \times B$ elemeinek a száma mn .

Ha $A = B$, akkor jelölés $A \times A = A^2$.

Példa. • $A = \{1, 2, 3\}$, $B = \{a, b\}$ esetén $A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$.

Feladatok. ▼ 1. Milyen A és B halmazokra igaz, hogy $A \setminus B = B \setminus A$?

▼ 2. Ha $A \cap C = \emptyset$, akkor igazoljuk, hogy $A \setminus (B \setminus C) = (A \setminus B) \setminus C$.

▼ 3. Határozzuk meg a következő halmaz elemeit:

$$A = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x^2 - (y + 1)^2 = 12\}.$$

▼ 4. Határozzuk meg a következő halmaz elemeit:

$$B = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x^2 + 2y^2 = 5\}.$$

1.2. Relációk

Legyen A egy tetszőleges halmaz. A $\rho = (A, R)$ párt, ahol $R \subseteq A \times A = A^2$, az A halmazon definiált **bináris reláció**nak, röviden **reláció**nak nevezzük.

Jelölés: $(a, b) \in R \Leftrightarrow a \rho b$, olvasd: a ρ relációban van b -vel. Ellenkező esetben (a nincs ρ relációban b -vel) a jelölés: $(a, b) \notin R \Leftrightarrow a \not\rho b$.

Példák. • 1) Legyen $A = \{a, b, c, d\}$ és $R = \{(a, a), (a, b), (b, c), (c, c)\}$. Itt például $a \rho a$, $a \rho b$ és $c \not\rho d$.

• 2) Egy sík háromszögeinek A halmazában a hasonlósági reláció $A \times A$ -nak azt a részhalmazát határozza meg, amely az egymással hasonló háromszögpárokból áll.

• 3) Az egész számok $\mathbb{Z}$ halmazán értelmezett oszthatósági reláció a következő: $\rho = (\mathbb{Z}, R)$, ahol $R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : a|b\} = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : \exists c \in \mathbb{Z} : b = ac\}$.

Legyen ρ reláció az A halmazon. Ekkor azt mondjuk, hogy

a) ρ **reflexív**, ha minden $x \in A$ esetén $x \rho x$ ($\forall x \in A \Rightarrow x \rho x$), azaz "minden elem relációban van önmagával";

b) ρ **transzitiv**, ha minden $x, y, z \in A$, $x \rho y$ és $y \rho z$ esetén $x \rho z$ ($\forall x, y, z \in A : x \rho y \wedge y \rho z \Rightarrow x \rho z$), azaz "valahányszor, ha egy elem relációban van egy másik elemmel és ez utóbbi elem relációban van egy harmadikkal, akkor az első is relációban van a harmadikkal";

c) ρ **szimmetrikus**, ha minden $x, y \in A$, $x \rho y$ esetén $y \rho x$ ($\forall x, y \in A : x \rho y \Rightarrow y \rho x$), azaz "valahányszor, ha egy elem relációban van egy másik elemmel, akkor ez utóbbi elem is relációban van az első elemmel";

d) ρ **antiszimmetrikus**, ha minden $x, y \in A$, $x \rho y$ és $y \rho x$ esetén $x = y$ ($\forall x, y \in A : x \rho y \wedge y \rho x \Rightarrow x = y$), azaz "valahányszor, ha egy elem relációban van egy másik elemmel és ha ez utóbbi elem is relációban van az elsővel, akkor a két elem egyenlő";

e) ρ **ekvivalenciareláció**, ha ρ reflexív, transzitiv és szimmetrikus.

f) ρ **rendezési reláció**, ha ρ reflexív, transzitiv és antiszimmetrikus. Ekkor (A, ρ) neve **rendezett halmaz**.

Példák. • 1) Az egész számok $\mathbb{Z}$ halmazán az oszthatósági reláció reflexív és transzitiv, de nem szimmetrikus és nem antiszimmetrikus, mert például $3|-3$ és $-3|3$, de $-3 \neq 3$.

• 2) Az $\mathbb{N}^*$ halmazon az oszthatóság rendezési reláció és $(\mathbb{N}^*, |)$ rendezett halmaz.

• 3) A $\mathbb{Z}$ halmazon az $a \equiv b \pmod{n} \Leftrightarrow n|a-b$ kongruencia reláció ekvivalenciareláció.

Ha ρ ekvivalenciareláció az A halmazon, akkor az egymással relációban lévő elemek halmazát **ekvivalenciaosztályoknak** nevezzük.

Példa. • Ha $n = 6$, akkor a $(\text{mod } 6)$ kongruencia relációhoz tartozó ekvivalenciaosztályok: $\widehat{0}, \widehat{1}, \widehat{2}, \widehat{3}, \widehat{4}, \widehat{5}$, ahol $\widehat{k} = \{x \in \mathbb{Z} : x \equiv k \pmod{6}\} = \{\dots, k-12, k-6, k, k+6, k+12, \dots\}$.

★ Legyen A egy nemüres halmaz és legyen $(B_i)_{i \in I}$ az A részhalmazainak egy rendszere (itt I egy ún. indexhalmaz): $B_i \subseteq A$ minden $i \in I$ -re. Azt mondjuk, hogy $(B_i)_{i \in I}$ egy **osztályfelbontása** vagy **osztályozása** A -nak, ha

- a) $B_i \neq \emptyset, \forall i \in I$,
- b) $B_i \cap B_j = \emptyset, \forall i, j \in I, i \neq j$, azaz bármely két különböző részhalmaz diszjunkt,
- c) $A = \cup_{i \in I} B_i$, azaz a $(B_i)_{i \in I}$ -beli részhalmazok uniója az adott A halmaz.

Példa. • Az $A = \{1, 2, 3, 4, 4, 6\}$ halmaznak a $B_1 = \{1, 2\}, B_2 = \{3, 4\}, B_3 = \{5\}, B_4 = \{6\}$ részhalmazok egy osztályfelbontását adják.

Az ekvivalenciarelációk és az osztályfelbontások kölcsönösen meghatározzák egymást. Ha ugyanis adott egy ekvivalenciareláció, akkor gyűjtsük össze az egymással relációban levő elemeket és egy osztályfelbontást kapunk. Ha pedig adott egy osztályfelbontás, akkor képezzük azt a relációt, mely szerint 2 elem relációban van, ha ugyanahhoz az osztályhoz tartoznak. Ez ekvivalenciareláció lesz.

Feladatok. ▼ 1) Legyen $A = \{1, 2, 3, 4\}$.

a) Ha $\rho = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (2, 1), (3, 2), (2, 3), (1, 3), (3, 1)\}$, határozzuk meg a megfelelő osztályfelbontást.

b) Ha adott az $\{1, 2\}, \{3\}, \{4\}$ osztályfelbontás, határozzuk meg a megfelelő ekvivalenciarelációt. ★

▼ 2. Az $\mathbb{N} \times \mathbb{N}$ halmazon a ρ relációt így definiáljuk: $(a, b) \rho (c, d) \Leftrightarrow a + d = b + c$. Igazoljuk, hogy ρ ekvivalenciareláció.

▼ 3. Adjuk meg az összes ekvivalenciarelációt az $A = \{1, 2, 3\}$ halmazon.

1.3. Függvények

Ha A és B adott halmazok az A halmaz minden elemének megfeleltetjük a B halmaz egy és csak egy elemét, akkor azt mondjuk, hogy A -n egy **függvényt** (vagy leképezést) értelmeztünk, amelynek értékei B -hez tartoznak. Jelölés: $f : A \rightarrow B$ vagy $A \xrightarrow{f} B$. Itt A az f **értelmezési halmaza** vagy **értelmezési tartománya**, a B halmaz az f **értékkészlete**.

Példa. • $f : \mathbb{R} \rightarrow \mathbb{R}, f(x) = x^2$, $g : \mathbb{Z} \rightarrow \mathbb{Z}, g(x) = x^2$ és $h : \mathbb{N}^* \rightarrow \mathbb{N}^*, h(n) = \text{"az } n \text{ pozitív osztóinak száma"}$ függvények.

Injektív, szürjektív és bijektív függvények. Legyen $f : A \rightarrow B$ egy függvény. Azt mondjuk, hogy

f **injektív**, ha A különböző elemeinek különböző képelemek felelnek meg, azaz, ha $\forall x_1, x_2 \in A, x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$. Ez egyenértékű a következő állítással: $\forall x_1, x_2 \in A, f(x_1) = f(x_2) \Rightarrow x_1 = x_2$;

f **szürjektív**, ha B -nek minden eleme képelem, azaz, ha $\forall y \in B \exists x \in A : f(x) = y$.

f **bijektív**, ha injektív és szürjektív, azaz, ha $\forall y \in B \exists! x \in A$ (létezik egy és csak egy $x \in A$): $f(x) = y$.

Példák. • Az $f : \mathbb{R} \rightarrow \mathbb{R}, f(x) = x^2$ függvény nem injektív, mert pl. $-1 \neq 1$ és $f(-1) = f(1) = 1$ és nem is szürjektív, mert pl. $y = -1 \in \mathbb{R}$ esetén nem létezik $x \in \mathbb{R}$ úgy, hogy $f(x) = x^2 = -1$ legyen.

• A $g : [0, \infty) \rightarrow \mathbb{R}, g(x) = x^2$ függvény injektív és nem szürjektív, $h : [0, \infty) \rightarrow [0, \infty), h(x) = x^2$ pedig injektív és szürjektív, tehát bijektív.

Feladatok. ▼ 1. Határozzuk meg mindazokat az $f : \mathbb{R} \rightarrow \mathbb{R}$ függvényeket, amelyekre $2f(x) + 3f(1-x) = 4x - 1, \forall x \in \mathbb{R}$.

Megoldás. x helyett $(1-x)$ -et írva: $3f(x) + 2f(1-x) = -4x + 3$, az eredetivel együtt ez egy egyenletrendszer. Kapjuk, hogy: $f(x) = -4x + 11/5$.

▼ 2. Határozzuk meg mindazokat az $f : \mathbb{R} \rightarrow \mathbb{R}$ függvényeket, amelyekre $f(x) - f(-x) = x^2, \forall x \in \mathbb{R}$.

Megoldás. $x = 1$ -re: $f(1) - f(-1) = 1$, $x = -1$ -re: $f(-1) - f(1) = 1$, ellentmondás, nincs ilyen függvény.

▼ 3. Igazoljuk, hogy $f : \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = 2x^4 + 3x^3 + 4$ nem injektív függvény, $g : \mathbb{R} \rightarrow \mathbb{R}$, $g(x) = x^3 + x + 2$ pedig injektív függvény.

Megoldás. $f(x) = x^3(2x+3) + 4$, itt $x^3(2x+3) = 0$, ha $x = 0$ vagy $x = -3/2$, tehát $f(0) = f(-3/2) = 4$, f nem injektív.

Ha $g(x_1) = g(x_2)$, akkor $x_1^3 + x_1 = x_2^3 + x_2$, $(x_1 - x_2)(x_1^2 + x_1x_2 + x_2^2 + 1) = 0$, ahol a második zárójel $(x_1^2 + x_2^2/2)^2 + 3x_2^2/4 + 1 \neq 0$, tehát $x_1 = x_2$, g injektív.

▼ 4. Injektívek-e, szürjektívek-e, illetve bijektívek-e a következő függvények:

a) $f : \{1, 2, 3\} \rightarrow \{a, b, c\}$, $f(1) = b$, $f(2) = c$, $f(3) = a$;

b) $f : \mathbb{Z} \rightarrow \mathbb{Z}$, $f(x) = 2x + 1$, c) $f : \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = 2x + 1$,

d) $f : \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = 3x^2 + 4$, e) $f : \mathbb{Z} \rightarrow \mathbb{Z}$, $f(x) = -x^2 + 4x$.

f) $f : \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = x^4 - 2x^2 + 3$.

▼ 5. Legyenek A és B egyenlő számosságú véges halmazok és legyen $f : A \rightarrow B$ egy függvény. Igazoljuk, hogy a következő állítások egyenértékűek:

i) f injektív, ii) f szürjektív, iii) f bijektív.

2. Algebrai struktúrák

2.1. Algebrai műveletek

Legyen A egy nemüres halmaz és $\varphi : A \times A \rightarrow A$, $(x, y) \mapsto \varphi(x, y)$ egy függvény. φ -t az A halmazon értelmezett **(algebrai) művelet**nek nevezzük. Jelölés: $\varphi(x, y) = x * y$ (vagy $x \circ y$, $x \Delta y$, stb.).

Példa. • Az $\mathbb{R}$ halmazon a ”+” összeadás és a ”·” szorzás műveletek.

• Egy adott halmaz részhalmazainak halmazán a ” $\cup$ ” unió és a ” $\cap$ ” metszetképzés műveletek.

Ha egy halmazon legalább egy algebrai műveletet értelmezünk, akkor **algebrai struktúráról** beszélünk. Ha $*$ és $\circ$ műveletek az A -n, akkor $(A, *)$ egyműveletes struktúra, $(A, *, \circ)$ kétműveletes struktúra.

Feladat. ▼ Algebrai struktúrát alkot-e

i) $\mathbb{N}$ a szorzásra nézve ii) $\{2n + 1 : n \in \mathbb{N}\}$ az összeadásra nézve

iii) $2\mathbb{Z}$ az összeadásra nézve iv) $\mathbb{R}^*$ az osztásra nézve.

v) $\mathbb{Z}$ az $x * y = \frac{x-1}{y^2+1}$ megfeleltetéssel.

Az A halmazon értelmezett $*$ művelet **asszociatív**, ha minden $x, y, z \in A$ esetén $(x * y) * z = x * (y * z)$. A $*$ művelet **kommutatív**, ha minden $x, y \in A$ esetén $x * y = y * x$.

Példák. • a $\mathbb{Z}$ halmazon az összeadás és a szorzás asszociatív és kommutatív

• $\mathbb{Z}$ -n a kivonás művelet: $\forall x, y \in \mathbb{Z} : x - y \in \mathbb{Z}$, de ” $-$ ” nem asszociatív, mert pl. $(3 - 7) - 1 = -5 \neq -3 = 3 - (7 - 1)$

• a halmazokra vonatkozó ” $\cup$ ” és ” $\cap$ ” műveletek asszociatívák és kommutatívák.

Feladat. ▼ Mutassuk meg, hogy

a) az $\mathbb{N}^*$ halmazon az $x * y = x^y$ művelet nem kommutatív és nem asszociatív,

b) az $A = [0, \infty)$ halmazon az $x * y = \frac{x+y}{2}$ művelet nem asszociatív, de kommutatív,

c) az $A = (0, \infty)$ halmazon az $x * y = x^{\ln y}$ művelet kommutatív és asszociatív.

Legyen $(A, *)$ egy struktúra. Az $e \in A$ elem **semleges elem**, ha minden $x \in A$ esetén $e * x = x * e = x$. Összeadás (illetve additív módon jelölt művelet) esetén e neve **zéruselem**, jelölés $e = 0$, szorzás (illetve multiplikatív módon jelölt művelet) esetén e neve **egységelem**, jelölés $e = 1$. Gyakran a $*$ -gal jelölt műveletre is egységelemet mondunk.

Ha létezik egységelem, akkor az egyértelmű. Valóban tegyük fel, hogy e és e' egységelemek. Akkor $e * e' = e'$, mert e egységelem és $e * e' = e$, mert e' egységelem. Kapjuk, hogy $e = e'$.

Példa. • $(\mathbb{Z}, +)$ -ban a 0 zéruselem, $(\mathbb{R}, \cdot)$ -ban az 1 egységelem.

Legyen $(A, *)$ egy struktúra, amelyben létezik e semleges elem és $x \in A$. Azt mondjuk, hogy x -nek $x' \in A$ **szimmetrikusa**, ha $x * x' = x' * x = e$.

Összeadás (illetve additív módon jelölt művelet) esetén az elnevezés **ellentett elem**, jelölés $x' = -x$, szorzás (illetve multiplikatív módon jelölt művelet) esetén **inverz elem**, jelölés $x' = x^{-1}$.

Belátható, hogy ha x -nek létezik szimmetrikus eleme, akkor az egyértelmű.

Példák. • $(\mathbb{Z}, +)$ -ban minden x -re $x' = -x$ létezik, $(\mathbb{R}, \cdot)$ -ban az egységelem az $e = 1$ és minden $x \neq 0$ esetén $x' = x^{-1} = 1/x$, $x = 0$ -nak nincs szimmetrikusa (inverze).

Ha $(A, *, \circ)$ kétműveletes struktúra és minden $x, y, z \in A$ esetén

$$x \circ (y * z) = (x \circ y) * (x \circ z) \quad \text{és} \quad (y * z) \circ x = (y \circ x) * (z \circ x),$$

akkor azt mondjuk, hogy a $\circ$ művelet **disztributív** a $*$ műveletre nézve.

Példák. • az $\mathbb{R}$ halmazon a szorzás disztributív az összeadásra nézve

- halmazok esetén $\cup$ disztributív a $\cap$ műveletre és $\cap$ disztributív a $\cup$ műveletre nézve.

2.2. A csoport, a gyűrű és a test fogalma

A $(G, *)$ struktúra **csoport**, ha G -n értelmezett egy $*$ művelet, amelyre

(G_1) $(x * y) * z = x * (y * z)$ minden $x, y, z \in G$ -re, azaz a művelet asszociatív,

(G_2) létezik $e \in G$ úgy, hogy $x * e = e * x = x$ minden $x \in G$ -re, azaz létezik egységelem,

(G_3) minden $x \in G$ -re létezik $x' \in G$ úgy, hogy $x * x' = x' * x = e$, azaz minden elemnek van szimmetrikusa (inverze).

Ha még teljesül

(G_4) $x * y = y * x$ minden $xy \in G$ -re, azaz a művelet kommutatív,

akkor **kommutatív csoportról** vagy **Abel-csoportról** beszélünk (Niels Henrik Abel, XIX. századi norvég matematikus).

Itt a G jelölés az angol group, illetve a német Gruppe szavak (jelentésük: csoport) kezdőbetűjéből származik.

Példák. • $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ Abel-csoportok,

• $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ nem csoportok, de $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ Abel-csoportok.

A következőkben kétműveletes struktúrákat vizsgálunk.

Az $(R, *, \circ)$ algebrai struktúrát **gyűrűnek** nevezzük, ha teljesül a következő három tulajdonság:

1. $(R, *)$ Abel-csoport,
2. a " $\circ$ " művelet asszociatív,
3. " $\circ$ " **disztributív** a " $*$ " műveletre nézve.

Megjegyzés. Itt az R jelölés az angol ring szó (jelentése: gyűrű) kezdőbetűjéből származik, és nem összetévesztendő az $\mathbb{R}$ -rel (valós számhalmaz).

Az egyszerűség kedvéért gyakran az $(R, +, \cdot)$ jelölést használjuk és gyűrű-összeadás és gyűrű-szorzás műveletekről beszélünk akkor is, ha nem a szokásos $+$ és $\cdot$ műveletekről van szó.

Ennek megfelelően az $(R, +)$ csoport semleges elemét a gyűrű **zéruselemének** nevezzük, jelölés: 0. Azt mondjuk, hogy $(R, +, \cdot)$ **kommutatív gyűrű**, ha " $\cdot$ " kommutatív művelet. $(R, +, \cdot)$ **egységelemes gyűrű**, ha létezik egységelem a " $\cdot$ " műveletre nézve: $\exists 1 \in R : 1a = a1 = a, \forall a \in R$.

Példák. • $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ kommutatív, egységelemes gyűrűk, az egységelem az 1 szám, a zéruselem pedig a 0 szám.

Az $(R, +, \cdot)$ gyűrű neve **test**, ha R legalább két elemű egységelemes gyűrű és minden $a \in R, a \neq 0$ elemnek létezik inverze, azaz létezik $a^{-1} \in R : aa^{-1} = a^{-1}a = 1$. Továbbá R **kommutatív test**, ha R test és " $\cdot$ " kommutatív.

Példák. • $(\mathbb{Z}, +, \cdot)$ kommutatív gyűrű és nem test, mert pl. a 2-nek nincs inverze, mert $2^{-1} = \frac{1}{2} \notin \mathbb{Z}$

• $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ kommutatív testek.

Feladatok. ▼ 1. A $\mathbb{Z}$ halmazon értelmezzük az $x * y = x + y - 1$ műveletet. Igazoljuk, hogy $(\mathbb{Z}, *)$ Abel-csoport! Mi itt az egységelem és mi x szimmetrikusa?

▼ 2. Legyen $G = (0, \infty) \setminus \{1\}$ és $x * y = x^{\ln y}$. Igazoljuk, hogy $(G, *)$ Abel-csoport.

▼ 3. Az alábbi halmazok közül melyek alkotnak gyűrűt (a szokásos összeadásra és szorzásra):

a) $\{a + b\sqrt{5} : a, b \in \mathbb{Z}\}$, b) $\{a + b\sqrt[3]{5} : a, b \in \mathbb{Z}\}$,

▼ 4. Az alábbi halmazok közül melyek alkotnak testet (az összeadásra és szorzásra):

a) $\{a + b\sqrt{5} : a, b \in \mathbb{Q}\}$, b) $\{a + b\sqrt[3]{3} : a, b \in \mathbb{Q}\}$.

3. Komplex számok

3.1. A komplex számok bevezetése, algebrai alakja

3.2. A komplex számok trigonometrikus alakja

3.3. Gyökvonás komplex számokból, komplex egységgyökök

Lásd Szendrei Ágnes, Diszkrét matematika, VI. fejezet, 117-130 old.

Egy feladat. ▼ Igazoljuk, hogy $\{1, -1, i, -i\}$ Abel-csoport a komplex számok szorzására nézve.

4. Egész számok oszthatósága

4.1. Oszthatóság

Az a egész számot a b egész szám **osztójának** nevezzük, ha létezik olyan x egész szám, hogy $b = ax$, jelölés $a|b$. Ekkor azt mondjuk még, hogy b **osztható** a -val és b **többszöröse** a -nak. Ha a nem osztója b -nek, akkor ezt így jelöljük: $a \nmid b$.

Például, $3|12$, $5|60$, $3|(-6)$, $(-4)|24$, $(-2)|(-12)$, $2 \nmid 5$, $5 \nmid (-4)$.

Megjegyezzük, hogy $0|0$, sőt $a|0$ minden $a \in \mathbb{Z}$ esetén, de $0 \nmid b$ ha $b \in \mathbb{Z}, b \neq 0$.

Tétel. Legyenek $a, b, c, m, n \in \mathbb{Z}$. Akkor

i) ha $a|b$, akkor $a|(-b)$, $(-a)|b$, $(-a)|(-b)$,

ii) $a|a$ (reflexivitás), $1|a$,

iii) ha $a|b$ és $b|c$, akkor $a|c$ (transzitivitás),

iv) ha $a|b$ és $a|c$, akkor $a|mb + nc$,

v) ha $a|b$ és $b \neq 0$, akkor $|a| \leq |b|$,

vi) ha $a|b$ és $b|a$, akkor $|a| = |b|$.

Bizonyítás. iv) Ha $a|b$ és $a|c$, akkor létezik $x, y \in \mathbb{Z}$ úgy, hogy $b = ax, c = ay$, ahonnan $mb + nc = max + nay = a(mx + ny)$, s kapjuk, hogy $a|mb + nc$.

v) Ha $a|b, b \neq 0$, akkor $b = ax$ valamely $x \in \mathbb{Z}$ számra és $x \neq 0$, mert $x = 0$ esetén $b = 0$ lenne, ami ellentmondás. Így $|b| = |a||x| \geq |a|$.

vi) Ha $a = b = 0$, akkor $|a| = |b| = 0$. Ha $a \neq 0, b \neq 0$ (más eset nincs), akkor v) alapján $|a| \leq |b|$ és $|b| \leq |a|$, tehát $|a| = |b|$. $\square$

Következmény. A $\mathbb{Z}$ halmazon az oszthatóság reflexív és tranzitív, de nem antiszimmetrikus. Az $\mathbb{N}$ halmazon az oszthatóság reflexív, tranzitív és antiszimmetrikus, azaz rendezési reláció.

Megjegyzések. 1. A Tétel i) pontja alapján az oszthatósági kérdések vizsgálatakor elegendő a természetes számokra szorítkozni.

2. iv) alapján ha a osztója b -nek és c -nek, akkor a osztója b és c minden lineáris kombinációjának, így ezek összegének és különbségének is. Ez fordítva nem igaz, ha például $a|b + c$, nem következik, hogy $a|b$ és $a|c$. A iv) tulajdonság így általánosítható: ha $a, b_i, m_i \in \mathbb{Z}, a|b_i, i \in \{1, 2, \dots, k\}$, akkor $a|m_1b_1 + m_2b_2 + \dots + m_kb_k$.

Láttuk, hogy 0-nak minden egész szám osztója. Igaz ugyanakkor a következő állítás.

Tétel. Minden nemnulla egész számnak véges sok osztója van.

Bizonyítás. Legyen $b \neq 0$ adott egész szám és $a|b$. Akkor az előző Tétel v) pontja alapján $|a| \leq |b|$, azaz $-|b| \leq a \leq |b|$, így a csak véges sok értéket vehet fel. $\square$

Az oszthatósági feladatok megoldása során gyakran alkalmazzuk a következő tulajdonságokat.

Tétel. Legyenek $a, b \in \mathbb{Z}$ és $n \in \mathbb{N}^*$. Akkor

i) $a - b|a^n - b^n$,

ii) ha n páratlan, akkor $a + b|a^n + b^n$,

iii) ha n páros, akkor $a + b|a^n - b^n$.

Bizonyítás. Azonnali az

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

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

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

azonosságok alapján. $\square$

Feladatok. Az alábbiakban legyenek $a, b, c, d, m, n, \dots$ egész számok (kivéve ha mást mondunk).

▼ 1. Igazoljuk, hogy ha $ac|bc$ és $c \neq 0$, akkor $a|b$. Igaz-e a fordított állítás?

Megoldás. Ha $ac|bc$, akkor $bc = (ac)x$ és $c \neq 0$ -val osztva $b = ax$, ahonnan $a|b$. A fordított állítás is igaz, mert ha $a|b$, akkor $b = ax$ és c -vel szorozva $bc = acx$, $ac|bc$.

▼ 2. Igazoljuk, hogy ha $a|b$ és $c|d$, akkor $ac|bd$. Igaz-e fordítva?

Megoldás. Ha $a|b$ és $c|d$, akkor $b = ax$, $d = cy$, innen $bd = acxy$ és $ac|bd$. Fordítva nem igaz: legyen például $a = 2$, $b = 3$, $c = 3$, $d = 2$, akkor $ac = 6|6 = bd$, de $a = 2 \nmid 3 = b$ és $c = 3 \nmid 2 = d$.

▼ 3. Igazoljuk, hogy $a + b|ma + nb$ akkor és csak akkor, ha $a + b|mb + na$.

Megoldás. $(m+n)(a+b) = ma+na+mb+nb$, így ha feltételezzük, hogy $a+b|ma+nb$, akkor $a+b|(m+n)(a+b) - (ma+nb) = mb+na$. Hasonlóképpen, ha $a+b|mb+na$, akkor $a+b|(m+n)(a+b) - (mb+na) = ma+nb$.

▼ 4. Vezessük le a 9-cel és 11 -gyel való oszthatóságra vonatkozó következő szabályokat: egy tízes számrendszerbeli természetes szám

a) akkor és csak akkor osztható 9-cel, ha a számjegyeinek összege osztható 9-cel,

b) akkor és csak akkor osztható 11-gyel, ha a páratlan helyein álló számjegyek összegéből kivonva a páros helyeken álló számjegyek összegét 11-gyel osztható számot kapunk.

Megoldás. a) $n = b_k b_{k-1} \dots b_1 b_0_{(10)} = b_k 10^k + b_{k-1} 10^{k-1} + \dots + b_1 10 + b_0 = b_k(10^k - 1) + b_{k-1}(10^{k-1} - 1) + \dots + b_1(10 - 1) + (b_k + b_{k-1} + \dots + b_1 + b_0)$, ahol Tétel szerint az első k tag osztható $10 - 1 = 9$ -cel, így az adott n szám akkor és csak akkor osztható 9-cel, ha $(b_k + b_{k-1} + \dots + b_1 + b_0) =$ a számjegyeinek összege osztható 9-cel.

b) $n = b_k b_{k-1} \dots b_1 b_0_{(10)} = b_k 10^k + b_{k-1} 10^{k-1} + \dots + b_2 10^2 + b_1 10 + b_0 = b_k(10^k + (-1)^{k+1}) + b_{k-1}(10^{k-1} + (-1)^k) + \dots + b_2(10^2 - 1) + b_1(10 + 1) + b_0(1 - 1) + (-1)^k(b_k - b_{k-1} + b_{k-2} - \dots + (-1)^{k-2}b_2 + (-1)^{k-1}b_1 + (-1)^k b_0)$, ahol Tétel szerint az első $k+1$ tag osztható 11-gyel, pontosabban, a $10^{2m} - 1$ alakú tagok a fenti Tétel /iii), a $10^{2m+1} + 1$ alakú tagok pedig a Tétel /ii) alapján. Így az adott n szám akkor és csak akkor osztható 11-gyel, ha az utolsó tag osztható 11-gyel, amit igazolnunk kellett.

▼ 5. Mutassuk meg, hogy $7|2^n - 1$ akkor és csak akkor, ha $3|n$, ahol $n \in \mathbb{N}^*$.

Megoldás. Három esetet vizsgálunk:

I. $n = 3k$ alakú, akkor $2^n - 1 = 2^{3k} - 1 = 8^k - 1$ osztható $8 - 1 = 7$ -tel.

II. $n = 3k + 1$ alakú, akkor $2^n - 1 = 2^{3k+1} - 1 = 2 \cdot 8^k - 1 = 2(8^k - 1) + 1$, itt az első tag osztható $8 - 1 = 7$ -tel, az 1 pedig nem osztható 7-tel, így az összeg sem osztható 7-tel.

III. $n = 3k + 2$ alakú, most $2^n - 1 = 2^{3k+2} - 1 = 4 \cdot 8^k - 1 = 4(8^k - 1) + 3$ és úgy járunk el mint a II. esetben.

▼ 6. Igazoljuk, hogy minden m páratlan számra $240|m^5 - m$.

▼ 7. Igazoljuk, hogy $(5n^2 + 3)(n^4 + 8)$ osztható 24-gyel minden $n \in \mathbb{N}$ szám esetén.

▼ 8. Legyen $P_n = (n+1)(n+2)\dots(n+n)$. Igazoljuk, hogy $2^n|P_n$ és $2^{n+1} \nmid P_n$ minden $n \in \mathbb{N}^*$ esetén.

Megoldás. n szerinti indukcióval: $n = 1$ -re $P_1 = 2$, a tulajdonság igaz.

$$P_{n+1} = (n+2)\dots(2n)(2n+1)(2n+2) = P_n \frac{(2n+1)(2n+2)}{n+1} = 2(2n+1)P_n.$$

Feltéve, hogy $P_n = 2^n \cdot m$ alakú, ahol m páratlan szám, kapjuk: $P_{n+1} = 2^{n+1}(2n+1)m$, ahol $(2n+1)m$ páratlan és kész vagyunk.

Másképp,

$$P_n = \frac{(2n)!}{n!} = \frac{(2 \cdot 4 \cdot 6 \cdots 2n)(3 \cdot 5 \cdot 7 \cdots (2n-1))}{n!} =$$

$$= \frac{2^n(1 \cdot 2 \cdot 3 \cdots n)(3 \cdot 5 \cdot 7 \cdots (2n-1))}{n!} = 2^n(3 \cdot 5 \cdot 7 \cdots (2n-1)),$$

ahol a zárójelben lévő szorzat páratlan, s innen következik a tulajdonság.

▼ 9. Mutassuk meg, hogy $4^{90} + 1$ osztható 17-tel.

Megoldás. $4^{90} + 1 = (4^2)^{45} + 1 = 16^{45} + 1$ osztható $16 + 1 = 17$ -tel a Tétel /ii) alapján.

4.2. Maradékos osztás, számrendszerek

Igazoljuk a következő tételt.

Tétel. (A maradékos osztás tétele) Ha $a, b \in \mathbb{Z}, a \neq 0$, akkor léteznek az egyértelműen meghatározott $q \in \mathbb{Z}$ és $r \in \mathbb{Z}$ számok úgy, hogy

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

Bizonyítás. Legyen $a > 0$ és tekintsük a következő halmazt, melynek elemei egy mindkét irányban végtelen számtani sorozatot alkotnak:

$$H = \{b - ax : x \in \mathbb{Z}\} = \{\dots, b - 3a, b - 2a, b - a, b, b + a, b + 2a, b + 3a, \dots\},$$

mely tartalmaz pozitív és negatív számokat is, s melynek létezik egy legkisebb nem-negatív eleme, legyen ez r . Így létezik $q \in \mathbb{Z}$ úgy, hogy

$$b - (q + 1)a < 0 \leq b - qa = r,$$

ahonnan $b = qa + r$ és $0 \leq r < a = |a|$.

Ha $a < 0$, akkor $-a > 0$ és a fentiek alapján létezik $q', r' \in \mathbb{Z}$ úgy, hogy

$$b = q'(-a) + r' = (-q')a + r', \quad \text{ahol} \quad 0 \leq r' < |-a| = |a|,$$

és a $q = -q', r = r'$ választással az állítás bizonyított.

Az egyértelműség igazolása végett tegyük fel, hogy $b = qa + r, 0 \leq r < |a|$ és $b = q_1a + r_1, 0 \leq r_1 < |a|$. Így $qa + r = q_1a + r_1, (q - q_1)a = r_1 - r$. Ha $r \neq r_1$, akkor $r_1 - r \neq 0, q - q_1 \neq 0$ és figyelembevételével, hogy $a \neq 0$ kapjuk, hogy $|r_1 - r| = |q - q_1||a| \geq |a|$. Másrészt, az r és r_1 számokra vonatkozó egyenlőtlenségek alapján $|r_1 - r| < |a|$, ami ellentmondást jelent. Következik, hogy $r = r_1$, ahonnan $q = q_1$. □

Megjegyzések. 1. A gyakorlatban a q **hányados** és az r **maradék**ot úgy kapjuk meg, hogy b -t elosztjuk a -val.

2. Az $a \neq 0$ egész szám akkor osztója b -nek ha a maradékos osztás tételében szereplő r maradék nulla, s ekkor a fenti x éppen a q hányados, amely egyértelműen meghatározott.

Példák. • a) Ha $b = 29$ és $a = 4$, akkor $q = 7, r = 1$, az osztás egyenlete pedig $29 = 4 \cdot 7 + 1$.

b) $b = -29$ és $a = 4$ esetén $q = -8, r = 3$, az osztás egyenlete pedig $-29 = 4 \cdot (-8) + 3$.

c) $b = 49, a = -5$, akkor $q = -9, r = 4$ és az osztás egyenlete $49 = (-5) \cdot (-9) + 4$.

d) Ha $b = 84$ és $a = 7$, akkor $q = 12$ és $r = 0$: $84 = 7 \cdot 12$.

3. A kapott r maradék a $0, 1, 2, \dots, |a| - 1$ számok valamelyike, s ezek száma $|a|$. Például b -t $a = 2$ -vel osztva a maradék 0 vagy 1 aszerint, hogy b páros ($b = 2q$) vagy b páratlan ($b = 2q + 1$). $a = 3$ -mal osztva a maradék 0, 1 vagy 2 lehet s ennek megfelelően $b = 3q, b = 3q + 1$ vagy $b = 3q + 2$ alakú, ahol $q \in \mathbb{Z}$, stb.

A maradékos osztás tételének fontos alkalmazása a számok adott alapú számrendszerben történő felírása.

Tétel. Ha $a \in \mathbb{N}, a > 1$ adott szám, akkor minden $n \in \mathbb{N}^*$ szám felírható

$$n = b_k a^k + b_{k-1} a^{k-1} + \dots + b_1 a + b_0$$

alakban, ahol $0 \leq b_i \leq a - 1, i \in \{1, 2, \dots, k\}, b_k \neq 0$ és a b_i számok (az n számjegyei) egyértelműen meghatározottak.

Bizonyítás. Az előző Tétel szerint n felírható

$$n = a q_0 + b_0, \quad 0 \leq b_0 \leq a - 1$$

alakban, ahol q_0 és b_0 egyértelműen meghatározottak. Hasonlóan,

$$q_0 = a q_1 + b_1, \quad 0 \leq b_1 \leq a - 1,$$

$$q_1 = a q_2 + b_2, \quad 0 \leq b_2 \leq a - 1,$$

.....

és $q_1, b_1, q_2, b_2, \dots$ egyértelműen meghatározottak.

Véges sok lépésen belül nulla hányadost kapunk, hiszen $a > 1$ miatt $q_0 > q_1 > q_2 > \dots$ természetes számokból álló szigorúan csökkenő sorozat. Legyen $q_k = 0$ az első nulla hányados, így az utolsó egyenlet

$$q_{k-1} = b_k, \quad 0 < b_k \leq a - 1,$$

visszahelyettesítve kapjuk, hogy

$$n = a(a q_1 + b_1) + b_0 = a(a(a q_2 + b_2) + b_1) + b_0 = \dots,$$

s elvégezve a műveleteket

$$n = b_k a^k + b_{k-1} a^{k-1} + \dots + b_1 a + b_0. \quad \square$$

Jelölés: $n = b_k b_{k-1} \dots b_1 b_0_{(a)}$.

Ha $a = 10$, akkor a természetes számok szokásos, tízes alapú felírását kapjuk a $0, 1, 2, \dots, 9$ számjegyek segítségével, ha pedig $a = 2$, akkor a kettes alapú (bináris) számrendszerhez jutunk, melyben két számjegy van: a 0 és az 1.

★ Az előbbi tétel közvetlen alkalmazásaként adódik, hogy minden $n \in \mathbb{N}^*$ szám egyértelműen felírható

$$n = 2^{k_r} + 2^{k_{r-1}} + \dots + 2^{k_1} + 2^{k_0}$$

alakban, ahol $k_r > k_{r-1} > \dots > k_1 > k_0 \geq 0$ egész számok. ★

Példa. • Írjuk fel a tízes számrendszerben a következő számokat: $1001001_{(2)}$ és $475_{(8)}$.

A Tétel alkalmazásával,

$$1001001_{(2)} = 1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 64 + 8 + 1 = 73,$$

$$475_{(8)} = 4 \cdot 8^2 + 7 \cdot 8 + 5 = 256 + 56 + 5 = 317.$$

Egy adott n számot a alapú számrendszerben a következőképpen írunk fel (vesd össze a Tétel bizonyításával):

Először n -et elosztjuk a -val. A kapott maradék adja a b_0 utolsó számjegyét. Ezután az előző osztás során kapott hányadost osztjuk el a -val és a kapott maradék adja a

b_1 utolsó előtti számjegyet. Majd ennek az osztásnak a hányadosát osztjuk el a -val és a kapott maradék lesz a b_2 számjegy, stb. Az algoritmus akkor ér véget, mikor valamely osztás során 0 hányadost kapunk, ennek az osztásnak a maradéka (azaz az előző hányados) lesz a b_k első jegy.

Példák. • a) Írjuk fel a kettes számrendszerben a 114 számot.

Az osztások a következők: $114 = 2 \cdot 57 + 0$, $57 = 2 \cdot 28 + 1$, $28 = 2 \cdot 14 + 0$, $14 = 2 \cdot 7 + 0$, $7 = 2 \cdot 3 + 1$, $3 = 2 \cdot 1 + 1$, $1 = 2 \cdot 0 + 1$ és $114 = 1110010_{(2)}$.

b) Írjuk fel a 6-os számrendszerben a 346 számot.

Most $346 = 6 \cdot 57 + 4$, $57 = 6 \cdot 9 + 3$, $9 = 6 \cdot 1 + 3$, $1 = 6 \cdot 0 + 1$ és $346 = 1334_{(6)}$.

Feladatok.

▼ 1. Mutassuk meg, hogy minden egész szám négyzete

- a) 3-mal osztva 0 vagy 1 maradékot ad;
- b) 4-gyel osztva 0 vagy 1 maradékot ad;
- c) 5-tel osztva 0 vagy 1 vagy 4 maradékot ad.

Vizsgáljuk a 6-tal, 7-tel és 8-cal való osztást.

Megoldás. a) A következő eseteket vizsgáljuk:

I. $n = 3q$, ekkor $n^2 = 9q^2 = 3 \cdot (3q^2)$, ami 3-mal osztva 0 maradékot ad,

II. $n = 3q + 1$, ekkor $n^2 = (3q + 1)^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1$, ami 3-mal osztva 1 maradékot ad,

III. $n = 3q + 2$, most $n^2 = (3q + 2)^2 = 9q^2 + 12q + 4 = 3(3q^2 + 4q + 1) + 1$ és 3-mal osztva újra 1 a maradék.

Rövidebben, II. és III. együtt: $n = 3q \pm 1$, ekkor $n^2 = (3q \pm 1)^2 = 9q^2 \pm 6q + 1 = 3(3q^2 \pm 2q) + 1$, ami 3-mal osztva 1 maradékot ad.

A többi hasonlóan.

▼ 2. Milyen számjegyre végződhet egy teljes négyzet (teljes köb) a tízes számrendszerben?

Megoldás. Minden n egész szám felírható $n = 10q + r$ alakban, ahol $0 \leq r \leq 9$ és $n^2 = (10q + r)^2 = 100q^2 + 20qr + r^2 = 10k + r^2$, tehát az utolsó jegyet az r^2 utolsó jegye adja. Ezért elegendő az egyjegyű számokat vizsgálni: $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 9$, $4^2 = 16$, $5^2 = 25$, $6^2 = 36$, $7^2 = 49$, $8^2 = 64$, $9^2 = 81$, az utolsó jegy tehát 0, 1, 4, 5, 6, 9 lehet és nem lehet 2, 3, 7, 8.

▼ 3. Határozzuk meg a -t úgy, hogy

- a) $231_{(a)} = 190$,
- b) $1182_{(a)} = 884$.

Megoldás. a) $a \geq 4$ egész szám, mert előfordul a 3-as számjegy. Kapjuk, hogy $2a^2 + 3a + 1 = 190$ és megoldva ezt a másodfokú egyenletet: $a = -21/2$ és $a = 9$. A megoldás $a = 9$.

b) Most $a \geq 9$ egész szám, mert a 8-as számjegy is előfordul, és az $a^3 + a^2 + 8a + 2 = 884$ harmadfokú egyenletet kellene megoldanunk. Ezt elkerülhetjük, ha megfigyeljük, hogy $a = 10$ -re $1182_{(10)} = 1182 > 884$ és $a > 10$ esetén $1182_{(a)} > 1182_{(10)} > 884$.

Továbbá, $a = 9$ -re $1182_{(9)} = 9^3 + 9^2 + 8 \cdot 9 + 2 = 884$, tehát a megoldás $a = 9$.

▼ 4. Igazoljuk, hogy a 16-os számrendszerben felírt $123456789ABCDEF$ szám osztható 15-tel, ahol $A = 10$, $B = 11$, $C = 12$, $D = 13$, $E = 14$, $F = 15$.

5. Legnagyobb közös osztó és legkisebb közös többszörös

5.1. Egész számok legnagyobb közös osztója

Most két egész szám közös osztóival foglalkozunk. Ha $a, b \in \mathbb{Z}$ és nem mindkettő nulla, akkor a közös osztók száma véges, s így van közöttük legnagyobb abszolút értékű. A $d \in \mathbb{Z}$ számot az a és b (nem mindkettő nulla) **legnagyobb közös osztójának** (inko-jának) nevezzük, ha d közös osztó és ha nincs nála nagyobb abszolút értékű közös osztó. Az $a = b = 0$ esetben a 0-t nevezzük legnagyobb közös osztónak. Ha d legnagyobb közös osztó, akkor $-d$ is az, s ezeken kívül nincs más legnagyobb közös osztó. Az a és b számok nemnegatív legnagyobb közös osztóját (a, b) -vel jelöljük, ahol $(a, b) = (b, a)$.

Példák. • $a = 36$ és $b = 24$ közös osztói: $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$, a legnagyobb közös osztók a ± 12 és $(36, 24) = 12$.

• $a = 15$ és $b = -12$ közös osztói: $\pm 1, \pm 3$, a legnagyobb közös osztók a ± 3 és $(15, -12) = 3$.

A legnagyobb közös osztó fogalma a következőképpen is értelmezhető. Az $a, b \in \mathbb{Z}$ számok **legnagyobb közös osztójának** nevezzük a $\delta \in \mathbb{Z}$ számot, ha

i) δ közös osztó ($\delta|a, \delta|b$),

ii) minden közös osztó δ -nak osztója (minden $c|a, c|b$ esetén $c|\delta$).

Ha $a = b = 0$, akkor minden $\delta \in \mathbb{Z}$ teljesíti ezeket a feltételeket. Nem triviális azonban, hogy létezik-e két adott szám (nem mindkettő nulla) δ legnagyobb közös osztója a második értelmezés szerint. Ha létezik ilyen δ , akkor $-\delta$ is legnagyobb közös osztó, s más szám nem rendelkezik ezzel a tulajdonsággal. Továbbá, ha δ az a és b második értelmezés szerinti legnagyobb közös osztója és $\delta \in \mathbb{N}$, akkor $\delta = (a, b)$, hiszen i) szerint $\delta \leq (a, b)$, másrészt $(a, b)|a, (a, b)|b$, így ii) szerint $(a, b)|\delta$, ahonnan $(a, b) \leq \delta$.

Tétel. Ha $a, b \in \mathbb{Z}$ (nem mindkettő nulla), akkor létezik e számok legnagyobb közös osztója a második értelmezés szerint.

Első bizonyítás. Legyen $A = \{ax + by : x, y \in \mathbb{Z}\}$. Az A halmaz tartalmazza a 0-t, tartalmaz negatív és pozitív egészeket is. Legyen δ az A halmaz legkisebb pozitív eleme, $\delta = ax_0 + by_0$. Megmutatjuk, hogy δ legnagyobb közös osztó. A maradékos osztás tétele szerint létezik $q, r \in \mathbb{Z}$ úgy, hogy $a = \delta q + r, 0 \leq r < \delta$. Így $r = a - \delta q = a - (ax_0 + by_0)q = a(1 - qx_0) + b(-qy_0) \in A$, ahonnan $r = 0$, s innen $\delta|a$. Hasonlóan $\delta|b$, tehát δ közös osztója a -nak és b -nek. Ha $c|a, c|b$, akkor $c|ax_0 + by_0 = \delta$. $\square$

Második bizonyítás. A maradékos osztás tételének ismételt alkalmazásával a következő összefüggéseket kapjuk (feltételezzük, hogy $b > 0$):

$$a = bq_1 + r_1, \quad 0 < r_1 < b,$$

$$b = r_1q_2 + r_2, \quad 0 < r_2 < r_1,$$

$$r_1 = r_2q_3 + r_3, \quad 0 < r_3 < r_2,$$

...

$$r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}, \quad 0 < r_{n-1} < r_{n-2},$$

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

$$r_{n-1} = r_nq_{n+1}, \quad r_{n+1} = 0$$

Ez az eljárás, az ún. **euklidészi algoritmus**, akkor ér véget ha a kapott maradék nulla, s ez véges sok lépés után bekövetkezik, hiszen $b > r_1 > r_2 > \dots$ szigorúan csökkenő nemnegatív tagú sorozat. r_n -nel jelölve az utolsó nemnulla maradékot, megmutatjuk, hogy $\delta = r_n$ az a és b számok legnagyobb közös osztója a második értelmezés szerint.

Az utolsó egyenletből $r_n | r_{n-1}$, az utolsó előttiből $r_n | r_{n-2}$ (lásd 4.1. szakasz Tétel), s visszafelé haladva rendre kapjuk, hogy $r_n | r_{n-3}, \dots, r_n | r_2, r_n | r_1, r_n | b, r_n | a$, tehát r_n közös osztó. Ha pedig $c | a, c | b$, akkor az első egyenletből $c | r_1$, a másodikból $c | r_2$, s lefelé haladva következik, hogy $c | r_3, \dots, c | r_{n-2}, c | r_{n-1}, c | r_n$, azaz $c | r_n$. $\square$

Megjegyzések. 1. A második bizonyítás konstruktív, nemcsak δ létezését igazolja, hanem elő is állítja azt.

2. A fenti két értelmezés tehát egyenértékű. Általánosabb struktúrákban, például gyűrűkben csak a második értelmezés használható, ugyanis ebben csak az oszthatósági reláció szerepel. $\square$

Tétel. Ha $a, b \in \mathbb{Z}$, akkor léteznek az $x_0, y_0 \in \mathbb{Z}$ számok úgy, hogy $(a, b) = ax_0 + by_0$.

Bizonyítás. Azonnali a fenti első bizonyítás alapján. $\square$

Megjegyzés. A tulajdonság az euklidészi algoritmus alapján is következik. Az utolsó előtti egyenletből $(a, b) = r_n = r_{n-2} - r_{n-1}q_n$, az azt megelőző egyenletből pedig $r_{n-1} = r_{n-3} - r_{n-2}q_{n-1}$, ahonnan $r_n = (1 + q_{n-1}q_n)r_{n-2} - q_n r_{n-3}$ az r_{n-2} és r_{n-3} lineáris kombinációja. Visszafelé haladva az egyenletekben, egymásutáni helyettesítésekkel kapjuk, hogy (a, b) az a és b számok egy lineáris kombinációja. $\square$

Példa. • Határozzuk meg az euklidészi algoritmus alapján az 1819 és 3587 d lnko-ját és keressünk olyan $x, y \in \mathbb{Z}$ számokat, melyekre $d = 1819x + 3587y$.

Megoldás. A megfelelő osztások elvégzésével:

$$3587 = 1819 \cdot 1 + 1768$$

$$1819 = 1768 \cdot 1 + 51$$

$$1768 = 51 \cdot 34 + 34$$

$$51 = 34 \cdot 1 + 17$$

$$34 = 17 \cdot 2 + 0$$

Így az lnko az utolsó nemnulla maradék: $d = (1819, 3587) = 17$.

Továbbá, az utolsó előtti egyenletből, az azt megelőzőből, stb. rendre kapjuk, hogy $17 = 51 - 34 = 51 - (1768 - 51 \cdot 34) = 35 \cdot 51 - 1768 = 35(1819 - 1768) - 1768 = 35 \cdot 1819 - 36(3587 - 1819) = 71 \cdot 1819 - 36 \cdot 3587$. Választható $x = 71, y = -36$.

Az $a, b \in \mathbb{Z}$ számokat **relatív prímeknek** nevezzük, ha $(a, b) = 1$.

Tétel. Az $a, b \in \mathbb{Z}$ számok akkor és csak akkor relatív prímek, ha léteznek az $x_0, y_0 \in \mathbb{Z}$ számok úgy, hogy $ax_0 + by_0 = 1$.

Bizonyítás. A feltétel szükségessége következik az előbbi Tételből, az elégségesség pedig így látható be: ha $ax_0 + by_0 = 1$ és $d | a, d | b, d \in \mathbb{N}$, akkor $d | 1$, tehát $d = 1$. $\square$

Tétel. Ha $a, b, m \in \mathbb{Z}$, akkor

i) $(ka, kb) = k(a, b)$, ahol $k \in \mathbb{N}^*$,

ii) $(\frac{a}{c}, \frac{b}{c}) = \frac{1}{c}(a, b)$, ahol $c \in \mathbb{N}^*, c | a, c | b$,

iii) $(a, b) = d$ akkor és csak akkor, ha $(\frac{a}{d}, \frac{b}{d}) = 1$, ahol $d \in \mathbb{N}^*, d | a, d | b$,

iv) $(a, m) = 1$ és $(b, m) = 1$ akkor és csak akkor, ha $(ab, m) = 1$,

v) ha $a | bm$ és $(a, m) = 1$, akkor $a | b$.

vi) ha $a | m, b | m$ és $(a, b) = 1$, akkor $ab | m$.

Bizonyítás. i) Az euklidészi algoritmust ka és kb -re alkalmazva ugyanazokat az egyenleteket kapjuk, mint ha az a és b -re vonatkozó algoritmusból minden egyenletet k -val szorzunk. Így r_n is k -val szorozódik és $(ka, kb) = kr_n = (a, b)$.

Másképp, a szakasz első Tételének első bizonyítása szerint $(a, b) = \min\{ax + by : x, y \in \mathbb{Z}, ax + by > 0\}$. Így $(ka, kb) = \min\{kax + kby : x, y \in \mathbb{Z}, kax + kby > 0\} = k \min\{ax + by : x, y \in \mathbb{Z}, ax + by > 0\} = k(a, b)$.

ii) $k = c$ -re alkalmazva az i) tulajdonságot kapjuk, hogy

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

ami egyenértékű a bizonyítandó összefüggéssel.

iii) A ii) pont alkalmazásával

$$(\frac{a}{d}, \frac{b}{d}) = \frac{1}{d}(a, b),$$

s innen következik az állítás.

iv) Ha $(a, m) = 1$ és $(b, m) = 1$, akkor létezik $x, y, u, v \in \mathbb{Z}$ úgy, hogy $ax + my = 1, bu + mv = 1$. Így $(ab)(xu) = (1 - my)(1 - mv) = 1 - mz$ alakú, $z \in \mathbb{Z}$, ahonnan $(ab)(xu) + mz = 1$ és használva az előző Tételt kapjuk, hogy $(ab, m) = 1$. Fordítva, ha $(ab, m) = 1$, akkor létezik $x_1, y_1 \in \mathbb{Z}$ úgy, hogy $(ab)x_1 + my_1 = a(bx_1) + my_1 = 1$, s innen Tétel alapján $(a, m) = 1$, hasonlóan $(b, m) = 1$.

v) Mivel a közös osztója ba -nek és bm -nek, osztója e két szám lnko-jának is:

$$a|(ba, bm) = b(a, m) = b.$$

vi) A feltételek szerint $m = ax = by$, ahonnan $b|ax$, de $(a, b) = 1$, így az v) tulajdonság alapján $b|x, x = bz, m = abz$, s következik, hogy $ab|m$. $\square$

Több szám legnagyobb közös osztóját (lnko-ját) ezek után a következőképpen definiáljuk. Ha $a_1, a_2, \dots, a_k \in \mathbb{Z}$ (nem mind nulla), akkor ezek lnko-ja a $\delta \in \mathbb{Z}$ szám, ha

i) δ közös osztó ($\delta|a_1, \delta|a_2, \dots, \delta|a_k$),

ii) δ -nak minden közös osztó osztója (minden $c|a_1, c|a_2, \dots, c|a_k$ esetén $c|\delta$).

A fenti δ létezése következik a szakasz első Tételéből és abból a tényből, hogy két szám közös osztóinak halmaza egyenlő a két szám lnko-ja osztóinak halmazával. A nemnegatív lnko-t $(a_1, a_2, \dots, a_k)$ -val jelölve például $k = 4$ -re:

$$(a_1, a_2, a_3, a_4) = ((a_1, a_2), a_3, a_4) = (((a_1, a_2), a_3), a_4).$$

Továbbá ha az adott számok nem mind nullák, akkor a δ lnko az előjeltől eltekintve egyértelműen meghatározott. Az $a_1 = a_2 = \dots = a_k = 0$ esetben megállapodás szerint $(0, 0, \dots, 0) = 0$.

Tétel. Ha $a_1, a_2, \dots, a_k \in \mathbb{Z}$, akkor léteznek az $x_1, x_2, \dots, x_k \in \mathbb{Z}$ számok úgy, hogy

$$(a_1, a_2, \dots, a_k) = a_1x_1 + a_2x_2 + \dots + a_kx_k.$$

Bizonyítás. Indukcióval bizonyítunk. Ha $k = 2$, akkor a tulajdonság igaz Tétel szerint. Tegyük fel, hogy a tulajdonság igaz valamely $k \geq 2$ számra, s legyenek $a_1, a_2, \dots, a_k, a_{k+1}$ adott egész számok. Akkor

$$\begin{aligned} (a_1, a_2, \dots, a_k, a_{k+1}) &= ((a_1, a_2), a_3, \dots, a_k, a_{k+1}) = (a_1, a_2)y + a_3x_3 + \dots + a_kx_k + a_{k+1}x_{k+1} \\ &= (a_1z + a_2t)y + a_3x_3 + \dots + a_kx_k + a_{k+1}x_{k+1} = a_1yz + a_2yt + a_3x_3 + \dots + a_kx_k + a_{k+1}x_{k+1} \\ &= a_1x_1 + a_2x_2 + a_3x_3 + \dots + a_kx_k + a_{k+1}x_{k+1}. \quad \square \end{aligned}$$

Az $a_1, a_2, \dots, a_k \in \mathbb{Z}$ számok **relatív prímek** ha $(a_1, a_2, \dots, a_k) = 1$. Az $a_1, a_2, \dots$ számok **páronként relatív prímek** ha $(a_i, a_j) = 1$ minden $i, j \in \{1, 2, \dots\}, i \neq j$ esetén.

Példák. • Az 5, 10, 12, 14 számok relatív prímek, mert $(5, 10, 12, 14) = 1$, de nem páronként relatív prímek, mert például $(5, 10) = 5 \neq 1$.

Az $F_n = 2^{2^n} + 1$, $n \geq 0$ sorozat tagjai páronként relatív prímek. Valóban, legyen $n, m \in \mathbb{N}, n \neq m$, feltehető, hogy $m < n$ és $d \in \mathbb{N}, d|F_n, d|F_m$. Akkor

$$\begin{aligned} F_n - 2 = 2^{2^n} - 1 &= (2^{2^{n-1}} + 1)(2^{2^{n-1}} - 1) = (2^{2^{n-1}} + 1)(2^{2^{n-2}} + 1) \dots (2^{2^m} + 1)(2^{2^m} - 1) \\ &= F_{n-1} F_{n-2} \dots F_m (2^{2^m} - 1) = k F_m \end{aligned}$$

alapján $d|2$, de $d = 2$ nem lehet, mert az F_n számok mind páratlanok, így $d = 1$.

5.2. Egész számok legkisebb közös többszöröse

Az $a, b \in \mathbb{Z}$ számok **legkisebb közös többszöröse** (lkkt-je) az $m \in \mathbb{Z}$ szám, ha

- i) m közös többszörös $(a|m, b|m)$,
- ii) minden közös többszörös m -nek többszöröse (minden $a|t, b|t$ esetén $m|t$).

Tétel. Ha $a, b \in \mathbb{Z}$, akkor létezik e számok lkkt-je.

Bizonyítás. Ha $a = 0$ vagy $b = 0$, akkor $[a, b] = 0$. Feltételezzük, hogy $a > 0, b > 0$. Igazoljuk, hogy

$$m = \frac{ab}{(a, b)}$$

az a és b számok lkkt-je. Valóban,

$$m = \frac{b}{(a, b)} a \quad \text{és} \quad m = \frac{a}{(a, b)} b$$

alapján $a|m, b|m$, tehát m közös többszörös. Ha most $a|t, b|t$, akkor az lko tulajdonságait használva

$$\left(\frac{t}{a}, \frac{t}{b}\right) = \left(\frac{ta}{ab}, \frac{tb}{ab}\right) = \frac{t(a, b)}{ab} = \frac{t}{m}$$

egész szám, ahonnan $m|t$. $\square$

Az lkkt az előjeltől eltekintve egyértelműen meghatározott. Az $a, b \in \mathbb{Z}$ számok nemnegatív lkkt-jét $[a, b]$ -vel jelöljük.

Példák. • $a = 4, b = 6$ esetén a közös többszörösök a $\pm 12, \pm 24, \pm 36, \dots$, a legkisebb közös többszörösök a ± 12 és $[4, 6] = 12$.

Ha $a = 5, b = 3$, akkor a közös többszörösök a $\pm 15, \pm 30, \pm 45, \dots$, a legkisebb közös többszörösök a ± 15 és $[5, 3] = 15$.

A Tétel szerint $ab = (a, b)[a, b]$. Így az lkkt kiszámítása és tulajdonságainak vizsgálata visszavezethető a lko kiszámítására illetve annak tulajdonságai vizsgálatára.

Hasonlóképpen definiálható több szám lkkt-je (Feladat!).

Ha n és m relatív prímek, azaz ha $(n, m) = 1$, akkor $[n, m] = nm$.

Példa. • Határozzuk meg 1819 és 3587 lkkt-jét.

Láttuk, hogy $(1819, 3587) = 17$. Így,

$$[1819, 3587] = \frac{1819 \cdot 3587}{17} = 107 \cdot 3587 = 383809.$$

Feladatok

▼ 1. Határozzuk meg az az euklidészi algoritmussal az 504 és 372 lko-ját. Mennyi e számok lkkt-je ?

▼ 2. Határozzuk meg az alábbi legnagyobb közös osztókat, ha $a, b \in \mathbb{Z}$ és $a|b$:

a) $(b, a + b)$,

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

▼ 3. Mutassuk meg, hogy minden $n \in \mathbb{N}$ esetén

a) $n^2 + 3n + 3$ és $n + 1$ relatív prímek.

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

▼ 4. Határozzuk meg azokat az $n \in \mathbb{N}$ számokat, melyekre $(5^n + 1, 39) = 1$.

6. Prímszámok

6.1. Felbonthatatlan számok és prímszámok

Egy a egész számot **egység**nek nevezünk, ha a minden egész számnak osztója.

Tétel. A $\mathbb{Z}$ halmazban két egység van, a -1 és az 1 .

Bizonyítás. $-1|a, 1|a$ minden $a \in \mathbb{Z}$ esetén. Másrészt, ha b egység, akkor $b|1$, és kapjuk, hogy b csak -1 és 1 lehet. $\square$

Minden $a \in \mathbb{Z}$ számnak osztói a $-1, -a, 1, a$. Ezeket **triviális osztóknak** nevezzük. A nem triviális osztók a **valódi osztók**. A továbbiakban azokat a számokat vizsgáljuk, melyeknek csak triviális osztók vannak. A $p \in \mathbb{Z} \setminus \{-1, 0, 1\}$ számot **felbonthatatlan (irreducibilis) számnak** nevezzük, ha nem létezik valódi osztója, azaz ha abból, hogy $p = ab$, ahol $a, b \in \mathbb{Z}$ következik, hogy $a \in \{-1, 1\}$ vagy $b \in \{-1, 1\}$. Ilyen számok például a $2, -2, 3, -3, 5, -5, \dots$. Az $a \in \mathbb{Z}, a \neq 0$ számot **összetett számnak** nevezzük, ha van a triviális osztóktól különböző osztója. Összetett szám például a $6, 8, -20, 60$, stb.

Ha $a|b$ vagy $a|c$, akkor $a|bc$, de fordítva ez általában nem igaz. A $q \in \mathbb{Z} \setminus \{-1, 0, 1\}$ számot **prímszámnak** nevezzük, ha minden $a, b \in \mathbb{Z}$ esetén úgy, hogy ha $q|ab$, akkor ebből $q|a$ vagy $q|b$ következik. Létezik-e prímszám? A választ a következő tétel adja meg.

Tétel. Ha p felbonthatatlan szám, akkor p prímszám.

Bizonyítás. Tegyük fel, hogy $p \in \mathbb{Z} \setminus \{-1, 0, 1\}$ felbonthatatlan és $p|ab$, ahol $a, b \in \mathbb{Z}$. Ha $p|a$, akkor az állítás bizonyított.

Ha $p \nmid a$, akkor megmutatjuk, hogy $p|b$. Először igazoljuk, hogy $(p, a) = 1$. Valóban, ha $d|p, d|a$, akkor mivel p felbonthatatlan, $d \in \{-p, -1, 1, p\}$, de $d \in \{-p, p\}, d|a$ ellentmondás, így $d \in \{-1, 1\}$, azaz $(p, a) = 1$. A $p|ab, p \nmid a$ összefüggések miatt így $p|(ab, pb) = b(a, p) = b$ következik, felhasználva egy korábbi Tételt. $\square$

Igaz a fordított állítás is, azaz

Tétel. Ha q prímszám, akkor q felbonthatatlan.

Bizonyítás. Tegyük fel, hogy $q \in \mathbb{Z} \setminus \{-1, 0, 1\}$ prímszám és q nem felbonthatatlan, azaz létezik $a, b \in \mathbb{Z} \setminus \{-1, 1\}$ úgy, hogy $q = ab$. Akkor $q|ab$, s mivel q prímszám következik, hogy $q|a$ vagy $q|b$, tehát $ab|a$ vagy $ab|b$, ahonnan kapjuk, hogy $b \in \{-1, 1\}$ vagy $a \in \{-1, 1\}$, ami ellentmondás. $\square$

A $\mathbb{Z}$ halmazon tehát egy szám akkor és csak akkor felbonthatatlan, ha prímszám, a továbbiakban többnyire a prímszám elnevezést használjuk.

Megjegyzés. A felbonthatatlan elem és a prímelem fogalma általánosabb algebrai struktúrákban, például gyűrűkben is definiálható és a fenti két fogalom általában nem esik egybe. Pontosabban, ha q prím, akkor abból mindig következik, hogy q felbonthatatlan, de fordítva nem.

★ Tekintsük a következő példát. Az $A = \mathbb{Z}[i\sqrt{5}] \equiv \{z = a + bi\sqrt{5} : a, b \in \mathbb{Z}\}$ halmaz, ahol i a képzetes egység, kommutatív, egységelemes, zérusosztómentes gyűrűt alkot a komplex számok összeadására és szorzására nézve. A $z \in A$ szám osztója $u \in A$ -nak, ha létezik $w \in A$ úgy, hogy $u = zw$. Könnyen látható, hogy az egységek (azok az A -beli elemek, melyek minden A -beli számnak osztói) itt is a -1 és a 1 . A felbonthatatlan elem és a prímelem fogalma ugyanúgy definiálható mint $\mathbb{Z}$ -ben. Megmutatjuk, hogy $3 \in A$ felbonthatatlan, de nem prím. Tegyük fel, hogy $3 = (a + ib\sqrt{5})(c + di\sqrt{5})$. Mindkét oldal komplex konjugáltját véve $3 = (a - ib\sqrt{5})(c - di\sqrt{5})$, ahonnan $9 = (a^2 + 5b^2)(c^2 + 5d^2)$. Ha $a^2 + 5b^2 = 1$, akkor $a = \pm 1, b = 0$ és $a + bi\sqrt{5} = \pm 1$ egység. Ha $a^2 + 5b^2 = 3$, akkor a, b -re nem kapunk egész szám megoldást, ha pedig $a^2 + 5b^2 = 9$, akkor $c^2 + 5d^2 = 1$, s következik, hogy $c + di\sqrt{5} = \pm 1$ egység. Továbbá, $3|9 = (2 + i\sqrt{5})(2 - i\sqrt{5})$, de

$3 \nmid 2 + i\sqrt{5}$ és $3 \nmid 2 - i\sqrt{5}$. Valóban, ha például $3 \mid 2 + i\sqrt{5}$, akkor létezik $x, y \in \mathbb{Z}$ úgy, hogy $2 + i\sqrt{5} = 3(x + iy\sqrt{5})$, ahonnan $x = 2/3, y = 1/3$, ellentmondás. $\square \star$

Tétel. Minden $a \in \mathbb{Z} \setminus \{-1, 0, 1\}$ számnak létezik felbonthatatlan osztója.

Bizonyítás. Ha a felbonthatatlan, akkor $a|a$ miatt az állítás bizonyított. Ha a összetett szám, akkor létezik valódi osztója, s legyen b legkisebb abszolút értékű valódi osztó ($b|a, |b| < |a|$). Ekkor b felbonthatatlan. Valóban, ellenkező esetben b -nek van c valódi osztója ($c|b, |c| < |b|$) és $c|a, |c| < |b|$ ellentmondás. $\square$

6.2. A prímszámok tulajdonságai

Tétel. Végtelen sok prímszám van.

Első bizonyítás. Megmutatjuk, hogy minden $n \in \mathbb{N}$ számnál van nagyobb prímszám. Feltehetjük, hogy $n \geq 3$. Legyen $N = n! - 1 > 1$, így N -nek van legalább egy p prímosztója az előző Tétel szerint. Itt $p > n$, mert ha $p \leq n$ lenne, akkor $p|n!$, ami ellentmondás. $\square$

Második bizonyítás. (Euklidész) Tegyük fel, hogy állításunk nem igaz, tehát véges sok prímszám létezik és legyenek ezek: $p_1, p_2, \dots, p_k$. Tekintsük az $A = p_1 p_2 \dots p_k + 1$ számot, amelynek az előző Tétel szerint van egy q prímosztója. A feltevés szerint $q = p_i$ valamely i -re, hiszen csak a $p_1, p_2, \dots, p_k$ prímek léteznek és következik, hogy $p_i|1$, ami ellentmondás. $\square$

$\star$ **Harmadik bizonyítás.** Tekintsük az $F_n = 2^{2^n} + 1, n \geq 0$ számsorozatot. Minden F_n számnak létezik egy q_n prímosztója. Láttuk (5.1. szakasz), hogy az $F_n = 2^{2^n} + 1$ sorozat tagjai páronként relatív prímek. Így a q_n prímszámok páronként különbözők, tehát $q_1, q_2, \dots$ prímszámok végtelen sorozata. $\square \star$

Tétel. Ha $n \in \mathbb{N}$ összetett szám, akkor van $\sqrt{n}$ -nél kisebb vagy ezzel egyenlő prímosztója.

Bizonyítás. Az n számnak léteznek pozitív prímosztói (Tétel) és legyen p a legkisebb ezek közül. Így $n = pn_1$ és $p \leq n_1$. Kapjuk, hogy $p^2 \leq pn_1 = n$, ahonnan $p \leq \sqrt{n}$. $\square$

Így egy adott n számról úgy dönthető el, hogy prímszám vagy sem, hogy megnézzük osztható-e egy $p \leq \sqrt{n}$ prímszámmal. Ha igen, akkor n összetett, ha nem, akkor n biztosan prímszám. Például $n = 401$ esetén $\sqrt{n} < 21$, s mivel 401 nem osztható a 21-nél kisebb prímekekkel, következik, hogy 401 prímszám.

A következő eljárás, az úgynevezett **eratoszteni szita**, arra szolgál, hogy meghatározzuk a prímekeket egy adott N számig. A $2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \dots, N$ sorozat első tagja, a 2 prím és húzzuk ki (szitáljuk ki) a 2 többi többszörösét, amelyek nem prímek. Az első megmaradt szám, a 3 prím és kiszitáljuk a 6, 9, 12, ... számokat, amelyek nem prímek (vannak olyan számok, például a 6, amelyek már az első szitálásnál kiestek). Az első megmaradt szám, az 5 ismét prím és kiszitáljuk az 5 többszörösöit: a 10, 15, ... számokat, stb. Az előző Tétel szerint a szitálást elegendő a $p \leq \sqrt{N}$ prímekekkel végezni és a megmaradt számok lesznek a keresett prímek:

$$2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, \dots, N$$

$\blacktriangledown$ **Feladat** Döntsük el, hogy prímszám-e 847 és 1037.

A 2 az egyedüli páros prímszám, a többi prím $4k - 1$ alakú (3, 7, 11, 19, ...) vagy $4k + 1$ alakú (5, 13, 17, 29, ...).

Tétel. Végtelen sok $4k - 1$ alakú prím létezik és végtelen sok $4k + 1$ alakú prím létezik.

Bizonyítás. Az euklidészi bizonyításhoz hasonlóan tegyük fel, hogy véges sok $4k - 1$ alakú prím létezik: $p_1, p_2, \dots, p_r$. Legyen $B = 4p_1 p_2 \dots p_r - 1$. Azonnali, hogy $2 \nmid B$ és

$p_1 \nmid B, p_2 \nmid B, \dots, p_r \nmid B$. Következik, hogy B -nek minden prímosztója $4k+1$ alakú, de akkor B maga is $4k+1$ alakú és ez ellentmondás.

A második állítás hasonlóképpen igazolható, de további előismeretek szükségesek hozzá. $\square$

Megjegyzés. Igazolható az is, hogy végtelen sok $6k-1$ alakú és végtelen sok $6k+1$ alakú prímszám létezik. Mindezeknél általánosabb a következő nevezetes tétel:

Ha $a, b \in \mathbb{N}$, $(a, b) = 1$, akkor az $a+b, 2a+b, 3a+b, \dots$ számtani sorozat tagjai között végtelen sok prímszám van (Dirichlet).

A következő tétel arra mutat rá, hogy az egymásutáni prímszámok közötti különbség tetszőlegesen nagy lehet.

Tétel. Minden $n \in \mathbb{N}^*$ számhoz megadható n egymásutáni összetett szám.

Bizonyítás. Legyen $a_k = (n+1)! + k + 1$, ahol $k \in \{1, 2, \dots, n\}$. Ezek egymásutáni számok és mindegyik összetett, hiszen $k+1 \mid a_k$ és $a_k > k+1$ minden $k \in \{1, 2, \dots, n\}$ esetén. $\square$

Megjegyzés. Ez a tétel nem jelenti azt, hogy nagy számokat vizsgálva a prímek egyre ritkábban fordulnak elő. Léteznek olyan prímszámok, melyek különbsége 2. Ilyen prímek, úgynevezett **ikerprímek**, például a következők: $(3, 5), (5, 7), (11, 13), (17, 19), \dots$. A prímszámtan egy nevezetes, mindmáig megoldatlan kérdése az, hogy létezik-e végtelen sok ikerprím páros.

▼ **Feladat.** Ha $k \in \mathbb{N}^*$ és $2^k + 1$ prímszám, akkor létezik $n \in \mathbb{N}$ úgy, hogy $k = 2^n$.

Megoldás. Ha $k = 2^n m$, ahol m páratlan, akkor $2^k + 1 = (2^{2^n})^m + 1$ osztható $2^{2^n} + 1$ -gyel (lásd 4.1. szakasz, Tétel) és így következik, hogy $2^{2^n} + 1 = 2^k + 1$, ahonnan $m = 1$.

Az $F_n = 2^{2^n} + 1, n \in \mathbb{N}$ számokat (lásd 5.1. és 6.2. szakaszok) **Fermat-számoknak**, az ilyen alakú prímekeket pedig **Fermat-prímeknek** nevezzük. Fermat azt sejtette, hogy az F_n számok mind prímek. Nos, $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ prímek, F_5 viszont nem prím, osztható 641-gyel (ezt először Euler igazolta). Következik az is, hogy az előző Feladat állításának a megfordítása nem igaz. Nem tudjuk, hogy léteznek-e további Fermat-prímek.

▼ **Feladat.** Ha $n \in \mathbb{N}$ és $2^n - 1$ prímszám, akkor n prímszám.

Megoldás. Ha n nem prím, akkor n felírható $n = ab$ alakban, ahol $a, b > 1$. Így $2^n - 1 = (2^a)^b - 1$ osztható $(2^a - 1)$ -gyel, lásd 4.1. szakasz, és $2^a - 1 \neq 1, \frac{2^n - 1}{2^a - 1} \neq 1$ a feltétel miatt, ami ellentmondás.

Az $M_p = 2^p - 1$ alakú számokat, ahol p prím, **Mersenne-számoknak** nevezzük. Az $M_p = 2^p - 1$ alakú prímszámokat, ahol p prím, **Mersenne-prímeknek** nevezzük. Itt $M_2 = 3, M_3 = 7, M_5 = 31$, stb. $M_{11} = 2^{11} - 1 = 23 \cdot 89$ nem prím, tehát a Feladatbeli fordított állítás nem igaz. Jelenleg (2005. szeptember) 42 Mersenne-prím ismert. Nem tudjuk, hogy általában mely M_p számok a prímek és nem tudjuk, hogy van-e végtelen sok Mersenne-féle prímszám.

Feladatok

▼ 1. Lehet-e $8^n + 1$ prímszám, ahol $n \geq 0$?

Megoldás. Nem! Ugyanis $8^n + 1 = (2^n)^3 + 1$ osztható $2^n + 1$ -gyel, így $8^n + 1$ minden n -re összetett szám.

▼ 2. Egy tízes alapú számrendszerben felírt prímszám minden számjegye 1. Igazoljuk, hogy a számjegyek száma prímszám. Igaz-e a fordított állítás?

Megoldás. Ha az 1-esek száma k , akkor $n = 11\dots 11_{(10)} = 10^{k-1} + 10^{k-2} + \dots + 10^2 + 10 + 1 = \frac{10^k - 1}{9}$. Feltételezve, hogy k összetett, $k = ab$ alakú, ahol $a > 1, b > 1$ és $n = \frac{(10^a)^b - 1}{9} = \frac{10^a - 1}{9}((10^a)^{b-1} + (10^a)^{b-2} + \dots + 10 + 1)$. Itt $\frac{10^a - 1}{9}$ egész szám és 1-nél

nagyobb, mert $a > 1$. Ugyanakkor $(10^a)^{b-1} + (10^a)^{b-2} + \dots + 10 + 1$ is egész szám és 1-nél nagyobb, mert $b > 1$. Így n összetett szám, ami ellentmond annak, hogy n prím.

Fordítva nem igaz, mert például $k = 3$ prím, de 111 nem prím, hiszen osztható 3-mal.

▼ 3. Ha p prím, akkor lehet-e $p^2 + 2$ is prím?

Megoldás. Ha $p \geq 5$, akkor p vagy $6k + 1$ alakú vagy $6k - 1$ alakú, ahol $k \geq 1$. Így $p^2 + 2 = (6k \pm 1)^2 + 2 = 36k^2 \pm 12k + 1 + 2 = 3(12k^2 \pm 4k + 1)$ osztható 3-mal 3-nál nagyobb, tehát $p^2 + 2$ nem prím.

$p = 2$ -re $p^2 + 2 = 4 + 2 = 6$ nem prím, $p = 3$ -ra $p^2 + 2 = 9 + 2 = 11$ prímszám.

▼ 4. Igazoljuk, hogy végtelen sok $6k - 1$ alakú prímszám van.

Megoldás. Tegyük fel, hogy véges sok $6k - 1$ alakú prím létezik: $p_1, p_2, \dots, p_r$. Legyen $N = 6p_1 p_2 \dots p_r - 1$. Azonnali, hogy $2 \nmid N$ és $p_1 \nmid N, p_2 \nmid N, \dots, p_r \nmid N$. Következik, hogy N -nek minden prímosztója $6k + 1$ alakú, de akkor N maga is $6k + 1$ alakú, s ez ellentmondás.

▼ 5. Ha $p, q \geq 5$ ikerprímek, akkor $12 \mid p + q$.

Megoldás. 6-tal osztva minden $p > 3$ prímszám $6k + 1$ vagy $6k + 5$ alakú ($6k, 6k + 2, 6k + 3$ vagy $6k + 4$ nem lehet, mert ezek biztos összetettek). A $6k + 5$ alakú számok helyett tekinthetjük a $6k - 1$ alakúakat.

Ha $p, q \geq 5$ ikerprímek, akkor így $p = 6k - 1$ és $q = 6k + 1$ alakú, ugyanazzal a k -val. Innen azonnali, hogy $p + q = 12k$ osztható 12-vel.

▼ 6. Lehetnek-e $2^n - 1$ és $2^n + 1$ ikerprímek, ahol $n \geq 1$?

Megoldás. Ha $2^n - 1$ prím, akkor n prím, ha pedig $2^n + 1$ prím, akkor $n = 2^k$ alakú, lásd korábbi Feladatok. Tehát ikerprímeket csak $n = 2$ -re kapunk és ezek a 3, 5.

Másképp: Ha $n = 1$, akkor 1, 3 nem ikerprímek, $n = 2$ -re 3, 5 ikerprímek. Ha $n \geq 3$, akkor $p = 2^n - 1, q = 2^n + 1 \geq 7$ és összegük $p + q = 2^{n+1}$ nem osztható 12-vel. Ezért az előző Feladat alapján nem lehetnek ikerprímek.

▼ 7. Lehet-e a $p, p + 2, p + 4$ számok mindegyike prímszám?

Megoldás. Ha $p = 3k + 1$ alakú, $k \geq 1$, akkor $p + 2 = 3k + 3$ nagyobb mint 3 és osztható 3-mal, tehát nem prím.

Ha $p = 3k - 1$ alakú, $k \geq 1$, akkor $p + 4 = 3k + 3$ nagyobb mint 3 és osztható 3-mal, tehát nem prím.

Marad a $p = 3$, amelyre 3, 5, 7 mind prímek, ezek az egyedüli "hármassikrek".

7. A számelmélet alaptétele

Tétel. (A számelmélet alaptétele) Minden $a \in \mathbb{Z} \setminus \{-1, 0, 1\}$ szám felírható véges sok felbonthatatlan szám (prímszám) szorzataként és ez a felírás lényegében (a sorrendtől és az egységtényezőktől eltekintve) egyértelmű.

Bizonyítás. I. Felbonthatóság. Feltehetjük, hogy $a > 1$ és hogy a felbontásban szereplő tényezők is pozitívak. Ha a felbonthatatlan, akkor $a = a$ egytényezős szorzat. Ha a nem felbonthatatlan, akkor a 6.1. szakasz utolsó Tétele szerint a -nak van p_1 felbonthatatlan valódi osztója és $a = p_1 a_1$ alakba írható. Ha most a_1 felbonthatatlan, akkor készen vagyunk, ha nem, akkor az előbbi tétel szerint a_1 -nek van p_2 felbonthatatlan valódi osztója és $a_1 = p_2 a_2$, azaz $a = p_1 p_2 a_2$. Hasonlóan folytatjuk az eljárást a_2 -vel. Véges sok lépésen belül egy $a_k = p_k$ felbonthatatlan számot kapunk, hiszen $a > a_1 > a_2 > \dots$ pozitív számokból álló szigorúan csökkenő sorozat és az $a = p_1 p_2 \dots p_k$ felbontáshoz jutunk.

II. Egyértelműség. Tegyük fel, hogy $a > 1$ két különböző módon is felbontható:

$$a = p_1 p_2 \dots p_k \quad \text{és} \quad a = q_1 q_2 \dots q_\ell,$$

ahol p_i és q_j pozitív felbonthatatlan számok (prímszámok), $i \in \{1, 2, \dots, k\}$, $j \in \{1, 2, \dots, \ell\}$. Innen

$$p_1 p_2 \dots p_k = q_1 q_2 \dots q_\ell.$$

Ha $p_i = q_j$ valamely i, j -kre, akkor egyszerűsíthetünk velük és feltehetjük, hogy egyszerűsítés után

$$p_1 p_2 \dots p_r = q_1 (q_2 \dots q_s),$$

ahol $p_i \neq q_j$ minden i, j -re és $r, s \geq 2$ (ha $r = 1$, akkor $p_1 = q_1 q_2 \dots q_s$ felbonthatatlan, ezért $s = 1$ kell legyen és $p_1 = q_1$, ellentmondás). Kapjuk, hogy $p_1 | q_1 (q_2 \dots q_s)$, ahonnan felhasználva, hogy p_1 prímtulajdonságú $p_1 | q_1$ vagy $p_1 | q_2 \dots q_s$ következik. Az első esetben $p_1 = q_1$ adódik, ami ellentmondás, második esetben pedig $p_1 | q_2$ vagy $p_1 | q_3 \dots q_s$ és ugyanígy folytatva $p_1 | q_s$, azaz $p_1 = q_s$, ami ellentmondás. $\square$

★ **Megjegyzés.** Ez a tétel triviálisnak tűnik, de nem mindig igaz általánosabb struktúrákban. Például, a $(\mathbb{Z}[i\sqrt{5}], +, \cdot)$ gyűrűben, lásd 6.1. szakasz, $6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ kétféleképpen is felbontható, vagy a páros egész számok $(2\mathbb{Z}, +, \cdot)$ gyűrűjében 2, 6, 10, 30 felbonthatatlan számok, a 60 összetett és kétféleképpen is felbontható: $60 = 2 \cdot 30 = 6 \cdot 10$. $\square$ ★

Egy $n \in \mathbb{N}$, $n > 1$ szám prímtenyezős felbontásában ugyanaz a prímszám többször is szerepelhet, így n a következő alakban írható:

$$(*) \quad n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r},$$

ahol $p_1, p_2, \dots, p_r$ különböző prímszámok és $a_1, a_2, \dots, a_r \geq 1$ egészek, amelyet n **kanonikus alakjának** nevezünk.

Az n szám kanonikus alakját úgy kapjuk meg, hogy megnézzük osztható-e n a 2, 3, 5, 7, 11, ... prímek valamelyikével. Ha igen, akkor elvégezzük az osztást, majd a hányadost tovább osztjuk a 2, 3, 5, 7, 11, ... prímeikkel, addig amíg hányadosul prímszámot nem kapunk.

Példa. • Írjuk fel 72, 1800 és 19649 kanonikus alakját:

$$72 = 2^3 \cdot 3^2, \quad 1800 = 2^3 \cdot 3^2 \cdot 5^2.$$

19649 nem osztható a 2, 3, 5 prímeikkel, osztható viszont 7-tel: $19649 = 7 \cdot 2807$. Az eredeti szám nem volt osztható 2, 3, 5-tel, így 2807 sem osztható ezekkel, de $7 | 2807$:

$2807 = 7 \cdot 401$ és $19649 = 7^2 \cdot 401$. Most nézzük a 401-et, ez nem osztható 2, 3, 5, 7-tel és nem osztható a soron következő 11, 13, 17, 19 prímekekkel sem. Tovább nem is kell folytatnunk, következik, hogy 401 prímszám, mert $\sqrt{401} < 21$, lásd korábbi Tételt és 19649 kanonikus alakja $19649 = 7^2 \cdot 401$.

Tétel. Legyen az $n > 1$ egész szám kanonikus alakja a fenti (*) és $d \in \mathbb{N}$. A d akkor és csak akkor osztója n -nek, ha d kanonikus alakja

$$d = p_1^{b_1} p_2^{b_2} \dots p_r^{b_r},$$

ahol $b_i \in \mathbb{N}, 0 \leq b_i \leq a_i, i \in \{1, 2, \dots, r\}$. Továbbá n pozitív osztóinak száma

$$\tau(n) = (a_1 + 1)(a_2 + 1) \dots (a_r + 1).$$

Bizonyítás. Ha $d|n$, akkor $n = dq$, így d kanonikus alakjában csak a p_i prímekek szerepelhetnek és legfeljebb a_i -hatványon, $i \in \{1, 2, \dots, r\}$, tehát d kanonikus alakja a megadott.

Fordítva, ha d kanonikus alakja a fenti, akkor a

$$q = p_1^{a_1-b_1} p_2^{a_2-b_2} \dots p_r^{a_r-b_r}$$

jelöléssel $n = dq$, s mivel $b_i \leq a_i$, kapjuk, hogy $a_i - b_i \geq 0$, tehát q egész szám, azaz $d|n$.

Ahhoz, hogy n összes pozitív osztóit megkapjuk a b_i kitevőket egymástól függetlenül, $(a_i + 1)$ -féleképpen választhatjuk meg, így $\tau(n)$ a számok szorzata. $\square$

Néha előnyös, ha megengedjük, hogy egy szám kanonikus alakjában bizonyos kitevők nullával is egyenlők lehessenek. Két szám lnko-jának és lkkt-jének kiszámítására vonatkozik az alábbi tétel, melynek bizonyítása azonnali az előző Tétel és az definíciók alapján.

Tétel. Ha az $n, m \in \mathbb{N}, n, m > 1$ számok kanonikus alakja

$$n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}, \quad m = p_1^{b_1} p_2^{b_2} \dots p_r^{b_r},$$

ahol $a_i, b_i \geq 0, i \in \{1, 2, \dots, r\}$ akkor n és m lnko-jának és lkkt-jének kanonikus alakja

$$(n, m) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \dots p_r^{\min(a_r, b_r)},$$

$$[n, m] = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \dots p_r^{\max(a_r, b_r)}. \quad \square$$

Példa. • Határozzuk meg a következő számok lnko-ját és lkkt-jét:

i) 72 és 54,

ii) 1819 és 3587.

iii) 12, 42, 360.

Megoldás. i) $72 = 2^3 \cdot 3^2$, $54 = 2 \cdot 3^3$, ahonnan $(72, 54) = 2 \cdot 3^2 = 18$ és $[72, 54] = 2^3 \cdot 3^3 = 8 \cdot 27 = 216$.

ii) (lásd még 5. fejezet) $1819 = 17 \cdot 107$, $3587 = 17 \cdot 211$, ahonnan $(1819, 3587) = 17$ és $[1819, 3587] = 17 \cdot 107 \cdot 211 = 383809$.

iii) $12 = 2^2 \cdot 3$, $42 = 2 \cdot 3 \cdot 7$, $360 = 2^3 \cdot 3^2 \cdot 5$ és $(12, 42, 360) = 2 \cdot 3 = 6$, $[12, 42, 360] = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520$.

Megjegyzés. Figyeljük meg, hogy $(n, m)[n, m] = nm$ (ezt láttuk már korábban is) és ha n és m relatív prímelek, azaz ha $(n, m) = 1$, akkor $[n, m] = nm$. $\square$

Feladatok

- ▼ 1. Írjuk fel 72 és $2^5 \cdot 3^4 \cdot 7^3 \cdot 11^{11}$ pozitív osztóit és határozzuk meg ezek számát.
- ▼ 2. Határozzuk meg azt a legkisebb n számot és az összes olyan n számot, amelyre $\tau(n) = 9$.
- ▼ 3. Határozzuk meg n -et úgy, hogy $\tau(n)$ páratlan szám legyen.
- ▼ 4. Igazoljuk, hogy minden $n \geq 2$ esetén
 - a) Ha d befutja n pozitív osztóit, akkor n/d is befutja ezeket (fordított sorrendben).
 - b) $\prod_{d|n} d = n^{\frac{\tau(n)}{2}}$,
 - c) $\tau(n) \leq 2\sqrt{n}$.
- ▼ 5. Ha $n, m \in \mathbb{N}$, $(n, m) = 1$ és $d|nm$, akkor $d = n'm'$ alakba írható, ahol $n'|n$, $m'|m$ és d -nek ez az előállítása egyértelmű.

8. Kongruenciák

8.1. Kongruenciák értelmezése és alaptulajdonságai

Azt mondjuk, hogy az a és b egész számok **kongruensek** az $m \in \mathbb{Z}$ számra nézve, vagy a kongruens b -vel modulo m , ha $m|a-b$, jelölés: $a \equiv b \pmod{m}$. Ellenkező esetben azt mondjuk, hogy a és b **inkongruensek** (nem kongruensek) modulo m , jelölés: $a \not\equiv b \pmod{m}$. Az m számot a kongruencia **modulusának** nevezzük.

Példák • $9 \equiv 2 \pmod{7}$, $-11 \equiv 4 \pmod{5}$, $8 \not\equiv 3 \pmod{4}$.

Az $a \equiv 0 \pmod{m}$ akkor teljesül ha $m|a$. Ha $m = 0$, akkor $a \equiv b \pmod{0}$ azt jelenti, hogy $a = b$, míg $a \equiv b \pmod{m}$ akkor és csak akkor igaz ha $a \equiv b \pmod{-m}$, így a kongruenciák vizsgálatakor elegendő pozitív modulusokat tekinteni.

Ezt a jelölést, amely leegyszerűsíti sok oszthatósági probléma tárgyalását, Gauss vezette be. Nézzük a kongruenciák alaptulajdonságait:

Tétel. Legyenek $a, b, m \in \mathbb{Z}, m \geq 1$. Az $a \equiv b \pmod{m}$ akkor és csak akkor teljesül ha a és b m -mel osztva ugyanazt a maradékot adja.

Bizonyítás. Legyen $a = mq + r, b = mq' + r'$, ahol $0 \leq r < m, 0 \leq r' < m$. Ha $a \equiv b \pmod{m}$, akkor $m|a-b = m(q-q') + (r-r')$ és így $m|r-r'$. De $0 \leq |r-r'| < m$, s következik, hogy $r = r'$.

Ha $r = r'$, akkor azonnali, hogy $m|a-b$, azaz $a \equiv b \pmod{m}$. $\square$

Tétel. A kongruencia $\pmod{m}$ ekvivalenciareláció, azaz reflexív, szimmetrikus és tranzitív.

Bizonyítás. Azonnal következik a definícióból, például a tranzitivitás: ha $a \equiv b \pmod{m}$ és $b \equiv c \pmod{m}$, akkor $m|a-b$ és $m|b-c$, ahonnan $m|(a-b) + (b-c) = a-c$, tehát $a \equiv c \pmod{m}$. $\square$

Ha $a \in \mathbb{Z}$, akkor az a -val kongruens $\pmod{m}$ egész számok halmazát az a által reprezentált $\pmod{m}$ **maradékosztály**nak nevezzük, jelölés $\hat{a}$, így

$$\hat{a} = \{b \in \mathbb{Z} : b \equiv a \pmod{m}\} = \{\dots, a-2m, a-m, a, a+m, a+2m, \dots\}.$$

A $\pmod{m}$ maradékosztályok a következők:

$$\begin{aligned}\hat{0} &:= \{\dots, -2m, -m, 0, m, 2m, \dots\}, \\ \hat{1} &:= \{\dots, -2m+1, -m+1, 1, m+1, 2m+1, \dots\}, \\ \hat{2} &:= \{\dots, -2m+2, -m+2, 2, m+2, 2m+2, \dots\}, \\ &\dots\dots\dots \\ \widehat{m-1} &:= \{\dots, -m-1, -1, m-1, 2m-1, \dots\}.\end{aligned}$$

Ezek a $\equiv \pmod{m}$ ekvivalenciarelációhoz tartozó ekvivalenciaosztályok. A $\pmod{m}$ **maradékosztályok halmaza**:

$$\mathbb{Z}_m := \{\hat{0}, \hat{1}, \hat{2}, \dots, \widehat{m-1}\}.$$

Feladat ▼ Adjuk meg a $\pmod{m}$ maradékosztályokat, ha $1 \leq m \leq 6$.

Tétel. (Műveleti tulajdonságok) Legyenek $a, b, c, d \in \mathbb{Z}$ és $m, m_1, m_2, k \in \mathbb{N}^*$.

i) Ha $a \equiv b \pmod{m}$ és $c \equiv d \pmod{m}$, akkor $a+c \equiv b+d \pmod{m}$ és $ac \equiv bd \pmod{m}$, tehát azonos modulusú kongruenciákat össze lehet adni és össze lehet szorozni;

ii) Ha $a \equiv b \pmod{m}$, akkor $a+c \equiv b+c \pmod{m}$ és $ac \equiv bc \pmod{m}$, tehát egy kongruencia mindkét oldalához hozzá lehet adni ugyanazt a számot és a kongruencia mindkét oldalát szorozni lehet ugyanazzal a számmal;

- iii) Ha $a \equiv b \pmod{m}$, akkor $a^k \equiv b^k \pmod{m}$, kongruenciát lehet hatványozni;
- iv) Ha $ac \equiv bc \pmod{m}$, akkor $a \equiv b \pmod{\frac{m}{d}}$, ahol $c \neq 0$ és $d = (c, m)$;
- v) Ha $ac \equiv bc \pmod{m}$ és $(c, m) = 1$, akkor $a \equiv b \pmod{m}$, kongruenciát lehet egyszerűsíteni egy, a modulussal relatív prím számmal és a modulus nem változik;
- vi) Ha $a \equiv b \pmod{m_1}$ és $a \equiv b \pmod{m_2}$, akkor $a \equiv b \pmod{[m_1, m_2]}$.
- vii) Ha $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$ és m_1, m_2 relatív prímek, akkor $a \equiv b \pmod{m_1 m_2}$.

Bizonyítás. i) A feltétel szerint $m|a-b$ és $m|c-d$, ahonnan $m|(a-b) + (c-d) = (a+c) - (b+d)$, tehát $a+c \equiv b+d \pmod{m}$, valamint $m|c(a-b) + b(c-d) = ac - bd$, azaz $ac \equiv bd \pmod{m}$.

ii) Speciális esete i)-nek, ahol $d = c$.

iii) Az i) ismételt alkalmazásával ($c = a, d = b$), ha $a \equiv b \pmod{m}$, akkor $a^2 \equiv b^2 \pmod{m}, \dots, a^k \equiv b^k \pmod{m}$. Abból is következik, hogy minden $k \in \mathbb{N}$ számra $a-b | a^k - b^k$, lásd Tétel.

iv) A feltétel szerint $m|ac - bc = (a-b)c$, így $\frac{m}{d} | (a-b) \frac{c}{d}$. Itt $(\frac{m}{d}, \frac{c}{d}) = 1$ és kapjuk, hogy $\frac{m}{d} | a-b$, azaz $a \equiv b \pmod{\frac{m}{d}}$, lásd Tétel.

v) Az előző pont speciális esete, ha $d = (c, m) = 1$.

vi) Ha $a \equiv b \pmod{m_1}$ és $a \equiv b \pmod{m_2}$, akkor $m_1 | a-b$ és $m_2 | a-b$, tehát $a-b$ közös többszöröse az m_1 és m_2 számoknak, s így $a-b$ többszöröse az $[m_1, m_2]$ lkkt-nek (az lkkt definíciója szerint).

vii) Speciális esete vi)-nak: ha $(m_1, m_2) = 1$, akkor $[m_1, m_2] = m_1 m_2$. $\square$

Figyeljük meg a hasonlóságot a kongruenciák és az egyenlőség ($=$) műveleti tulajdonságai között. Felhívjuk a figyelmet a iv) és v) tulajdonságokra: például a $12 \equiv 18 \pmod{6}$ kongruenciát 3-mal "egyszerűsítve", $4 \equiv 6 \pmod{6}$ -ot kapunk, ami nem igaz, csak $4 \equiv 6 \pmod{2}$ következik.

Példák. • 1. A fenti tulajdonságok illusztrálásaként igazoljuk, hogy $641 | F_5 = 2^{2^5} + 1$.

Valóban, $641 = 640 + 1 = 5 \cdot 2^7 + 1$, így $5 \cdot 2^7 \equiv -1 \pmod{641}$, s ezt negyedik hatványra emelve: $5^4 \cdot 2^{28} \equiv 1 \pmod{641}$. Másrészt, $641 = 625 + 16 = 5^4 + 2^4$, ahonnan $2^4 \equiv -5^4 \pmod{641}$. Összeszorozva ez utóbbi két kongruenciát $5^4 \cdot 2^{32} \equiv -5^4 \pmod{641}$, s osztva 5^4 -nel, ahol $(5^4, 641) = 1$, kapjuk, hogy $2^{32} + 1 = 2^{2^5} + 1 \equiv 0 \pmod{641}$, lásd Fermat-számok a 6.2. szakaszban.

• 2. Ha f egy egész együtthatós polinom és $x \equiv y \pmod{m}$, akkor $f(x) \equiv f(y) \pmod{m}$.

Valóban, legyen $f = a_0 X^n + a_1 X^{n-1} + \dots + a_{n-1} X + a_n$. Mivel $x \equiv y \pmod{m}$, kapjuk, hogy $x^k \equiv y^k \pmod{m}$ minden $k \in \{0, 1, 2, \dots, n\}$ -re és összegezve $f(x) \equiv f(y) \pmod{m}$.

• 3. Vezessük le a 11-re vonatkozó következő oszthatósági szabályt. Egy tízes számrendszerbeli szám akkor osztható 11-gyel ha a páratlan helyein álló számjegyek összegéből kivonva a páros helyeken álló számjegyek összegét 11-gyel osztható számot kapunk. Legyen

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

egy adott szám. Mivel $10 \equiv -1 \pmod{11}$, kapjuk, hogy $10^i \equiv (-1)^i \pmod{11}$, s innen

$$n = \sum_{i=0}^k a_{k-i} 10^i \equiv \sum_{i=0}^k (-1)^i a_i \pmod{11}.$$

8.2. Teljes maradékrendszerek és redukált maradékrendszerek

Az egész számok egy T rendszere **teljes maradékrendszer** $(\text{mod } m)$, ha minden $x \in \mathbb{Z}$ esetén létezik egy és csak egy T -beli a szám úgy, hogy $x \equiv a \pmod{m}$. Következik, hogy ha T teljes maradékrendszer $(\text{mod } m)$, akkor T tartalmaz egy és csak egy elemet minden maradékosztályból $(\text{mod } m)$. Így

Tétel. Az egész számok egy T rendszere akkor és csak akkor teljes maradékrendszer $(\text{mod } m)$, ha T elemeinek a száma m és ezek páronként inkongruensek $(\text{mod } m)$. $\square$

Teljes maradékrendszer $(\text{mod } m)$ például a $0, 1, 2, \dots, m-1$, ennek neve **legkisebb nemnegatív teljes maradékrendszer** $(\text{mod } m)$ és a következő, **legkisebb abszolútértékű teljes maradékrendszer** $(\text{mod } m)$, amely $-\frac{m-1}{2}, \dots, -2, -1, 0, 1, 2, \dots, \frac{m-1}{2}$, ha m páratlan és $-(\frac{m}{2}-1), \dots, -2, -1, 0, 1, 2, \dots, \frac{m}{2}-1, \frac{m}{2}$, ha m páros.

Gyakran használjuk a következő tulajdonságot:

Tétel. Ha $r_1, r_2, \dots, r_m$ egy teljes maradékrendszer $(\text{mod } m)$ és $a, b \in \mathbb{Z}, (a, m) = 1$, akkor $ar_1 + b, ar_2 + b, \dots, ar_m + b$ is teljes maradékrendszer $(\text{mod } m)$.

Bizonyítás. Azt kell igazolnunk, hogy az $ar_i + b$ számok páronként inkongruensek $(\text{mod } m)$. Valóban, ha $ar_i + b \equiv ar_j + b \pmod{m}$, akkor $a(r_i - r_j) \equiv 0 \pmod{m}$, de $(a, m) = 1$, így $r_i - r_j \equiv 0 \pmod{m}$, azaz $r_i \equiv r_j \pmod{m}$, ahonnan $r_i = r_j$. $\square$

Tétel. Ha $a, b \in \mathbb{Z}, (a, m) = 1$, akkor minden teljes maradékrendszernek $(\text{mod } m)$ létezik egy és csak egy x eleme úgy, hogy $ax \equiv b \pmod{m}$.

Bizonyítás. Ha $r_1, r_2, \dots, r_m$ teljes maradékrendszer $(\text{mod } m)$, akkor az előző Tétel szerint $ar_1 - b, ar_2 - b, \dots, ar_m - b$ is teljes maradékrendszer $(\text{mod } m)$, tehát létezik egy és csak egy $x = r_i$ elem úgy, hogy $ar_i - b \equiv 0 \pmod{m}$, amit bizonyítanunk kellett. $\square$

Tétel. Ha $a \equiv b \pmod{m}$, akkor $(a, m) = (b, m)$.

Bizonyítás. Feltétel szerint $m|a-b$, azaz $a-b = km$, ahol $k \in \mathbb{Z}$. Így, mivel $(a, m)|a$ és $(a, m)|m$, következik, hogy $(a, m)|b$, tehát (a, m) közös osztója b -nek és m -nek, ahonnan $(a, m)|(b, m)$, lásd a lko második definícióját (5.1. szakasz). Hasonlóképpen kapjuk, hogy $(b, m)|(a, m)$, s így $(a, m) = (b, m)$. $\square$

Az $\hat{a} \pmod{m}$ maradékosztály neve **redukált maradékosztály** $(\text{mod } m)$, ha $(a, m) = 1$. Az előző Tétel szerint ez az definíció nem függ a reprezentáns megválasztásától.

A $(\text{mod } m)$ redukált maradékosztályok számát $\phi(m)$ -mel jelöljük, ez az **Euler-függvény**.

Példa. • $m = 12$ esetén a $(\text{mod } 12)$ redukált maradékosztályok: $\hat{1}, \hat{5}, \hat{7}, \hat{11}$ és ezek száma $\phi(12) = 4$.

$\phi(m)$ azoknak a számoknak a száma $(\text{mod } m)$, amelyek m -hez relatív prímek. A legkisebb nemnegatív teljes maradékrendszert tekintve így $\phi(m)$ azoknak az x számoknak a száma, amelyekre $0 \leq x \leq m-1$ és $(x, m) = 1$.

Feladat. ▼ Mennyi $\phi(6), \phi(7), \phi(24)$?

Igazolható, hogy ha n kanonikus alakja $n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$, akkor

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right).$$

Az egész számok egy R rendszere **redukált maradékrendszer** $(\text{mod } m)$, ha minden $x \in \mathbb{Z}, (x, m) = 1$ szám esetén létezik egy és csak egy R -beli a szám úgy, hogy $x \equiv a \pmod{m}$. Következik, hogy R akkor redukált maradékrendszer $(\text{mod } m)$ ha R minden redukált maradékosztályból $(\text{mod } m)$ tartalmaz egy és csak egy elemet. Ez a következőképpen is megfogalmazható:

Tétel. Az egész számok egy R rendszere akkor és csak akkor redukált maradékrendszer $(\text{mod } m)$, ha

- i) R elemeinek a száma $\phi(m)$,
- ii) R elemei páronként inkongruensek $(\text{mod } m)$,
- iii) R minden eleme relatív prím m -hez. $\square$

Tétel. Ha $r_1, r_2, \dots, r_{\phi(m)}$ redukált maradékrendszer $(\text{mod } m)$ és $a \in \mathbb{Z}$, $(a, m) = 1$, akkor $ar_1, ar_2, \dots, ar_{\phi(m)}$ is redukált maradékrendszer $(\text{mod } m)$.

Bizonyítás. Alkalmazzuk az előző Tételt. Az ar_i elemek száma $\phi(m)$ és ezek páronként inkongruensek $(\text{mod } m)$. Valóban, ha $ar_i \equiv ar_j \pmod{m}$, akkor a -val osztva, ahol $(a, m) = 1$, kapjuk, hogy $r_i \equiv r_j \pmod{m}$, ahonnan $r_i = r_j$. Továbbá minden ar_i elem relatív prím m -mel, hiszen $(r_i, m) = 1$ és $(a, m) = 1$ alapján $(ar_i, m) = 1$. $\square$

Feladatok

▼ 1. Igazoljuk, hogy ha m páratlan, akkor $2, 4, 6, \dots, 2m$ teljes maradékrendszer $(\text{mod } m)$.

▼ 2. Igazoljuk, hogy ha $m > 2$, akkor $1^2, 2^2, 3^2, \dots, m^2$ nem teljes maradékrendszer $(\text{mod } m)$.

8.3. Az Euler, Fermat és Wilson tételek

Tétel. (Euler kongruencia tétele) Ha $a \in \mathbb{Z}$ és $(a, m) = 1$, akkor

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

Bizonyítás. Legyen $r_1, r_2, \dots, r_{\phi(m)}$ egy redukált maradékrendszer $(\text{mod } m)$. Tétel szerint akkor $ar_1, ar_2, \dots, ar_{\phi(m)}$ is redukált maradékrendszer $(\text{mod } m)$ és így minden ar_i -hez létezik egy és csak egy r_j úgy, hogy $ar_i \equiv r_j \pmod{m}$, továbbá különböző ar_i -khez különböző elemek tartoznak az eredeti redukált maradékrendszerből. Kapjuk, hogy $ar_1 \equiv s_1 \pmod{m}$, $ar_2 \equiv s_2 \pmod{m}$, $ar_{\phi(m)} \equiv s_{\phi(m)} \pmod{m}$, ahol $s_1, s_2, \dots, s_{\phi(m)}$ az $r_1, r_2, \dots, r_{\phi(m)}$ egy permutációja. Összeszorozva ezeket a kongruenciákat:

$$a^{\phi(m)} r_1 r_2 \dots r_{\phi(m)} \equiv r_1 r_2 \dots r_{\phi(m)} \pmod{m},$$

majd egyszerűsítve $r_1 r_2 \dots r_{\phi(m)}$ -hez, amely m -mel relatív prím, kapjuk, hogy $a^{\phi(m)} \equiv 1 \pmod{m}$. $\square$

Tétel. (Fermat kongruencia tétele vagy kis Fermat tétel)

- a) Ha p prímszám, $a \in \mathbb{Z}$ és $p \nmid a$, akkor $a^{p-1} \equiv 1 \pmod{p}$.
- b) Ha p prímszám és $a \in \mathbb{Z}$, akkor $a^p \equiv a \pmod{p}$.

Bizonyítás. a) Azonnal következik az Euler tételéből, ahol $m = p$ és $\phi(p) = p - 1$.

b) Ha $p \nmid a$, azaz ha $(a, p) = 1$, akkor az a) pont szerint $a^{p-1} \equiv 1 \pmod{p}$ és a -val szorozva $a^p \equiv a \pmod{p}$. Ha $p \mid a$, akkor $p \mid a^p$, így $p \mid a^p - a$, tehát a kongruencia ebben az esetben is igaz. $\square$

Példa. • Ha $n \in \mathbb{Z}$ nem osztható 11-gyel, akkor $n^5 - 1$ vagy $n^5 + 1$ osztható 11-gyel. Valóban, a Fermat-tétel szerint $(a = n, p = 11)$: $n^{10} \equiv 1 \pmod{11}$, ahonnan $11 \mid n^{10} - 1 = (n^5 - 1)(n^5 + 1)$ és mivel 11 prím, kapjuk, hogy $11 \mid n^5 - 1$ vagy $11 \mid n^5 + 1$.

A Fermat-tétel fordítottja nem igaz. Ha $a^n \equiv a \pmod{n}$ valamely $a \in \mathbb{Z}$ számra, akkor nem következik, hogy n prímszám.

Példa • Ha $a = 2$ és $n = 341 = 11 \cdot 31$, akkor $2^{341} \equiv 2 \pmod{341}$. Valóban, $2^{10} = 1024 \equiv 1 \pmod{11}$, közvetlen számítással vagy a Fermat tétel alapján, ahonnan $2^{340} \equiv 1 \pmod{11}$. Továbbá, $2^{10} = 1024 \equiv 1 \pmod{31}$, $2^{340} \equiv 1 \pmod{31}$ és kapjuk, hogy $2^{340} \equiv 1 \pmod{11 \cdot 31}$, tehát $2^{341} \equiv 2 \pmod{341}$.

Tétel. (Wilson-tétel) Ha p prímszám, akkor $(p-1)! \equiv -1 \pmod{p}$.

Bizonyítás. Ellenőrizhető, hogy a tétel igaz $p=2$ és $p=3$ esetén. Legyen $p > 3$ és $H = \{2, 3, 4, \dots, p-2\}$. Megmutatjuk, hogy minden $a \in H$ -ra létezik egy és csak egy $a' \in H$ úgy, hogy $a' \neq a$ és $aa' \equiv 1 \pmod{p}$. Valóban, tekintsük az $T = \{0, 1, 2, \dots, p-1\}$ legkisebb nemnegatív $\pmod{p}$ teljes maradékrendszert. A 8.2. szakasz harmadik Tétele szerint létezik egy és csak egy $x \in T$ úgy, hogy $ax \equiv 1 \pmod{p}$. Itt $x \neq 0, x \neq 1, x \neq p-1, x \neq a$. Ha például $x = a$ lenne, akkor $a^2 \equiv 1 \pmod{p}$, ahonnan $p \mid (a-1)(a+1)$, s mivel p prím kapjuk, hogy $p \mid a-1$ vagy $p \mid a+1$, ami ellentmondást jelent.

Ugyanakkor így különböző a értékekhez különböző a' értékek tartoznak és a H halmaz elemei párba állíthatók úgy, hogy minden párban az elemek szorzata 1-gyel kongruens $\pmod{p}$. Összeszorozva ezeket a kongruenciákat: $(p-2)! \equiv 1 \pmod{p}$ és innen $(p-1)! = (p-1)(p-2)! \equiv p-1 \equiv -1 \pmod{p}$. $\square$

Megjegyzés. Igaz a fordított állítás is: Ha $n \in \mathbb{N}$ és $(n-1)! \equiv -1 \pmod{n}$, akkor n prímszám. Valóban, ha n nem lenne prím, akkor létezne $k \mid n, 1 < k < n$. Az $n \mid (n-1)! + 1$ feltételből $k \mid (n-1)! + 1$ és mivel $k \leq n-1$, ezért $k \mid (n-1)!$, ahonnan $k \mid 1$, ami ellentmondás.

Feladatok

- ▼ 1. Igazoljuk, hogy $42 \mid n^7 - n$ minden $n \in \mathbb{N}$ esetén.
- ▼ 2. Ha $p > 3$ prím és $a \in \mathbb{Z}$, igazoljuk, hogy $a^p \equiv a \pmod{6p}$.
- ▼ 3. Mutassuk meg, hogy ha $p > 5$ prím, akkor minden 10-es alapú számrendszerben felírt, $p-1$ azonos számjegyből álló szám osztható p -vel.
- ▼ 4. Legyen $a \in \mathbb{Z}, n \in \mathbb{N}, (a, n) = 1$. Mutassuk meg, hogy $a^{(n-1)!} \equiv 1 \pmod{n}$.
- ▼ 5. Igazoljuk, hogy ha p prím, $n \in \mathbb{N}$ és $1 \leq n \leq p$, akkor $(p-n)!(n-1)! \equiv (-1)^n \pmod{p}$. (a Wilson-tétel általánosítása)
- ▼ 6. Igazoljuk, hogy

$$(n-1)! \equiv \begin{cases} -1, & \text{ha } n \text{ prím,} \\ 2, & \text{ha } n = 4, \\ 0, & \text{ha } n \geq 6 \text{ összetett szám.} \end{cases} \pmod{n}.$$

Megoldás. Legyen $n \geq 6$ összetett szám és tegyük fel, hogy $n = ab$, ahol $a, b > 1$ és $a \neq b$. Akkor az $(n-1)! = 1 \cdot 2 \cdot 3 \cdots (n-1)$ szorzat tényezői között szerepel a is és b is, s így $n = ab \mid (n-1)!$. Ha $n \geq 6$ összetett és n -nek nincs ilyen felírása, akkor $n = p^2$ alakú, ahol $p > 2$ prím. Most $(n-1)! = 1 \cdot 2 \cdot 3 \cdots (p^2-1)$ és a tényezők között van p is és $2p$ is, mivel $2p \leq p^2-1$, azaz $2p < p^2$, azaz $p > 2$, ami igaz.

8.4. Elsőfokú kongruenciák

Tekintsük az $f = a_0X^n + a_1X^{n-1} + \dots + a_{n-1}X + a_n$ egész együtthatós polinomot és az $f(x) \equiv 0 \pmod{m}$ kongruenciát, ahol $m \in \mathbb{N}^*$. Ezt **n -edfokú kongruenciának** nevezzük, ha $a_0 \not\equiv 0 \pmod{m}$, azaz, ha $m \nmid a_0$, s ennek **megoldása** minden olyan $x = x_0 \in \mathbb{Z}$ szám, melyre $f(x_0) \equiv 0 \pmod{m}$ fennáll.

Ha x_0 megoldás és $x \equiv x_0 \pmod{m}$, akkor x is megoldása az adott kongruenciának, hiszen $f(x) \equiv f(x_0) \equiv 0 \pmod{m}$, lásd 8.1. szakasz. Így, ha x_0 megoldás, akkor az $\widehat{x_0}$ maradékosztály $\pmod{m}$ minden eleme megoldás, tehát végtelen sok megoldás van. Ezért elegendő egy teljes maradékrendszer, például a legkisebb nemnegatív teljes maradékrendszer elemeit vizsgálni.

Példák. • A $3x^2 + 2x - 1 \equiv 0 \pmod{5}$ másodfokú kongruenciának $x = 2$ és $x = 4$ megoldása, így megoldás minden $x = 2 + 5k$ és $x = 4 + 5k, k \in \mathbb{Z}$ szám és más megoldás nincs (erről behelyettesítéssel győződhetünk meg).

• A $3x^3 + 3x^2 + 1 \equiv 0 \pmod{6}$ harmadfokú kongruenciának nincs megoldása, mert minden $x \in \mathbb{Z}$ -re $3x^3 + 3x^2 = 3x^2(x+1)$ osztható 6-tal, de 6 $\nmid 1$.

Az $f(x) \equiv 0 \pmod{m}$ kongruencia **megoldásai számának** a páronként inkongruens $\pmod{m}$ megoldások számát nevezzük.

Egy kongruenciát célszerű redukálni, azaz minden együtthatóját helyettesíteni a vele kongruens $\pmod{m}$ legkisebb nemnegatív, illetve legkisebb abszolútértékű számmal. Például, redukálva az $x^4 + 12x^3 + 7x^2 - 8x + 2 \equiv 0 \pmod{6}$ kongruenciát kapjuk a vele egyenértékű $x^4 + x^2 - 2x + 2 \equiv 0 \pmod{6}$ kongruenciát.

Két kongruenciát **egyenértékűnek** nevezünk, ha megoldáshalmazaik egyenlőek.

Ha a modulus kis szám, akkor egy kongruencia megoldásait megkaphatjuk próbálgatással.

A továbbiakban elsőfokú kongruenciákkal foglalkozunk, amelyek általános alakja $a_0x + a_1 \equiv 0 \pmod{m}$, ahol $m \nmid a_0$, illetve

$$(1) \quad ax \equiv b \pmod{m},$$

ahol $a, b \in \mathbb{Z}$ és $m \nmid a$.

Tétel. Ha $a, b \in \mathbb{Z}$ és $(a, m) = 1$, akkor az (1) kongruencia megoldható és 1 megoldása van.

Bizonyítás. Azonnal következik a 8.2. szakasz harmadik Tételéből. $\square$

Tétel. Legyen $a, b \in \mathbb{Z}$ és $d = (a, m)$.

i) Az (1) kongruencia akkor és csak akkor oldható meg, ha $d \mid b$ és ekkor a megoldások száma d .

ii) Ha x_0 az (1) kongruencia egy megoldása, akkor (1) összes megoldásai

$$x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \dots, x_0 + (d-1)\frac{m}{d}.$$

Bizonyítás. Tegyük fel, hogy $x = x_0$ megoldás, akkor $m \mid ax_0 - b$, ahonnan $ax_0 - b = km, k \in \mathbb{Z}$. Mivel $d \mid a$ és $d \mid b$, kapjuk, hogy $d \mid b$.

Ha $d \mid b$, akkor legyen $b = db_1, a = da_1$ és $m = dm_1$, ahol $(a_1, m_1) = 1$. Az $ax \equiv b \pmod{m}$ kongruencia egyenértékű az $a_1x \equiv b_1 \pmod{m_1}$ kongruenciával, lásd kongruenciák tulajdonságai (Tétel, 8.1. szakasz). Ez utóbbi kongruenciának, mivel $(a_1, m_1) = 1$, Tétel szerint van megoldása (és pontosan egy megoldás), így az eredeti kongruencia is megoldható.

Legyen $r_1, r_2, \dots, r_{m_1}$ egy teljes maradékrendszer $\pmod{m_1}$. Ekkor az előbbiek szerint létezik pontosan egy $x_0 = r_i$, mely megoldása az $a_1x \equiv b_1 \pmod{m_1}$ kongruenciának, az eredeti (1) kongruencia megoldásai pedig $r_i + km_1$ alakúak, $k \in \mathbb{Z}$, s kiválasztjuk ezek közül azokat, amelyek páronként inkongruensek $\pmod{m}$.

Tekintsük az

$$(2) \quad x_0, x_0 + m_1, x_0 + 2m_1, \dots, x_0 + (d-1)m_1$$

számokat. Ha $x_0 + im_1 \equiv x_0 + jm_1 \pmod{m}$, ahol $0 \leq i, j \leq d-1$, akkor $m \mid (i-j)m_1$, azaz $d \mid i-j$, de $0 \leq |i-j| \leq d-1$, s kapjuk, hogy $i = j$. A (2) rendszer számai tehát páronként inkongruensek $\pmod{m}$. Ha $x_0 + km_1$ egy más megoldás, ahol $k = dq + r$ és $0 \leq r \leq d-1$, akkor $x_0 + km_1 = x_0 + (dq + r)m_1 = x_0 + mq + rm_1 \equiv x_0 + rm_1 \pmod{m}$. Ezzel igazoltuk, hogy a megoldások száma $d = (a, m)$. $\square$

Jegyezzük meg, hogy ha adott az (1) $ax \equiv b \pmod{m}$ kongruencia és $(a, m) = d|b$, akkor (1) megoldásához előbb meg kell oldanunk az

$$(3) \quad \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

kongruenciát, amelynek mindig 1 megoldása van. (1)-nek pedig d megoldása van, amelyeket a fentiek szerint írhatunk fel.

Ha (3)-ban a modulus kicsi, akkor ennek megoldását próbálgatással kaphatjuk meg. Ellenkező esetben célszerű más megoldási módot keresni.

Tétel. Ha $(a, m) = 1$, akkor az (1) kongruencia egyetlen megoldása $x \equiv a^{\phi(m)-1}b \pmod{m}$.

Bizonyítás. Hogy egyetlen megoldás van, az következik a jelen szakasz Tételeiből. Ha $x \equiv a^{\phi(m)-1}b \pmod{m}$, akkor x valóban megoldás, hiszen az Euler-tétel szerint $ax \equiv a^{\phi(m)}b \equiv b \pmod{m}$. $\square$

Megjegyzés. Nagy m esetén e tétel alkalmazása meglehetősen sok számolással jár. Egy más, és talán a legjobb általános módszer az euklidészi algoritmus alkalmazása: Ha adott az (1) kongruencia, akkor meghatározzuk a $d = (a, m)$ értéket és egyúttal olyan u és v egész számokat, melyekre $au + mv = d$, lásd 5.1. szakasz. Innen $\frac{a}{d}u + \frac{m}{d}v = 1$, $\frac{a}{d}u \equiv 1 \pmod{\frac{m}{d}}$, s b/d -vel szorozva $\frac{a}{d}(bu/d) \equiv b/d \pmod{\frac{m}{d}}$, azaz $x = bu/d$ a (3) kongruencia egy megoldása és innen meghatározható (1) összes megoldása.

Példák. • 1. Oldjuk meg a $13x \equiv 5 \pmod{29}$ kongruenciát.

Mivel $(13, 29) = 1$, a kongruencia megoldható, 1 megoldása van $\pmod{29}$, s ez $x \equiv 16 \pmod{29}$, mely megkapható próbálgatással, de ez hosszadalmas.

Az előbbi Tétel alkalmazásával $x \equiv 13^{\phi(29)-1} \cdot 5 = 13^{27} \cdot 5 = 169^{13} \cdot 13 \cdot 5 = (6 \cdot 29 - 5)^{13} \cdot 13 \cdot 5 \equiv -5^{13} \cdot 65 \equiv -25^6 \cdot 5(2 \cdot 29 + 7) \equiv -(29 - 4)^6 \cdot 5 \cdot 7 \equiv -4^6 \cdot 35 \equiv -4^6 \cdot 6 \equiv -(2^5)^2 \cdot 24 \equiv -3^2(-5) \equiv 45 \equiv 16 \pmod{29}$, de látjuk, hogy ez is hosszadalmas számításokat igényel.

Másképp, az euklidészi algoritmus segítségével:

$$29 = 2 \cdot 13 + 3,$$

$$13 = 4 \cdot 3 + 1,$$

$$3 = 3 \cdot 1 + 0,$$

s innen $1 = 13 - 4 \cdot 3 = 13 - 4(29 - 2 \cdot 13) = 9 \cdot 13 - 4 \cdot 29$. Kapjuk, hogy $13 \cdot 9 \equiv 1 \pmod{29}$, 5-tel szorozva $13 \cdot 45 \equiv 5 \pmod{29}$, $13 \cdot 16 \equiv 5 \pmod{29}$, tehát $x \equiv 16 \pmod{29}$.

Sok esetben gyorsabban célba érünk, ha a kongruenciához hozzáadjuk a modulust vagy annak alkalmas többszörösét, illetve a kongruenciát szorozzuk vagy osztjuk egy alkalmas számmal (osztás esetén ez legyen relatív prím a modulussal). Itt például 3-mal szorozva $39x \equiv 15 \pmod{29}$, $10x \equiv 15 \pmod{29}$, amit 5-tel osztva $2x \equiv 3 \pmod{29}$, majd 15-tel szorozva $30x \equiv 45 \pmod{29}$, $x \equiv 16 \pmod{29}$.

• 2. Oldjuk meg a $21x \equiv 14 \pmod{35}$ kongruenciát.

Most $(21, 35) = 7|14$, a kongruencia tehát megoldható és 7 megoldás van $\pmod{35}$. Felírva a (3)-nak megfelelő $3x \equiv 2 \pmod{5}$ kongruenciát, ennek egyedüli megoldása $x \equiv 4 \pmod{5}$ és innen $x \equiv 4, 9, 14, 19, 24, 29, 34 \pmod{35}$.

Feladat. ▼ Oldjuk meg a következő kongruenciákat:

a) $26x \equiv 6 \pmod{68}$, b) $19x \equiv 11 \pmod{24}$, c) $36x \equiv 7 \pmod{20}$.

8.5. Elsőfokú diofántoszi egyenletek

Az elsőfokú kongruenciák szoros kapcsolatban vannak a kétismeretlenes elsőfokú (lineáris) **diofántoszi egyenletekkel**, amelyek általános alakja

$$ax + by = c,$$

ahol az a, b, c együtthatók egész számok és az x, y ismeretleneket is a $\mathbb{Z}$ halmazban keressük.

Tétel. Az $ax + by = c$ diofántoszi egyenletnek akkor és csak akkor van megoldása ha $(a, b) | c$ és ekkor a megoldások száma végtelen.

Bizonyítás. Ha van megoldás, akkor $ax_0 + by_0 = c$, $ax_0 \equiv c \pmod{b}$ valamilyen $x_0, y_0 \in \mathbb{Z}$ számokra, így azt kapjuk, hogy az $ax \equiv c \pmod{b}$ kongruenciának van megoldása és ekkor Tétel szerint $(a, b) | c$. Fordítva, ha ez a feltétel teljesül, akkor ismét e Tétel alapján létezik $x_0 \in \mathbb{Z}$ úgy, hogy $ax_0 \equiv c \pmod{b}$, s létezik $y_0 \in \mathbb{Z}$, amelyre $ax_0 - c = by_0$, azaz $x_0, -y_0$ megoldása az egyenletnek. Ekkor $x = x_0 + kb, y = -y_0 - ka$ megoldás minden $k \in \mathbb{Z}$ esetén. $\square$

Példa. • Oldjuk meg az előbbi $13x \equiv 5 \pmod{29}$ kongruenciát úgy, hogy elsőfokú diofántoszi egyenletre vezetjük vissza. A megfelelő egyenlet $13x - 29y = 5$, fejezzük ki x -et: $x = \frac{29y+5}{13} = 2y + \frac{3y+5}{13}$, ahol legyen $\frac{3y+5}{13} = z \in \mathbb{Z}$. Kapjuk a $3y+5 = 13z$ egyenletet, melyből fejezzük ki az y -t: $y = \frac{13z-5}{3} = 4z - 2 + \frac{z-1}{3}$, s innen $\frac{z-1}{3} = t \in \mathbb{Z}$, $z+1 = 3t$, újabb egyenlet, ahonnan $z = 3t-1$. Visszahelyettesítve, $y = 12t-4-2+t = 13t-6$, $x = 26t-12+3t-1 = 29t-13$. Tehát az eredeti egyenlet megoldása $x = 29t-13, y = 13t-6$, ahol $t \in \mathbb{Z}$, a kongruencia megoldása pedig $x \equiv -13 \equiv 16 \pmod{29}$.

Megjegyzés. Ez a módszer minden $ax + by = c$ diofántoszi egyenlet megoldására alkalmazható, rendre az abszolútértékben kisebb együtthatójú ismeretlent fejezzük ki és belátható, hogy ekkor véges sok lépés után eredményre jutunk.

Feladatok

▼ 1. Oldjuk meg: a) $18x+5y=2$, b) $36x+15y=51$.

▼ 2. Igazoljuk, hogy az $a_1x_1 + a_2x_2 + \dots + a_kx_k = c$ diofántoszi egyenletnek akkor és csak akkor van megoldása ha $(a_1, a_2, \dots, a_k) | c$.

Útmutatás. Használjuk az 5.1. szakasz utolsó Tételét.

8.6. Elsőfokú kongruenciarendszerek

A továbbiakban lineáris kongruenciarendszerekkel foglalkozunk, ezek általános alakja a következő :

$$\begin{aligned} a_1x &\equiv b_1 \pmod{m_1} \\ a_2x &\equiv b_2 \pmod{m_2} \\ &\dots \\ a_kx &\equiv b_k \pmod{m_k}. \end{aligned}$$

A rendszer megoldhatóságának szükséges feltétele, hogy az egyes kongruenciák megoldhatóak legyenek és ezek megoldásait tekintve

$$(4) \quad \begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\dots \\ x &\equiv c_k \pmod{m_k} \end{aligned}$$

alakú kongruenciarendszert kapunk. Ilyen rendszerre vonatkozik az alábbi tétel.

Tétel. (Kínai maradéktétel) Ha az $m_1, m_2, \dots, m_k$ modulusok páronként relatív prímek és $c_1, c_2, \dots, c_k$ tetszőleges egész számok, akkor a (4) rendszernek létezik megoldása és egy megoldás van $(\text{mod } m_1 m_2 \dots m_k)$.

Bizonyítás. Legyen $m = m_1 m_2 \dots m_k$ és tekintsük az

$$(5) \quad \frac{m}{m_i} x \equiv 1 \pmod{m_i}$$

kongruenciákat, $1 \leq i \leq k$. Mivel $(\frac{m}{m_i}, m_i) = 1$, Tétel alapján (5)-nek létezik megoldása, legyen egy megoldás $x = e_i$. Így

$$(6) \quad \frac{m}{m_j} e_j \equiv \begin{cases} 1 \pmod{m_i}, & \text{ha } j = i, \\ 0 \pmod{m_i}, & \text{ha } j \neq i. \end{cases}$$

Legyen most

$$x_0 = \sum_{j=1}^k \frac{m}{m_j} e_j c_j.$$

(6) alapján kapjuk, hogy minden i -re $x_0 \equiv c_i \pmod{m_i}$, tehát x_0 megoldása a (4) rendszernek. Ha x'_0 egy másik megoldás, akkor $m_i | x_0 - c_i$ és $m_i | x'_0 - c_i$, ahonnan $m_i | x_0 - x'_0$ minden i -re, s kapjuk, hogy $m_1 m_2 \dots m_k = m | x_0 - x'_0$, azaz $x_0 \equiv x'_0 \pmod{m}$.
□

Feladatok

▼ 1. Oldjuk meg a következő kongruenciarendszereket:

a) $x \equiv 3 \pmod{5}$, $x \equiv 1 \pmod{6}$, $x \equiv 2 \pmod{7}$;

b) $5x \equiv 3 \pmod{7}$, $3x \equiv 7 \pmod{8}$.

▼ 2. Határozzuk meg azokat a 4-jegyű számokat, amelyek 72-vel osztva 46 maradékot, 127-tel osztva pedig 97 maradékot adnak.

9. Számelméleti függvények

9.1. Multiplikatív függvények

Számelméleti függvénynek nevezünk minden $f : \mathbb{N}^* \rightarrow \mathbb{C}$ függvényt, ahol $\mathbb{C}$ a komplex számok halmaza, a számelméleti függvények halmazát $\mathcal{F}$ -fel jelöljük. Ez az definíció megegyezik a komplex számsorozatok definíciójával. Elsősorban azok a függvények érdekelnek bennünket, amelyek valamely számelméleti fogalomhoz kapcsolódnak.

Ilyen számelméleti függvények például a τ és ϕ , ahol $\tau(n) = \sum_{d|n} 1$ az n szám pozitív osztóinak a száma, lásd 7. fejezet, ϕ az Euler-függvény, lásd 8.2. szakasz. Ilyen a σ függvény is, ahol $\sigma(n) = \sum_{d|n} d$ az n pozitív osztóinak az összege.

Legyen $f \in \mathcal{F}$ egy számelméleti függvény. Azt mondjuk, hogy

- i) f **multiplikatív**, ha minden $m, n \in \mathbb{N}^*$, $(m, n) = 1$ esetén $f(mn) = f(m)f(n)$,
- ii) f **teljesen multiplikatív** ha minden $m, n \in \mathbb{N}^*$ számpárra $f(mn) = f(m)f(n)$.

Ha f teljesen multiplikatív, akkor f multiplikatív és fordítva nem.

Tétel. Ha $f \in \mathcal{F}$ nem azonosan nulla multiplikatív függvény, akkor $f(1) = 1$.

Bizonyítás. Létezik olyan $n_0 \in \mathbb{N}$, amelyre $f(n_0) \neq 0$ és így a multiplikativitás alapján $f(n_0) = f(1 \cdot n_0) = f(1)f(n_0)$, ahonnan $f(1) = 1$. $\square$

Legyen a továbbiakban $n > 1$ kanonikus alakja $n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$.

Tétel. Ha f multiplikatív függvény, akkor f értékeit elegendő a prímszámokra ismerni:

$$f(n) = f(p_1^{a_1})f(p_2^{a_2}) \dots f(p_r^{a_r}).$$

Bizonyítás. Valóban, a multiplikativitás alapján

$$f(n) = f(p_1^{a_1})f(p_2^{a_2} \dots p_r^{a_r}) = f(p_1^{a_1})f(p_2^{a_2})f(p_3^{a_3} \dots p_r^{a_r}) = \dots = f(p_1^{a_1})f(p_2^{a_2}) \dots f(p_r^{a_r}). \quad \square$$

Tétel. Ha f teljesen multiplikatív függvény, akkor f értékeit elegendő a prímszámokra ismerni:

$$f(n) = f(p_1)^{a_1} f(p_2)^{a_2} \dots f(p_r)^{a_r}.$$

Bizonyítás. Ha p^a prímszám, akkor $f(p^a) = f(p)f(p^{a-1}) = (f(p))^2 f(p^{a-2}) = \dots = (f(p))^a$ és alkalmazzuk az előző Tételt. $\square$

Ha $f \in \mathcal{F}$, akkor a

$$g(n) = \sum_{d|n} f(d), \quad n \in \mathbb{N}^*$$

képlettel értelmezett g függvényt, ahol az összegzés n pozitív d osztóira vonatkozik, az f **összegzési függvényének** nevezzük.

Tétel. Ha f multiplikatív függvény, akkor f összegzési függvénye is multiplikatív.

Ez az állítás következik az alábbi általánosabb tételből.

Tétel. Ha f és g multiplikatív függvények és

$$h(n) = \sum_{d|n} f(d)g(n/d), \quad n \in \mathbb{N}^*,$$

akkor h is multiplikatív.

Bizonyítás. Legyen $m, n \in \mathbb{N}^*$, $(m, n) = 1$, akkor az mn minden d osztója felírható egyértelműen $d = d_1 d_2$ alakban, ahol $d_1 | m$, $d_2 | n$, lásd 7. fejezet, 5. Feladat. Így

$$h(mn) = \sum_{d|mn} f(d)g(n/d) = \sum_{d_1|m} \sum_{d_2|n} f(d_1 d_2)g(mn/d_1 d_2).$$

Itt $(d_1, d_2) = 1$ és $(m/d_1, n/d_2) = 1$, és használva, hogy f és g multiplikatív kapjuk, hogy

$$\begin{aligned} h(mn) &= \sum_{d_1|m} \sum_{d_2|n} f(d_1)f(d_2)g(m/d_1)g(n/d_2) \\ &= \sum_{d_1|m} f(d_1)g(m/d_1) \sum_{d_2|n} f(d_2)g(n/d_2) = h(m)h(n). \quad \square \end{aligned}$$

Ha ebben a Tételben $g(n) = 1, n \in \mathbb{N}^*$, akkor h az f összegzési függvénye és az ezt megelőző Tételt kapjuk.

Ha $s \in \mathbb{R}$ adott szám, akkor legyen $\sigma_s(n) = \sum_{d|n} d^s$ az n pozitív osztóinak s -edik hatványösszege. Ha $s = 1$, akkor $\sigma_1(n) = \sigma(n) = \sum_{d|n} d$ az n osztóinak összege, ha pedig $s = 0$, akkor $\sigma_0(n) = \tau(n)$ az n osztóinak száma.

Tétel. A σ_s, σ, τ függvények multiplikatívak és

$$\begin{aligned} \sigma_s(n) &= \frac{p_1^{s(a_1+1)} - 1}{p_1^s - 1} \cdots \frac{p_r^{s(a_r+1)} - 1}{p_r^s - 1}, \quad s \neq 0, \\ \sigma(n) &= \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdots \frac{p_r^{a_r+1} - 1}{p_r - 1}, \\ \tau(n) &= (a_1 + 1) \cdots (a_r + 1). \end{aligned}$$

Bizonyítás. Az $f(n) = n^s$ függvény multiplikatív (sőt teljesen multiplikatív) és így ennek összegzési függvénye, a σ_s is multiplikatív Tétel szerint. Elegendő $\sigma_s(p^a)$ meghatározása, ahol p^a egy prímszám. Azt kapjuk, hogy

$$\sigma_s(p^a) = 1 + p^s + p^{2s} + \cdots + p^{as} = \frac{p^{s(a+1)} - 1}{p^s - 1}, \quad s \neq 0,$$

a mértani sorozat összegzési képlete szerint. Ha $s = 0$, akkor $\sigma_0(p^a) = \tau(p^a) = a + 1$. $\square$

Megjegyzések. 1) A $\tau(n)$ -re vonatkozó képletet már láttuk a 7. fejezetben.

2) A σ_s, σ, τ függvények nem teljesen multiplikatívak, például $\tau(4) = 3 \neq 2 \cdot 2 = \tau(2)\tau(2)$.

Az $n \in \mathbb{N}^*$ számot **tökéletes számnak** nevezzük ha n egyenlő az önmagánál kisebb osztóinak összegével, azaz ha $\sigma(n) = 2n$. Például $n = 6$ és $n = 28$ tökéletes számok, mert $6 = 1 + 2 + 3$ és $28 = 1 + 2 + 4 + 7 + 14$, illetve $\sigma(6) = 1 + 2 + 3 + 6 = 2 \cdot 6 = 12$ és $\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 2 \cdot 28 = 56$.

Tétel. (Euklidész) Ha $2^k - 1$ prímszám, akkor $n = 2^{k-1}(2^k - 1)$ tökéletes szám.

Bizonyítás. A σ függvény multiplikativitása alapján

$$\sigma(n) = \sigma(2^{k-1}(2^k - 1)) = \sigma(2^{k-1})\sigma(2^k - 1) = (2^k - 1)(1 + 2^k - 1) = 2^k(2^k - 1) = 2n.$$

$\square$

Tétel. (Euler) Ha n páros tökéletes szám, akkor $n = 2^{k-1}(2^k - 1)$ alakú, ahol $2^k - 1$ prímszám.

★ **Bizonyítás.** Legyen $n = 2^a m$, ahol $a \geq 1$ és m páratlan. Így $\sigma(n) = \sigma(2^a m) = \sigma(2^a)\sigma(m) = (2^{a+1} - 1)\sigma(m)$ és innen $\sigma(n) = 2n$ alapján $(2^{a+1} - 1)\sigma(m) = 2^{a+1}m$. Következik, hogy $2^{a+1} - 1 \mid 2^{a+1}m$, s mivel $(2^{a+1} - 1, 2^{a+1}) = 1$ kapjuk, hogy $2^{a+1} - 1 \mid m$, azaz $m = (2^{a+1} - 1)m_1$, amit visszahelyettesítve: $(2^{a+1} - 1)\sigma(m) = (2^{a+1} - 1)2^{a+1}m_1$, ahonnan $\sigma(m) = 2^{a+1}m_1$. Az m_1 és m osztói m -nek, $m_1 < m$ és $m_1 + m = m_1 + (2^{a+1} - 1)m_1 = 2^{a+1}m_1 = \sigma(m)$. Így m -nek m_1 -en és m -en kívül nincs más osztója, s kapjuk,

hogy $m_1 = 1$ és $m = 2^{a+1} - 1$ prímszám. Tehát az $a = k - 1$ jelöléssel $n = 2^{k-1}(2^k - 1)$, ahol $2^k - 1$ prímszám. $\square \star$

Így n akkor és csak akkor páros tökéletes szám, ha $n = 2^{p-1}M_p$ alakú, ahol M_p Mersenne-prím, lásd 6.2. szakasz. További tökéletes számok $n = 2^3M_5 = 496, 2^6M_7 = 8128$. Jelenleg (2005. szeptember) 42 tökéletes szám ismert annak megfelelően, hogy 42 Mersenne-prímet ismerünk. Nem tudjuk, hogy létezik-e végtelen sok Mersenne-féle prímszám, így azt sem tudjuk, hogy van-e végtelen sok tökéletes szám. Arra a kérdésre sem ismerjük a választ, hogy létezik-e páratlan tökéletes szám.

Most az Euler-féle ϕ függvényt vizsgáljuk.

Tétel. a) A ϕ függvény multiplikatív, azaz minden $m, n \in \mathbb{N}^*, (m, n) = 1$ esetén $\phi(mn) = \phi(m)\phi(n)$.

b) Ha n kanonikus alakja $n = p_1^{a_1}p_2^{a_2}\dots p_r^{a_r}$, akkor

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right).$$

Bizonyítás. a) Rendezzük az $1, 2, 3, \dots, mn$ számokat a következő táblázatba:

1	2	3	...	m
$m + 1$	$m + 2$	$m + 3$	...	$2m$
$2m + 1$	$2m + 2$	$2m + 3$	...	$3m$
...	...	...	...	...
$(n - 1)m + 1$	$(n - 1)m + 2$	$(n - 1)m + 3$	...	nm

Számoljuk le kétféleképpen a táblázat mn -hez relatív prím k számait. Ezek száma egyrészt $\phi(mn)$, az Euler függvény definíciója szerint.

Másrészt, $(k, mn) = 1 \Leftrightarrow (k, m) = 1$ és $(k, n) = 1$ (lásd Tétel). Válasszuk ki először az m -mel relatív prímeket. A táblázat mindegyik sora egy-egy teljes maradékrendszer $(\text{mod } m)$, így mindegyik sor $\phi(m)$ számú m -hez relatív prím számot tartalmaz úgy, hogy ha egy szám m -hez relatív prím, akkor annak oszlopában mindegyik szám m -hez relatív prím (igazoljuk!). Most ezek közül válasszuk ki az n -hez relatív prímeket. Mindegyik oszlop egy-egy teljes maradékrendszer $(\text{mod } n)$, ahol $(m, n) = 1$, lásd 8.2. szakasz Tétel, így mindegyik oszlopban $\phi(n)$ szám relatív prím n -hez. Kapjuk, hogy a keresett szám $\phi(m)\phi(n)$.

b) Az a) alapján

$$\phi(n) = \phi(p_1^{a_1}p_2^{a_2}\dots p_r^{a_r}) = \phi(p_1^{a_1})\phi(p_2^{a_2}\dots p_r^{a_r}) = \dots = \phi(p_1^{a_1})\phi(p_2^{a_2})\dots\phi(p_r^{a_r}).$$

Így elegendő $\phi(p^a)$ meghatározása, ahol p^a egy prímszám. Az $1, 2, 3, \dots, p^a$ számok közül a p^a -hoz nem relatív prímelek a $p, 2p, 3p, \dots, p^{a-1}p = p^a$, ezek száma p^{a-1} , így a p^a -hoz relatív prímelek száma $p^a - p^{a-1} = p^a(1 - 1/p)$.

Kapjuk, hogy

$$\begin{aligned} \phi(n) &= p_1^{a_1}(1 - 1/p_1)p_2^{a_2}(1 - 1/p_2)\dots p_r^{a_r}(1 - 1/p_r) = \\ &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right). \quad \square \end{aligned}$$

Megjegyzés. Használatos a következő jelölés:

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

ahol a szorzat az n összes p prímosztójára vonatkozik.

Tétel. Minden $n \in \mathbb{N}$ esetén

$$\sum_{d|n} \phi(d) = n,$$

ahol az összegzés n pozitív d osztóira vonatkozik.

Bizonyítás. Tekintsük az $\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \dots, \frac{n}{n}$ törtet, ezek száma n . Ugyanakkor, egyszerűsítve mindegyik tört $\frac{k}{d}$ alakú lesz, ahol $d|n$ és $(k, d) = 1, k \leq d$. Az n minden d pozitív osztója esetén lesz d nevezőjű tört és az ugyanolyan d nevezőjű törtek száma $\phi(d)$. Így a törtek száma összesen $\sum_{d|n} \phi(d)$, s ezzel bizonyítottuk a képletet. $\square$

Feladatok

▼ 1. Határozzuk meg a $\tau(n), \sigma(n)$ és $\phi(n)$ értékeket, ahol $n = 12, n = 24, n = 120$, illetve $n = p^2 q^3, p \neq q$ prímek.

▼ 2. Legyenek f és g multiplikatív függvények. Vizsgáljuk, hogy multiplikatív-e az fg szorzatfüggvény és az $f + g$ összegfüggvény.

▼ 3. Lehet-e prímszám vagy prímszámhatvány tökéletes szám?

▼ 4. Igazoljuk, hogy n akkor és csak akkor tökéletes szám, ha n osztói reciprokainak az összege 2.

▼ 5. Igazoljuk, hogy ha n páros tökéletes szám, akkor n utolsó számjegye (10-es számrendszerben) 6 vagy 8.

▼ 6. Igazoljuk, hogy minden $m, n \geq 1$ esetén $\tau(mn) \leq \tau(m)\tau(n)$.

Mikor áll fenn az egyenlőség?

▼ 7. Igazoljuk, hogy minden $n \geq 1$ -re $\phi(n^2) = n\phi(n)$.

▼ 8. Igazoljuk, hogy minden $n > 1$ esetén

$$\sum_{\substack{k=1 \\ (k,n)=1}}^n k = \frac{n\phi(n)}{2},$$

9.2. Additív függvények

Legyen $f \in \mathcal{F}$ egy számelméleti függvény. Azt mondjuk, hogy

i) f **additív**, ha minden $m, n \in \mathbb{N}^*, (m, n) = 1$ esetén $f(mn) = f(m) + f(n)$,

ii) f **teljesen additív**, ha minden $m, n \in \mathbb{N}^*$ számpárra $f(mn) = f(m) + f(n)$.

Ha f teljesen additív, akkor f additív, és fordítva nem.

Definiáljuk az ω és Ω függvényeket a következőképpen. Legyen $\omega(1) = \Omega(1) = 0$ és ha $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} > 1$, akkor legyen $\omega(n) = r$ az n különböző prímosztóinak száma és $\Omega(n) = a_1 + a_2 + \dots + a_r$ az n különböző prímszámhatvány osztóinak száma.

Tétel. Az ω függvény additív, Ω pedig teljesen additív.

Bizonyítás. Ha $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}, m = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$ és $(n, m) = 1$, akkor nm kanonikus alakja $nm = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$ és $\omega(nm) = r + s = \omega(n) + \omega(m)$. Továbbá minden n, m esetén $\Omega(nm) = a_1 + a_2 + \dots + a_r + b_1 + b_2 + \dots + b_s = \Omega(n) + \Omega(m)$. $\square$

Az ω nem teljesen additív, mert például $\omega(12) = \omega(2^2 \cdot 3) = 2 \neq 3 = 2 + 1 = \omega(2 \cdot 3) + \omega(2)$.

További fontos példa a logaritmusfüggvény, amely teljesen additív. Nézzük az additív függvények tulajdonságait.

Tétel. Ha $f \in \mathcal{F}$ additív függvény, akkor $f(1) = 0$.

Bizonyítás. Valóban, $f(1) = f(1 \cdot 1) = f(1) + f(1)$ alapján $f(1) = 0$. $\square$

Legyen a továbbiakban $n > 1$ kanonikus alakja $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$.

Tétel. Ha f additív függvény, akkor f értékeit elegendő a prímszámokra ismerni:

$$f(n) = f(p_1^{a_1}) + f(p_2^{a_2}) + \dots + f(p_r^{a_r}).$$

Bizonyítás. Valóban, az additivitás alapján $f(n) = f(p_1^{a_1}) + f(p_2^{a_2} \dots p_r^{a_r}) =$

$$= f(p_1^{a_1}) + f(p_2^{a_2}) + f(p_3^{a_3} \dots p_r^{a_r}) = \dots = f(p_1^{a_1}) + f(p_2^{a_2}) + \dots + f(p_r^{a_r}). \quad \square$$

Tétel. Ha f teljesen additív függvény, akkor f értékeit elegendő a prímszámokra ismerni:

$$f(n) = a_1 f(p_1) + a_2 f(p_2) + \dots + a_r f(p_r).$$

Bizonyítás. Ha p^a prímszám, akkor $f(p^a) = f(p) + f(p^{a-1}) = \dots = af(p)$ és alkalmazzuk az előző Tételt. $\square$

A multiplikatív és additivitás kapcsolatára mutat rá a következő tétel.

Tétel. Ha f additív, g teljesen additív és $k \neq 0$ valós szám, akkor $F(n) = k^{f(n)}$ multiplikatív, $G(n) = k^{g(n)}$ pedig teljesen multiplikatív függvény.

Fordítva, ha F multiplikatív, G teljesen multiplikatív és pozitív értékű függvények, akkor $f(n) = \ln F(n)$ additív, $g(n) = \ln G(n)$ teljesen additív.

Feladat. $\blacktriangledown$ Igazoljuk ezt.

★ A prímszámelméletben fontos szerepe van a Λ -val jelölt, ún. **von Mangoldt függvénynek**, amely így adott:

$$\Lambda(n) = \begin{cases} \ln p, & \text{ha } n = p^a \text{ prímszám,} \\ 0, & \text{ha } n \text{ nem prímszám.} \end{cases}$$

Tétel. A Λ függvény összegzési függvénye az $\ln$ logaritmusfüggvény, azaz

$$\sum_{d|n} \Lambda(d) = \ln n, \quad n \geq 1.$$

Bizonyítás. Ha $n = p_1^{a_1} \dots p_r^{a_r}$ alakú, akkor figyelembe véve, hogy Λ csak a prímszámokon vesz fel nullától különböző értékeket:

$$\sum_{d|n} \Lambda(d) = \sum_{b_1=0}^{a_1} \Lambda(p_1^{b_1}) + \dots + \sum_{b_r=0}^{a_r} \Lambda(p_r^{b_r})$$

$$= a_1 \ln p_1 + \dots + a_r \ln p_r = \ln(p_1^{a_1} \dots p_r^{a_r}) = \ln n. \quad \square \star$$

Feladatok

$\blacktriangledown$ 1. Legyenek f és g additív függvények. Vizsgáljuk, hogy additív-e az $f + g$ összeg, az $f - g$ különbség és az fg szorzatfüggvény.

$\blacktriangledown$ 2. Igazoljuk, hogy $2^{\omega(n)} \leq \tau(n) \leq 2^{\Omega(n)}$ minden $n \geq 1$ -re.

$\blacktriangledown$ 3. Igazoljuk, hogy a $\lambda(n) = (-1)^{a_1 + \dots + a_r}$, $n = p_1^{a_1} \dots p_r^{a_r} > 1$, $\lambda(1) = 1$ függvény (Liouville-függvény) teljesen multiplikatív és határozzuk meg a $\sum_{d|n} \lambda(d)$ összegzési függvényt.

Tartalomjegyzék

Bevezetés	1
További irodalom	1
1. Halmazok, relációk, függvények	2
1.1. Halmazok	2
1.2. Relációk	3
1.3. Függvények	4
2. Algebrai struktúrák	6
2.1. Algebrai műveletek	6
2.2. A csoport, a gyűrű és a test fogalma	7
3. Komplex számok	8
3.1. A komplex számok bevezetése, algebrai alakja	8
3.2. A komplex számok trigonometrikus alakja	8
3.3. Gyökvonás komplex számokból, komplex egységgyökök	8
4. Egész számok oszthatósága	9
4.1. Oszthatóság	9
4.2. Maradékos osztás, számrendszerek	11
5. Legnagyobb közös osztó és legkisebb közös többszörös	14
5.1. Egész számok legnagyobb közös osztója	14
5.2. Egész számok legkisebb közös többszöröse	17
6. Prímszámok	19
6.1. Felbonthatatlan számok és prímszámok	19
6.2. A prímszámok tulajdonságai	20
7. A számelmélet alaptétele	23
8. Kongruenciák	26
8.1. Kongruenciák definíciója és alaptulajdonságai	26
8.2. Teljes maradékrendszerek és redukált maradékrendszerek	28
8.3. Az Euler, Fermat és Wilson tételek	29
8.4. Elsőfokú kongruenciák	30
8.5. Elsőfokú diofántoszi egyenletek	33
8.6. Elsőfokú kongruenciarendszerek	33
9. Számelméleti függvények	35
9.1. Multiplikatív függvények	35
9.2. Additív függvények	38