Diszkrét matematika 2.

Szoftvertervező szakirány
Számelmélet

Juhász Zsófia
jzsofia@inf.elte.hu, jzsofi@gmail.com
Mérai László diái alapján

Komputeralgebra Tanszék

2020. ősz

Bevezetés

„Isten megteremtette a természetes számokat, minden más az ember műve." (Leopold Kroenecker, 1823 – 1891)

A **számelmélet** az egész számok tulajdonságaival foglalkozik.

Alkalmazásai:

- kriptográfia: nyilvános kulcsú rejtjelezés
- kódolás: hibajavító kódok
- számítógépes számelmélet
- sok eredménye általánosítható más struktúrákra: más számhalmazokra, polinomgyűrűkre, ill. ún. egységelemes integritási tartományokra

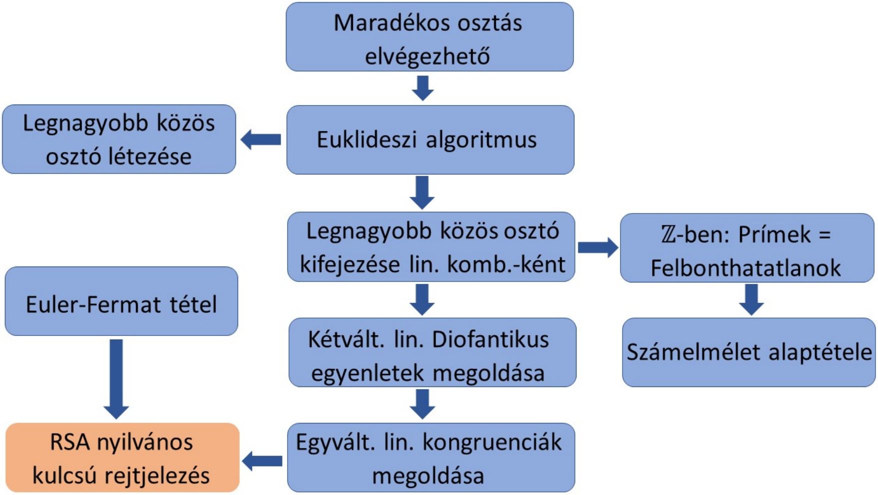
⋮

Áttekintés: Mit tanulunk Számelméletből?

A teljesség igénye nélkül:

- Alapfogalmak, például:
  - oszthatóság és alaptulajdonságai, legnagyobb közös osztó (lnko), legkisebb közös többszörös (lkkt), irreducibilis számok, prímek, maradékos osztás és következményei ...
  - (Bővített) euklideszi algoritmus és következményei
  - Számelmélet alaptétele, kanonikus alak, lnko és lkkt meghatározása a kanonikus alakból, Euler-féle φ-függvény
- Diofantikus egyenletek: kétváltozós lineáris diofantikus egyenletek megoldása
- Kongruenciák: kongruenciák és alaptulajdonságaik, maradékosztályok, egyváltozós lineáris kongruenciák megoldása, szimultán kongruenciarendszerek megoldása a Kínai maradéktétel segítségével
- Euler-Fermat tétel és egy alkalmazása: az RSA nyilvános kulcsú rejtjelező algoritmus
- Prímekről: néhány klasszikus eredmény, bizonyítás nélkül

Néhány összefüggés tanult számelméleti tételek között



Oszthatóság

Ha a és b racionális 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 (oszthatóság)

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 (Oszthatóság alaptulajdonságai, HF)

Minden $a, b, c, \ldots \in \mathbb{Z}$ *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. $a \mid b_1, \ldots, b_k \Rightarrow$
   $\Rightarrow a \mid c_1 b_1 + \ldots + c_k b_k$;
8. $a \mid 0$, *ui.* $a \cdot 0 = 0$;
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 (egységek)

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

Állítás (Egységek az egészek körében)

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: $a + bi = i(b - ai)$.

Állítás (Egységek ekvivalens jellemzése)

Pontosan 1 *osztói az egységek.*

Asszociáltak

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

Definíció (asszociáltak)

Két szám asszociált, ha $a \mid b$ és $b \mid a$.

Állítás (Asszociáltak ekvivalens jellemzése)

Két szám a és b pontosan akkor asszociált, ha egymás egységszeresei.

Bizonyítás

$\Longrightarrow$: *Legyen* $b = ab_1$ *és* $a = ba_1$. *Ekkor* $b = ab_1 = ba_1b_1$, *így* $a_1b_1 = 1$, *vagyis* a_1 *és* b_1 *is egységek.*
$\Longleftarrow$: *Ha* $b = \varepsilon a$ *és* $a = \varepsilon' b$, *ahol* $\varepsilon, \varepsilon'$ *egységek, akkor* $a|b$ *és* $b|a$ *nyilvánvaló.*

Definíció (triviális osztók)

Egy számnak az asszociáltjai és az egységek a triviális osztói.

Prímek, felbonthatatlanok

Definíció (felbonthatatlan számok)

Egy nem-nulla, nem egység a számot felbonthatatlannak (irreducibilisnek) nevezünk, ha $\forall b, c \in \mathbb{Z} : a = bc \Rightarrow b$ egység vagy c egység.

Példa $2, -2, 3, -3, 5, -5$ felbonthatatlanok.
6 nem felbonthatatlan, mert $6 = 2 \cdot 3$.

Állítás (Felbonthatatlanok ekvivalens jellemzése)

Egy nem-nulla, nem egység szám pontosan akkor felbonthatatlan, ha a triviális osztóin kívül nincs más osztója.

Definíció (prímek)

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 prím felbonthatatlan)

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 (Maradékos osztás tétele az egész számok körében)

Tetszőleges a egész számhoz és $b \neq 0$ egész számhoz 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 $1 \leq a < b$, akkor $a = b \cdot 0 + a$ ($q = 0$, $r = a$).*
   - *Legyen $a \geq b$ és tegyük fel, hogy az a-nál kisebb számok mind felírhatók ilyen alakban. Az indukciós feltevés értelmében $a - b = bq^* + r^*$. Ekkor $a = b(q^* + 1) + r^*$ ($q = q^* + 1$, $r = r^*$).*
2. *Egyértelműség: Legyen $a = bq_1 + r_1 = bq_2 + r_2$ valamely q_1, q_2, r_1, r_2 egészekre, ahol $0 \leq r_1, r_2 < b$. Tf. indirekt, hogy $q_1 \neq q_2$. Ekkor $b(q_1 - q_2) = r_2 - r_1$. Így $q_1 \neq q_2$ miatt $|b(q_1 - q_2)| = |b| \cdot |q_1 - q_2| \geq |b| \cdot 1 = |b|$, míg $0 \leq r_1, r_2 < b$ miatt $|r_2 - r_1| < |b|$, így $|b(q_1 - q_2)| \neq |r_2 - r_1|$, ami ellentmondás. Ezért $q_1 = q_2$ és $r_1 = r_2$.*

Maradékos osztás

Definíció (osztási maradék)

Legyenek a és b egész számok ($b \neq 0$). Legyen $a = b \cdot q + r$, ahol q és r egészek, $0 \leq r < |b|$. Ekkor $a \bmod b = r$ az a szám b-vel vett osztási maradéka.

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

Példa

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

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:

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

Tétel (Számok felírása különböző számrendszerekben)

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

- Ez a felírás n b alapú számrendszerben történő felírása.
- b a számrendszer alapja.
- $a_0, \ldots, a_k$ az n jegyei.
- $k = \lfloor \log_b n \rfloor$.

Számrendszerek

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

Bizonyítás

A tételt indukcióval bizonyítjuk.

1. $n < b$ *esetén* $a_0 = n$ *választással* $n = a_0 b^0$. *A felírás egyértelműsége triviális (Miért?).*
2. *Legyen* $n \geq b$ *és tfh. az állítás igaz minden* n*-nél kisebb pozitív egészre. Legyen* r *és* q *az* n*-nek* b*-vel vett osztási maradéka, ill. hányadosa* $(n = bq + r)$. *Mivel* $1 \leq q < n$, *az indukciós feltevés alapján* q *felírható a kívánt* $q = \sum_{i=1}^{k} a_i b^{i-1}$ *alakban. Ekkor* $a_0 = r$ *választással* $n = bq + r = \sum_{i=1}^{k} a_i b^i + a_0 = \sum_{i=0}^{k} a_i b^i$ *az* n *felírása.*

   Az egyértelműséghez vegyük észre, hogy n *bármely* $n = \sum_{i=0}^{k} a_i b^i$ *felírása esetén* $a_0 = r$, *ami egyértelmű. A többi „jegy" egyértelműsége abból következik, hogy* $q = (n - r) : b = \left(\sum_{i=0}^{k} a_i b^i - a_0\right) : b = \sum_{i=1}^{k} a_i b^{i-1}$ *a* q *egy felírása* b *alapú számrendszerben, ami az ind. feltevés alapján egyértelmű.*

$\square$

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 (legnagyobb közös osztó)

Az a és b számoknak a d szám legnagyobb közös osztója (kitüntetett 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.
- Jelölés: Legyen $(a, b) = lnko(a, b)$ a nemnegatív legnagyobb közös osztó!

Definíció (relatív prímek)

$(a, b) = 1$ esetén azt mondjuk, hogy a és b relatív prímek.

Definíció (legkisebb közös többszörös)

Az a és b számoknak az m szám legkisebb közös többszöröse (kitüntetett közös töbszöröse), 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 legkisebb közös többszörös!

Legnagyobb közös osztó kiszámolása, euklideszi algoritmus

Tétel (Euklideszi algoritmus az egészek körében)

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.)

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

Az algoritmus véges sok lépésben véget ér: $|b| > r_1 > r_2 > \ldots$.
Az r_n maradék közös osztó: $r_n \mid r_{n-1} \Rightarrow r_n \mid r_{n-1}q_n + r_n = r_{n-2} \Rightarrow \ldots \Rightarrow$
$\Rightarrow r_n \mid b \Rightarrow r_n \mid a$.
Az r_n maradék a legnagyobb közös osztó: legyen $c \mid a$, $c \mid b \Rightarrow$
$c \mid a - bq_1 = r_1 \Rightarrow c \mid b - r_1q_2 = r_2 \Rightarrow \ldots \Rightarrow c \mid r_{n-2} - r_{n-1}q_n = r_n$. □

Legnagyobb közös osztó kiszámolása, euklideszi algoritmus

Példa

Számítsuk ki $(172, 62)$ értékét!

i	r_i	q_i	$r_{i-2} = r_{i-1}q_i + r_i$
-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 (Legnagyobb közös osztó kiszámolása rekurzióval)

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. Egyébként* $a = bq + (a \bmod b)$ *valamely* q *egészre,így* a *a* b *és* $a \bmod b$ *egy egész együtthatójú lin. komb.-ja. Ezért* $(b, a \bmod b) \mid a$*, tehát* $(b, a \bmod b) \mid (a, b)$*. Hasonlóan,* $a \bmod b = a - bq$ *miatt* $a \bmod b$ *egész együtthatójú lin. komb.-ja* a*-nak és* b*-nek, így* $(a, b) \mid (b, a \bmod b)$*. Innen* $(a, b) = (b, a \bmod b)$ *következik.*

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: $(a_1, a_2, \ldots, a_n)$.

Definíció (legnagyobb közös osztó általános esetben)

Az $a_1, a_2, \ldots, a_n$ számoknak egy d szám legnagyobb közös osztója, ha $d|a_i$ $(1 \leq i \leq n)$ és $\forall c \in \mathbb{Z} : c|a_i$ $(1 \leq i \leq n) \Rightarrow c|d$.

Állítás (Legnagyobb közös osztó létezése általános esetben)

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 (Bővített euklideszi algoritmus)

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

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

Bővített 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.

Tétel (Kétvált. lin. diofant. egyelet megoldhatósága)

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

Tétel (Kétvált. lin. diofant. egyelet összes megoldása)

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_0, y_0) *és* (x', y') *megoldások. Ekkor* $ax_0 + by_0 = c = ax' + by'$, *amiből* $a(x' - x_0) = b(y_0 - y')$, *így* $b|a(x' - x_0)$, *továbbá* $\frac{b}{(a,b)}|\frac{a}{(a,b)}(x' - x_0)$.

Mivel $\left(\frac{b}{(a,b)}, \frac{a}{(a,b)}\right) = 1$ *(Miért?), ezért a korábbi állítás értelmében* $\frac{b}{(a,b)}|(x' - x_0)$. *Tehát* $x' - x_0 = \frac{b}{(a,b)}t$, *azaz* $x' = x_0 + \frac{b}{(a,b)}t$ *valamely* $t \in \mathbb{Z}$*-re.*

Behelyettesítve $ax' + by' = c$*-be adódik* $y' = y_0 - \frac{a}{(a,b)}t$.

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: f nem-nulla, nem-egység és $\forall b, c \in \mathbb{Z} : f = bc \implies b$ egység vagy c egység,
  ami azzal ekvivalens, hogy
  f nem-egység és csak triviális osztói vannak: ε, $\varepsilon \cdot f$ típusú osztók (ahol ε egy egység).
- p prím: p nem-nulla, nem-egység és $\forall a, b \in \mathbb{Z} : p \mid ab \Rightarrow p \mid a$ vagy $p \mid b$.

Ha p prím, akkor p felbonthatatlan.
Az egész számok körében a fordított irány is igaz:

Tétel ($\mathbb{Z}$-ben minden felbonthatatlan szám prím)

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: $p \mid a$. $\square$

Számelmélet alaptétele

Tétel (Számelmélet alaptétele)

Minden 0-tól és egységektől különböző egész szám sorrendtől és asszociáltaktól eltekintve egyértelműen felírható prímszámok szorzataként.

Bizonyítás

Csak nemnegatív számokra.
Létezés: *Indukcióval:*

- $n = 2$ *esetén igaz (prím).*
- *Legyen* $n > 2$ *és tegyük fel, hogy minden* n*-nél kisebb,* 2*-nél nagyobb vagy egyenlő szám felírható prímek szorzataként. Ha* n *prím, akkor készen vagyunk („egytényezős szorzat"). Ha nem, akkor felbontható, és ezért szorzatra bomlik nemtriviális módon, azaz* $n = ab$ *alakba írható, ahol* a *és* b *egyike sem egység. Feltehető, hogy* a *és* b *pozitívak, így* $2 \leq a, b$ *és ezért* $2 \leq a = \frac{n}{b} \leq \frac{n}{2}$ *és* $2 \leq b = \frac{n}{a} \leq \frac{n}{2}$*. Tehát* a *és* b *az indukciós feltevés alapján már előáll prímek szorzataként, és így* n *is.*

Számelmélet alaptétele

Bizonyítás (folytatás)

Egyértelműség: *Indukcióval:*

- $n = 2$ *esetén igaz (felbonthatatlan).*
- *Legyen* $n > 2$ *és tegyük fel, hogy minden* n*-nél kisebb,* 2*-nél nagyobb vagy egyenlő szám felírása prímek szorzataként lényegében egyértelmű. Ha* n *felbonthatatlan, akkor csak „egytényezős szorzatként" írható fel prímek szorzataként, mert több tényezős szorzatra csak úgy bontható, hogy legalább egy tényező egység a szorzatban, ami nem prím. Így a felbontás egyértelmű.*

  Tfh. n *felbontható. Legyen* $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell$ *az* n *két felbontása. Az általánosság megszorítása nélkül feltehető, hogy* $p_1, p_2, \ldots, p_k$ *és* $q_1, q_2, \ldots, q_\ell$ *mind pozitívak. Ekkor* $p_1 p_2, \cdots p_k = q_1 q_2 \cdots q_\ell$ *és* p_1 *osztja a bal oldalt, ezért osztja a jobb oldalt, így a prímtulajdonság miatt osztja annak valamelyik tényezőjét; feltehető* $p_1 | q_1$*. Mivel* q_1 *felbonthatatlan (hiszen prím), ezért* $p_1 = q_1$*. (Miért?) Egyszerűsítve:* $n' = p_2 \cdots p_k = q_2 \cdots q_\ell$*. Indukció alapján ez már egyértelmű.*

$\square$

Számelmélet alaptétele

Definíció (kanonikus alak)

Egy 0-tól és egységektől különböző n 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 különböző pozitív prímek, α_1, α_2,..., α_ℓ pozitív egészek.

Következmény

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

1. $(n, m) = p_1^{\min\{\alpha_1,\beta_1\}} p_2^{\min\{\alpha_2,\beta_2\}} \cdots p_\ell^{\min\{\alpha_\ell,\beta_\ell\}}$;
2. $[n, m] = p_1^{\max\{\alpha_1,\beta_1\}} p_2^{\max\{\alpha_2,\beta_2\}} \cdots p_\ell^{\max\{\alpha_\ell,\beta_\ell\}}$;
3. $(n, m) \cdot [n, m] = n \cdot m$;
4. *ha* $(n, m) = 1$, *akkor* $[n, m] = n \cdot m$.

Osztók száma

Definíció ($\tau(n)$)

Egy $n > 0$ egész esetén legyen $\tau(n)$ az n pozitív osztóinak száma.

Példa

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

Tétel (Osztók száma a kanonikus alakból)

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

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. $\square$

Példa

$\tau(2 \cdot 3) = (1 + 1) \cdot (1 + 1) = 4$; $\tau(2^5 \cdot 3) = (5 + 1) \cdot (1 + 1) = 12$.

Kongruenciák

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

- hét napjai;
- órák száma.

Példa

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

Definíció (kongruencia relációk)

Legyenek $a, b, m \neq 0$ egészek, ekkor $a \equiv b \pmod m$ (a és b kongruensek modulo m), ha $m \mid a - b$, és $a \not\equiv b \pmod m$ (a és b inkongruensek), ha $m \nmid a - b$.

Ekvivalens megfogalmazás: $a \equiv b \pmod m \Leftrightarrow a \bmod m = b \bmod m$, azaz m-mel osztva ugyanazt az osztási maradékot adják. ($m \neq 0$ esetén)

Példa

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

Kongruencia tulajdonságai

Tétel (A kongruenciák néhány alaptulajdonsága)

Minden a, b, c, d, $m \neq 0$ *és* $m' \neq 0$ *egész számra igaz:*

1. $a \equiv a \pmod{m}$; *(reflexivitás)*
2. $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$; *(szimmetria)*
3. $a \equiv b \pmod{m}$, $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$; *(tranzitivitás)*
4. $a \equiv b \pmod{m}$, $c \equiv d \pmod{m} \Rightarrow a + c \equiv b + d \pmod{m}$;
5. $a \equiv b \pmod{m}$, $c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$;
6. $a \equiv b \pmod{m}$, $m' \mid m \Rightarrow a \equiv b \pmod{m'}$.

Bizonyítás

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

Kongruencia tulajdonságai: maradékosztályok

Az előbbi tétel 1., 2. és 3. pontjai alapján tetszőleges m egész esetén a modulo m kongruencia ($\equiv$) ekvivalenciareláció $\mathbb{Z}$-n. Ennek ekvivalenciaosztályait modulo m maradékosztályoknak nevezzük.

Definíció (maradékosztályok modulo m)

Egy rögzített m modulus és a egész esetén, az a-val kongruens elemek halmazát az a által reprezentált maradékosztálynak nevezzük:
$\overline{a} = \{x \in \mathbb{Z} : x \equiv a \pmod{m}\} = \{a + \ell m : \ell \in \mathbb{Z}\}$.

Megjegyzések:

- Két szám pontosan akkor tartozik ugyanahhoz a $\bmod m$ maradékosztályhoz, ha m-mel való osztási maradékuk megegyezik.
- A $\bmod m$ maradékosztályok száma m.

Kongruencia tulajdonságai

Emlékeztető:

- $a \equiv b \pmod{m},\ c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$
- $a \equiv b \pmod{m},\ c \equiv d \pmod{m} \Rightarrow a + c \equiv b + d \pmod{m}$

Példa

Mi lesz $345 \bmod 7 =?$

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

Emlékeztető: $a \equiv b \pmod{m},\ c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$.

Következmény: $a \equiv b \pmod{m} \Rightarrow ac \equiv bc \pmod{m}$.

Példa

$14 \equiv 6 \pmod{8} \Rightarrow 42 \equiv 18 \pmod{8}$

A másik irány nem igaz!

$2 \cdot 7 \equiv 2 \cdot 3 \pmod{8} \not\Rightarrow 7 \equiv 3 \pmod{8}$.

Kongruencia tulajdonságai

Tétel (Kongruencia osztása)

Legyenek a, b, $c \neq 0$, $m \neq 0$ *egész számok. Ekkor*
$ac \equiv bc \pmod{m} \Leftrightarrow a \equiv b \left(\bmod \frac{m}{(c,m)}\right)$

Következmény: $(c, m) = 1$ esetén $ac \equiv bc \pmod{m} \Leftrightarrow a \equiv b \pmod{m}$.

Példa

$2 \cdot 7 \equiv 2 \cdot 3 \pmod{8} \Rightarrow 7 \equiv 3 \ (\bmod \frac{8}{2})$.

Bizonyítás

Legyen $d = (c, m)$. *Ekkor*
$ac \equiv bc \pmod{m} \Leftrightarrow m \mid c(a-b) \Leftrightarrow \frac{m}{d} \,\Big|\, \frac{c}{d}(a-b)$. *Mivel* $\left(\frac{m}{d}, \frac{c}{d}\right) = 1$,
ezért $\frac{m}{d} \,\Big|\, \frac{c}{d}(a-b) \Leftrightarrow \frac{m}{d} \,\Big|\, (a-b) \Leftrightarrow a \equiv b \left(\bmod \frac{m}{d}\right)$. $\square$

Lineáris kongruenciák

Oldjuk meg a $2x \equiv 5 \pmod{7}$ kongruenciát!

Ha x egy megoldás és $x \equiv y \pmod{7}$, akkor y szintén megoldás.

Keressük a megoldást a $\{0, 1, \ldots, 6\}$ halmazból!

$$x = 0 \Rightarrow 2x = 0 \not\equiv 5 \pmod{7};$$
$$x = 1 \Rightarrow 2x = 2 \not\equiv 5 \pmod{7};$$
$$x = 2 \Rightarrow 2x = 4 \not\equiv 5 \pmod{7};$$
$$x = 3 \Rightarrow 2x = 6 \not\equiv 5 \pmod{7};$$
$$x = 4 \Rightarrow 2x = 8 \equiv 1 \not\equiv 5 \pmod{7};$$
$$x = 5 \Rightarrow 2x = 10 \equiv 3 \not\equiv 5 \pmod{7};$$
$$x = 6 \Rightarrow 2x = 12 \equiv 5 \pmod{7}.$$

A kongruencia megoldása: $\{6 + 7\ell : \ \ell \in \mathbb{Z}\}$.

Van-e jobb módszer?

Oldjuk meg a $23x \equiv 4 \pmod{211}$ kongruenciát! Kell-e 211 próbálkozás?

Lineáris kongruenciák

Tétel (Lineáris kongruenciák megoldása)

Legyenek a, b, $m \neq 0$ *egész számok. Ekkor az* $ax \equiv b \pmod{m}$ *kongruencia pontosan akkor oldható meg, ha* $(a, m) \mid b$. *Ez esetben pontosan* (a, m) *darab páronként inkongruens megoldás van* $\bmod m$. *(Más szóval a megoldáshalmaz* (a, m) *különböző modulo* m *maradékosztály uniója.)*

Bizonyítás

$ax \equiv b \pmod{m} \Leftrightarrow m|b - ax \Leftrightarrow ax + my = b$ *valamely* y *egészre.*
Tehát $ax \equiv b \pmod{m}$ *megoldásai pontosan* $ax + my = b$ *„*x*-beli" megoldásai lesznek. Mivel* $ax + my = b$ *pontosan akkor oldható meg, ha* $(a, m) \mid b$, *így* $ax \equiv b$ *megoldhatóságának is ugyanez a feltétele. A kétváltozós, lineáris, diofantikus egyenletekről tanultak alapján tehát a kongruencia megoldásai az* $x_t = x_0 + \frac{m}{(a,m)} \cdot t$ *alakú számok lesznek, ahol* $t \in \mathbb{Z}$ *és* x_0 *egy tetszőleges megoldás.*
Tekintsük a következő (a, m) *db megoldást:*
$x_k = x_0 + k\frac{m}{(a,m)}$: $k = 0, 1, \ldots, (a, m) - 1$.
Ezek páronként inkongruensek $\bmod m$ *(Miért?), és bármely* x *megoldás esetén van köztük* x*-szel kongruens* $\bmod m$ *(Miért?).*

Lineáris kongruenciák

1. $ax \equiv b \pmod m \Leftrightarrow \exists y \in \mathbb{Z} : ax + my = b$.
2. Pontosan akkor van megoldás, ha $(a, m) \mid b$.
3. Oldjuk meg az $ax' + my' = (a, m)$ egyenletet (bővített euklideszi algoritmus)!
4. Kongruencia egy megoldása: $x_0 = \frac{b}{(a,m)} x'$
5. Inkongruens megoldások: $x_k = x_0 + k\frac{m}{(a,m)}$: $k = 0, 1, \dots, (a, m) - 1$.
6. Összes megoldások halmaza: inkongruens megoldások modulo m maradékosztályainak uniója

Példa Oldjuk meg a $23x \equiv 4 \pmod{211}$ kongruenciát!

i	r_i	q_i	x'_i
-1	23	–	1
0	211	–	0
1	23	0	1
2	4	9	-9
3	3	5	46
4	1	1	-55
5	0	3	–

Algoritmus: $r_{i-2} = r_{i-1}q_i + r_i$,
$x'_{-1} = 1$, $x'_0 = 0$,
$x'_i = x'_{i-2} - q_i x'_{i-1}$.

Lnko: $(23, 211) = 1 \mid 4 \Rightarrow$
Egy megoldás: $x_0 = 4(-55) \equiv 202 \pmod{211}$.

Összes megoldás: $\{202 + 211\ell : \ \ell \in \mathbb{Z}\}$.

(Ell.: ezek megoldások: $23 \cdot (202 + 211\ell) - 4 = 4642 + 211\ell = (22 + \ell) \cdot 211$)

Lineáris kongruenciák

Példa

Oldjuk meg a $10x \equiv 8 \pmod{22}$ kongruenciát!

i	r_i	q_i	x'_i
-1	10	–	1
0	22	–	0
1	10	0	1
2	2	2	-2
3	0	5	–

Algoritmus: $r_{i-2} = r_{i-1}q_i + r_i$,
$x'_{-1} = 1$, $x'_0 = 0$,
$x'_i = x'_{i-2} - q_i x'_{i-1}$

Lnko: $(10, 22) = 2 \mid 8 \Rightarrow$
Két inkongruens megoldás:
$x_0 = 4(-2) \equiv 14 \pmod{22}$
$x_1 = 4(-2) + 1 \cdot \frac{22}{2} \equiv 14 + 11 \equiv 3 \pmod{22}$.

Összes megoldás: $\{14 + 22\ell : \ \ell \in \mathbb{Z}\} \bigcup \{3 + 22\ell : \ \ell \in \mathbb{Z}\}$.

Ezek megoldások: $x_0 = 14$: $10 \cdot 14 - 8 = 132 = 6 \cdot 22$,
$x_1 = 3$: $10 \cdot 3 - 8 = 22 = 1 \cdot 22$.

Szimultán kongruenciák

Szeretnénk olyan x egészet, mely egyszerre elégíti ki a következő kongruenciákat:

$$\left.\begin{aligned} 2x &\equiv 1 \pmod{3} \\ 4x &\equiv 3 \pmod{5} \end{aligned}\right\}$$

A kongruenciákat külön megoldva:

$$\left.\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 2 \pmod{5} \end{aligned}\right\}$$

Látszik, hogy $x = 2$ megoldás lesz!

Vannak-e más megoldások?

- $2, 17, 32, \ldots, 2 + 15\ell$;
- további megoldások?
- hogyan oldjuk meg az általános esetben:

$$\left.\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \end{aligned}\right\}$$

Szimultán kongruenciák

Feladat: Oldjuk meg a következő kongruenciarendszert:

$$\left.\begin{aligned} a_1x &\equiv b_1 \pmod{m_1} \\ a_2x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ a_nx &\equiv b_n \pmod{m_n} \end{aligned}\right\}$$

Az egyes $a_ix \equiv b_i \pmod{m_i}$ lineáris kongruenciák külön megoldhatóak:

$$\left.\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_n \pmod{m_n} \end{aligned}\right\}$$

Szimultán kongruenciák

Feladat: Oldjuk meg a következő kongruenciarendszert:

$$\left.\begin{array}{c} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \\ \vdots \\ x \equiv c_n \pmod{m_n} \end{array}\right\}$$

Feltehető, hogy az $m_1, m_2, \ldots, m_n$ modulusok páronként relatív prímek, mert az általános eset mindig visszavezethető erre az esetre.

Kínai maradéktétel

Tétel (Kínai maradéktétel)

Legyenek $m_1, m_2, \ldots, m_n \neq 0$ *páronként relatív prím számok,* $c_1, c_2, \ldots, c_n$ *egészek. Ekkor az*

$$\left.\begin{array}{l} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \\ \quad\vdots \\ x \equiv c_n \pmod{m_n} \end{array}\right\}$$

kongruenciarendszer megoldható, és bármely két megoldás kongruens egymással modulo $m_1 \cdot m_2 \cdots m_n$*.*

Kínai maradéktétel

$x \equiv c_1 \pmod{m_1}$, $x \equiv c_2 \pmod{m_2}$, $\ldots$, $x \equiv c_n \pmod{m_n}$. $x = ?$

Bizonyítás

A bizonyítás konstruktív!
Legyen $m = m_1 m_2$. A bővített euklideszi algoritmussal oldjuk meg az $m_1 x_1 + m_2 x_2 = 1$ egyenletet. Legyen $c_{1,2} = m_1 x_1 c_2 + m_2 x_2 c_1$. Ekkor $c_{1,2} \equiv c_j \pmod{m_j}$ $(j = 1, 2)$ (Miért?). Ha $x \equiv c_{1,2} \pmod{m}$, akkor x megoldása az első két kongruenciának. Megfordítva: ha x megoldása az első két kongruenciának, akkor $x - c_{1,2}$ osztható m_1-gyel, m_2-vel, így a szorzatukkal is: $x \equiv c_{1,2} \pmod{m}$, mivel m_1 és m_2 relatív prímek. Az eredeti kongruenciarendszer ekvivalens az

$$\left.\begin{array}{l} x \equiv c_{1,2} \pmod{m_1 m_2} \\ x \equiv c_3 \pmod{m_3} \\ \quad\vdots \\ x \equiv c_n \pmod{m_n} \end{array}\right\}$$

kongruenciarendszerrel. n szerinti indukcióval adódik az állítás. $\square$

Szimultán kongruenciák

Példa

$$\left.\begin{array}{l} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{array}\right\}$$

Oldjuk meg az $3x_1 + 5x_2 = 1$ egyenletet!
Megoldások: $x_1 = 2$, $x_2 = -1$. $\Rightarrow$
$\Rightarrow c_{1,2} = 3 \cdot 2 \cdot 3 + 5 \cdot (-1) \cdot 2 = 18 - 10 = 8$.
Összes megoldás: $\{8 + 15\ell : \ \ell \in \mathbb{Z}\}$.

Példa

$$\left.\begin{array}{l} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 4 \pmod{7} \end{array}\right\} \overset{c_{1,2}=8}{\Longrightarrow} \left.\begin{array}{l} x \equiv 8 \pmod{15} \\ x \equiv 4 \pmod{7} \end{array}\right\}$$

Oldjuk meg a $15x_{1,2} + 7x_3 = 1$ egyenletet!
Megoldások: $x_{1,2} = 1$, $x_3 = -2$. $\Rightarrow$
$\Rightarrow c_{1,2,3} = 15 \cdot 1 \cdot 4 + 7 \cdot (-2) \cdot 8 = 60 - 112 = -52$.
Összes megoldás: $\{-52 + 105\ell : \ \ell \in \mathbb{Z}\} = \{53 + 105\ell : \ \ell \in \mathbb{Z}\}$.

Teljes maradékrendszer

Definíció (teljes maradékrendszer)

Egy rögzített m modulus esetén egy olyan számhalmazt, amely minden modulo m maradékosztályból pontosan egy számot tartalmaz, teljes maradékrendszernek nevezzük modulo m.

Példa

$\{33, -5, 11, -11, -8\}$ teljes maradékrendszer modulo 5.

Gyakori választás teljes maradékrendszerekre ($m > 0$ feltehető, különben alább $|m|$ írandó mindenhol m helyett)

- Lehetséges $\bmod m$ maradékok („Legkisebb nemnegatív maradékok"): $\{0, 1, \ldots, m-1\}$;
- „Legkisebb abszolút értékű maradékok":
  $\left\{0, \pm 1, \ldots, \pm \frac{m-1}{2}\right\}$, ha $2 \nmid m$;
  $\left\{0, \pm 1, \ldots, \pm \frac{m-2}{2}, \frac{m}{2}\right\}$, ha $2 \mid m$.

Redukált maradékrendszer

Megjegyzés: ha egy maradékosztály valamely eleme relatív prím a modulushoz, akkor az összes eleme az: $(a+\ell m, m) = (a, m) = 1$. Ezeket a maradékosztályokat redukált maradékosztályoknak nevezzük.

Definíció (redukált maradékrendszer)

Rögzített m modulus esetén egy olyan számhalmazt, amely pontosan egy számot tartalmaz minden modulo m redukált maradékosztályból, redukált maradékrendszernek nevezünk modulo m.

Példa

$\{1, 2, 3, 4\}$ redukált maradékrendszer modulo 5.
$\{1, -1\}$ redukált maradékrendszer modulo 3.
$\{1, 19, 29, 7\}$ redukált maradékrendszer modulo 8.
$\{0, 1, 2, 3, 4\}$ nem redukált maradékrendszer modulo 5.

Euler-féle φ függvény

Definíció (Euler-féle φ függvény)

Egy $m > 0$ egész szám esetén legyen $\varphi(m)$ az m-nél kisebb, hozzá relatív prím természetes számok száma $\varphi(m) = |\{j: \ 0 \leq j < m, (m, j) = 1\}|$.

Példa

$\varphi(5) = 4$: 5-höz relatív prím természetes számok: $1, 2, 3, 4$.
$\varphi(6) = 2$: 6-hoz relatív prím természetes számok: $1, 5$.
$\varphi(12) = 4$: 12-höz relatív prím természetes számok: $1, 5, 7, 11$.
$\varphi(15) = 8$: 15-höz relatív prím természetes számok:
$1, 2, 4, 7, 8, 11, 13, 14$.

Megjegyzés: $\varphi(m)$ a redukált maradékosztályok száma modulo m.

Euler-féle φ függvény

$$\varphi(m) = |\{j:\ 0 \leq j < m, (m,j) = 1\}|$$

Tétel ($\varphi(m)$ kiszámítása m kanonikus alakjából)

Legyen m kanonikus alakja $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell}$. Ekkor

$$\varphi(m) = m \cdot \prod_{i=1}^{\ell} \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^{\ell} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}).$$

Példa

$\varphi(5) = 5\left(1 - \frac{1}{5}\right) = 5^1 - 5^0 = 4;$
$\varphi(6) = 6\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = (2^1 - 2^0)(3^1 - 3^0) = 2;$
$\varphi(12) = 12\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = (2^2 - 2^1)(3^1 - 3^0) = 4;$
$\varphi(15) = 15\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = (3^1 - 3^0)(5^1 - 5^0) = 8.$

Euler-Fermat tétel

Tétel (Euler-Fermat tétel)

Legyen $m > 0$ *egész szám,* a *olyan egész, melyre* $(a, m) = 1$. *Ekkor*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Következmény (Fermat tétel)

Legyen p *prímszám,* $p \nmid a$. *Ekkor* $a^{p-1} \equiv 1 \pmod{p}$,
illetve tetszőleges a *esetén* $a^p \equiv a \pmod{p}$.

Példa

$\varphi(6) = 2 \Rightarrow 5^2 = 25 \equiv 1 \pmod{6}$;
$\varphi(12) = 4 \Rightarrow 5^4 = 625 \equiv 1 \pmod{12}$; $7^4 = 2401 \equiv 1 \pmod{12}$.

Figyelem! $2^4 = 16 \equiv 4 \not\equiv 1 \pmod{12}$, mert $(2, 12) = 2 \neq 1$.

Euler-Fermat tétel bizonyítása

Lemma (Teljes, ill. redukált maradékrendszer lineáris transzformációi)

Legyen $m > 0$ *egész,* $a_1, a_2, \ldots, a_m$ *teljes maradékrendszer modulo* m*. Ekkor minden* a, b *egészre, melyre* $(a, m) = 1$, $a \cdot a_1 + b$, $a \cdot a_2 + b, \ldots,$ $a \cdot a_m + b$ *szintén teljes maradékrendszer. Továbbá, ha* $a_1, a_2, \ldots, a_{\varphi(m)}$ *redukált maradékrendszer modulo* m*, akkor* $a \cdot a_1$, $a \cdot a_2, \ldots,$ $a \cdot a_{\varphi(m)}$ *szintén redukált maradékrendszer.*

Bizonyítás

Tudjuk, hogy $aa_i + b \equiv aa_j + b \pmod{m} \Leftrightarrow aa_i \equiv aa_j \pmod{m}$*. Mivel* $(a, m) = 1$*, egyszerűsíthetünk* a*-val:* $a_i \equiv a_j \pmod{m}$*. Tehát* $a \cdot a_1 + b$, $a \cdot a_2 + b, \ldots,$ $a \cdot a_m + b$ *páronként inkongruensek. Mivel számuk* m*, így teljes maradékrendszert alkotnak.*

$(a_i, m) = 1 \wedge (a, m) = 1 \Rightarrow (a \cdot a_i, m) = 1$*. Továbbá* $a \cdot a_1$, $a \cdot a_2, \ldots,$ $a \cdot a_{\varphi(m)}$ *páronként inkongruensek, számuk* $\varphi(m) \Leftrightarrow$ *redukált maradékrendszert alkotnak.* $\square$

Euler-Fermat tétel bizonyítása

Tétel (Euler-Fermat) $(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod m$.

Bizonyítás

Legyen $a_1, a_2, \ldots, a_{\varphi(m)}$ egy redukált maradékrendszer modulo m. Mivel $(a, m) = 1 \Rightarrow a \cdot a_1,\ a \cdot a_2, \ldots,\ a \cdot a_{\varphi(m)}$ szintén redukált maradékrendszer.

Innen

$$a^{\varphi(m)} \prod_{j=1}^{\varphi(m)} a_j = \prod_{j=1}^{\varphi(m)} a \cdot a_j \equiv \prod_{j=1}^{\varphi(m)} a_j \pmod m.$$

Mivel $\prod_{j=1}^{\varphi(m)} a_j$ relatív prím m-hez, így egyszerűsíthetünk vele:

$a^{\varphi(m)} \equiv 1 \pmod m$.

□

Euler-Fermat tétel

Tétel (Euler-Fermat) $(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod m$

Példa

Mi lesz a 3^{111} utolsó számjegye tízes számrendszerben?
Mi lesz $3^{111} \bmod 10$?
$\varphi(10) = 4 \Rightarrow$
$3^{111} = 3^{4\cdot 27+3} = \left(3^4\right)^{27} \cdot 3^3 \equiv 1^{27} \cdot 3^3 = 3^3 = 27 \equiv 7 \pmod{10}$

Oldjuk meg a $2x \equiv 5 \pmod 7$ kongruenciát!
$\varphi(7) = 6$. Szorozzuk be mindkét oldalt 2^5-nel. Ekkor
$5 \cdot 2^5 \equiv 2^6 x \equiv x \pmod 7$. És itt $5 \cdot 2^5 = 5 \cdot 32 \equiv 5 \cdot 4 = 20 \equiv 6 \pmod 7$.

Oldjuk meg a $23x \equiv 4 \pmod{211}$ kongruenciát!
$\varphi(211) = 210$. Szorozzuk be mindkét oldalt 23^{209}-nel. Ekkor
$4 \cdot 23^{209} \equiv 23^{210} x \equiv x \pmod{211}$. És itt $4 \cdot 23^{209} \equiv \ldots \pmod{211}$.

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 (Miért?), így 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 $a + kd$ alakú ($k \in \mathbb{N}$) prím van.

Prímekről

Tetszőleges $x \in \mathbb{N}^+$ esetén $\pi(x)$ jelöli az x-nél nem nagyobb, pozitív prímek számát.

Tétel (Prímszámtétel, NB.)

$\pi(x) \sim \frac{x}{\ln x}$. (*Sok prím van!*)

Prímek száma:

x	$\pi(x)$	$x/\ln x$
10	4	4,33
100	25	21,71
1000	168	144,76
10000	1229	1085,73

Eratoszthenész 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 húzzuk ki. A következő (ki nem húzott) szám a 3, ez szintén prím. A 3 (valódi) többszörösei nem prímek, ezeket húzzuk ki... Ismételjük az eljárást $\sqrt{n}$-ig. A ki nem húzott számok mind prímek.

RSA

Ron **Rivest**, Adi **Shamir** és Leonard **Adleman** 1977-ben a következő eljárást javasolták:

Kulcsgenerálás: Legyen p, q két (nagy, 1024 bites) prím, $n = p \cdot q$.
Legyen $1 < e < \varphi(n)$ olyan, hogy $(e, \varphi(n)) = 1$.
Legyen d az $ex \equiv 1 \pmod{\varphi(n)}$ kongruencia megoldása.
Kulcsok: - nyilvános kulcs (n, e),
- titkos kulcs d.

Titkosítás: Adott $0 \leq m < n$ üzenet titkosítása:
$c = m^e \bmod n$.

Kititkosítás Adott $0 \leq c < n$ titkosított üzenet kititkosítása:
$m = c^d \bmod n$.

Algoritmus helyessége:
$c^d = (m^e)^d = m^{e \cdot d} = m^{k \cdot \varphi(n)+1} \overset{\text{E-F}}{\equiv} m \pmod{n}$

RSA

Valóságban az m üzenet egy titkos kulcs további titkosításhoz.

Az eljárás biztonsága azon múlik, hogy nem tudjuk hatékonyan faktorizálni az $n = p \cdot q$ szorzatot.

Feladat

Találjuk meg a következő szám osztóit.
RSA-100 =
1522605027922533360535618378132637429718068114961380688
6579084945801229632589528976540003506920061139

RSA-2048=

2519590847565789349402718324004839857142928212620403202777713783604366202070759555
6264018525880784406918290641249515082189298559149176184502808489120072844992687392
807287776735971418347270261896375014971824691165077613379859095700097330459748808428
401797429100642458691817195118746121515172654632282216869987549182422433637259085141
8654620435767984233871847744479207399342365848238242811981638150106748104516603773
06056201619676256133844143603833904414952634432190114657544454178424020924616515723
35077870774981712577246796292638635637328991215483143816789988504044536402352738195
1378636564391212010397122822120720357

RSA

RSA-2048 faktorizálása:

Próbaosztás (Eratoszthenész szitája): n szám esetén $\sim \sqrt{n}$ osztást kell végezni:

RSA-2048 $n \sim 2^{2048}$, $\sqrt{n} \sim 2^{1024}$ próbaosztás.

Ha 1 másodperc alatt $\sim 10^9 \approx 2^{30}$ osztás $\Rightarrow$ $2^{1024}/2^{30} = 2^{994}$ másodperc kell a faktorizáláshoz.

2^{994} másodperc $\approx 2^{969}$ év.

Ugyanezt 2 db géppel: 2^{968} év.

Ugyanezt a legjobb (ismert) algoritmussal:
$2500000000000000000000000000000$ év ($= 2,5 \cdot 10^{30}$)

Univerzum életkora: $1,38 \cdot 10^{10}$ év.

RSA

Példa

Kulcsgenerálás:

Legyen $p = 61$, $q = 53$ és $n = 61 \cdot 53 = 3233$, $\varphi(3233) = 3120$.

Legyen $e = 17$. Bővített euklideszi algoritmussal: $d = 2753$.

Nyilvános kulcs: $(n = 3233, e = 17)$;

Titkos kulcs: $d = 2753$.

Titkosítás: Legyen $m = 65$.

$c = 2790 \equiv 65^{17} \pmod{3233}$

Kititkosítás: Ha $c = 2790$:

$2790^{2753} \equiv 65 \pmod{3233}$

Digitális aláírást is lehet generálni: e és d felcserélésével:

(Ekkor külön n', e', d' kell a titkosításhoz!)

Aláírás Legyen $s = m^d \bmod n$, ekkor az aláírt üzenet: (m, s).

Ellenőrzés $m \stackrel{?}{\equiv} s^e \pmod{n}$.