

Diszkrét matematika I. középszint

8. előadás

Mérai László diái alapján

Komputeralgebra Tanszék

2014. ősz

Oszthatóság

Ha a és b **racióális** számok ($b \neq 0$), akkor az a/b osztás mindig elvégezhető (és az eredmény szintén racionális).

Ha a és b **egész** számok, az a/b osztás **nem** mindig végezhető el (a hányados nem feltétlenül lesz egész).

Definíció

Az a egész **osztja** a b egészet (b **osztható** a -val): $a \mid b$, ha létezik olyan c egész, mellyel $a \cdot c = b$ (azaz $a \neq 0$ esetén b/a szintén egész).

Példák

- $1 \mid 13$, mert $1 \cdot 13 = 13$;
- $1 \mid n$, mert $1 \cdot n = n$;
- $6 \mid 12$, mert $6 \cdot 2 = 12$;
- $-6 \mid 12$, mert $(-6) \cdot (-2) = 12$.

A definíció kiterjeszthető például a **Gauss-egészekre**: $\{a + bi : a, b \in \mathbb{Z}\}$.

Példák

- $i \mid 13$, mert $i \cdot (-13i) = 13$;
- $1 + i \mid 2$, mert $(1 + i) \cdot (1 - i) = 2$.

Oszthatóság tulajdonságai

Állítás (HF)

Minden $a, b, c, \dots \in \mathbb{Z}$ esetén

- 1 $a \mid a$;
- 2 $a \mid b$ és $b \mid c \Rightarrow a \mid c$;
- 3 $a \mid b$ és $b \mid a \Rightarrow a = \pm b$;
- 4 $a \mid b$ és $a' \mid b' \Rightarrow aa' \mid bb'$;
- 5 $a \mid b \Rightarrow ac \mid bc$;
- 6 $ac \mid bc$ és $c \neq 0 \Rightarrow a \mid b$;
- 7 $a \mid b_1, \dots, b_k \Rightarrow$
 $\Rightarrow a \mid c_1 b_1 + \dots + c_k b_k$;
- 8 $a \mid 0$, u.i. $a \cdot 0 = 0$;
- 9 $0 \mid a \Leftrightarrow a = 0$;
- 10 $1 \mid a$ és $-1 \mid a$;

Példák

- 1 $6 \mid 6$;
- 2 $2 \mid 6$ és $6 \mid 12 \Rightarrow 2 \mid 12$;
- 3 $a \mid 3$ és $3 \mid a \Rightarrow a = \pm 3$;
- 4 $2 \mid 4$ és $3 \mid 9 \Rightarrow 2 \cdot 3 \mid 4 \cdot 9$;
- 5 $3 \mid 6 \Rightarrow 5 \cdot 3 \mid 5 \cdot 6$;
- 6 $3 \cdot 5 \mid 6 \cdot 5$ és $5 \neq 0 \Rightarrow 3 \mid 6$;
- 7 $3 \mid 6, 9 \Rightarrow 3 \mid 6c_1 + 9c_2$

Egységek

Definíció

Ha egy ε szám bármely másiknak osztója, akkor ε -t **egységnek** nevezzük.

Állítás

Az egész számok körében két egység van: 1 , -1 .

Bizonyítás

A ± 1 nyilván egység.

Megfordítva: ha ε egység, akkor $1 = \varepsilon \cdot q$ valamely q egész számra. Mivel $|\varepsilon| \geq 1$, $|q| \geq 1 \Rightarrow |\varepsilon| = 1$, azaz $\varepsilon = \pm 1$. \square

Példa A Gauss-egészek körében az i is egység: $a + bi = i(b - ai)$.

Megjegyzés

Pontosan 1 osztói az egységek.

Asszociáltak

Oszthatóság szempontjából nincs különbség a 12 ill. -12 között.

Definíció

Két szám **asszociált**, ha egymás egységszeresei.

Megjegyzés (HF)

a és b pontosan akkor asszociált, ha $a \mid b$ és $b \mid a$.

Definíció

Egy számnak az asszociáltjai és az egységek a **triviális osztói**.

Prímek, felbonthatatlanok

Definíció

Ha egy nem-nulla, nem egység számnak a triviális osztóin kívül nincs más osztója, akkor **felbonthatatlannak** (**irreducibilisnek**) nevezzük.

Példa $2, -2, 3, -3, 5, -5$ felbonthatatlanok.

6 nem felbonthatatlan, mert $6 = 2 \cdot 3$.

Definíció

Egy nem-nulla, nem egység p számot **prímszámnak** nevezünk, ha
 $p \mid ab \Rightarrow p \mid a$ vagy $p \mid b$.

Példa $2, -2, 3, -3, 5, -5$.

6 nem prímszám, mert $6 \mid 2 \cdot 3$ de $6 \nmid 2$ és $6 \nmid 3$.

Prímek, felbonthatatlanok

Állítás

Minden prímszám felbonthatatlan.

Bizonyítás

Legyen p prímszám és legyen $p = ab$ egy felbontás. Igazolnunk kell, hogy a vagy b egység.

Mivel $p = ab$, így $p \mid ab$, ahonnan például $p \mid a$. Ekkor $a = pk = a(bk)$, azaz $bk = 1$, ahonnan következik, hogy b és k is egység. \square

A fordított irány nem feltétlenül igaz:

- \mathbb{Z} -ben igaz, (lásd később);
- $\{a + bi\sqrt{5} : a, b \in \mathbb{Z}\}$ -ben nem igaz.

Maradékos osztás

A számelméletben a fő eszközünk a **maradékos osztás** lesz:

Tétel

Tetszőleges a , $b \neq 0$ egész számokhoz egyértelműen léteznek q , r egészek, hogy

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

Bizonyítás

A tételt csak nemnegatív számok esetében bizonyítjuk.

- ① Létezés: a szerinti indukcióval.
 - Ha $a < b$, akkor $a = b \cdot 0 + a$ ($q = 0$, $r = a$).
 - Ha $a \geq b$, akkor tegyük fel, hogy a -nál kisebb számok már felírhatók ilyen alakban. Legyen $a - b = bq^* + r^*$. Ekkor $a = b(q^* + 1) + r^*$ és legyen $q = q^* + 1$, $r = r^*$.
- ② Egyértelműség: legyen $a = bq + r = bq^* + r^*$. Ekkor $b(q - q^*) = r^* - r$. Ez csak akkor lehet, ha $q = q^*$ és $r = r^*$. □

Maradékos osztás

Definíció

Legyenek a, b egész számok ($b \neq 0$). Legyen $a = b \cdot q + r$ ($0 \leq r < |b|$). Ekkor $a \bmod b = r$.

Megjegyzés:

$q = \lfloor a/b \rfloor$, ha $b > 0$, és $q = \lceil a/b \rceil$, ha $b < 0$.

Példa

- $123 \bmod 10 = 3$, $123 \bmod 100 = 23$, $123 \bmod 1000 = 123$;
- $123 \bmod -10 = 3$, ...
- $-123 \bmod 10 = 7$, $-123 \bmod 100 = 77$, $-123 \bmod 1000 = 877$;
- $-123 \bmod -10 = 7$, ...

Maradékos osztás

Példa

- 1 Ha most 9 óra van, hány óra lesz 123 óra múlva?
Osszuk el maradékosan 123-at 24-gyel: $123 = 24 \cdot 5 + 3$. Tehát $9 + 3 = 12$: déli 12 óra lesz!
- 2 Ha most 9 óra van, hány óra lesz 116 óra múlva?
Osszuk el maradékosan 116-ot 24-gyel: $116 = 24 \cdot 4 + 20$. Tehát $9 + 20 = 29$. Újabb redukció: $29 = 24 \cdot 1 + 5$: hajnali 5 óra lesz!
- 3 Milyen napra fog esni jövőre november 11-e?
Milyen napra esett három éve november 15-e?

hétfő $\mapsto 0$

kedd $\mapsto 1$

szerda $\mapsto 2$

csütörtök $\mapsto 3$

péntek $\mapsto 4$

szombat $\mapsto 5$

vasárnap $\mapsto 6$

Osszuk el maradékosan 365-öt 7-tel: $365 = 7 \cdot 52 + 1$.

$\text{kedd} + 1 \text{ nap} \leftrightarrow 1+1=2 \leftrightarrow \text{szerda}$

Osszuk el maradékosan $-(365+365+366)$ -ot (2012. szökőév) 7-tel: $-1096 = 7 \cdot (-157) + 3$.

$\text{szombat} + 3 \text{ nap} \leftrightarrow 5 + 3 = 8 \stackrel{\text{redukció}}{=} 1 \leftrightarrow \text{kedd}$

Számrendszerek

10-es számrendszerben a 123:

$$123 = 100 + 20 + 3 = 1 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0.$$

2-es számrendszerben a 123:

$$\begin{aligned} 1111011_{(2)} &= 1 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0_{(10)} \\ &= 1 \cdot 64 + 1 \cdot 32 + 1 \cdot 16 + 1 \cdot 8 + 0 \cdot 4 + 1 \cdot 2 + 1 \cdot 1_{(10)} \end{aligned}$$

Tétel

Legyen $q > 1$ rögzített egész. Ekkor bármely n pozitív egész

egyértelműen felírható $n = \sum_{i=0}^k a_i q^i$ alakban, ahol $0 \leq a_i < q$ egészek, $a_k \neq 0$.

- Ez a felírás n q számrendszerben történő felírása.
- q a számrendszer alapja.
- a_0, \dots, a_k az n jegyei.
- $k = \lfloor \log_q n \rfloor$.

Számrendszerek

n felírása a q alapú számrendszerben: $n = \sum_{i=0}^k a_i q^i$.

Bizonyítás

A tételt indukcióval bizonyítjuk.

- 1 $n = 0$ esetén a tétel igaz.
- 2 Tfh minden n -nél kisebb számot fel tudunk írni egyértelműen q alapú számrendszerben. A **maradékos osztás tétele** alapján létezik egyértelműen $0 \leq a_0 < q$ egész, hogy $q \mid n - a_0$. Indukció alapján

írjuk fel q alapú számrendszerben $\frac{n - a_0}{q} = \sum_{i=1}^k a_i q^{i-1}$, indukció

alapján a felírás egyértelmű. Ekkor $n = \sum_{i=0}^k a_i q^i$. □

Számrendszerek

Az előbbi bizonyítás módszert is ad a felírásra:

Példa

Írjuk fel az $n = 123$ 10-es számrendszerben felírt számot 2-es számrendszerben.

i	n	$n \bmod 2$	$\frac{n-a_i}{2}$	jegyek
0	123	1	$\frac{123-1}{2}$	1
1	61	1	$\frac{61-1}{2}$	11
2	30	0	$\frac{30-0}{2}$	011
3	15	1	$\frac{15-1}{2}$	1011
4	7	1	$\frac{7-1}{2}$	11011
5	3	1	$\frac{3-1}{2}$	110011
6	1	1	$\frac{1-1}{2}$	1110011

Legnagyobb közös osztó

Definíció

Az a és b számoknak a d szám **kitüntetett közös osztója** (**legnagyobb közös osztója**), ha : $d \mid a$, $d \mid b$, és $c \mid a$, $c \mid b \Rightarrow c \mid d$.

Figyelem! Itt a „legnagyobb” nem a szokásos rendezésre utal:
12-nek és 9-nek legnagyobb közös osztója lesz a -3 is.

A legnagyobb közös osztó csak asszociáltság erejéig egyértelmű.

Definíció

Legyen $(a, b) = \text{Inko}(a, b)$ a **nemnegatív** kitüntetett közös osztó!

Definíció

Az a és b számoknak az m szám **kitüntetett közös többszöröse** (**legkisebb közös többszöröse**), ha : $a \mid m$, $b \mid m$, és $a \mid c$, $b \mid c \Rightarrow m \mid c$.

Legyen $[a, b] = \text{lkkt}(a, b)$ a **nemnegatív** kitüntetett közös többszörös!

Legnagyobb közös osztó kiszámolása, euklideszi algoritmus

Tétel

Bármely két egész számnak létezik legnagyobb közös osztója, és ez meghatározható az euklideszi algoritmussal.

Bizonyítás

Ha valamelyik szám 0 , akkor a legnagyobb közös osztó a másik szám. Tfh a , b nem-nulla számok. Végezzük el a következő osztásokat:

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

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

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

$$\vdots$$

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

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

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

Itt $a = r_{-1}$, $b = r_0$.

Euklideszi algoritmus helyessége

Bizonyítás (folyt.)

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

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

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

$$\vdots$$

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

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

Az algoritmus véges sok lépésben véget ér: $|b| > r_1 > r_2 > \dots$

Az r_n maradék közös osztó: $r_n \mid r_{n-1} \Rightarrow r_n \mid r_{n-1}q_n + r_n = r_{n-2} \Rightarrow \dots \Rightarrow r_n \mid b \Rightarrow r_n \mid a$.

Az r_n maradék a legnagyobb közös osztó: legyen $c \mid a, c \mid b \Rightarrow$

$c \mid a - bq_1 = r_1 \Rightarrow c \mid b - r_1q_2 = r_2 \Rightarrow \dots \Rightarrow c \mid r_{n-2} - r_{n-1}q_n = r_n$. \square

Legnagyobb közös osztó kiszámolása, euklideszi algoritmus

Példa

Számítsuk ki $(172, 62)$ értékét!

i	r_i	q_i	$r_{i-2} = r_{i-1}q_i + r_i$
-1	172	–	–
0	62	–	–
1	48	2	$172 = 62 \cdot 2 + 48$
2	14	1	$62 = 48 \cdot 1 + 14$
3	6	3	$48 = 14 \cdot 3 + 6$
4	2	2	$14 = 6 \cdot 2 + 2$
5	0	3	$6 = 2 \cdot 3 + 0$

A legnagyobb közös osztó: $(172, 62) = 2$

Legnagyobb közös osztó kiszámolása rekurzióval

Tétel

Legyen $a \neq 0$. Ha $b = 0$, akkor $(a, b) = a$. Ha $b \neq 0$, akkor $(a, b) = (|b|, a \bmod |b|)$.

Bizonyítás

Ha $b = 0$, akkor a tétel nyilvánvaló. Mivel $(a, b) = (|a|, |b|)$, feltehető, hogy $a, b > 0$. Ha $b \neq 0$, osszuk el maradékosan a -t b -vel: $a = b \cdot q + (a \bmod b)$. Ez az euklideszi algoritmus első sora.

Példa

Számítsuk ki $(172, 62)$ értékét!

(a, b)	$a \bmod b $
$(172, 62)$	48
$(62, 48)$	14
$(48, 14)$	6
$(14, 6)$	2
$(6, 2)$	0

A legnagyobb közös osztó: $(172, 62) = 2$.

Legnagyobb közös osztó, további észrevételek

Hasonló módon definiálható több szám legnagyobb közös osztója is (HF):
 (a_1, a_2, \dots, a_n) .

Állítás (HF)

Bármely a_1, a_2, \dots, a_n egész számokra létezik (a_1, a_2, \dots, a_n) és
 $(a_1, a_2, \dots, a_n) = ((\dots (a_1, a_2), \dots, a_{n-1}), a_n)$.

Állítás (HF)

Bármely a, b, c egész számokra $(ca, cb) = c(a, b)$.

Bővített euklideszi algoritmus

Tétel

Minden a , b egész számok esetén léteznek x , y egészek, hogy
 $(a, b) = x \cdot a + y \cdot b$.

Bizonyítás

Legyenek q_i , r_i az euklideszi algoritmussal megkapott hányadosok, maradékok.

Legyen $x_{-1} = 1$, $x_0 = 0$ és $i \geq 1$ esetén legyen $x_i = x_{i-2} - q_i x_{i-1}$.

Hasonlóan legyen $y_{-1} = 0$, $y_0 = 1$ és $i \geq 1$ esetén legyen

$$y_i = y_{i-2} - q_i y_{i-1}.$$

Ekkor $i \geq 1$ esetén $x_i a + y_i b = r_i$. (Biz.: HF, indukcióval)

Speciálisan $x_n a + y_n b = r_n = (a, b)$.

Bővített euklideszi algoritmus

Algoritmus: $r_{i-2} = r_{i-1}q_i + r_i$,
 $x_{-1} = 1, x_0 = 0, x_i = x_{i-2} - q_i x_{i-1}$,
 $y_{-1} = 0, y_0 = -1, y_i = y_{i-2} - q_i y_{i-1}$.

Példa

Számítsuk ki $(172, 62)$ értékét, és oldjuk meg a $172x + 62y = (172, 62)$ egyenletet!

i	r_n	q_n	x_i	y_i	$r_i = 172x_i + 62y_i$
-1	172	—	1	0	$172 = 172 \cdot 1 + 62 \cdot 0$
0	62	—	0	1	$62 = 172 \cdot 0 + 62 \cdot 1$
1	48	2	1	-2	$48 = 172 \cdot 1 + 62 \cdot (-2)$
2	14	1	-1	3	$14 = 172 \cdot (-1) + 62 \cdot 3$
3	6	3	4	-11	$6 = 172 \cdot 4 + 62 \cdot (-11)$
4	2	2	-9	25	$2 = 172 \cdot (-9) + 62 \cdot 25$
5	0	3	—	—	—

A felírás: $2 = 172 \cdot (-9) + 62 \cdot 25, x = -9, y = 25$.