

# MBLK12: Számelmélet (levelező)

(előadásvázlat)

Maróti Miklós

## 1. OSZTHATÓSÁG, EUKLIDESZI ALGORITMUS, DIOFANTOSZI EGYENLET

**1. Definíció.** Azt mondjuk, hogy az  $a$  egész szám **osztója** a  $b$  egész számnak ( $b$  **többszöröse**  $a$ -nak), ha létezik olyan  $c$  egész szám, amelyre  $ac = b$ . Ha  $a$  osztója  $b$ -nek, akkor ezt úgy jelöljük, hogy  $a \mid b$ .

**2. Tétel (oszthatóság tulajdonságai).** Tetszőleges  $a, b, c, d$  egész számokra érvényesek az alábbiak:

- |   |  |
|---|--|
| (1) $a \mid a$ ;                                      | (6) $a \mid b$ akkor és csak akkor, ha $ a  \mid  b $ ;    |
| (2) ha $a \mid b$ és $b \mid a$ , akkor $a = \pm b$ ; | (7) ha $a \mid b$ és $a \mid c$ , akkor $a \mid b \pm c$ ; |
| (3) ha $a \mid b$ és $b \mid c$ , akkor $a \mid c$ ;  | (8) ha $a \mid b$ , akkor $a \mid bc$ ;                    |
| (4) $1 \mid a$ ;                                      | (9) ha $a \mid b$ és $c \mid d$ , akkor $ac \mid bd$ .     |
| (5) $a \mid 0$ ;                                      | (10) ha $ac \mid bc$ és $c \neq 0$ , akkor $a \mid b$ .    |

**3. Definíció.** A  $c$  számot az  $a$  és  $b$  számok **közös osztójának** nevezzük, ha  $c \mid a$  és  $c \mid b$ . A  $c$  szám az  $a$  és  $b$  **legnagyobb közös osztója**, ha közös osztója, és  $a$  és  $b$  minden  $d$  közös osztójára  $d \mid c$ . Hasonlóan definiáljuk a **közös többszöröst** és a **legkisebb közös többszöröst**.

**4. Lemma.** Tetszőleges  $a, b, c$  egész számokra érvényesek az alábbiak:

- (1) ha  $c$  legnagyobb közös osztója  $a$  és  $b$ -nek, akkor  $-c$  is az és rajtuk kívül nincsen másik;
- (2)  $0$  és  $a$  legnagyobb közös osztója  $a$  és  $-a$ ;
- (3)  $a$  és  $b$  közös osztói ugyan azok mint  $a + bc$  és  $b$  közös osztói;

**5. Tétel (maradékos osztás).** Ha  $a$  és  $b$  egész számok és  $b \neq 0$ , akkor léteznek olyan egyértelműen meghatározott  $q$  és  $r$  egész számok, amelyekre  $a = bq + r$  és  $0 \leq r < |b|$ .

**6. Definíció.** Adott  $a$  és  $b$  egész számok esetén az előző tételbeli  $q$  és  $r$  kiszámítását **maradékos osztásnak** nevezzük. Az  $a$  szám az **osztandó**,  $b$  az **osztó**,  $q$  a **hányados**, és  $r$  a **maradék**.

**7. Tétel (euklideszi algoritmus).** Bármely két  $a$  és  $b$  természetes számnak van legnagyobb közös osztója, amely az alábbi euklideszi algoritmussal megkapható. Az  $r_0 = a$  és  $r_1 = b$  természetes számokon végrehajtott euklideszi algoritmus maradékos osztások ismételt elvégzését jelenti:

$$\begin{aligned} r_0 &= q_1 r_1 + r_2 & (0 < r_2 < r_1); \\ r_1 &= q_2 r_2 + r_3 & (0 < r_3 < r_2); \\ &\vdots \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n & (0 < r_n < r_{n-1}); \\ r_{n-1} &= q_n r_n + r_{n+1} & (r_{n+1} = 0). \end{aligned}$$

Az eljárás véges számú lépés után véget ér, azaz létezik olyan  $n$  természetes szám, hogy  $r_{n+1} = 0$ . Ekkor a legnagyobb közös osztó az utolsó nemnulla maradék, azaz  $\text{lko}(a, b) = r_n$ .

**8. Jelölés.** Az  $a$  és  $b$  egész számok legnagyobb közös osztóját  $\text{lko}(a, b)$ -vel, míg a legkisebb közös többszörösét  $\text{lkkt}(a, b)$ -vel jelöljük. Ez csak előjeltől eltekintve egyértelmű, de mi általában a nemnegatív tekintjük.

**9. Következmény.** Az  $a$  és  $b$  legnagyobb közös osztója kifejezhető a két szám „lineáris kombinációjaként”, azaz léteznek olyan  $x$  és  $y$  egész számok, hogy  $\text{lko}(a, b) = xa + yb$ .

**10. Definíció.** Az  $a$  és  $b$  számok **relatív prímelek**, ha  $\text{lko}(a, b) = 1$ .

**11.\* Tétel.** Tetszőleges  $a$  és  $b$  egészekre ha  $\text{lko}(a, b) \neq 0$ , akkor  $\frac{a}{\text{lko}(a, b)}$  és  $\frac{b}{\text{lko}(a, b)}$  relatív prímelek.

**12.\* Lemma.** Tetszőleges  $a, b, c$  egész számokra ha  $\text{luko}(a, c) = 1$ , akkor  $c \mid ab$  akkor és csak akkor teljesül, ha  $c \mid b$ .

**13.\* Tétel (Euklidesz lemmája).** Tetszőleges  $a, b, c$  egész számokra ha  $\text{luko}(a, c) \neq 0$ , akkor  $c \mid ab$  akkor és csak akkor teljesül, ha  $\frac{c}{\text{luko}(a, c)} \mid b$ .

**14. Tétel (diofantoszi egyenlet).** Tetszőleges  $a, b, c$  nemnulla egész számok esetén az  $ax + by = c$  kétismeretlenes lineáris diofantoszi egyenlet akkor és csak akkor oldható meg, ha  $\text{luko}(a, b) \mid c$ . Ha  $x_0, y_0$  egy megoldása az egyenletnek, akkor minden  $t$  egész számra az

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

is megoldás, és minden megoldás ilyen alakban megkapható.

## 2. PRÍMSZÁM, SZÁMELMÉLET ALAPTÉTELE, PRÍMSZÁMOK ELOSZLÁSA

**15. Definíció.** A  $p \geq 2$  egész szám **felbonthatatlan**, ha minden  $p = ab$  egészek szorzatára való felbontás **triviális**, azaz  $a = \pm p$  vagy  $b = \pm p$ . Ilyenkor a másik tényező szükségképpen  $\pm 1$ .

**16. Definíció.** A  $p \geq 2$  egész szám **prím**, ha valahányszor osztója egy szorzatnak ( $p \mid ab$ ), mindannyiszor osztója valamelyik tényezőnek ( $p \mid a$  vagy  $p \mid b$ ).

**17. Tétel.** A prímszámok és felbonthatatlan számok ugyanazok.

**18. Tétel (számelmélet alaptétele).** Bármely természetes szám felbontható prímszámok szorzatára, és ez a felbontás a tényezők sorrendjétől eltekintve egyértelmű.

**19. Következmény.** Legyen az  $a$  és  $b$  természetes számok prímfelbontása  $a = p_1^{\alpha_1} \cdot \dots \cdot p_n^{\alpha_n}$  és  $b = p_1^{\beta_1} \cdot \dots \cdot p_n^{\beta_n}$  (azokat a prímeket amelyek csak az egyik számban fordulnak elő, a másik számban nulla kitevővel tüntetjük fel). Ekkor teljesülnek az alábbiak:

- (1)  $a \mid b$  akkor és csak akkor, ha  $\alpha_i \leq \beta_i$  minden  $i$ -re;
- (2)  $\text{luko}(a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdot \dots \cdot p_n^{\min(\alpha_n, \beta_n)}$ ;
- (3)  $\text{lkt}(a, b) = p_1^{\max(\alpha_1, \beta_1)} \cdot \dots \cdot p_n^{\max(\alpha_n, \beta_n)}$ .

**20. Következmény.** Bármely két természetes számnak létezik legkisebb közös többszöröse, és

$$\text{luko}(a, b) \cdot \text{lkt}(a, b) = ab.$$

**21. Tétel.** Végtelen sok prímszám van.

**22. Tétel.** Végtelen sok  $4k - 1$  alakú prímszám van.

**23.\* Tétel.** Végtelen sok  $4k + 1$  alakú prímszám van.

**24.\* Tétel (Dirichlet tétele).** Ha egy számtani sorozat kezdőtagja és pozitív differenciája egymáshoz relatív prím, akkor a számtani sorozatban végtelen sok prímszám található.

**25.\* Tétel (Csebisev tétele).** Bármely pozitív szám és a kétszerese között van prímszám. Pontosabban, minden  $n$  pozitív egészre létezik olyan  $p$  prím, hogy  $n < p \leq 2n$ .

**26. Definíció.** Két prímszámot **ikerprímnak nevezünk**, ha különbségük 2.

**27. Tétel.** A szomszédos prímelek között tetszőlegesen nagy hézagok találhatóak.

**28. Definíció.** A  $\pi(x) = |\{p \text{ prím} \mid p \leq x\}|$  függvényt, amely megadja az  $x$ -nél nem nagyobb prímelek számát, **prímszámláló függvénynek** nevezük.

**29.\* Tétel (prímszámtétel).**  $\lim_{x \rightarrow \infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1$ .

### 3. SZÁMELMÉLETI KONGRUENCIÁK, LINEÁRIS KONGRUENCIARENDSZEREK

**30. Definíció.** Legyenek  $a, b, m$  egész számok. Ha  $m \mid a - b$ , akkor azt mondjuk, hogy  $a$  **kongruens  $b$ -vel modulo  $m$** , és az  $a \equiv b \pmod{m}$  jelölést használjuk. Az  $m$  számot a kongruencia **modulusának** nevezzük.

**31. Tétel.** Tetszőleges  $m \neq 0$  és  $a, b$  egészek esetén  $a \equiv b \pmod{m}$  akkor és csak akkor teljesül, ha  $a$  és  $b$  ugyan azt a maradékot adja  $m$ -el osztva.

**32. Tétel (kongruenciák tulajdonságai).** Tetszőleges  $a, b, c, d, m, n$  egész számokra érvényesek az alábbiak:

- (1)  $a \equiv a \pmod{m}$ ;
- (2) ha  $a \equiv b \pmod{m}$ , akkor  $b \equiv a \pmod{m}$ ;
- (3) ha  $a \equiv b \pmod{m}$  és  $b \equiv c \pmod{m}$ , akkor  $a \equiv c \pmod{m}$ ;
- (4) ha  $a \equiv b \pmod{m}$  és  $c \equiv d \pmod{m}$ , akkor  $a \pm c \equiv b \pm d \pmod{m}$ ;
- (5) ha  $a \equiv b \pmod{m}$  és  $c \equiv d \pmod{m}$ , akkor  $a \cdot c \equiv b \cdot d \pmod{m}$ ;
- (6)  $ca \equiv cb \pmod{m}$  akkor és csak akkor, ha  $a \equiv b \pmod{\frac{m}{\text{Inko}(c,m)}}$ , feltéve hogy  $\text{Inko}(c,m) \neq 0$ ;
- (7) ha  $a \equiv b \pmod{m}$  és  $a \equiv b \pmod{n}$  akkor és csak akkor, ha  $a \equiv b \pmod{\text{lkkt}(m,n)}$ ;
- (8) ha  $a \equiv b \pmod{m}$ , akkor  $\text{Inko}(a,m) = \text{Inko}(b,m)$ .

**33. Definíció.** **Lineáris kongruenciának** nevezzük az  $ax \equiv b \pmod{m}$  alakú egyenletet, ahol  $a, b$  és  $m$  adott egész számok és az  $x$  ismeretlent is az egészek között keressük.

**34. Tétel.** Tetszőleges  $a, b, m$  egészekre az  $ax \equiv b \pmod{m}$  lineáris kongruencia akkor és csak akkor oldható meg, ha  $\text{Inko}(a,m) \mid b$ . Ha  $c$  egy megoldása a lineáris kongruenciának, akkor az általános megoldás  $x \equiv c \pmod{\frac{m}{\text{Inko}(a,m)}}$  alakú.

**35. Definíció.** Adott  $a_i, b_i, n_i$  ( $i = 1, 2, \dots, k$ ) egész számok esetén az alábbi egyenletrendszert **lineáris kongruenciarendszernek** nevezzük, ahol az  $x$  ismeretlen értékét az egész számok között keressük.

$$\begin{aligned} a_1x &\equiv b_1 \pmod{n_1}, \\ a_2x &\equiv b_2 \pmod{n_2}, \\ &\vdots \\ a_kx &\equiv b_k \pmod{n_k}. \end{aligned}$$

A 34. tétel segítségével az egyes lineáris kongruenciák külön megoldhatók (ha  $\text{Inko}(a_i, n_i) \mid b_i$ ) és a rendszer a következő **egyszerűsített alakra** hozható:

$$\begin{aligned} x &\equiv c_1 \pmod{m_1}, \\ x &\equiv c_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv c_k \pmod{m_k}. \end{aligned}$$

**36. Lemma.** A  $k = 2$  esetre az egyszerűsített alakú lineáris kongruenciarendszer akkor és csak akkor oldható meg, ha  $\text{Inko}(m_1, m_2) \mid c_1 - c_2$ . Ha van megoldás, akkor a megoldás modulo  $\text{lkkt}(m_1, m_2)$  egyértelműen meghatározott.

**37.\* Tétel.** Az egyszerűsített alakú lineáris kongruenciarendszer akkor és csak akkor oldható meg, ha bármely két kongruenciából álló részrendszere megoldható (speciálisan, ha a modulusok páronként relatív prímek). Ha van megoldás, akkor a megoldás modulo  $\text{lkkt}(m_1, m_2, \dots, m_k)$  egyértelműen meghatározott.

**38.\* Tétel (kínai maradéktétel).** Tegyük fel, hogy az  $m_1, m_2, \dots, m_k$  modulusok páronként relatív prímek. Legyen  $M = m_1 \cdot m_2 \cdot \dots \cdot m_k$  és  $M_i = \frac{M}{m_i}$ , illetve  $y_i$  az  $M_i y_i \equiv 1 \pmod{m_i}$  segédkongruencia

egy megoldása ( $i = 1, \dots, k$ ). Ekkor tetszőleges  $c_1, c_2, \dots, c_k$  egészekre az

$$x \equiv c_1 \pmod{m_1},$$

$$x \equiv c_2 \pmod{m_2},$$

$\vdots$

$$x \equiv c_k \pmod{m_k}.$$

speciális lineáris kongruenciarendszer általános megoldása

$$x \equiv \sum_{i=1}^k c_i M_i y_i \pmod{M}.$$