Diszkrét matematika 2

1. előadás
Számelmélet

Mérai László
merai@inf.elte.hu
https://sites.google.com/view/laszlomerai

Komputeralgebra Tanszék

2023 ősz

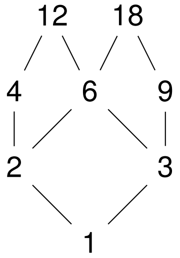
Oszthatóság

Definíció

Az a egész osztja a b egészet: $a \mid b$, ha létezik olyan c egész, mellyel $a \cdot c = b$ (azaz $a \neq 0$ esetén $b/a \in \mathbb{Z}$).

Példa

- $1 \mid 13$, 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 $(-6) \cdot (-2) = 12$;
- $7 \mid 0$, mert $7 \cdot 0 = 0$;
- $0|0$, mert $0 \cdot 0 = 0$.



A $\{1, 2, 3, 4, 6, 9, 12, 18\}$ számok oszthatósági hálója.

Az oszthatóság a szokásos tulajdonságokat teljesíti.

Oszthatóság tulajdonságai – kiegészítő anyag

Az oszthatóság a szokásos tulajdonságokat teljesíti:

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. $a \mid b_1, \dots, b_k \Rightarrow a \mid c_1b_1 + \dots + c_kb_k$
8. $a \mid 0$, u.i. $a \cdot 0 = 0$;
9. $0 \mid a \Leftrightarrow a = 0$;
10. $1 \mid a$ és $-1 \mid a$;

- $6 \mid 6$;
- $2 \mid 6$ és $6 \mid 12 \Rightarrow 2 \mid 12$;

- $2 \mid 4$ és $3 \mid 9 \Rightarrow 2 \cdot 3 \mid 4 \cdot 9$;
- $3 \mid 6 \Rightarrow 5 \cdot 3 \mid 5 \cdot 6$;
- $3 \cdot 5 \mid 6 \cdot 5$ és $5 \neq 0 \Rightarrow 3 \mid 6$;
- $3 \mid 6, 9 \Rightarrow 3 \mid 6c_1 + 9c_2$

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.

- 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 $q = q^* + 1$, $r = r^*$.
- 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

A számelméletben a fő eszközünk a maradékos osztás lesz:

Tétel

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

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

Megjegyzés:

- Jelölés: $r = a \bmod b$.
- $q = \lfloor a/b \rfloor$, ha $a, b > 0$.

Példa

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

Legnagyobb közös osztó

Definíció

Legyenek $a, b \in \mathbb{Z}$. A d nemnegatív egész szám az a és b legnagyobb közös osztója, ha

- $d \mid a$ és $d \mid b$;
- minden $k \in \mathbb{Z}$ esetén, ha $k \mid a$, $k \mid b$, akkor $k \mid d$.

Jelölése: $d = (a, b) = \mathrm{lnko}(a, b) = \gcd(a, b)$. Definíció szerint $(0, 0) = 0$.

Példa

$$(3, 12) = 3, \quad (25, 45) = 5, \quad (-25, -45) = 5, \quad (0, 5) = 5.$$

A következő kérdések merülnek fel:

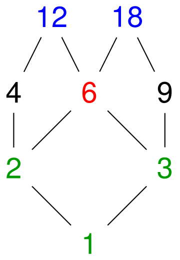
- Létezik-e legnagyobb közös osztó?
- Hogyan lehet kiszámolni?

Legnagyobb közös osztó

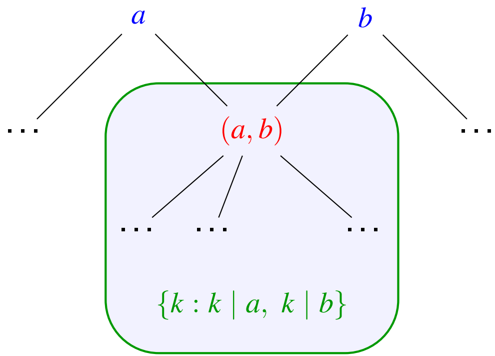
Tétel

Minden $a, b \in \mathbb{Z}$ esetén létezik az (a, b) legnagyobb közös osztó.

Megjegyzés: A tétel szerint egész számok körében az oszthatóság egy nagyon speciális részben rendezés.



$6 = (12, 18)$.



Euklidészi algoritmus

A tétel bizonyítása algoritmikus.

Bizonyítás. Feltehetjük, hogy $(a,b) \neq (0,0)$.
Végezzük el a következő osztásokat:

$$\begin{aligned}
a &= bq_1 + r_1, \quad 0 < r_1 < |b|,\\
b &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1,\\
r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2,\\
&\vdots\\
r_{n-2} &= r_{n-1} q_n + r_n, \quad 0 < r_n < r_{n-1},\\
r_{n-1} &= r_n q_{n+1}.
\end{aligned}$$

Ekkor az Inko az utolsó nem-nulla maradék: $(a,b) = r_n$.
Itt $a = r_{-1}$, $b = r_0$.

Euklidészi algoritmus, példa

Példa
Számoljuk ki $(12, 18) = ?$
Végezzük el a következő osztásokat:

$$18 = 1 \cdot 12 + 6,$$
$$12 = 2 \cdot 6,$$

tehát $(12, 18) = 6$

Példa
Számoljuk ki $(351, 123) = ?$
Végezzük el a következő osztásokat:

$$\begin{aligned} 351 &= 2 \cdot 123 + 105, \\ 123 &= 1 \cdot 105 + 18, \\ 105 &= 5 \cdot 18 + 15, \\ 18 &= 1 \cdot 15 + 3, \\ 15 &= 5 \cdot 3, \end{aligned}$$

tehát $(351, 123) = 3$.

Euklidészi algoritmus, bizonyítás

$$
\begin{aligned}
a &= bq_1 + r_1, \quad 0 < r_1 < |b|,\\
b &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1,\\
r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2,\\
&\vdots\\
r_{n-2} &= r_{n-1} q_n + r_n, \quad 0 < r_n < r_{n-1},\\
r_{n-1} &= r_n q_{n+1}.
\end{aligned}
$$

- Az algoritmus véges sok lépésben véget ér: $|b| > r_1 > r_2 > \cdots > r_n$.
- r_n közös osztó: $r_n \mid r_{n-1} \Rightarrow r_n \mid r_{n-1}q_n + r_n = r_{n-2} \Rightarrow \ldots \Rightarrow r_n \mid b \Rightarrow r_n \mid a$.
- r_n legnagyobb közös osztó: $c \mid a$, $c \mid b \Rightarrow c \mid r_1 \Rightarrow c \mid r_2 \Rightarrow \ldots \Rightarrow c \mid r_n$.

$\square$

Euklidészi algoritmus, további észrevételek

Legnagyobb közös osztó kiszámolása rekurzióval

Legyen $a \neq 0$.

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

(a, b)	$a \bmod \lvert b \rvert$
$(351, 123)$	105
$(123, 105)$	18
$(105, 18)$	15
$(18, 15)$	3
$(15, 3)$	0
$(3, 0)$	$-$

Az euklidészi algoritmus hatékony

- Futási idő $\approx 2 \log a \quad (|b| < a)$
  Bizonyítás. $r_i < \frac{1}{2} r_{i-2}$.
- Prímtényezős felbontással: $\approx e^{\sqrt{\log a \log \log a}}$

$a, b \approx$	2^{50}	2^{100}	2^{150}	2^{200}	2^{250}
eukl. alg.	0,009 ms	0,005 ms	0,005 ms	0,012m	0,007ms
prímtényező	10 ms	10 ms	75 ms	217 ms	14 704 ms

Diofantikus egyenletek

Példa

Adott egy 5 dl-es és egy 7 dl-es söröskorsó. Kimérhetünk a segítségükkel 3 dl sört? Milyen mennyiségeket tudunk segítségükkel kimérni?

(Rendelkezésünkre áll tetszőleges mennyiségű és nagyságú további tárolóedény is.)

Amit ki tudunk mérni:

$$2\,\mathrm{dl} = 7\,\mathrm{dl} - 5\,\mathrm{dl}, \quad 4\,\mathrm{dl} = 7\,\mathrm{dl} - 3\,\mathrm{dl} \quad 3\,\mathrm{dl} = 3 \cdot 5\,\mathrm{dl} - 3 \cdot 4\,\mathrm{dl}$$

Általában:

Adott két pozitív egész szám a, b. Milyen további számok írhatók fel

$$ax + by, \quad x, y \in \mathbb{Z}$$

alakban?

Megjegyzés:

Az $ax + by = c$, $x, y \in \mathbb{Z}$ egyenleteket lineáris diofantikus egyenletek hívjuk.

Bővített euklideszi algoritmus

Tétel

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

Bizonyítás. Elég $c = (a, b)$ esetet vizsgálni.

- Legyenek q_i, r_i az euklideszi algoritmussal megkapott hányadosok, maradékok: $r_{i-2} = r_{i-1}q_i + r_i$
- 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 $x_i a + y_i b = r_i$, speciálisan $x_n a + y_n b = r_n = (a, b)$:
  - $i = -1, 0$ estre igaz: $r_{-1} = a = 1 \cdot a + 0 \cdot b$, $r_0 = b = 0 \cdot a + 1 \cdot b$
  - Általában, ha

$$\begin{aligned} r_{i-2} &= x_{i-2}a + y_{i-2}b \\ r_{i-1} &= x_{i-1}a + y_{i-1}b \\ r_i &= r_{i-2} - r_{i-1}q_i \end{aligned} \quad \Longrightarrow \quad \begin{aligned} r_i &= (x_{i-2}a + y_{i-2}b) - (x_{i-1}a + y_{i-1}b)q_i \\ &= (x_{i-2} - q_i x_{i-1})a + (y_{i-2} - q_i y_{i-1})b \end{aligned}$$

Bővített euklideszi algoritmus, példa

Bővített euklideszi algoritmus:

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

Példa

$(351, 123) = 3 = 351x + 123y$, $x, y = ?$

i	r_i	q_i	x_i	y_i	$x_i \cdot a + y_i \cdot b = r_i$
-1	351	–	1	0	$1 \cdot 351 + 0 \cdot 123 = 351$
0	123	–	0	1	$0 \cdot 351 + 1 \cdot 123 = 123$
1	105	2	1	-2	$1 \cdot 351 + (-2) \cdot 123 = 105$
2	18	1	-1	3	$-1 \cdot 351 + 3 \cdot 123 = 18$
3	15	5	6	-17	$6 \cdot 351 + (-17) \cdot 123 = 15$
4	3	1	-7	20	$(-7) \cdot 351 + 20 \cdot 123 = 3$