

Diszkrét matematika 2

3. előadás Számelmélet

Mérai László

`merai@inf.elte.hu`

`https://sites.google.com/view/laszlomerai`

Komputeralgebra Tanszék

2023 ősz

Szimultán kongruenciák

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

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

A kongruenciákat külön megoldva:

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

Látszik, hogy $x = 2$ megoldás lesz! **Vannak-e más megoldások?**

Szimultán kongruenciák

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

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

A kongruenciákat külön megoldva:

$$\left. \begin{array}{l} x \equiv 2 \pmod{3} \\ x \equiv 4 \pmod{5} \end{array} \right\}$$

Van-e megoldás?

Az első kongruencia összes **egész** megoldása: $\dots, -4, -1, 2, 5, 8, 11, 14, 17, \dots$

Az második kongruencia összes **egész** megoldása: $\dots, -6, -1, 4, 9, 14, 19, \dots$

Van megoldás, például $x = 14$. **Vannak-e más megoldások?**

Szimultán kongruenciák

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

$$\left. \begin{array}{l} 2x \equiv 1 \pmod{15} \\ 4x \equiv 1 \pmod{5} \end{array} \right\}$$

Van-e megoldás? Nincs!

A fenti kongruencia rendszer egyenértékű a következő rendszerrel:

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

A kongruenciákat külön megoldva:

$$\left. \begin{array}{l} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 4 \pmod{5} \end{array} \right\}$$

Az utolsó két kongruencia **nem** elégíthető ki szimultán.

Szimultán kongruenciák

Feladat: Oldjuk meg a következő kongruencia rendszert:

$$\left. \begin{array}{l} a_1x \equiv b_1 \pmod{n_1} \\ a_2x \equiv b_2 \pmod{n_2} \\ \vdots \\ a_kx \equiv b_k \pmod{n_k} \end{array} \right\}$$

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

$$\left. \begin{array}{l} x \equiv c_1 \pmod{n_1} \\ x \equiv c_2 \pmod{n_2} \\ \vdots \\ x \equiv c_k \pmod{n_k} \end{array} \right\}$$

Szimultán kongruenciák

Feladat: Oldjuk meg a következő kongruencia rendszert:

$$\left. \begin{array}{l} x \equiv c_1 \pmod{n_1} \\ x \equiv c_2 \pmod{n_2} \\ \vdots \\ x \equiv c_k \pmod{n_k} \end{array} \right\}$$

Felthető, hogy az n_1, n_2, \dots, n_k modulusok relatív prímek.

Ha pl. $n_1 = n'_1 d$, $n_2 = n'_2 d$, akkor az első két sor helyettesíthető (Biz.: később)

$$\begin{array}{l} x \equiv c_1 \pmod{n'_1} \\ x \equiv c_1 \pmod{d} \\ x \equiv c_2 \pmod{n'_2} \\ x \equiv c_2 \pmod{d} \end{array}$$

Ha itt $c_1 \not\equiv c_2 \pmod{d}$, akkor nincs megoldás, különben az egyik sor törölhető.

Kínai maradék tétel

Tétel

Legyenek $1 < n_1, n_2, \dots, n_k$ relatív prím számok, c_1, c_2, \dots, c_k egészek. Ekkor a

$$\left. \begin{array}{l} x \equiv c_1 \pmod{n_1} \\ x \equiv c_2 \pmod{n_2} \\ \vdots \\ x \equiv c_k \pmod{n_k} \end{array} \right\}$$

kongruencia rendszer megoldható, és bármely két megoldás kongruens egymással modulo $n_1 \cdot n_2 \cdots n_k$.

Kínai maradék tétel bizonyítása

Bizonyítás. A bizonyítás algoritmikus.

Legyen először $k = 2$:

$$\left. \begin{array}{l} x \equiv c_1 \pmod{n_1} \\ x \equiv c_2 \pmod{n_2} \end{array} \right\}$$

- A **bővített euklideszi algoritmussal** oldjuk meg az $n_1x_1 + n_2x_2 = 1$ egyenletet.
- Legyen $c_{1,2} = n_1x_1c_2 + n_2x_2c_1$.
- Ekkor $c_{1,2} \equiv c_j \pmod{n_j}$ ($j = 1, 2$) u.i.:

$$c_{1,2} = n_1x_1c_2 + n_2x_2c_1 \equiv n_2x_2c_1 \equiv (1 - n_1x_1)c_1 \equiv c_1 \pmod{n_1}.$$

- Ha $x \equiv c_{1,2} \pmod{n_1n_2}$, akkor x megoldása a két kongruenciának.
- Megfordítva: ha x megoldása a két kongruenciának, akkor $x - c_{1,2}$ osztható n_1 -gyel, n_2 -vel, így a szorzatukkal is: $x \equiv c_{1,2} \pmod{n_1n_2}$ (u.i. $(n_1, n_2) = 1$).

Kínai maradék tétel bizonyítása

Bizonyítás. A bizonyítás algoritmikus.

Általános eset. A

$$\left. \begin{array}{l} x \equiv c_1 \pmod{n_1} \\ x \equiv c_2 \pmod{n_2} \\ x \equiv c_2 \pmod{n_3} \\ \vdots \\ x \equiv c_k \pmod{n_k} \end{array} \right\}$$

szimultán kongruencia equivalens a

$$\left. \begin{array}{l} x \equiv c_{1,2} \pmod{n_1 n_2} \\ x \equiv c_2 \pmod{n_3} \\ \vdots \\ x \equiv c_k \pmod{n_k} \end{array} \right\}$$

rendszerrel. Iterálva az eljárást kapjuk az $x \equiv c_{1,\dots,k} \pmod{n_1 \cdots n_k}$ kongruenciát.



Lineáris kongruenciák még egyszer

Tekintsük az $ax \equiv b \pmod n$ lineáris kongruenciát.

Emlékeztető: ez megoldható, ha $(a, n) \mid b$.

Ha $(a, n) = 1$, akkor a kongruencia **mindig** megoldható.

Példa

A $3x \equiv b \pmod 8$ minden b -re megoldható, míg $2x \equiv b \pmod 8$ csak a páros b -kre oldható meg.

Példa

Az $ax \equiv b \pmod 5$ minden $a \neq 0$ és b esetén megoldható.

Adott n moduluszhoz tekintsük a **jó** a együtthatók számát:

Definíció

Adott n nemnegatív egész esetén legyen

$$\varphi(n) = \#\{1 \leq a < n : (a, n) = 1\}$$

az **Euler-függvény**.

Euler-féle φ függvény

Legyen $\varphi(n) = \#\{1 \leq a < n : (a, n) = 1\}$.

Példa

- $\varphi(5) = 4$: $a = 1, 2, 3, 4$ esetén $(a, 5) = 1$.
- $\varphi(6) = 2$: $a = 1, 5$ esetén $(a, 6) = 1$.
- $\varphi(7) = 6$: $a = 1, 2, 3, 4, 5, 6$ esetén $(a, 7) = 1$.
- $\varphi(8) = 4$: $a = 1, 3, 5, 7$ esetén $(a, 8) = 1$.

Tétel (NB)

Legyen n prímtényezős felbontása $n = p_1^{e_1} p_2^{e_2} \cdots p_\ell^{e_\ell}$. Ekkor

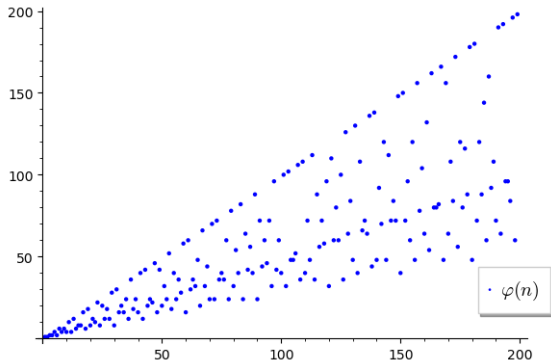
$$\varphi(n) = n \cdot \prod_{i=1}^{\ell} \left(1 - \frac{1}{p_i}\right)$$

Euler-féle φ függvény

Emlékeztető: $\varphi(n) = \#\{1 \leq a < n : (a, n) = 1\} = n \cdot \prod_{i=1}^{\ell} \left(1 - \frac{1}{p_i}\right)$

Példa

- $\varphi(5) = 5(1 - 1/5) = 4$.
- $\varphi(6) = 6(1 - 1/2)(1 - 1/3) = 2$.
- $\varphi(7) = 7(1 - 1/7) = 6$.
- $\varphi(8) = 8(1 - 1/2) = 4$.



Oszthatósági szabályok

Példa

3-mal való oszthatósági szabály:

123 pontosan akkor osztható 3-mal, ha $1 + 2 + 3 = 6$ osztható.

Pecízen:

$$123 = 1 \cdot 100 + 2 \cdot 10 + 3 \cdot 1 \equiv 1 \cdot 1 + 2 \cdot 1 + 3 \cdot 1 \equiv 1 + 2 + 3 \pmod{3}$$

Általában

$$n = \sum_{i=0}^k n_i \cdot 10^i \equiv \sum_{i=0}^k n_i \cdot 1^i \equiv \sum_{i=0}^k n_i, \quad \text{u.i.} \quad 10 \equiv 1 \pmod{3}.$$

Oszthatósági szabályok

Példa

7-tel való oszthatósági szabály:

$$123 = 1 \cdot 10^2 + 2 \cdot 10 + 3 \cdot 1 \equiv 1 \cdot 3^2 + 2 \cdot 3 + 3 \cdot 1 \equiv 1 \cdot 2 + 2 \cdot 3 + 3 \cdot 1 \pmod{7}$$

$$\text{u.i. } 10^2 \equiv 3^2 \equiv 9 \equiv 2 \pmod{7}$$

Általában: $10^i \equiv ? \pmod{7}$

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	...
$10^i \pmod{7}$	1	3	2	6	4	5	1	3	2	6	4	5	1	3	2	...

Tehát

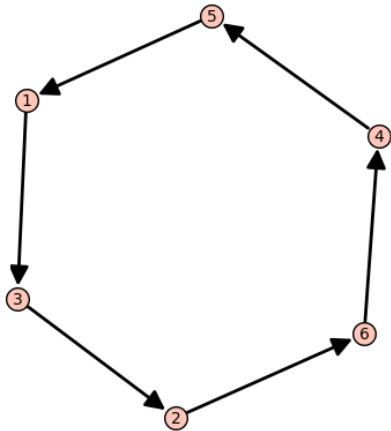
$$123 = 1 \cdot 10^2 + 2 \cdot 10 + 3 \cdot 1 \equiv 1 \cdot 2 + 2 \cdot 3 + 3 \cdot 1 = 11 \equiv 1 \cdot 3 + 1 \cdot 1 = 4 \pmod{7}$$

Általában

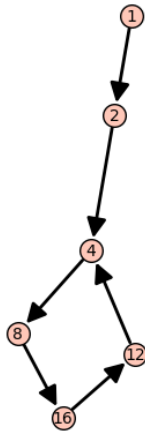
- Mindig van oszthatósági szabály.
- Az $a^i \pmod{n}$ hatványmaradékok **periódikusan ismétlődnek!**

Hatványmaradékok

Az $a^i \bmod n$ hatványok:



$10^i \bmod 7$



$2^i \bmod 20$

Euler-Fermat tétel

Tétel (Euler-Fermat)

Legyenek $a, n \in \mathbb{Z}$, $(a, n) = 1$. Ekkor

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

ahol φ az Euler-féle függvény.

Példa

- $2^6 \equiv 1 \pmod{7}$, mert $\varphi(7) = 6$.
- $3^6 \equiv 1 \pmod{7}$, mert $\varphi(7) = 6$.
- $9^{12} \equiv 1 \pmod{20}$, mert $\varphi(20) = 12$.

Figyelem, kisebb hatvány is lehet 1:

- $1^6 = 1 \equiv 1 \pmod{7}$,
- $2^3 = 8 \equiv 1 \pmod{7}$,
- $9^2 = 81 \equiv 1 \pmod{20}$.