

# Matematika informatikusoknak 1.

## Diszkrét matematika I.

Kátai-Urbán Kamilla

8. előadás

# Mire használható a számelmélet?

- Titkosítás (RSA, ECC)
- Algoritmusok: euklideszi algoritmus, prímtesztek, gyors hatványozás, kínai maradéktétel
- Adatkódolás, hibajavítás (Hamming-kód, Reed–Solomon kód (Dimat3))
- Bonyolultságelmélet
- Véletlenszám generálás
- Digitális aláírás

# Oszthatóság

## Relációként

$\alpha = \{(x, y) : x \text{ osztója } y\text{-nak}\}$  az  $A$  halmazon.

Megadjuk az oszthatóság precíz definícióját **természetes számokon**.

## Definíció.

Az  $a$  természetes szám **osztója** a  $b$  természetes számnak ( $b$  **többszöröse**  $a$ -nak), ha létezik olyan  $k$  természetes szám, amelyre  $a \cdot k = b$ . Ha  $a$  osztója  $b$ -nek, akkor ezt úgy jelöljük, hogy  $a \mid b$ . Formálisan:

$$a \mid b \stackrel{\text{def.}}{\iff} \exists k \in \mathbb{N} : a \cdot k = b.$$

## Példa.

- $3 \mid 18$ , mert  $k = 6$ -ra teljesül a definíció, azaz  $3 \cdot 6 = 18$ .
- $3 \nmid 14$ , mert nincs olyan  $k \in \mathbb{N}$ , amelyre  $3 \cdot k = 14$

# Oszthatóság különböző alaphalmazon

Az oszthatósági reláció tulajdonságai függnnek attól, hogy milyen  $A$  alaphalmazon tekintjük.

$$A = \mathbb{N}$$

Korábban már láttuk, hogy a természetes számok halmazán az oszthatóság részbenrendezés, és az  $(\mathbb{N}; |)$  részbenrendezett halmaz legkisebb eleme 1.

$$A = \mathbb{Z}$$

Ha az oszthatóság relációt  $\mathbb{Z}$ -n tekintjük, akkor a reláció már nem antiszimmetrikus, például  $2 \mid -2$  és  $-2 \mid 2$ , de  $2 \neq -2$ .

$$A = \mathbb{Q} \setminus \{0\}$$

Ha az oszthatóságot a nemnulla racionális számok halmazán értelmezzük, ott minden  $a, b$  elem relációban áll, ugyanis minden  $a, b$  elemre  $\frac{b}{a}$  is eleme a halmaznak, így  $a \cdot \frac{b}{a} = b$ . Ezért ezen a halmazon nem túl érdekes az oszthatóság.

## Definíció.

A  $p$  természetes szám **felbonthatatlan (irreducibilis)**, ha  $p \geq 2$  és csak úgy bontható fel két természetes szám szorzatára, hogy valamelyik tényező 1, formálisan:

$$\forall a, b \in \mathbb{N}: p = ab \Rightarrow a = 1 \text{ vagy } b = 1.$$

## Definíció.

Egy  $p$  természetes szám **prímszám**, ha  $p \geq 2$  ha valahányszor osztója egy szorzatnak, mindannyiszor osztója valamelyik tényezőnek, formálisan:

$$\forall a, b \in \mathbb{N}: p \mid ab \Rightarrow p \mid a \text{ vagy } p \mid b.$$

# Felbonthatatlanok, prímek

## Példa.

6 nem prím, mert van olyan szorzat, például  $3 \cdot 4$ , amelyre  $6 \mid 3 \cdot 4$ , de  $6 \nmid 3$  és  $6 \nmid 4$ .

## Tétel.

Egy  $p$  természetes szám pontosan akkor felbonthatatlan, ha prímszám.

## Megjegyzés.

A természetes számok körében a két fogalom egybeesik, középiskolában a felbonthatatlansággal definiálják a prímeket. Vannak azonban olyan algebrai struktúrák, ahol a két fogalom szétválik (pl. páros számok).

## Tétel.

Végtelen sok prímszám létezik.

**Biz.** lásd. 6. feladatsor.

# A számelmélet alaptétele

## A számelmélet alaptétele.

Minden (1-nél nagyobb) természetes szám felbontható prímszámok szorzatára, és ez a felbontás a tényezők sorrendjétől eltekintve egyértelmű.

## Megjegyzés.

Ha szorzatként megengedjük az üres szorzatot, akkor azt definíció szerint 1-nek tekintjük, és a tétel tetszőleges természetes szám esetén kimondható.

A prímtényezős felbontáshoz a prímeket sorravesszük, és vizsgáljuk, hogy melyik osztója a számnak. Ha találtunk prímosztót, akkor a kapott hányadost, ismét elosztjuk. A következő példában a szokásos, táblázatos formában ábrázoljuk az algoritmust.

## Példa.

Felbontjuk a 252 természetes számot prímtényezőkre. A táblázat második oszlopában a prímosztók szerepelnek, az első oszlop következő helyére pedig az osztás hányadosa kerül. Az algoritmust akkor áll le, ha a hányados 1.

|     | osztó |
|-----|-------|
| 252 | 2     |
| 126 | 2     |
| 63  | 3     |
| 21  | 3     |
| 7   | 7     |
| 1   |       |

A prímtényezős felbontás:  $252 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 7$ .

# Prímhatványtényezős felbontás

A számelmélet alaptételének következménye az alábbi.

## Tétel.

Bármely természetes szám előáll páronként különböző prímszámok hatványainak szorzataként, és ez a felbontás a tényezők sorrendjétől eltekintve egyértelmű.

## Példa.

A  $252 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 7$  prímtenyezős felbontás prímhatványtényezős alakban:  
 $252 = 2^2 \cdot 3^2 \cdot 7$ .

A prímhatványtényezős alak könnyebben áttekinthető, például a legnagyobb közös osztó és a legkisebb közös többszörös is könnyebben számolható ebben a formában.

## Definíció.

A  $d$  természetes számot az  $a$  és  $b$  természetes számok **legnagyobb közös osztójának** nevezzük, ha teljesülnek a következők:

(KO)  $d \mid a$  és  $d \mid b$  (közös osztó);

(LN)  $\forall k \in \mathbb{N}: (k \mid a \text{ és } k \mid b) \Rightarrow k \leq d \text{ (} k \mid d \text{)}$  (közös osztók közül a legnagyobb).

Az  $a$  és  $b$  természetes számok legnagyobb közös osztóját  $\text{Inko}(a, b)$ -vel jelöljük.

A definíció (LN) pontjában  $k \leq d$  mellett azért szerepel  $k \mid d$  is, mert az, hogy  $d$  legnagyobb a közös osztók között, nem csak akkor igaz, ha a  $\leq$  (részben)rendezést tekintjük, hanem akkor is, ha az oszthatóság reláció szerinti részbenrendezést nézzük a közös osztók halmazán (ennek  $\mathbb{Z}$ -n lesz fontos szerepe).

## Definíció.

Az  $a$  és  $b$  természetes számok **relatív prímek**, ha  $\text{Inko}(a, b) = 1$ .

## Definíció.

A  $t$  természetes számot az  $a$  és  $b$  természetes számok **legkisebb közös többszörösének** nevezzük, ha teljesülnek a következők:

(KT)  $a \mid t$  és  $b \mid t$  (közös többszörös);

(LK)  $\forall k \in \mathbb{N}: (a \mid k \text{ és } b \mid k) \Rightarrow t \leq k$  ( $t \mid k$ ) (közös többszörösök közül a legkisebb).

Az  $a$  és  $b$  természetes számok legkisebb közös többszörösét  $\text{lkkt}(a, b)$ -vel jelöljük.

A definíció (LK) pontjában az lko-hoz hasonlóan mindkét részbenrendezést feltüntettük:  $t \leq k$  és  $t \mid k$  is teljesül, ha  $k$  egy tetszőleges közös többszörös,  $t$  pedig a legkisebb közös többszörös.

## Tétel.

Legyen az  $a$  és  $b$  természetes számok prímszámhatványtényezős felbontása

$$a = p_1^{\alpha_1} \cdot \dots \cdot p_n^{\alpha_n} \text{ és } b = p_1^{\beta_1} \cdot \dots \cdot p_n^{\beta_n}$$

(azokat a prímeket, amelyek csak az egyik szám felbontásában szerepelnek, a másik számban nulla kitevővel tüntetjük fel). Ekkor teljesülnek az alábbiak:

- ❶  $\text{Inko}(a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdot \dots \cdot p_n^{\min(\alpha_n, \beta_n)}$ ;
- ❷  $\text{lkkt}(a, b) = p_1^{\max(\alpha_1, \beta_1)} \cdot \dots \cdot p_n^{\max(\alpha_n, \beta_n)}$ .

## Példa.

Meghatározzuk 135 és 252 legnagyobb közös osztóját és legkisebb közös többszörösét a fenti tétel segítségével.

Mivel  $135 = 3^3 \cdot 5$  és  $252 = 2^2 \cdot 3^2 \cdot 7$ , ezért a tételben szereplő formában:

$135 = 2^0 \cdot 3^3 \cdot 5 \cdot 7^0$ ,  $252 = 2^2 \cdot 3^2 \cdot 5^0 \cdot 7$ , így:

$$\text{Inko}(135, 252) = 2^{\min(0,2)} \cdot 3^{\min(3,2)} \cdot 5^{\min(1,0)} \cdot 7^{\min(0,1)} = 2^0 \cdot 3^2 \cdot 5^0 \cdot 7^0 = 9,$$

$$\text{lkkt}(135, 252) = 2^{\max(0,2)} \cdot 3^{\max(3,2)} \cdot 5^{\max(1,0)} \cdot 7^{\max(0,1)} = 2^2 \cdot 3^3 \cdot 5^1 \cdot 7^1 = 3780.$$

## Tétel.

Tetszőleges  $a$  és  $b$  természetes szám esetén

$$\text{Inko}(a, b) \cdot \text{lkkt}(a, b) = a \cdot b.$$

## Példa.

Az előző példában kapott felbontások segítségével szemléltetjük a tételt.

$$\begin{aligned} & \text{Inko}(135, 252) \cdot \text{lkkt}(135, 252) = \\ & (2^{\min(0,2)} 3^{\min(3,2)} 5^{\min(1,0)} 7^{\min(0,1)}) \cdot (2^{\max(0,2)} 3^{\max(3,2)} 5^{\max(1,0)} 7^{\max(0,1)}) \end{aligned}$$

Mivel az egyik tényezőben a kitevők minimuma a másikon a kitevők maximuma szerepel, így mindkét számban szereplő kitevők elő fognak fordulni:

$$(2^0 3^2 5^0 7^0) \cdot (2^2 3^3 5^1 7^1) = (3^3 \cdot 5) \cdot (2^2 \cdot 3^2 \cdot 7) = 135 \cdot 252.$$

# Osztók száma

## Jelölés

Tetszőleges  $a$  természetes szám **osztóinak számát**  $\tau(a)$  jelöli.

## Tétel.

Legyen az  $a$  természetes szám prímszámhatványtényezős felbontása:

$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_n^{\alpha_n}$ . Ekkor  $a$  osztóinak száma:

$$\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1) \cdot \dots \cdot (\alpha_n + 1).$$

**Biz.** Ha csak egy  $p^\alpha$  prímszámhatványt tekintünk, akkor annak osztói:

$1, p, p^2, \dots, p^\alpha$ . Tehát a  $p^\alpha$  prímszámhatványnak  $\alpha + 1$  osztója van. Amikor az  $a$  szám osztóit keressük, a különböző prímszámok kitevőit egymástól függetlenül választhatjuk meg, tehát alkalmazható a kombinatorikából ismert szorzási szabály, az osztók száma:  $\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1) \cdot \dots \cdot (\alpha_n + 1)$ .

## Tétel.

Legyen az  $a$  természetes szám prímszaktényezős felbontása:

$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_n^{\alpha_n}$ . Ekkor  $a$  osztóinak száma:

$$\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1) \cdot \dots \cdot (\alpha_n + 1).$$

## Példa.

Meghatározzuk a 252 természetes szám (pozitív) osztóinak számát.

Először tekintjük a prímszaktényezős felbontását:  $252 = 2^2 \cdot 3^2 \cdot 7$ . A fenti tétel alapján az osztók száma a következő:

$$\tau(252) = (2 + 1)(2 + 1)(1 + 1) = 18.$$

# Maradékos osztás $\mathbb{Z}$ -n

A Számrendszerekről szóló előadásban már szerepelt a maradékos osztás természetes számok esetén, most egész számok körében is megadjuk.

## Maradékos osztás tétele.

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  $0 \leq r < |b|$ , ahol  $a$  az **osztandó**,  $b$  az **osztó**,  $q$  a **hányados**,  $r$  a **maradék**.

## Példa.

- Ha 0-t maradékosan osztjuk 2-vel:  $0 = 2 \cdot 0 + 0$ , a hányados 0, maradék 0.
- Ha  $-28$ -at maradékosan osztjuk 6-tal:  $-28 = 6 \cdot (-5) + 2$ , a hányados  $-5$ , maradék 2. Hányadosnak azért nem választhattuk a  $-4$ -et, mert a tétel szerint a maradék mindig nemnegatív.
- Ha  $-33$ -at maradékosan osztjuk  $-5$ -tel:  $-33 = (-5) \cdot 7 + 2$ , a hányados 7, maradék 2. Az előzőhöz hasonló okból nem felelt volna meg, ha a hányadost 6-nak választjuk.

# Oszthatóság tulajdonságai $\mathbb{Z}$ -n

$$\forall a, b \in \mathbb{Z}: a \mid b \stackrel{\text{def}}{\iff} \exists k \in \mathbb{Z}: a \cdot k = b.$$

## Oszthatóság tulajdonságai.

Tetszőleges  $a, b, c$  **egész számokra** teljesülnek az alábbiak:

- (1)  $a \mid a$ ; (reflexív)
- (2)  $(a \mid b \text{ és } b \mid c) \Rightarrow a \mid c$ ; (tranzitív)
- (3)  $1 \mid a$ ;
- (4)  $a \mid 0$ ;
- (5)  $a \mid b \Rightarrow a \mid bc$ ;
- (6)  $(a \mid b \text{ és } a \mid c) \Rightarrow a \mid b \pm c$ ;
- (7)  $(a \mid b \text{ és } b \mid a) \Leftrightarrow a = \pm b$ ;
- (8) ha  $c \neq 0$ , akkor  $a \mid b \Leftrightarrow ac \mid bc$ ;
- (9)  $(a \mid b \text{ és } b \neq 0) \Rightarrow |a| \leq |b|$ .

# Oszthatóság tulajdonságai $\mathbb{Z}$ -n

(1) Bármely  $a \in \mathbb{Z}$ -re  $a \mid a$ .

**Biz.**  $k = 1$  teljesíti a definícióban megadott feltételt:  $a \cdot 1 = a$ .

(2) Bármely  $a, b, c \in \mathbb{Z}$ -re,  $(a \mid b \text{ és } b \mid c) \Rightarrow a \mid c$ .

**Biz.**  $a \mid b \Leftrightarrow \exists k_1 \in \mathbb{Z}: a \cdot k_1 = b$  és  $b \mid c \Leftrightarrow \exists k_2 \in \mathbb{Z}: b \cdot k_2 = c$ , az utóbbi egyenletbe  $b$  helyére a korábban szereplő  $(a \cdot k_1)$ -et behelyettesítve:  $(a \cdot k_1) \cdot k_2 = a \cdot (k_1 \cdot k_2) = c$ , így  $k = k_1 \cdot k_2 \in \mathbb{Z}$  választással teljesül az oszthatóság definíciója:  $a \mid c$ .

(3) Bármely  $a \in \mathbb{Z}$ -re  $1 \mid a$ .

**Biz.**  $k = a$  teljesíti a definícióban megadott feltételt:  $1 \cdot a = a$ .

# Oszthatóság tulajdonságai $\mathbb{Z}$ -n

(4) Bármely  $a \in \mathbb{Z}$ -re  $a \mid 0$ .

**Biz.**  $k = 0$  teljesíti a definícióban megadott feltételt:  $a \cdot 0 = 0$ .

(5)  $a \mid b \Rightarrow a \mid bc$ ;

**Biz.**  $a \mid b \Leftrightarrow \exists k \in \mathbb{Z}: a \cdot k = b$ . Ha az egyenlőség mindkét oldalát szorozzuk  $c$ -vel, akkor  $a \cdot (k \cdot c) = b \cdot c$ , mivel  $k \cdot c \in \mathbb{Z}$ , így teljesül, hogy  $a \mid bc$ .

(6) Bármely  $a, b, c \in \mathbb{Z}$ -re,  $(a \mid b \text{ és } a \mid c) \Rightarrow a \mid b \pm c$ ;

**Biz.**  $a \mid b \Leftrightarrow \exists k_1 \in \mathbb{Z}: a \cdot k_1 = b$  és  $a \mid c \Leftrightarrow \exists k_2 \in \mathbb{Z}: a \cdot k_2 = c$ . Ha összeadjuk a két egyenletet, és kiemelünk  $a$ -t:

$a \cdot k_1 + a \cdot k_2 = a \cdot (k_1 + k_2) = b + c$ , így  $k = k_1 + k_2 \in \mathbb{Z}$  választással teljesül az oszthatóság definíciója:  $a \mid b + c$ . Hasonlóan kaphatjuk, hogy  $a \mid b - c$  is teljesül.

(7) Bármely  $a, b, c \in \mathbb{Z}$ -re,  $(a \mid b \text{ és } b \mid a) \Leftrightarrow a = \pm b$ .

**Biz.**  $a \mid b$  és  $b \mid a \Leftrightarrow \exists k_1, k_2 \in \mathbb{Z}: a \cdot k_1 = b$  és  $b \cdot k_2 = a$ , a második egyenletbe  $b$  helyére behelyettesítve az elsőt:  $(a \cdot k_1) \cdot k_2 = a \cdot (k_1 \cdot k_2) = a$ . Ha  $a = 0$ , akkor tetszőleges  $k_1, k_2$  esetén teljesül. Ha  $a \neq 0$ , akkor az egyenlet mindkét oldalát  $a$ -val leosztva:  $k_1 \cdot k_2 = 1$ . Ez egész számok körében pontosan akkor teljesül, ha  $|k_1| = |k_2| = 1$ , és az előjelük megegyezik, ami ekvivalens azal, hogy  $a = \pm b$ .

## Definíció.

Az  $a, b \in \mathbb{Z}$  számok **asszociáltak**, ha  $a \mid b$  és  $b \mid a$ . Ami az előző tétel alapján ekvivalens azzal, hogy  $a = \pm b$ , vagy másként  $|a| = |b|$ . Ha  $a$  és  $b$  asszociáltak, akkor ezt úgy jelöljük, hogy  $a \sim b$ .

## Tétel.

Az asszociáltság ekvivalenciareláció  $\mathbb{Z}$ -n.

## Tétel.

Az asszociáltság ekvivalenciareláció  $\mathbb{Z}$ -n.

**Biz(onygatás).** Az asszociáltság reflexív, mert az oszthatóság reflexív. Az asszociáltság szimmetrikus, mert az asszociáltság definíciója is „szimmetrikus”. Az asszociáltság tranzitív, mert az oszthatóság tranzitív.

## Példa.

$0 \sim 0, 1 \sim 1, 1 \sim -1, 8 \sim -8, 103 \sim -103.$

## Osztályozás

$\mathbb{Z} / \sim = \{\{a, b\} : |a| = |b|\} = \{\{a, -a\} : a \in \mathbb{Z}\} \subseteq \mathcal{P}(\mathbb{Z}).$

## Definíció.

A  $d$  egész számot az  $a$  és  $b$  egész számok **legnagyobb közös osztójának** nevezzük, ha teljesülnek a következők:

(KO)  $d \mid a$  és  $d \mid b$  (közös osztó);

(LN)  $\forall k \in \mathbb{N} (k \mid a \text{ és } k \mid b) \Rightarrow k \mid d$  (közös osztók közül „a legnagyobb”).

A definíció (LN) pontjában  $k \mid d$  szerepel, ami most nem helyettesíthető  $k \leq d$ -vel, mert nem tudnánk értelmezni a 0-nak saját magával vett közös osztóját. Ugyanis nullának minden egész szám osztója, így nem létezne közöttük legnagyobb  $\leq$  szerint.

Valójában tetszőleges két nemnulla egész szám esetén az oszthatóság szerint sem létezik egyetlen legnagyobb elem a közös osztók halmazán, hiszen korábban láttuk, hogy  $\mathbb{Z}$ -n az oszthatóság reláció nem antiszimmetrikus, így nem kapunk részbenrendezést az oszthatóságra nézve.

## Megjegyzés.

A legnagyobb közös osztó az egész számok körében nem egyértelműen meghatározott, ha  $d$  legnagyobb közös osztó, akkor  $-d$  is. Azaz a legnagyobb közös osztó az egész számok halmazán csak asszociáltság erejéig egyértelmű. Az  $a$  és  $b$  egész számok legnagyobb közös osztóit  $\text{Inko}(a, b)$  jelöli.

## Példa.

A 135 és  $-252$  egész számok legnagyobb közös osztója megkapható úgy, hogy először a 135 és 252 természetes számok legnagyobb közös osztóját meghatározzuk. Korábban már megkaptuk, hogy ez 9. Így

$$\text{Inko}(135, -252) \sim 9$$

teljesül, ahol  $\sim$  a korábban definiált asszociáltsági relációt jelöli, azaz 9 és  $-9$  is teljesíti a legnagyobb közös osztó definícióját.

## Tétel.

Tetszőleg  $a$  egész szám esetén  $\text{Inko}(a, 0) \sim a$ . (Speciálisan:  $\text{Inko}(0, 0) \sim 0$ .)

**Biz.**  $a \mid a$  és  $a \mid 0$  teljesül (17. dia (1)(4)), tehát  $a$  közös osztó, és tetszőleges  $k$  közös osztóra  $k \mid a$  érvényes, tehát  $a$  legnagyobb közös osztó.

A prímtényezőkre bontás nagy számok esetén nem könnyű, ezen alapul több titkosítási módszer is (pl. RSA). A következő dián található euklideszi algoritmusban maradékos osztások sorozatát kell elvégezni, így könnyen algoritmizálható.

A 0-val vett legnagyobb közös osztó a fenti tétel szerint kapható meg. Ahogy korábban már láttuk, nemnulla egész számok Inko-ja asszociáltság erejéig megegyezik az abszolútértékük Inko-jával, így az euklideszi algoritmust elég természetes számok körében megfogalmazni.

## Tétel.

Bármely  $a$  és  $b$  természetes számnak van legnagyobb közös osztója, amely az alábbi euklideszi algoritmussal megkapható. Az  $a$  és  $b$  természetes számokon végrehajtott euklideszi algoritmus maradékos osztások ismételt elvégzését jelenti:

$$a = q_1 b + r_2 \qquad (0 < r_2 < b)$$

$$b = q_2 r_2 + r_3 \qquad (0 < r_3 < r_2)$$

$$\vdots$$

$$r_{n-2} = q_{n-1} r_{n-1} + r_n \qquad (0 < r_n < r_{n-1})$$

$$r_{n-1} = q_n r_n + r_{n+1} \qquad (r_{n+1} = 0).$$

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

## Példa.

Euklideszi algoritmussal meghatározzuk a  $-75$  és  $27$  egész számok legnagyobb közös osztóját.

A számok abszolútértékére alkalmazzuk az euklideszi algoritmust:

$$75 = 2 \cdot 27 + 21 \quad (0 < 21 < 27)$$

$$27 = 1 \cdot 21 + 6 \quad (0 < 6 < 21)$$

$$21 = 3 \cdot 6 + 3 \quad (0 < 3 < 6)$$

$$6 = 2 \cdot 3 + 0$$

A második lépésben az osztandó megegyezik az első lépésben szereplő osztóval. Továbbá, a második lépésben az osztó az első lépésben a maradék. Ez a további lépésekben is hasonlóan alakul.

A legnagyobb közös osztó az utolsó nemnulla maradék, azaz esetünkben  $3$ . Mivel egész számok körében keressük a legnagyobb közös osztót, így a  $-3$  is legnagyobb közös osztó:  $\text{Inko}(-75, 27) \sim 3$ .

$$a = q_1 b + r_2 \quad (0 < r_2 < b)$$

$$b = q_2 r_2 + r_3 \quad (0 < r_3 < r_2)$$

$$\vdots$$

$$r_{n-2} = q_{n-1} r_{n-1} + r_n \quad (0 < r_n < r_{n-1})$$

$$r_{n-1} = q_n r_n + 0$$

A maradékok nemnegatív számok szigorúan monoton csökkenő sorozatát alkotják, így **az algoritmus véges lépésben véget ér.**

**KO:** Az algoritmus garantálja, hogy a legutolsó nemnulla maradék ( $r_n$ ) közös osztó, ugyanis az utolsó sornál a maradék 0, tehát  $r_n$  osztója  $r_{n-1}$ -nek, majd az oszthatóság tulajdonságait felhasználva (17. dia (1)(5)(6)) belátható, hogy  $r_{n-2}$ -nek is osztója  $r_n$ . Ezt megismételhetjük minden sor esetén, tehát  $r_n$  osztója  $a$ -nak és  $b$ -nek is.

**LN:** Ha tekintünk egy  $k$  közös osztót, ami osztója  $a$ -nak és  $b$ -nek, akkor az oszthatóság tulajdonságait felhasználva az 1. sorra (17. dia (5)(6))  $r_2$ -nek is osztója lesz, ami szintén minden sorra átvihető, tehát  $r_n$ -re is igaz.

Így  $r_n$  legnagyobb közös osztó (**LNKO**).

## Definíció.

A  $t$  egész számot az  $a$  és  $b$  egész számok **legkisebb közös többszörösének** nevezzük, ha teljesülnek a következők:

(KT)  $a \mid t$  és  $b \mid t$  (közös osztó);

(LK)  $\forall k \in \mathbb{N} (a \mid k \text{ és } b \mid k) \Rightarrow t \mid k$  (közös többszörösök közül a „legkisebb”).

## Megjegyzés.

Ahogy a legnagyobb közös osztó, úgy a legkisebb közös többszörös is csak asszociáltság erejéig egyértelmű, jele:  $\text{lkkt}(a, b)$ . Ha meghatároztuk az  $\text{lko}$ -t, akkor  $\text{lkkt}$  is megkapható a következő tétel segítségével.

## Tétel.

Tetszőleges  $a$  és  $b$  egész számok esetén

$$\text{lko}(a, b) \cdot \text{lkkt}(a, b) \sim a \cdot b.$$

## Feladat.

Határozzuk meg 300 prímszaktényezős felbontását, és osztóinak számát.

Megoldás: ld. előadáson.

Végeredmény:  $2^2 \cdot 3 \cdot 5^2$ ,  $\tau(300) = 18$ .

## Feladat.

Határozzuk meg a  $-300$  és a  $735$  legnagyobb közös osztóját prímszámhatványtényezőkre bontással és euklideszi algoritmussal is. Adjuk meg a legkisebb közös többszörösüket (nem kell számmal megadni, elég szorzatként).

Megoldás: ld. előadáson.

Végeredmény:  $\text{Inko}(-300, 735) \sim 15$ ,  $\text{lkkt}(-300, 735) \sim (-20) \cdot 735$ .

A 6. elektronikus teszt nov. 21-én indul!

## E-teszt.

- $\text{Inko}(644, 217) = 7$ . **Igaz**, mert  $644 = 2^2 \cdot 7 \cdot 23$  és  $217 = 7 \cdot 31$ .
- $\text{lkkt}(33, 117) = 3861$ . **Hamis**, mert  $33 = 3 \cdot 11$  és  $117 = 3^2 \cdot 13$ , így  $\text{lkkt}(33, 117) = 11 \cdot 117 = 1287$ .
- A 279 és 620 számok relatív prímek. **Hamis**, mert  $279 = 3^2 \cdot 31$ ,  $620 = 2^2 \cdot 5 \cdot 31$ , így  $\text{Inko}(279, 620) = 31$ .