

# 1. Kitüntetett közös osztó

## A legnagyobb közös osztó

### Definíció (FGy1.3.1)

Ha  $a, b \in \mathbb{Z}$  nem mindkettő nulla, akkor a közös osztóik közül a legnagyobbat  $a$  és  $b$  legnagyobb közös osztójának nevezzük.

Jele:  $(a, b)$ . Nyilván  $(0, 0)$  nem létezik (minden egész közös osztó).

$(-12, 8) = 4$ , mert közös osztóik  $\pm 1, \pm 2, \pm 4$ .  $(6439, 8357) = ?$

Probléma: nem látjuk az osztóikat. Tegyük fel, hogy  $d$  közös osztó.

Ekkor  $d \mid 8357 - 6439 = 1918$ . Ezért  $d \mid 6439 - 3 \cdot 1918 = 685$ .

Így  $d \mid 1918 - 3 \cdot 685 = -137$ . Tovább nem megy, mert  $137 \nmid 685$ .

De ez jó, mert akkor visszafelé haladva  $137 \mid 1918, 6439, 8357$ .

Vagyis  $(6439, 8357) = 137$ . Ez az eljárás az *euklideszi algoritmus*. Gyors, és alkalmazható akkor is, ha a számainkat nem tudjuk prímtényezőkre bontani.

## Az euklideszi algoritmus

### Tétel (FGy1.3.3)

Ha  $a, b \in \mathbb{Z}$  és  $b \neq 0$ , akkor legyen

$a = bq_1 + r_1$ , ahol  $(0 < r_1 < |b|)$ ,

$b = r_1q_2 + r_2$ , ahol  $(0 < r_2 < r_1)$ ,

$r_1 = r_2q_3 + r_3$ , ahol  $(0 < r_3 < r_2)$ , és így tovább,

$r_{n-2} = r_{n-1}q_n + r_n$ , ahol  $(0 < r_n < r_{n-1})$ , végül

$r_{n-1} = r_nq_{n+1} + 0$ .

Ekkor az utolsó nem nulla maradék  $r_n = (a, b)$ .

Továbbá  $r_n$  többszöröse  $a$  és  $b$  minden közös osztójának.

### Definíció (FGy1.3.2, K3.1.19)

Az  $a, b \in \mathbb{Z}$ -nek  $d$  kitüntetett közös osztója (KKO), ha közös osztó, és minden közös osztónak többszöröse.

Tehát a legnagyobb közös osztó kitüntetett közös osztó is.

## Az euklideszi algoritmus: bizonyítás

$a = bq_1 + r_1$ , ahol  $(0 < r_1 < |b|)$ ,

$b = r_1q_2 + r_2$ , ahol  $(0 < r_2 < r_1)$ ,

$r_1 = r_2q_3 + r_3$ , ahol  $(0 < r_3 < r_2)$ , és így tovább,

$r_{n-2} = r_{n-1}q_n + r_n$ , ahol  $(0 < r_n < r_{n-1})$ , végül

$r_{n-1} = r_nq_{n+1} + 0$ .

Az utolsó sor miatt  $r_n \mid r_{n-1}$ , az utolsó előtti miatt  $r_n \mid r_{n-2}$ . És így tovább, fölfelé haladva végül  $r_n \mid a, b$ . Tehát  $r_n$  közös osztó. Ha viszont  $t \mid a$  és  $t \mid b$ , akkor az első sorból  $t \mid r_1$ , és lefelé haladva  $t \mid r_2, r_3, \dots$ , végül az utolsó előtti sorból  $t \mid r_n$ . Tehát  $r_n$  minden közös osztónak többszöröse, azaz kitüntetett.  $\square$

**Tétel (FGy1.3.4, K3.1.23)**

Ha  $c > 0$ , akkor  $(ac, bc) = (a, b)c$  (kiemelési tulajdonság).

Valóban, szorozzuk be mindegyik fenti sort  $c$ -vel. □

**A kitüntetett közös osztó egyértelműsége****Tétel (K3.1.20)**

Ha az  $a, b \in \mathbb{Z}$  számoknak  $d_1$  és  $d_2$  is kitüntetett közös osztója, akkor  $d_1$  és  $d_2$  egymás asszociáltjai.

Valóban, mivel  $d_1$  közös osztó és  $d_2$  kitüntetett, ezért  $d_1 \mid d_2$ . Szerepcserével  $d_2 \mid d_1$ . □

- (1) Kitüntetett közös osztó asszociáltja is kitüntetett közös osztó.
- (2) Ha  $a$  és  $b$  nem mindkettő nulla, és van egy  $d$  kitüntetett közös osztójuk, akkor a legnagyobb közös osztójuk  $|d|$ .
- (3) Az  $a = 0$  és  $b = 0$  egyetlen kitüntetett közös osztója a 0.
- (4) Az euklideszi algoritmust gyorsítja, ha mindig a legkisebb abszolút értékű maradékot vesszük.
- (5) A kitüntetett közös osztó polinomok esetében is értelmes.

**Relatív prím számok****Definíció (FGy1.3.7, 1.3.8)**

$a_1, \dots, a_n \in \mathbb{Z}$  *relatív prímelek*, ha minden közös osztójuk egység. *Páronként relatív prímelek*, ha bármely kettő relatív prím.

Példa: 6, 10, 15 relatív prímelek, de semelyik kettő sem az.

**Tétel (FGy1.3.9)**

Ha  $c \mid ab$  és  $(c, a) = 1$ , akkor  $c \mid b$ .

Valóban, ekkor  $c \mid (cb, ab) = (c, a)b = b$ . □

Ha  $p$  felbonthatatlan, akkor  $p$  prímtulajdonságú.

Valóban, tegyük fel, hogy  $p \mid ab$ , de  $p \nmid a$ . Ekkor  $(p, a) \neq p$ , tehát  $(p, a) \mid p$  miatt  $(p, a) = 1$ . Alkalmazzuk az előző tételt. □

## Lineáris diofantikus egyenlet

### Tétel (FGy1.3.5)

Ha  $a, b \in \mathbb{Z}$ , akkor van olyan  $x, y \in \mathbb{Z}$ , hogy  $(a, b) = ax + by$ .

Az euklideszi algoritmus első sorából  $r_1 = a - bq_1$ . A másodiktól

$$r_2 = b - r_1q_2 = b - (a - bq_1)q_2 = -q_2a + (q_1q_2 + 1)b.$$

Lefelé haladva és visszahelyettesítve mindegyik  $r_i$  felírható a kívánt alakban, így végül  $r_n = (a, b)$  is.  $\square$

### Tétel (FGy1.3.6)

Ha  $a, b, c \in \mathbb{Z}$ , akkor az  $ax + by = c$  lineáris diofantikus egyenlet akkor és csak akkor oldható meg alkalmas  $x, y \in \mathbb{Z}$ -re, ha  $(a, b) \mid c$ .

Valóban, ha van ilyen  $x, y$ , akkor  $(a, b) \mid ax + by = c$ .

Megfordítva, legyen  $c = d(a, b)$ . Az előző tétel szerint  $(a, b) = x_0a + y_0b$  alakban írható, így  $c = (dx_0)a + (dy_0)b$ .  $\square$

## Az általános megoldás

### Tétel (FGy7.1.1)

Ha  $a, b, c \in \mathbb{Z}$ , akkor az  $ax + by = c$  lineáris diofantikus egyenlet akkor és csak akkor oldható meg alkalmas  $x, y \in \mathbb{Z}$ -re, ha  $(a, b) \mid c$ .

Ha van egy  $(x_0, y_0)$  megoldás, akkor végtelen sok megoldás van:

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

Behelyettesítéssel látszik, hogy a fenti  $(x, y)$  tényleg megoldás.

Megfordítva, tegyük föl, hogy  $x, y$  is megoldás,

$$\text{azaz } ax + by = c = ax_0 + by_0.$$

$$\text{Átrendezve és } (a, b)\text{-vel osztva } \frac{a}{(a,b)}(x - x_0) = \frac{b}{(a,b)}(y_0 - y).$$

A kiemelési tulajdonság miatt  $\frac{a}{(a,b)}$  és  $\frac{b}{(a,b)}$  már relatív prímek,

ezért  $\frac{b}{(a,b)} \mid x - x_0$ , azaz  $x - x_0 = t \frac{b}{(a,b)}$  alkalmas  $t$ -re.

Ebből  $y_0 - y = t \frac{a}{(a,b)}$  adódik.  $\square$

Az lineáris diofantikus egyenlet konkrét megoldási technikájára a lineáris kongruenciáknál látunk majd példát.

## 2. A számelmélet alaptétele

### Felbonthatatlanok és prímek

#### Definíció (FGy1.4.1)

A  $p$  egész szám *felbonthatatlan*, ha nem nulla, nem egység, és nincs nemtriviális felbontása.

Másképp:  $p$ -nek pontosan négy osztója van az egészek között:  $1, -1, p$  és  $-p$ .

#### Definíció (FGy1.4.2)

A  $p$  egész szám *prím*, ha nem nulla, nem egység, és egy szorzatnak csak úgy lehet osztója, ha osztja valamelyik tényezőt.

**Tétel (FGy1.4.3, az egyik irányt beláttuk)**

Egy  $p$  egész akkor és csak akkor felbonthatatlan, ha prím.

HF: Mutassuk meg, hogy minden prímszám felbonthatatlan.

Cél: Az egészeket egyértelműen felírni prímszámok szorzataként.

**A felbontás létezése****Tétel (FGy1.5.1)**

Minden nullától és egységtől különböző  $c$  egész szám felírható felbonthatatlan számok szorzataként.

Tegyük fel, hogy az állítás nem igaz, és legyen  $c$  a legkisebb abszolút értékű azon számok között, ami nem nulla, nem egység, és nem írható fel felbonthatatlan számok szorzataként.

Ekkor  $c$  nem felbonthatatlan, hiszen különben  $c = c$  (1-tényező) felbontás lenne. Ezért létezik egy  $c = ab$  nemtriviális felbontás. Tehát  $a, b$  nem egység, így abszolút értékük kisebb, mint  $|c|$ . De akkor  $|c|$  minimalitása miatt  $a$  és  $b$  felbonthatatlanok szorzata. A két felbontást egymás mellé fűzve  $c$  megfelelő felbontását kapjuk.  $\square$

HF (K3.2.14): Adaptáljuk ezt a bizonyítást valós együtthatós polinomokra. Abszolút érték helyett használjuk a polinomok fokát.

**Mit jelent az egyértelműség?****Ismétlés: példa egyértelmű és nem egyértelmű felbontásra**

$$6 = 2 \cdot 3 = 3 \cdot 2 = (-2) \cdot (-3) = (-3) \cdot (-2).$$

Csak a tényezők *sorrendjében*, illetve *egységszeresben* különböznek.

$2 \cdot 3 = 6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ . A 2, 3 és  $1 \pm i\sqrt{5}$  felbonthatatlan, és páronként nem asszociáltak: *nem egyértelmű* a felbontás.

**Tétel (FGy1.5.1)**

Ha  $c = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$  két felbontás felbonthatatlanok szorzatára, akkor  $m = n$ , és a tényezők megfeleltethetők egymásnak úgy, hogy az egymásnak megfelelő felbonthatatlanok asszociáltak.

A felbontás *sorrendtől és egységszerestől* eltekintve egyértelmű.

Például  $6 = 2 \cdot 3 = (-3) \cdot (-2)$  esetén  $2 \leftrightarrow (-2)$  és  $3 \leftrightarrow (-3)$ .

### Az egyértelműség bizonyítása

Legyen  $c = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$  két felbontás felbonthatatlanok szorzatára, feltehető, hogy  $n \geq m$ . Mivel  $p_1$  prímtulajdonságú, van olyan  $j$ , hogy  $p_1 \mid q_j$ , ezek egy párt fognak alkotni. Mivel mindkettő felbonthatatlanok (és így  $p_1$  nem egység), ezért  $p_1$  és  $q_j$  asszociáltak. Tehát  $q_1 = e p_1$  alkalmas  $e$  egységre. Egyszerűsíthetünk  $p_1$ -gyel, mert  $p_1 \neq 0$ . Ezért  $p_2 \dots p_n = e q_1 q_2 \dots q_{j-1} q_{j+1} \dots q_m$ . Az eljárást folytassuk  $p_2$ -vel. Mivel  $q_2 \nmid e$ , ezért neki is lesz párja, és ismét tudunk egyszerűsíteni. Amikor a bal oldal elfogy, a jobb oldalon is elfognak a felbonthatatlanok, mert  $n \geq m$ . Ezért  $n = m$  is teljesül.  $\square$

Ez a bizonyítás is adaptálható  $\mathbb{R}[x]$  polinomjaira (K3.2.13). Ehhez is meg kell mutatni, hogy a felbonthatatlanok prímtulajdonságúak.

## 3. Polinom gyökeinek meghatározása

### A racionális gyökteszt

#### A racionális gyökteszt (K3.3.10. Tétel)

$f(x) = a_0 + a_1 x + \dots + a_n x^n$  egész együtthatós polinom. Ha a  $p/q$  nem egyszerűsíthető tört gyöke  $f$ -nek, akkor  $p \mid a_0$  (a számláló osztja  $f$  konstans tagját), és  $q \mid a_n$  (a nevező osztja  $f$  főegyütthatóját).

#### Bizonyítás

$$0 = f(p/q) = a_0 + a_1(p/q) + \dots + a_{n-1}(p/q)^{n-1} + a_n(p/q)^n.$$

$$q^n\text{-nel szorozva } a_0 q^n + a_1 p q^{n-1} + \dots + a_{n-1} p^{n-1} q + a_n p^n = 0.$$

Mindegyik tag osztható  $p$ -vel, kivéve esetleg a legelső. Mivel  $p \mid 0$ , ezért a legelső tag is:  $p \mid a_0 q^n$ . A  $p/q$  nem egyszerűsíthető, így  $p$  és  $q$  relatív prímek. Tehát  $p \mid a_0 q^n$ -ből  $p \mid a_0$  következik. Ugyanezzel a módszerrel kapjuk a  $q \mid a_n$  oszthatóságot is.  $\square$

### Példa a racionális gyöktesztre

#### Példa

Határozzuk meg  $f(x) = 4x^4 + 4x^3 - 11x^2 - 12x - 3$  gyökeit.

#### Megoldás

Ha a  $p/q$  egyszerűsíthetetlen tört gyök, akkor  $p \mid -3$  és  $q \mid 4$ . Ezért  $p = \pm 1$  vagy  $\pm 3$  és  $q = \pm 1, \pm 2$  vagy  $\pm 4$ . Így  $p/q \in \{\pm 1, \pm 1/2, \pm 1/4, \pm 3, \pm 3/2, \pm 3/4\}$ . Ezeket *végigpróbálgatva* kapjuk, hogy *csak*  $-1/2$  racionális gyök.

Hornerrel leosztva  $f(x) = (x + (1/2))(4x^3 + 2x^2 - 12x - 6)$ .

Itt  $4x^3 + 2x^2 - 12x - 6$ -nak *csak*  $-1/2$  lehet racionális gyöke. Ez tényleg gyök:  $f(x) = (x + (1/2))^2 (4x^2 - 12)$ . Mivel  $4x^2 - 12 = 4(x^2 - 3) = 4(x + \sqrt{3})(x - \sqrt{3})$ , ezért  $f$  gyökei:  $-1/2$  (kétszeres),  $\sqrt{3}$  és  $-\sqrt{3}$ .

Gyöktényezőssé alakja  $f(x) = 4(x + (1/2))^2 (x + \sqrt{3})(x - \sqrt{3})$ .

## 4. Összefoglaló

### A 9. előadáshoz tartozó vizsgaanyag

#### Fogalmak

Legnagyobb és kitüntetett közös osztó (FGy1.3.1, 1.3.2, K3.1.19).  
(Páronként) relatív prím számok (FGy1.3.7, 1.3.8).

#### Tételek

Euklideszi algoritmus (FGy1.3.3). A KKO egyértelműsége,  
kiemelési tulajdonsága (FGy1.3.4, K3.1.20, K3.1.23).

Ha  $c \mid ab$ , és  $(c, a) = 1$ , akkor  $c \mid b$  (FGy1.3.9).

Lineáris diofantikus egyenlet (FGy1.3.5, 1.3.6, 7.1.1).

A számelmélet alaptétele (FGy1.5.1, K3.2.14).

A racionális gyökteszt (K3.3.10).