$126x^{281} + \ldots \equiv 0 \pmod 5$ $\quad$ de: $p \nmid a \quad a^{p-1} \equiv 1 \pmod p$

$1 \cdot (x^3)^{70} \cdot (x^1)$

$p \nmid x \quad (x \not\equiv 0 \pmod p)$ $\quad\quad$ $x^{p-1} \equiv 1 \pmod p$

$$a_n x^n + \ldots + a_p \underbrace{x^p}_{\ldots x} + a_{p+} \underbrace{x^{p-1}}_{\ldots 1} + a_{p-2} x^{p-2} + \ldots + a_0 \equiv 0 \pmod p$$

A Fermat-ban a legmagasabb fok: x^{p-2}

$$\boxed{b_{p-2} x^{p-2} + b_{p-3} x^{p-3} + \ldots + b_0 \equiv 0 \pmod p}$$

Ha $\underline{\underline{x=0}}$ megoldás: akkor:

$a^p \equiv a \pmod p$

ha lehúzzuk, h. a_0 p többszöröse $\Rightarrow$ egyből a 0 is.

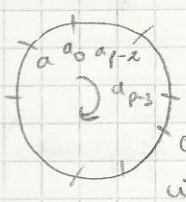
$$\boxed{c_{p-1} x^{p-1} + \ldots + c_0 \equiv 0 \pmod p}$$

Minden p prímmodulusú Fermat. ismeretlenű $p-1$-edfokúra (ha $x=0$ megoldás), és $p-2$-edfokúra (ha nem)

König Gyula – Rados Gusztáv tétel

(*) $f(x) = a_{p-2} x^{p-2} + a_{p-3} x^{p-3} + \ldots + a_0 \equiv 0 \pmod p$

$$H = \begin{pmatrix} a_{p-2} & a_{p-3} & \ldots & a_1 & a_0 \\ a_{p-3} & a_{p-n} & \ldots & a_0 & a_{p-2} \\ \vdots & & & & \\ a_0 & a_{p-2} & \ldots & a_2 & a_1 \end{pmatrix}$$



cirkulánsmátrix

jelölve r az M modulo p rangját

ha megoldható: $(p-2)$ → a determináns értéke ne legyen p-vel osztható

tétel: (*) ⟺ oldható meg, ha $\det(M) \equiv 0 \mod p$

a megoldások száma $p-1-r$.

BIZ.: —

Prímmodulusú binom kongr.-ák

$ax^n \equiv b \pmod{p}$, $p \nmid a$; $p \geq 3$

$y := x^n$ $(n \leq p-1)$

$ay \equiv b \pmod{p}$ → megoldható, mert $p \nmid a$ → lin kongr.

⇓

$\exists y_0$ úh. $a y_0 \equiv b \pmod{p}$

(inkongruens megoldás 1 db van)

$x^n \equiv y_0 \pmod{p}$

Tekintsük az $x^n \equiv a \pmod{p}$ kongruenciát!

speciális esetben : $x^n \equiv 1 \pmod{p}$

Def.: Ha $p \nmid a$ és $a^k \equiv 1 \pmod{p}$, de $a^l \not\equiv 1 \pmod{p}$, ha $0 < l < k$ ⟹ k-t az a modulo p rendjének nevezzük.

(rend: az a legkisebb ⊕ kitevő, amelyre előző teljesül, ui. $a^k \equiv 1 \pmod{p}$.)

- Létezik mindig rend?

Mivel $p \nmid a$ miatt $a^{p-1} \equiv 1 \pmod{p} \Rightarrow$ mindig $\exists$ rend modulo p, amely $\leq p-1$

Rend tulajdonságai:

I., ha $a \equiv b \pmod{p} \Rightarrow$ a és b modulo p rendje azonos.

II., ha a mod p rendje k és $a^u \equiv 1 \pmod{p} \Rightarrow k \mid u$

III., ha a modulo p rendje $\ell \Rightarrow \ell \mid p-1$

IV., ha a modulo p rendje ℓ és $a^i \equiv a^j \pmod{p} \Rightarrow i \equiv j \pmod{b}$

BIZ.: (lsd TK)

Def: $g \in \mathbb{Z}$ $p \nmid g$

g primitív kongruenciagyök modulo p, ha g modulo p rendje: $p-1$.

(T: primitív kongruenciagyök létezése bizonyítható. lsd tk)

Tétel: Ha g primitív kongruenciagyök modulo p, akkor

$g^0, g^1, g^2 \dots g^{p-2}$ redukált maradékrendszer modulo p.

BIZ.: (lsd tk)

redukált maradékrendszer: $1 \to g^0$, $2 \to g^{i_1}$, $3 \to g^{i_2}$, $\dots$, $p-1 \to g^{p-2}$

$\forall a \in \mathcal{P}_p$ (redukált maradékrendszer) egyértelm. $\exists i$: $g^i \equiv a \pmod{p}$

$0 \leq i \leq p-2$

i-t az a egész g alapú INDEX-ének nevezzük
(diszkrét logaritmus)

$$g^{\operatorname{ind}_g a} \equiv a \pmod{p}$$

Indextáblázat:

$p = 7$

$g \neq 1$

$g = 2$ $\quad 2^0 = 1$
$2^1 \equiv 1$
$2^2 \equiv 4$
$2^3 \equiv 1$ → nem primitív Zongruenciagyök, mert a rendje 3, nem $7-1=6$.

$g = 5$ $\quad 5^0 \equiv 1$
$5^1 \equiv 5$
$5^2 \equiv 4$
$5^3 \equiv 6$
$5^4 \equiv 2$
$5^5 \equiv 3$
$5^6 \equiv 1$ a rendje 6 : prim. Zongrgyök.

$p = 7$

a	1	2	3	4	5	6
$\operatorname{ind}_5 a$	0	4	5	2	1	3

indextáblázat modulo 7-re $g = 5$-re.

$p \nmid a$; $p \nmid b$ $\qquad 1 \leq a, b \leq p-1$

TULAJDONSÁGOK!

I.) $\operatorname{ind}_g (a \cdot b) \equiv \operatorname{ind}_g a + \operatorname{ind}_g b \pmod{p-1}$

II.) $\operatorname{ind}_g a^k \equiv k \operatorname{ind}_g a \pmod{p-1}$ $\qquad k \in \mathbb{N}^+$

III.) g és g primitív Zongruenciagyök

$$\operatorname{ind}_g b \cdot \operatorname{ind}_g a \equiv \operatorname{ind}_g b \pmod{p-1}$$

5. előadás **37. tétel** III. 11.

Binom kongruencia megoldása indextáblázattal

* $x^u \equiv a \pmod p$; $p \geq 3$ prím $p \nmid a$. $(\underbrace{2 \leq u \leq p-2}_{p \geq 5})$

BIZ.:

g primitív kongruencia mod p

$$x^u \equiv a \pmod p \quad / \operatorname{ind}_g$$

$$u \cdot \underbrace{\operatorname{ind}_g x}_{y} \equiv \operatorname{ind}_g a \pmod{p-1}$$

$$\underbrace{uy \equiv \operatorname{ind}_g a \pmod{p-1}}_{\text{lin kongr.}}$$

$\Updownarrow$

oldható meg $(u, p-1) \mid \operatorname{ind}_g a$

Tétel: * $\Leftrightarrow$ oldható meg, ha $(u, p-1) \mid \operatorname{ind}_g a$

pl.:

$$x^5 \equiv 3 \pmod 7 \qquad g = 5$$

$\Updownarrow$

oldható meg, ha $(\overset{5}{g}, \overset{6}{p-1}) = 1 \mid \operatorname{ind}_5 3$

$$5 \cdot \operatorname{ind}_5 x \equiv \underbrace{\operatorname{ind}_5 3}_{5} \pmod 6$$

$$\operatorname{ind}_5 x \equiv 1 \pmod 6$$

$\boxed{x \equiv 5 \pmod 7}$ ← megoldás

T.: $x^n \equiv a \pmod p$

($p \geq 3$ $\quad p \nmid a$)

Akkor és csak akkor oldható meg, ha

$$a^{\frac{p-1}{(n,p-1)}} \equiv 1 \pmod p$$

BIZ.: (lsd TK.)

Def.: Ha $x^n \pmod p$ $\quad (p \geq 3,\ p \nmid a)$, megoldható, akkor a-t n-edik hatványmaradéknak nevezzük, különben nem n-edik —"—

általában: $a \cdot x^n \equiv b \pmod p$ $\quad p \nmid a,\ p \nmid b$

$\operatorname{ind}_g a + n \operatorname{ind}_g x \equiv \operatorname{ind}_g b \pmod{p-1}$

⇕

oldható meg, ha

$(n, p-1) \mid \operatorname{ind}_g b - \operatorname{ind}_g a$

Kvadratikus kongruenciák

(másodfokú)

$a x^2 \equiv b \pmod p$ ✓

$c_1 x^2 + c_2 x + c_3 \equiv 0 \pmod p$ → nem binom $\quad (p \geq 3 \quad p \nmid c_1)$ $/ \cdot 4c_1$

$4c_1^2 x^2 + 4c_1 \cdot c_2 x + 4c_1 \cdot c_3 \equiv 0 \pmod p$ $\quad$ (A négy relatív prím a mod-hoz, mert az 3.)

$(2c_1 x + c_2)^2 \equiv c_2^2 - 4c_1 c_3 \pmod p$ $\quad$ teljes négyzetté alakítás

($2c_1x + c_2$ = y, $c_2^2 - 4c_1c_3$ = a)

$\boxed{y^2 \equiv a \pmod p}$ → ezt megoldjuk ⇒ $y_0 \equiv 2c_1 x + c_2 \pmod p$

⇓

x megoldás

g tougrgyö? (?)

T: $x^2 \equiv a \pmod{p}$ $(p \nmid a, p \geq 3$ prím$)$ $\Leftrightarrow$

oldható meg, ha $(2, \underbrace{p-1}_{\text{páros}}) \mid \text{ind}_g a \Rightarrow 2 \mid \text{ind}_g a$

vagy

$$a^{\frac{p-1}{(2,p-1)}} \equiv 1 \pmod{p} \Rightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

Def.: Ha $x^2 \equiv a \pmod{p}$ $(p \geq 3, p \nmid a)$ megoldható, akkor a-t kvadratikus maradéknak, ellenkező esetben nem kvadratikus maradéknak nevezzük.

Euler-lemma: (→ kisTétel)

$p \nmid a$, $p \geq 3$

- Ha ‚a' kvadratikus maradék $\Rightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.
- Ha ‚a' nem kv. maradék $\Rightarrow a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

BIZ.:

$x^{p-1} - 1 \equiv 0 \pmod{p}$ kis Fermat tétel

megoldásai: $1, 2, \dots, p-1$ $(p-1$ db$)$

$$x^{p-1} - 1 \equiv \left(x^{\frac{p-1}{2}} - 1\right)\left(x^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p}$$

vagy az egyiknek, vagy a másiknak gyöke $\Rightarrow$ csak $\frac{p-1}{2}$ gyöke lehet. Nem több, nem kevesebb!

—o—

(később)

Legendre-szimbólum:

$p \nmid a$ $p \geq 3$ prím

$$\left(\frac{a}{p}\right) := \begin{cases} 1, \text{ ha } & a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \\ -1, \text{ ha } & a^{\frac{p-1}{2}} \equiv -1 \pmod{p} \end{cases}$$

Legendre-szimbólum tulajdonságai:

- $a \equiv b \pmod p \quad (p \nmid a \Rightarrow p \nmid b)$

$$\Downarrow$$

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \Rightarrow$$ b per p Legendre szimbóluma

- $\left(\frac{a^2}{p}\right)$ $\left(a^2 \equiv x \text{ megoldható-e}\right) = 1 \Rightarrow \left(\frac{1}{p}\right) = 1$

- $p \nmid a$ és $p \nmid b$

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$$

BIZ.: $\left(\frac{ab}{p}\right) \equiv (a \cdot b)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \pmod p$

$$p \Big| \underbrace{\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)}_{0 \text{ v. } \pm 2}$$

mivel a $p \geq 3 \Rightarrow$ csak $p \mid 0$ teljesül.

$$\Downarrow$$

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$$

$a = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \qquad p \neq p_i \qquad (1 \leq i \leq r) \qquad p \geq 3$

$$\left(\frac{a}{p}\right) = \left(\frac{p_1^{\alpha_1}}{p}\right) \cdots \left(\frac{p_r^{\alpha_r}}{p}\right)$$

$$\left(\frac{p_i^{\alpha_i}}{p}\right) = \begin{cases} 1, \text{ ha } \alpha = 2k \quad k \in \mathbb{N}^+ \\ \left(\frac{p_i}{p}\right), \text{ ha } \alpha = 2k+1 \quad k \in \mathbb{N}^+ \end{cases}$$

$\left(\frac{2}{p}\right) = ?$ $\qquad \left(\frac{q}{p}\right) = ?$ $\qquad p \geq 3$ prím

$q \neq p$ $\quad q$ olan prím

páratlan

$\left(\frac{q}{p}\right) = ?$ $\quad q \geq 3$, $p \geq 3$ prím $\quad p \neq q$

Gauss-féle reciprocitási tétel

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & p \vee q \ 4k+1 \text{ alakú} \\ -\left(\frac{p}{q}\right), & \text{ha } p = q \equiv -1 \pmod 4 \end{cases}$$

$p \vee q \ 4k-1$ alakú

(312.: —)

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{ha } p = 4k+1 \text{ alakú} \\ -1, & \text{ha } p = 4k-1 \text{ alakú} \end{cases}$$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \pmod p$$

pl.:

$$x^2 \equiv -\underbrace{3^{84} \cdot 7^{813} \cdot 5^{913} \cdot 11^{19}}_{a} \pmod{23}$$

(„Csak úgy mondom!")

$4k-1$

$$\left(\frac{a}{23}\right) = \left(\frac{-1}{23}\right) \cdot \left(\frac{3^{84}}{23}\right) \cdot \left(\frac{7^{813}}{23}\right) \cdot \left(\frac{5^{913}}{23}\right) \cdot \left(\frac{11^{19}}{23}\right) \Rightarrow$$

$$\left(\frac{-1}{23}\right) = -1 \qquad \left(\frac{3^{84}}{23}\right) = 1$$

$$\left(\frac{7^{812}}{23}\right) \cdot 7 \qquad \left(\frac{5^{913}}{23}\right) = \left(\frac{5}{23}\right) \qquad \left(\frac{11^{19}}{23}\right) = \left(\frac{11}{23}\right)$$

$$1 \cdot \left(\frac{7}{23}\right)$$

$$\Rightarrow \left(\frac{a}{23}\right) = 1$$

$\left(\frac{7}{23}\right)$ → mivel a kettő $4k-1$ alakú → (290)

$$\left(\frac{7}{23}\right) = -\left(\frac{23}{7}\right) = -\left(\frac{2}{7}\right) = -1$$

$$\left(\frac{5}{23}\right) = \left(\frac{23}{5}\right) \overset{4k+1}{=} \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$$

$$\left(\frac{11}{23}\right) = -\left(\frac{23}{11}\right) = -\left(\frac{1}{11}\right) = -1$$

↓ mivel 1 négyzetszám

Számelméleti függvények (10. rész)

Def.: f számelméleti fgv. : $\mathbb{N}^+ \to \mathbb{R}$. Ezt számelméleti fgv-nek nevezzük. (tehát számok halmazán értelmezett fgv-t számelméleti fgv-nek nevezzük)

sorozat

$1 \mapsto a_1 \in \mathbb{R}$
$2 \mapsto a_2 \in \mathbb{R}$
$\vdots$
$a_n \mapsto a_n \in \mathbb{R}$

→ valós számsorozat

Def.:
f számelméleti fgv. multiplikatív, ha $\forall\ a,b \in \mathbb{N}^+$-ra, ha $(a,b)=1 \Rightarrow$
$f(a\cdot b) = f(a)\cdot f(b)$

T: Tfh $a_1, a_2 \dots a_n \in \mathbb{N}^+$, $(a_i, a_j) = 1$ $(1 \le i < j \le n)$

$$f\left(\prod_{i=1}^{n} a_i\right) = \prod_{i=1}^{n} f(a_i)$$

biz teljes indukcióval ✓ (nem kell)

$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_r^{\alpha_r}$ $\alpha_i \ge 1$ $\qquad f(n) = \prod_{i=1}^{r} f(p_i^{\alpha_i})$

Def.:
Ha $\forall\ a,b \in \mathbb{N}^+$-ra $f(a\cdot b) = f(a)\cdot f(b) \Rightarrow f$-et TOTÁLISAN MULTIPLIKATÍVNAK NEVEZZÜK.

$$\Downarrow$$

$n = p^{\alpha_1} \cdot \dots \cdot p^{\alpha_r}$ $\qquad f(n) = \prod_{i=1}^{r} f(p_i^{\alpha_i}) = \prod_{i=1}^{r} \left(f(p_i)\right)^{\alpha_i}$

csak prímhelyeken kell ismerni.