(Nincs olyan lépés, amely biztosítaná, h. $\exists$ megoldás.)

– ha $f(x_0) \equiv 0 \pmod m$ és $x_0 \equiv x_1 \pmod m \Rightarrow f(x_1) \equiv 0 \pmod m$

$$0 \equiv f(x_0) = a_n x_0^n + a_{n-1} x_0^{n-1} + \dots + a_1 x_0 + a_0 \equiv a_n x_1^n + a_{n-1} x^{n-1} + \dots + a_{x_1} + a_0 =$$

$$= f(x_1) \pmod m$$

$$x_0^{n'} \equiv x_1^{n'} \pmod m$$

(A megoldás tulajdonsága nem az egész számé, hanem a maradékosztályé)

$f(x) \equiv 0 \pmod m$ megoldásainak a száma = az inkongruens megoldásai számával.

Ha megoldható, legfeljebb n lehet emiatt.

Felső korlát a modulus.

$f(x) \equiv 0 \pmod{m_1}$ és $g(x) \equiv 0 \pmod{m_2}$ ekvivalens kongruenciák, ha ugyanazon egész számok a megoldásaik, amelyek különböző maradékosztályokba esnek mod m_1 és mod m_2

11.26.

3. előadás

Lineáris algebrai kongruenciák

$ax \equiv b \pmod m$ $\qquad$ $(ax - b \equiv 0 \mod m)$

ahol $a \not\equiv 0 \pmod m$

Kérdés: Megoldható-e minden.? nem!

Tétel: $ax \equiv b \pmod m \Leftrightarrow$ oldható meg, ha $\underbrace{(a,m) = d \mid b}_{d \mid b}$

d: a és m lnko-ja

- az inkongruens megoldások száma d

az összes inkongruens megoldás: $x_0,\ x_0 + \frac{m}{d},\ x_0 + 2\frac{m}{d},\ \dots,\ x + (d-1)\frac{m}{d}$

ahol $ax_0 \equiv b \pmod m$

Biz: a) $(a,m) = 1 = d \Rightarrow a^{\varphi(m)} \equiv 1 \pmod m$ (kis-Fermat-t.)

- 1 megoldás

$ax \equiv b \pmod m$ $\qquad / a^{\varphi(m)-1}$

$a \cdot a^{\varphi(m)-1} x = b \cdot a^{\varphi(m)-1} \pmod m$

$1 \cdot x \equiv b \cdot a^{\varphi(m)-1} \pmod m$

$\boxed{x_0 \equiv b \cdot a^{\varphi(m)-1} \pmod m}$ lineáris kongruencia megoldóképlete

- inkongruens megoldások száma 1.

INDIREKT $x_0 \not\equiv x_1 \pmod m$

$ax_0 \equiv b \pmod m$

$ax_1 \equiv b \pmod m$

$\Big\} \Rightarrow ax_0 \equiv ax_1 \pmod m$ (mivel $(a,m) = 1$ ezért lehet egyszerűsíteni)

$x_0 \equiv x_1 \pmod m$ ↯

A tétel igaz.

Mj.: x_0 algoritmikusan is meghatározható:

$\exists x_0', y_0' \in \mathbb{Z} \quad ax_0' + my_0' = 1$

euklideni alg-ból fejezhető ki

$a x_0' b + m y_0' b = b \Rightarrow a(x_0' b) \equiv b \pmod m$

x_0

$a x_0 \equiv b \pmod m$

b:

$(a, m) = d > 1$

1., $\exists x_0 \in \mathbb{Z}$, hogy $ax_0 \equiv b \pmod m$

$ax_0 - b = my \qquad y \in \mathbb{Z}$

$d \mid ax_0$ ↓ 'a' miatt

$d \mid my$, 'm' miatt

$d \mid b$

2., Tfh.: $d \mid b$

Segédtétel: $ax \equiv b \pmod m$ ekvivalens $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$ -val

* Nem lehet kongruenciát egyszerűsíteni, csak úgy, ha a modulust is megnézzük.

$\left(\frac{a}{d}, \frac{m}{d}\right) = 1$

* $\frac{m}{(m,d)}$ mivel $d \mid m \Rightarrow \frac{m}{d}$

$\Rightarrow ax_0 \equiv b \pmod m \Rightarrow ax_0 + my = b \quad y \in \mathbb{Z}$

$\frac{a}{d}x_0 + \frac{m}{d}y = \frac{b}{d}$ (modulus lesz)

$\frac{a}{d}x_0 \equiv \frac{b}{d} \pmod{\frac{m}{d}}$

⇐ (HF)

$\frac{a}{d} x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$ ← Elegendő megoldani, mivel ekvivalensek.

$\left(\frac{a}{d}, \frac{m}{d}\right) = 1 \Rightarrow x_0 \equiv \frac{b}{d} \cdot \left(\frac{a}{d}\right)^{\varphi\left(\frac{m}{d}\right)-1} \pmod{\frac{m}{d}}$ ✓

Megoldható, a megoldás:

x megoldásai: $x_0 + t \cdot \frac{m}{d}$ $(t \in \mathbb{Z})$ / euklideszi osztás d-re nézve.

$t = dq + r \qquad 0 \leq r \leq d-1$

$k = k_0 + (dq + r)\frac{m}{d} = x_0 + r\frac{m}{d} + dq\frac{m}{d} \Rightarrow \boxed{x \equiv x_0 + r\frac{m}{d} \pmod{m}}$

MEGOLDÓKÉPLET

Megoldásai.

Pl.:

$50x \equiv 20 \pmod{40}$

$(50, 40) = 10 \mid 20$

↳ 10 megoldás lesz (ez a d)

Megoldás:

$5x \equiv 2 \pmod{4}$

$5 \equiv 1 \pmod{4}$ ✓ ezért lenyelhető

$x_0 = 2 \cdot 5^{\varphi(4)-1} = 10 \equiv 2 \pmod{4}$

$\varphi(4) = 2$

$2^2 - 2^1 = 2$

Összes megoldás: $2, 6, 10, 14, 18, 22, 26, 30, 34, 38$

$\frac{m}{d}$

Lineáris kongruenciarendszer (szimultán)

$$\left.\begin{aligned} a_1 x &\equiv b_1 \pmod{m_1} \\ a_2 x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ a_n x &\equiv b_n \pmod{m_n} \end{aligned}\right\} \text{ lin. kong. r.}$$

x_0 **megoldás**, ha $\forall \; 1 \le i \le n$-re

$$a_i x_0 \equiv b_i \pmod{m_i}$$

Megoldás: minden kongr.-nak megoldása

Megoldhatósághoz szükséges, h. $\forall i$-re $(1 \le i \le n)$ megoldható legyen $a_i x \equiv b \pmod{m_i}$.

Külön-külön megoldva

$$\left.\begin{aligned} x &\equiv c_{1j_1} \pmod{m_1} \\ x &\equiv c_{2j_2} \pmod{m_2} \\ &\vdots \\ x &\equiv c_{nj_n} \pmod{m_n} \end{aligned}\right\} j_1 \cdot j_2 \cdot \ldots \cdot j_n \text{ db kong. rendsz.}$$

Tétel:

$$\left.\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ &\vdots \\ x &\equiv c_n \pmod{m_n} \end{aligned}\right\} \Leftrightarrow \text{oldható meg, ha } \forall \; 1 \le i < j \le n \text{-re}$$

$(m_i, m_j) = d_{ij} \mid c_i - c_j$. A megoldásos modulo $[m_1, m_2 \ldots m_n]$-re egyértelmű.

BIZ: CSAK $n=2$-re ($n \ge 3$-ra teljes ind.)

$$x \equiv c_1 \pmod{m_1}$$

$$x \equiv c_2 \pmod{m_2}$$

$\Rightarrow$

$\exists\, x_0 \in \mathbb{Z}$, hogy $x_0 \equiv c_1 \pmod{m_1} \wedge x_0 \equiv c_2 \pmod{m_2}$

$x_0 - c_1 = q_1 \cdot m_1$ $\qquad$ $x_0 - c_2 = q_2 m_2$ $\qquad$ $(q_1, q_2) \in \mathbb{Z}$

$d \mid$ $\qquad$ $d \mid$

(mivel benne van az m_1)

$(m_1, m_2) = d$

$$\left.\begin{aligned} x_0 - c_1 &= q_1' d \\ x_0 - c_2 &= q_2' d \end{aligned}\right\}$$ második-ből kivonjuk az elsőt

$c_1 - c_2 = (q_2' - q_1') d$

$\Downarrow$

$d \mid c_1 - c_2$

$\Leftarrow$ (tk)

Rl.:

$$\left.\begin{aligned} 5x &\equiv 2 \pmod 4 \\ 3x &\equiv 8 \pmod 5 \\ 4x &\equiv 7 \pmod{11} \end{aligned}\right\} \Rightarrow \checkmark \quad (5,4) = 1 \quad 1 \mid 8-2$$

megoldható

Megp.: $5x \equiv 2 \pmod 4$

$x \equiv 2 \pmod 4$ $\qquad$ $x = 2 + 4t$ $\quad (t \in \mathbb{Z})$

$3(2+2t) \equiv 8 \pmod 5$

$6 + 12t \equiv 8 \pmod 5$ $\qquad$ ($12 \bmod 5 = 2$)

$2t \equiv 2 \pmod 5$

$t \equiv 1 \pmod 5$

$t = 1 + 5f$ $\quad (f \in \mathbb{Z})$

$x = 2 + 4 \cdot (1 + 5f) = 6 + 20f$

$4(6+20f) \equiv 7 \pmod{11}$

$24+80f \equiv 7 \pmod{11}$

$3f \equiv 5 \pmod{11}$ $/ \cdot 4$ olyat kell szorozni, ami a modulussal relatív prím

$f \equiv 20 \equiv -2 \pmod{11}$

$f = 2 + 11k \quad (k \in \mathbb{Z})$

$x = 6 + 20(-2 + 11k)$

$x = -34 + 220$

$\boxed{x \equiv -34 \pmod{220}}$

Kínai maradéktétel:

$$\left.\begin{aligned} a_1 x &\equiv b_1 \pmod{m_1} \\ &\vdots \\ a_n x &\equiv b_n \pmod{m_n} \end{aligned}\right\} \quad (a_i, m_i) = 1 \qquad 1 \le i \le n$$

↓ mindegyiknek 1 megoldása van

$(m_i, m_j) = 1 \qquad (1 \le i < j \le n)$
a modulusok páronként prímek

↓
(Van együttható
nem algoritmikus
külön-külön oldjuk meg,
nem egymásba helyettesítve)

$$m_i' := \frac{\prod_{j=1}^{n} m_j}{m_i}$$ nevezzük össes modulust, kivéve amiről szó van

kijelöltük a mego-t.

$a_1 m_1' y \equiv b_1 \pmod{m_1} \Rightarrow \exists\, y_1$ mo.

$a_2 m_2' y \equiv b_2 \pmod{m_2} \Rightarrow \exists\, y_2$ mego.

$\vdots$

$a_n m_n' y \equiv b_n \pmod{m_n} \Rightarrow \exists\, y_n$ mego

Megoldás: $x = \sum_{i=1}^{n} m_i' y_i$

BIZ.: lsd (TK)

Magasabb fokú algebrai kongruenciák

$f(x) \equiv a_n x^n + \dots + a_0 \equiv 0 \pmod{m}$; f modulo m foka $n \ge 2$

$m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_r^{\alpha_r}$
prímfaktorizációs alak
p_i-k prímek
$\alpha_i \ge 1$

Ha $\exists$ $x_0 \in \mathbb{Z}$, hogy $f(x_0) \equiv 0 \pmod{m} \iff$

$f(x_0) \equiv 0 \pmod{p_1^{\alpha_1}}$
$f(x_0) \equiv 0 \pmod{p_2^{\alpha_2}}$
$\vdots$
$f(x_0) \equiv 0 \pmod{p_r^{\alpha_r}}$

mert $p_1^{\alpha_1} \mid m$ ... stb

ekvivalensek

$x \equiv c_{1,j_1} \pmod{p_1^{\alpha_1}}$
$x \equiv c_{r,j_r} \pmod{p_r^{\alpha_r}}$

a modulusok lkkt-e m

$f(x) \equiv 0 \pmod{p^\alpha}$ prímhatvány modulusú kongr.

kisebb a modulus, mert 1 prímek hatványa

(Keresgjük prímhatványokra, aztán ha megoldható a prímhatvány modulusú kong $\Rightarrow$ kapunk lin kong.-rendszer.)

$f(x) \equiv 0 \pmod{p^\alpha}$

Keressük az x megoldást : $x = x_0 + p x_1 + p^2 x_2 + \dots + p^{\alpha-1} x_{\alpha-1}$ alakban;

ahol $x_0, x_1, \dots x_{\alpha-1}$ meghatározandó egészek.

$\underline{x_0}$: $\underbrace{f(x) = f(x_0 + p x_1 + \dots + p^{\alpha-1} x_{\alpha-1})}_{}\equiv 0 \pmod{p^\alpha}$
$\quad$ — // — $\equiv 0 \pmod{p}$

$f(x_0) \equiv 0 \pmod{p}$ prímmodulusú kongr.

x_1 :
x_2 :
⋮

lsd (TK) rel. GYAK.

alkalmas lineáris kongruenciák megoldásai, ahol a modulus mindig prím.

———— ∘ ————

4. előadás

III. 4.

36. tétel

Prímmodulusú magasabbfokú kongruenciákról

redukciós eljárás : - együtthatók redukciója

- modulus redukció (prímhatvány mod → prímmodulus)

$$u \to p^{\alpha} \to \boxed{E}$$

$$f(x) \equiv 0 \pmod p \quad ; \quad p \nmid a_n$$

megoldás lehet : $\bar{0}, \bar{1} \dots, \overline{p-1}$; ellenőrzéssel kiválasztható a tényleges megoldás !

áll.: $p \geq 3$ prím

———— ∘ ————

Következtetés: Egy modulo p n-edfokú kongruenciának legfeljebb n inkongruens megoldása lehet. (lehet, n. egy sincs)

BIZ.: Teljes indukció (mert $n \in \mathbb{N}$)

1. $n = 1$:

$ax \equiv b \pmod p$ $\quad p \nmid a$ ✓ a lin kongr. megoldhatósági feltétele $(a, p) = d \mid b$
$1 \mid b$ ✓

II. ind. feltétel ✓

III. biz. $(n+1)$-re ✓ (bd. tk)

Ha egy prímmodulusú kongr.-nak több megoldása van, mint n $\Rightarrow$ nem ennek fokszáma. (10o *)

! Mj.: Ha egy polinomnak több zérushelye (gyöke) van, mint a modulo p foka $(n) \Rightarrow$ a polinomnak $\not\equiv$ mod p foka (azaz, minden együtthatója kongruens $0 \pmod p$)

Példa:

$$f(x) = x^{p-1} - 1 - \overbrace{(x-1)(x-2)\dots(x-(p-1))}^{x^{p-1}\dots, \text{ha összevonnánk, lenne } x^{p-1}}$$

$f(x) \equiv 0 \pmod p$, melynek modulo p foka $\leq p-2$

inkongr. gyökei: $\underbrace{1, 2, 3 \dots}_{p-1 \text{ db gyöke van}}$

a nullával 1 esetén $x-1=0 \Rightarrow$ a nullát 0.

A kis Fermat-tétel nélkül $\Rightarrow$ megoldás 1.

főszámtétel $\Rightarrow$ $f(x)$ minden együtthatója $\equiv 0 \pmod p$

$\Downarrow$

$f(x)$ konstans tagja $\equiv 0 \pmod p$

azaz: $-1 - (-1)(-2)\dots\cdot(-(p-1)) \equiv 0 \pmod p$

$-1 + (-1)^p (p-1)! \equiv 0 \pmod p$ | feltétel: $p \geq 3$

$(p-1)! \equiv -1 \pmod p$

Wilson tétel