Diszkrét matematika II.
1. előadás

Fancsali Szabolcs Levente
nudniq@inf.elte.hu

ELTE IK Komputeralgebra Tanszék

Mérai László diái alapján

Oszthatóság

Ha a és b racionális számok, 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: $a \mid b$, ha létezik olyan c egész, mellyel $a \cdot c = b$, azaz 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 pédául 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

Az oszthatóság tulajdonságai:

Állítás (HF)

Minden $a, b, c, \cdots \in \mathbb{Z}$ 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. $a \mid b_1, \ldots, b_k \Rightarrow a \mid c_1 b_1 + \cdots + c_k b_k$ minden $c_1, \ldots, c_k$ esetén.
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. $2 \mid 4$ és $3 \mid 9 \Rightarrow 2 \cdot 3 \mid 4 \cdot 9$;
4. $3 \mid 6 \Rightarrow 5 \cdot 3 \mid 5 \cdot 6$;
5. $3 \cdot 5 \mid 6 \cdot 5$ és $5 \neq 0 \Rightarrow 3 \mid 6$;
6. $3 \mid 6, 9 \Rightarrow 3 \mid 6c_1 + 9c_2$

Egységek

A ± 1 oszthatóság szempontjából nem különbözteti meg az egész számokat

Definíció

Ha egy szám bármely másiknak osztója, akkor egységnek nevezzük.

Állítás

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

Bizonyítás

Az ± 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 $\varepsilon = \pm 1$. □

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

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 kívűl nincs más osztója, akkor felbonthatatlanak (irreducibilisnek) nevezzük.

Példa $2, -2, 3, -3, 5, -5$ felbonthatatalnok.
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. □

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 létenek 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 felirhatók 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

- $a \bmod b = r$;
- $q = \lfloor a/b \rfloor$, 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 104 óra múlva?
   Osszuk el maradékosan 104-at 24-gyel: $104 = 24 \cdot 4 + 20$. Tehát $9 + 20 = 29$. Újabb redukció: $29 = 24 \cdot 1 + 5$: hajnali 5 óra lesz!
3. Milyen napra fog esni jövőre szeptember 16?
   Milyen napra esett két éve szeptember 20?

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: $365 = 7 \cdot 22 + 1$.
szerda + 1 nap = 2+1=3=csütörtök

Osszuk el maradékosan -(365 +366)-ot (2020. szökőév) 7-tel: $-731 = 7 \cdot (-104) - 3$.
vasárnap - 3 nap = $6 - 3 = 3$ =csütörtök

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

Tétel

Legyen $q > 1$ rögzített egész. Ekkor bármely n pozitív egész egyértelműen felírható $n = \sum_{i=0}^{k} a_i q^i$ alakban, ahol $0 \leq a_i < q$, $a_k \neq 0$.

- Ez a felírás n q számrendszerben történő felírása.
- q a számrendszer alapja.
- $a_0, \ldots, a_k$ az n jegyei.
- $k = \lceil \log_q n \rceil$.

Számrendszerek

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

Bizonyítás

A tételt indukcióval bizonyítjuk.

1. $n = 0$ esetén a tétel igaz.
2. Tfh minden n-nél kisebb számot feltudunk 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 elöbbi bizonyítás módszert is ad a felírásra:

Példa

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

i	n	n mod 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 legnagyobb közös osztója a d szám: $d = (a, b) = lnko(a, b)$, ha $c \mid a$ és $c \mid b \Rightarrow c \mid d$.

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.

Mostantól (a, b) legyen a pozitív legnagyobb közös osztó!

Definíció

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

Hasonlóan legyen $[a, b]$ mostantól a pozitív legkisebb közös többszörös.

Legnagyobb közös osztó kiszámolása, euklideszi algoritmus

Tétel

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

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 utólsó nem-nulla maradék: $(a, b) = r_n$.

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 végetér: $|b| > r_1 > r_2 > \ldots$.
Az r_n maradék közös osztó: $r_n \mid r_{n-1} \Rightarrow r_n \mid r_{n-1}q_n + r_n = r_{n-2} \Rightarrow \ldots \Rightarrow r_n \mid b \Rightarrow r_n \mid a$.
Az r_n maradék a legnagyobb közös osztó: legyen $c \mid a$, $c \mid b \Rightarrow c \mid a - bq_1 = r_1 \Rightarrow c \mid b - r_1 q_2 = r_2 \Rightarrow \ldots \Rightarrow c \mid r_{n-2} - r_{n-1}q_n = r_n$. □

Legnagyobb közös osztó kiszámolása, euklideszi algoritmus

Példa

Számítsuk ki $(172, 62)$ értékét!

i	r_i	q_i	$r_{i-2} = r_{i-1}q_i + r_i$
–	172	–	–
–	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.
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 (HF): $(a_1, a_2, \ldots, a_n)$.

Állítás (HF)

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 (HF)

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

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

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 az $172x + 62y = (172, 62)$ egyenletet!

i	r_i	q_{i+1}	x_i	y_i	$r_i = 172x_i + 62y_i$
-1	172	–	1	0	$172 = 172 \cdot 1 + 62 \cdot 0$
0	62	2	0	1	$62 = 172 \cdot 0 + 62 \cdot 1$
1	48	1	1	-2	$48 = 172 \cdot 1 + 62 \cdot (-2)$
2	14	3	-1	3	$14 = 172 \cdot (-1) + 62 \cdot 3$
3	6	2	4	-11	$6 = 172 \cdot 4 + 62 \cdot (-11)$
4	2	3	-9	25	$2 = 172 \cdot (-9) + 62 \cdot 25$
5	0	–	31	-86	$0 = 172 \cdot (31) + 62 \cdot (-86)$

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

Felbonthatatlanok, prímek

Emlékeztető: t felbonthatatlan: csak triviális osztói vannak: ε, t, $\varepsilon \cdot t$ típusú osztók (ahol ε egy egység). **Más szavakkal:**

t felbonthatatlan: $t = ab \Rightarrow a$ vagy b egység.

p prím: $p \mid ab \Rightarrow p \mid a$ vagy $p \mid b$.

p prím $\Rightarrow p$ 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. A bővített euklideszi algoritmussal kaphatunk x, y egészeket, hogy $px + by = 1$. Innen $pax + aby = a$. Mivel p osztója a baloldalnak, így osztója a jobboldalnak is: $p \mid a$. □

Számelmélet alaptétele

Tétel

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

Bizonyítás

Csak nemnegatív számokra.
Létezés: Indukcióval: $n = 2$, $n = 3$ esetén igaz (prímek). Általában ha n prím, akkor készen vagyunk, ha nem, akkor szorzatra bomlik nemtriviális módon. A tényezők már felbonthatók indukció alapján.
Egyértelműség: Indukcióval: $n = 2$, $n = 3$ esetén igaz (prímek). Tfh. $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell$, ahol $p_1, p_2 \cdots, p_k, q_1, q_2, \ldots, q_\ell$ prímek. p_1 osztja a bal oldalt $\Rightarrow$ osztja a jobb oldalt, felthehető $p_1 = q_1$.
Egyszerűsítve: $n' = p_2 \cdots p_k = q_2 \cdots q_\ell$. Indukció alapján ez már egyértelmű. □

Számelmélet alaptétele

Definíció

Egy n nem-nulla egész szám kanonikus alakja:

$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell} = \pm \prod_{i=1}^{\ell} p_i^{\alpha_i}$, ahol p_1, p_2,..., p_ℓ pozitív prímek, α_1, α_2,..., α_ℓ pozitív egészek.

Következmény (HF)

Legyenek n, $m > 1$ pozitív egészek: $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell}$,
$m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_\ell^{\beta_\ell}$, (ahol most α_i, $\beta_i \geq 0$ nemnegatív egészek!).
Ekkor

$(m, n) = p_1^{\min\{\alpha_1,\beta_1\}} p_2^{\min\{\alpha_2,\beta_2\}} \cdots p_\ell^{\min\{\alpha_\ell,\beta_\ell\}}$,

$[m, n] = p_1^{\max\{\alpha_1,\beta_1\}} p_2^{\max\{\alpha_2,\beta_2\}} \cdots p_\ell^{\max\{\alpha_\ell,\beta_\ell\}}$,

$(m, n) \cdot [m, n] = m \cdot n$.

Osztók száma

Definíció

Egy $n > 1$ egész esetén legyen $\tau(n)$ az n pozitív osztóinak száma.

Példa

$\tau(6) = 4$: osztók: 1, 2, 3, 6; $\tau(96) = 12$: osztók: 1, 2, 3, 4, 6, 8, ...

Tétel

Legyen $n > 1$ egész, $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell}$ kanonikus alakkal. Ekkor $\tau(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 2) \cdots (\alpha_\ell + 1)$.

Bizonyítás

n lehetséges osztóit úgy kapjuk, hogy a $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_\ell^{\beta_\ell}$ kifejezésben az összes β_i kitevő végigfut a $\{0, 1, \ldots, \alpha_i\}$ halmazon. Így ez a kitevő $\alpha_i + 1$ féleképpen választható. □

Példa

$\tau(2 \cdot 3) = (1 + 1) \cdot (1 + 1)$; $\tau(2^5 \cdot 3) = (5 + 1) \cdot (1 + 1)$.

Prímekről

Tétel (Euklidesz)

Végtelen sok prím van.

Bizonyítás

Indirekt tfh csak véges sok prím van. Legyenek ezek $p_1, \ldots, p_k$. Tekintsük az $n = p_1 \cdots p_k + 1$ számot. Ez nem osztható egyetlen $p_1, \ldots, p_k$ prímmel sem, igy n prímtényezős felbontásában kell szerepelnie egy újabb prímszámnak. $\square$

Tétel (Dirichlet, NB)

Ha a, d egész számok, $d > 0$, $(a, d) = 1$, akkor végtelen sok $ak + d$ alakú prím van.

Prímekről

Prímszámtétel: x-ig a prímek száma $\sim \frac{x}{\ln x}$. (Sok prím van!)

Prímek száma:

x	prímek száma	$x/\ln x$
10	4	4, 343
100	25	21, 715
1000	168	144, 765
10000	1229	1085, 736

Erathoszthenész szitája: Keressük meg egy adott n-ig az összes prímet. Soroljuk fel 2-től n-ig az egész számokat. Ekkor 2 prím. A 2 (valódi) többszörösei nem prímek, ezeket huzzuk ki. A következő szám 3 szintén prím. A 3 (valódi) többszörösei nem prímek, ezeket huzzuk ki. . . Ismételjük az eljárást $\sqrt{n}$-ig. A ki nem húzott számok mind prímek.

Kongruenciák

Oszthatósági kérdésekben sokszor csak a maradékos osztás esetén csak a maradék fontos:

- hét napjai;
- órák száma, ...

Példa

$16 \bmod 3 = 1$ $4 \bmod 3 = 1$: 3-mal való oszthatóság esetén 16 "=" 4.

Definíció

Legyenek a, b, m egészek, akkor $a \equiv b \mod m$ (a és b kongruensek), ha $m \mid a - b$, és $a \not\equiv b \mod m$ (a és b inkongruensek), ha $m \nmid a - b$.

Ekvivalens megfogalmazás: $a \equiv b \mod m \Leftrightarrow a \bmod m = b \bmod m$, azaz m-mel osztva ugyan azt az osztási maradékot adják.

Példa

$16 \equiv 4 \mod 3$ u.i. $3 \mid 16 - 4 \Leftrightarrow 16 \bmod 3 = 1 = 4 \bmod 3$;
$16 \equiv 4 \mod 2$ u.i. $2 \mid 16 - 4 \Leftrightarrow 16 \bmod 2 = 0 = 4 \bmod 2$;
$16 \not\equiv 4 \mod 5$ u.i. $5 \nmid 16 - 4 \Leftrightarrow 16 \bmod 5 = 1 \neq 4 = 4 \bmod 5$.

Kongruencia tulajdonságai

Tétel

Minden a, b, c, d és m egész számra igaz

1. $a \equiv a \mod m$; (reflexív)
2. $a \equiv b \mod m$, $m' \mid m \Rightarrow a \equiv b \mod m'$;
3. $a \equiv b \mod m \Rightarrow b \equiv a \mod m$; (szimmetrikus)
4. $a \equiv b \mod m$, $b \equiv c \mod m \Rightarrow a \equiv c \mod m$; (tranzitív)
5. $a \equiv b \mod m$, $c \equiv d \mod m \Rightarrow a + c \equiv b + d \mod m$;
6. $a \equiv b \mod m$, $c \equiv d \mod m \Rightarrow ac \equiv bd \mod m$.

Bizonyítás

1. $m \mid 0 = a - a$;
2. $m' \mid m \mid a - b \Rightarrow m' \mid a - b$;
3. $m \mid a - b \Rightarrow m \mid b - a = -(a - b)$;
4. $m \mid a - b$, $m \mid b - c \Rightarrow m \mid a - c = (a - b) + (b - c)$;
5. $m \mid a - b$, $m \mid c - d \Rightarrow m \mid (a + c) - (b + d) = (a - b) + (c - d)$;
6. $a = q_1 m + b$, $c = q_2 m + d \Rightarrow$
   $ac = (q_1 m + b)(q_2 m + d) = m(q_1 q_2 m + q_1 d + q_2 b) + bd$. □

Kongruencia tulajdonságai

Példa

Mi lesz 345 mod 7 =?

$345 = 34 \cdot 10 + 5 \equiv 6 \cdot 3 + 5 = 18 + 5 \equiv 4 + 5 = 9 \equiv 2 \mod 7.$

Emlékeztető: $a \equiv b \mod m$, $c \equiv d \mod m \Rightarrow ac \equiv bd \mod m$

Következmény: $a \equiv b \mod m \Rightarrow ac \equiv bc \mod m$.

Példa

$14 \equiv 6 \mod 8 \Rightarrow 42 \equiv 18 \mod 24$

A másik irány nem igaz!

$2 \cdot 7 \equiv 2 \cdot 3 \mod 8 \not\Rightarrow 7 \equiv 3 \mod 8.$

Kongruencia tulajdonságai

Tétel (NB)

Legyenek a, b, c, m egész számok. Ekkor
$ac \equiv bc \mod m \Leftrightarrow a \equiv b \mod \frac{m}{(c,m)}$

Következmény: $ac \equiv bc \mod m, (c,m) = 1 \Leftrightarrow a \equiv b \mod m.$

Példa

$2 \cdot 7 \equiv 2 \cdot 3 \mod 8 \Rightarrow 7 \equiv 3 \mod \frac{8}{2}.$

Bizonyítás

Legyen $d = (c,m)$. Ekkor
$m \mid c(a-b) \Leftrightarrow \frac{m}{d} \mid \frac{c}{d}(a-b)$. Mivel $\left(\frac{m}{d}, \frac{c}{d}\right) = 1,$
ezért $\frac{m}{d} \mid (a-b) \Leftrightarrow a \equiv b \mod \frac{m}{d}.$ □