Diszkrét matematika 1. középszint

9. előadás

Nagy Gábor
nagygabr@gmail.com
nagy@compalg.inf.elte.hu
compalg.inf.elte.hu/∼ nagy
Mérai László diái alapján

Komputeralgebra Tanszék

2017. ősz

Emlékeztető

- oszthatóság és tulajdonságai;
- egység, illetve asszociált fogalma;
- felbonthatatlan elem, prímtulajdonság;
- maradékos osztás.

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. Tegyük fel, hogy ma 2014. november 11-e (kedd) van.
   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: $365 = 7 \cdot 52 + 1$.
kedd + 1 nap $\leftrightarrow$ 1+1=2$\leftrightarrow$ szerda

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

szombat + 3 nap $\leftrightarrow 5 + 3 = 8 \overset{\text{redukció}}{=} 1 \leftrightarrow$ 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:
$$1111011_{(2)} = 1 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$
$$= 1 \cdot 64 + 1 \cdot 32 + 1 \cdot 16 + 1 \cdot 8 + 0 \cdot 4 + 1 \cdot 2 + 1 \cdot 1$$

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.
- $a_0, \ldots, a_k$ 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. $n = 1$ esetén a tétel igaz: $1 = 1 \cdot q^0$ $(k = 0,\ a_0 = 1)$.
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	$\frac{3-1}{2}$	111011
6	1	1	$\frac{1-1}{2}$	1111011

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 $(c \mid a \wedge c \mid b) \Rightarrow c \mid d$.

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 $(a, b) = lnko(a, b)$ a nemnegatív kitüntetett közös osztó!
$(a, b) = 1$ esetén azt mondjuk, hogy a és b relatív prímek.

Definíció

Az a és b számoknak az m szám kitüntetett közös többszöröse (legkisebb közös többszöröse), ha: $a \mid m$, $b \mid m$, és $(a \mid c \wedge b \mid c) \Rightarrow m \mid c$.
Legyen $[a, b] = lkkt(a, b)$ 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:

$$\begin{aligned}
a &= bq_1 + r_1, \quad 0 < r_1 < |b|,\\
b &= r_1q_2 + r_2, \quad 0 < r_2 < r_1,\\
r_1 &= r_2q_3 + r_3, \quad 0 < r_3 < r_2,\\
&\vdots\\
r_{n-2} &= r_{n-1}q_n + r_n, \quad 0 < r_n < r_{n-1},\\
r_{n-1} &= r_nq_{n+1}.
\end{aligned}$$

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

Euklideszi algoritmus helyessége

Bizonyítás (folyt.)

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

Az algoritmus véges sok lépésben véget ér: $|b| > r_1 > r_2 > \dots$.
Az r_n maradék közös osztó: $r_n \mid r_{n-1} \Rightarrow r_n \mid r_{n-1}q_n + r_n = r_{n-2} \Rightarrow \dots \Rightarrow$
$\Rightarrow r_n \mid b \Rightarrow r_n \mid a$.
Az r_n maradék a legnagyobb közös osztó: legyen $c \mid a$, $c \mid b \Rightarrow$
$c \mid a - bq_1 = r_1 \Rightarrow c \mid b - r_1 q_2 = r_2 \Rightarrow \dots \Rightarrow c \mid r_{n-2} - r_{n-1}q_n = r_n$. □

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, b egész szám. 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, $b \geq 0$. 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)	$a \bmod \lvert b \rvert$
$(172, 62)$	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: $(a_1, a_2, \ldots, a_n)$.

Állítás

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

Állítás

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

Bizonyítás

HF.
Ötlet: alkalmazzuk az euklideszi-algoritmust ca-ra és cb-re.

Bővített euklideszi algoritmus

Tétel

Minden a, b egész szám 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 $x_i = x_{i-2} - q_i x_{i-1}$, továbbá $y_{-1} = 0$, $y_0 = 1$ és $i \geq 1$ esetén legyen $y_i = y_{i-2} - q_i y_{i-1}$.
Teljes indukcióval bebizonyítjuk, hogy $r_{-1} = a$ és $r_0 = b$ jelöléssel $i \geq -1$ esetén $r_i = x_i a + y_i b$.
$i = -1$-re $a = 1 \cdot a + 0 \cdot b$, $i = 0$-ra $b = 0 \cdot a + 1 \cdot b$.
Feltéve, hogy i-nél kisebb értékekre teljesül az összefüggés az euklideszi algoritmus i-edik sora alapján:

$$r_i = r_{i-2} - q_i r_{i-1} = x_{i-2}a + y_{i-2}b - q_i(x_{i-1}a + y_{i-1}b) =$$
$$= (x_{i-2} - q_i x_{i-1})a + (y_{i-2} - q_i y_{i-1})b = x_i \cdot a + y_i \cdot b$$

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

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

Bővitett euklideszi algoritmus

Állítás

$\forall a, b, c \in \mathbb{Z} : (a|bc \wedge (a, b) = 1) \Rightarrow a|c$

Bizonyítás

A bővített euklideszi algoritmus alapján létezik $x, y \in \mathbb{Z}$, hogy $1 = xa + yb$, így $c = xac + ybc = (xc) \cdot a + y \cdot (bc)$. Az oszthatóság lineáris kombinációra vonatkozó tulajdonsága alapján $a|c$.

Diofantikus egyenletek

Diofantikus egyenletek: egyenletek egész megoldásait keressük.

Kétváltozós lineáris diofantikus egyenlet: $ax + by = c$, ahol a, b, c egészek adottak, valamint x, y egészek ismeretlenek.

Állítás

Az $ax + by = c$ diofantikus egyenlet pontosan akkor oldható meg, ha $(a, b) \mid c$. A bővített euklideszi algoritmus segítségével megadható egy megoldás.

Bizonyítás

$\Longrightarrow$: Mivel (a, b) osztója a-nak és (a, b) osztója b-nek, ezért tetszőleges lineáris kombinációjuknak is, így $x, y \in \mathbb{Z}$ esetén $ax + by$-nak is, ami egyenlő c-vel, ha (x, y) megoldás.

$\Longleftarrow$: A bővített euklideszi algoritmus segítségével megadható olyan $x', y' \in \mathbb{Z}$, hogy $ax' + by' = (a, b)$. Mindkét oldalt $\frac{c}{(a,b)} \in \mathbb{Z}$-val szorozva az $a\frac{x'c}{(a,b)} + b\frac{y'c}{(a,b)} = c$ egyenletet kapjuk, amiből leolvasható az $x_0 = \frac{x'c}{(a,b)}$, $y_0 = \frac{y'c}{(a,b)}$ megoldása az egyenletnek.

Diofantikus egyenletek

Állítás

Ha az $ax + by = c$ diofantikus egyenletnek (x_0, y_0) megoldása, akkor az összes megoldás megadható a következő alakban:

$$x_t = x_0 + \frac{b}{(a,b)}t, \quad y_t = y_0 - \frac{a}{(a,b)}t, \quad t \in \mathbb{Z}.$$

Bizonyítás

$ax_t + by_t = ax_0 + \frac{ab}{(a,b)}t + by_0 - \frac{ab}{(a,b)}t = ax_0 + by_0 = c$, így ezek tényleg megoldások.
Legyenek (x_1, y_1) és (x_2, y_2) megoldások. Ekkor $ax_1 + by_1 = c = ax_2 + by_2$, amiből $a(x_1 - x_2) = b(y_2 - y_1)$, így $b|a(x_1 - x_2)$, továbbá $\frac{b}{(a,b)}|\frac{a}{(a,b)}(x_1 - x_2)$. Mivel $(\frac{b}{(a,b)}, \frac{a}{(a,b)}) = 1$, ezért a korábbi állítás értelmében $\frac{b}{(a,b)}|(x_1 - x_2)$. Hasonlóan $\frac{a}{(a,b)}|(y_1 - y_2)$ is bizonyítható.

Diofantikus egyenletek

Példa

Oldjuk meg a $172x + 62y = 6$ egyenletet az egész számok halmazán!
$(172, 62) = 2|6$, ezért van megoldás. A bővített euklideszi algoritmus alapján:
$2 = 172 \cdot (-9) + 62 \cdot 25 \ / \cdot 3$
$6 = 172 \cdot (-27) + 62 \cdot 75$
$x_0 = -27$, $y_0 = 75$
$x_t = -27 + 31 \cdot t$,
$y_t = 75 - 86 \cdot t$,
ahol $t \in \mathbb{Z}$ tetszőleges.

Felbonthatatlanok, prímek

Emlékeztető: f felbonthatatlan: csak triviális osztói vannak: ε, $\varepsilon \cdot f$ típusú osztók (ahol ε egy egység).
p prím: $p \mid ab \Rightarrow p \mid a$ vagy $p \mid b$.
Ha p prím, akkor p felbonthatatlan.

Az egész számok körében a fordított irány is igaz:

Tétel

Minden felbonthatatlan szám prímszám.

Bizonyítás

Legyen p felbonthatatlan, és legyen $p \mid ab$. Tfh. $p \nmid b$. Ekkor p és b relatív prímek (Miért?). A bővített euklideszi algoritmussal kaphatunk x, y egészeket, hogy $px + by = 1$. Innen $pax + aby = a$. Mivel p osztója a bal oldalnak, így osztója a jobb oldalnak is: $p \mid a$. □

Számelmélet alaptétele

Tétel

Minden nem-nulla, nem egység egész szám sorrendtől és asszociáltaktól eltekintve egyértelműen felírható prímszámok szorzataként.