Diszkrét matematika 2

2. előadás
Számelmélet

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

Komputeralgebra Tanszék

2023 ősz

Prímszámok

"The obvious mathematical breakthrough would be development of an easy way to factor large prime numbers." – Bill Gates

(Nagy matematikai áttörés lenne nagy prímszámok faktorizációja (szorzattá bontása).)

Definíció

Egy $p \neq 0, \pm 1$ szám prímszám, ha

$$p = a \cdot b \Longrightarrow p = \pm a \quad \text{vagy} \quad p = \pm b.$$

Példa $2, 3, 5$ számok prímek, a $4 = 2 \cdot 2, 6 = 2 \cdot 3$ nem prímek.

- Ekvivalens definíció: $p \mid a \cdot b \Longrightarrow p \mid a \quad$ vagy $\quad p \mid b.$
- Nagy matematikai áttörés lenne nagy számok prímfaktorizációja, azaz megtalálni nagy számok prímosztóit.
  Precízen: adott két prímszám p, q, a szorzatból $p \cdot q$ számoljuk ki p-t.

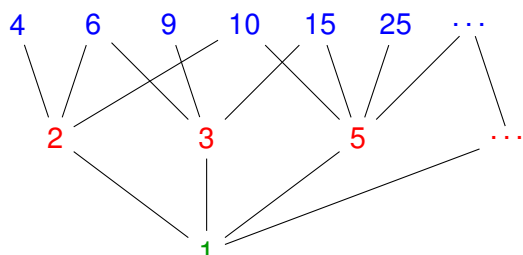
Prímszámok

Definíció

Egy $p \neq 0, \pm 1$ szám prímszám, ha

$$p = a \cdot b \Longrightarrow p = \pm a \quad \text{vagy} \quad p = \pm b.$$

A prímszámok azok az elemek az oszthatósági hálóban, melyek rögtön az 1 fölött helyezkednek el.



Számelmélet alaptétele

Tétel

Minden $n \neq 0, \pm 1$ egész szám sorrendtől és előjeltől eltekintve egyértelműen felírható prímszámok szorzataként: $n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell} = \pm \prod_{i=1}^{\ell} p_i^{\alpha_i}$, ahol $p_1, p_2, \ldots, p_\ell$ pozitív prímek, $\alpha_1, \alpha_2, \ldots, \alpha_\ell$ 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 $\alpha_i, \beta_i \geq 0$ nemnegatív egészek).
Ekkor

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

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

$(a, b) \cdot [a, b] = a \cdot b$.

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, így n prímtényezős felbontásában kell szerepelnie egy újabb prímszámnak. □

Figyelem: $p_1 \cdots p_k + 1$ nem feltétlen prím: $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 59 \cdot 509$

Prímszámtétel:

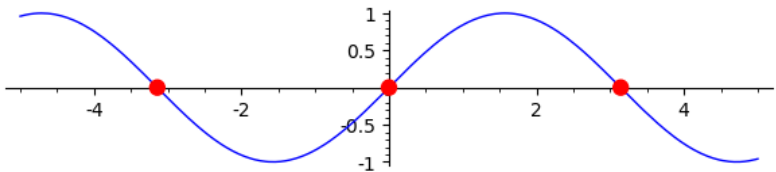
x-ig a prímek száma $\sim \frac{x}{\ln x}$.

(Sok prím van!)

x	prímek száma	$x/\ln x$
10	4	4,34
100	25	21,71
1000	168	144,76
10000	1229	1085,73

Osztási maradékok

Példa $sin(x) = 0$, ha $x = 2k\pi$ vagy $x = \pi + 2k\pi$ ($k \in \mathbb{Z}$)

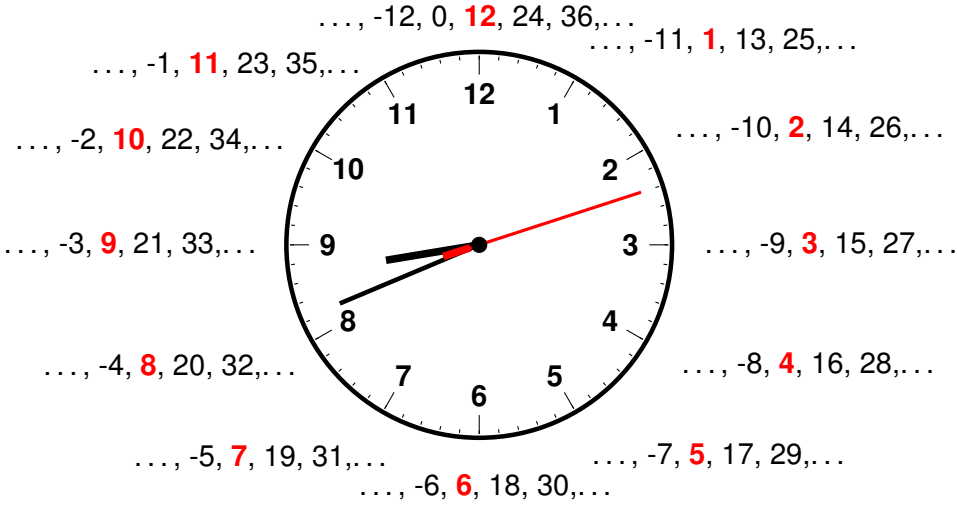


Példa Jelenleg 11 óra 43 perc van. Hány óra lesz 2 óra múlva? És 35 óra múlva? És 683625755919 óra múlva?

- 2 óra múlva 13 óra 43 perc lesz.
- Mivel $35 - 24 = 11$, így 35 óra múlva 22 óra 43 perc.
- Osszuk el 683625755919-et 24-gyel maradékosan: $683625755919 \bmod 24 = 3$, így 683625755919 óra múlva 14 óra 43 perc lesz.

Osztási maradékok

Sokszor nem egész számokkal, csak osztási maradékokkal számolunk.



Kongruenciák

Két számot azonosnak tekintünk, ha osztási maradékuk megegyezik.

Példa $0\,\mathrm{h}$ azonos $12\,\mathrm{h}$-val, $1\,\mathrm{h}$ azonos $13\,\mathrm{h}$-val, $3\,\mathrm{h}$ azonos $683625755919\,\mathrm{h}$-val, ...

Definíció

Adott $n \neq 0$ és a, b egészek esetén, a kongruens b-vel modulo n,

$$a \equiv b \mod n \quad \text{ha} \quad n \mid a - b.$$

Példa $0 \equiv 12 \mod 12$, $1 \equiv 13 \mod 12$, $683625755919 \equiv 3 \mod 12$.

Kongruenciák

A kongruencia úgy viselkedik, mint az egyenlőség.

Tétel

A kongruencia ekvivalencia reláció.

Bizonyítás.

- Reflexivitás: $a \equiv a \mod n$ u.i. $n \mid a - a = 0$.
- Tranzitivitás: $a \equiv b \mod n$ és $b \equiv c \mod n \Longrightarrow a \equiv c \mod n$, u.i.

$$n \mid a - b,\ n \mid b - c \quad \Longrightarrow \quad n \mid (a - b) + (b - c) = a - c.$$

- Szimmetria: $a \equiv b \mod n \Longrightarrow b \equiv a \mod n$,u.i.

$$n \mid a - b \quad \Longrightarrow \quad n \mid (-1) \cdot (a - b) = b - a$$

Kongruenciák

A kongruencia kompatibilis az összeadással és szorzással.

Tétel

Legyenek $a, b, c, d, n \in \mathbb{Z}$, $n \neq 0$. Ekkor

- $a \equiv b \mod n$ és $c \equiv d \mod n$ esetén $a + c \equiv b + d \mod n$.
- $a \equiv b \mod n$ és $c \equiv d \mod n$ esetén $a \cdot c \equiv b \cdot d \mod n$.

Bizonyítás. HF.

Példa

- $1 \equiv 13 \mod 12$, $2 \equiv 14 \mod 12 \Longrightarrow (1 + 2) = 3 \equiv 27 = (13 + 14) \mod 12$.
- $1 \equiv 7 \mod 6 \Longrightarrow (2 \cdot 1) = 2 \equiv 14 = (2 \cdot 7) \mod 6$

Azonban

- $2 \equiv 8 \mod 6 \not\Longrightarrow 1 \equiv 4 \mod 6$.

Példa: ISBN

Az ISBN egy 13 jegyű azonosító, egy számjegy elgépelését jelzi.

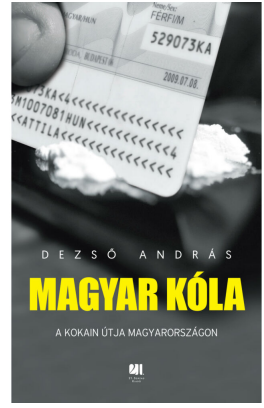
Egy $a_1a_2a_3 - a_4a_5a_6 - a_7a_8a_9 - a_{10}a_{11}a_{12} - a_{13}$ utolsó a_{13} számjegyét úgy határozzák meg, hogy

$$a_1 + 3 \cdot a_2 + a_3 + 3 \cdot a_4 + a_5 + 3 \cdot a_6 + a_7 + 3 \cdot a_8 + a_9 + 3 \cdot a_{10} + a_{11} + 3 \cdot a_{12} + a_{13} \equiv 0 \mod 10$$

Példa

$$9 + 3 \cdot 7 + 8 + 3 \cdot 9 + 6 + 3 \cdot 3 + 5 + 3 \cdot 6 + 8 + 3 \cdot 0 + 0 + 3 \cdot 0 + 9 \equiv$$
$$9 + 1 + 8 + 7 + 6 + 9 + 5 + 8 + 8 + 0 + 9 \equiv 0 \mod 10$$

Példa



ISBN:
978–963–568–000–9

Lineáris kongruenciák

Emlékeztető:

- $2 \equiv 8 \mod 6 \not\Longrightarrow 1 \equiv 4 \mod 6$.

Tétel

Legyenek $a, b, c, n \in \mathbb{Z}$, $n \neq 0$. Ekkor

$$ab \equiv ac \mod n \iff b \equiv c \mod \frac{n}{(a,n)}.$$

Példa

- $2 \equiv 8 \mod 6 \Longrightarrow 1 \equiv 4 \mod 3 = \frac{6}{2}$.

Lineáris kongruenciák

Tétel

Legyenek $a, b, c, n \in \mathbb{Z}$, $n \neq 0$. Ekkor

$$ab \equiv ac \mod n \iff b \equiv c \mod \tfrac{n}{(a,n)}.$$

Bizonyítás. Legyen $d = (a, n)$ és tfh. $n \mid ab - ac = a(b - c)$. Ekkor

$$\frac{n}{d} \cdot d \mid \frac{a}{d} \cdot d(b - c)$$

azaz létezik olyan $k \in \mathbb{Z}$, hogy

$$k \cdot \frac{n}{d} \cdot d = \frac{a}{d} \cdot d(b - c).$$

Egyszerűsítve d-vel kapjuk, hogy

$$\frac{n}{d} \mid \frac{a}{d}(b - c).$$

Azonban n/d és a/d relatív prímek, így $\frac{n}{d} \mid (b - c)$. (A másik irány triviális.) □

Lineáris kongruenciák

Mi történik, ha nem egyszerűsíteni, hanem osztani szeretnénk, azaz szeretnénk az $ax \equiv b \mod n$ kongruenciát megoldani.

Példa

Milyen x egészek elégítik ki a $2x \equiv 3 \mod 5$ kongruenciát.

- Ha $x \equiv y \mod 5$, akkor $2x \equiv 2y \mod 5$, így elég inkongruens számok között keresni, pl. $\{0, 1, 2, 3, 4\}$ halmazon. Véges számú lehetőség!
- A véges számú lehetőséget végigpróbálhatjuk:

$$2 \cdot 0 \equiv 0, \quad 2 \cdot 1 \equiv 2, \quad 2 \cdot 2 \equiv 4, \quad 2 \cdot 3 \equiv 1, \quad 2 \cdot 4 \equiv 3 \mod 5.$$

Azaz a megoldások: $x \equiv 4 \mod 5$. Figyelem, ez végtelen sok (de egymással kongruens) megoldás: $\{\ldots, -6, -1, 4, 9, 14, \ldots\}$

Példa

Milyen x egészek elégítik ki a $2x \equiv 3 \mod 126765060022822940149670320565 3$ kongruenciát. (Ez kb 2^{100} próbálkozás.)

Lineáris kongruenciák

Tétel

Legyenek a, b, n egész számok, $n > 1$. Ekkor az $ax \equiv b \mod n$ megoldható $\iff$ $(a, n) \mid b$. Ez esetben pontosan (a, n) darab inkongruens megoldás van $\mod n$.

Bizonyítás. A bizonyítás algoritmikus.

$$ax \equiv b \mod n \iff ax + ny = b.$$

Szükséges feltétel: Mivel (a, n) osztja a bal oldalt, osztja a jobb oldalt is.

Elégséges feltétel: A bővített euklideszi algoritmus szerint létezik olyan x_0, y_0, hogy $x_0 a + y_0 n = (a, n)$. Beszorozva $b/(a, n)$-el kapjuk a megoldást.

Megoldások száma: Legyen $a' = a/(a, n)$, $b' = b/(a, n)$, $n' = n/(a, n)$. Ekkor $(a', n') = 1$.Ha (x_0, y_0) és (x_1, y_1) két megoldása az $a'x + n'y = b'$ egyenletnek,akkor $a'(x_0 - x_1) + n'(y_0 - y_1) = 0$. Ekkor $x_0 \equiv x_1 \mod n'$. További megodások: $\frac{b}{(a,n)} x + k \cdot n'$ ahol $k = 0, \ldots, (a, n) - 1$. □

Lineáris kongruenciák

Algoritmus

1. $ax \equiv b \mod n \iff ax + ny = b$.
2. Oldjuk meg az $ax + ny = (a, n)$ egyenletet (bővített euklideszi algoritmus).
3. Ha $(a, n) \mid b$, akkor van (a, n) megoldás.
4. megoldások: $x_i = \frac{b}{(a,n)}x + k\frac{n}{(a,n)}$: $k = 0, \ldots, (a, n) - 1$.

Példa

Oldjuk meg a $23x \equiv 4 \mod 211$ kongruencát!

i	r_n	q_n	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: $x = 4(-55) \equiv 202 \mod 211$.

Ekkor $23 \cdot 202 = 4646 \equiv 4 \mod 211$.

Összes megoldás $\{202 + 211 \cdot k, k \in \mathbb{Z}\}$

Lineáris kongruenciák

Algoritmus

1. $ax \equiv b \mod n \iff ax + ny = b$.
2. Oldjuk meg az $ax + ny = (a, n)$ egyenletet (bővített euklideszi algoritmus).
3. Ha $(a, n) \mid b$, akkor van (a, n) megoldás.
4. megoldások: $x_i = \frac{b}{(a,n)}x + k\frac{n}{(a,n)}$: $k = 0, \ldots, (a, n) - 1$.

Példa

Oldjuk meg a $10x \equiv 8 \mod 22$ kongruencát!

i	r_n	q_n	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: $(10, 22) = 2 \mid 8 \Rightarrow$ Egy megoldás pár:

$x_1 = 4(-2) \equiv 14 \mod 22$

$x_2 = 4(-2) + \frac{22}{2} \equiv 14 + 11 \equiv 3 \mod 22$.

Összes megoldás:

$\{14 + 22 \cdot k, k \in \mathbb{Z}\} \cup \{3 + 22 \cdot k, k \in \mathbb{Z}\}$