37. tétel

Binom kongruenciák megoldása indextáblázattal. Kvadratikus kongruenciák (mod p). Euler-lemma, Gauss-lemma, Legendre-szimbólum. Gauss-féle reciprocitás tétel.

Tétel: Az $x^k \equiv a \pmod p$ $(p \nmid a)$ kongruencia $\Leftrightarrow$ oldható meg, ha $(k, p-1) \mid \operatorname{ind} a$, vagy ami ezzel ekvivalens, ha $a^{\frac{p-1}{(k,p-1)}} \equiv 1 \pmod p$.

Ha megoldható, $\Rightarrow$ az inkongruens megoldások száma: $(k, p-1)$.

Def.: Az $a \in \mathbb{Z}$-t k-adik hatványmaradéknak nevezzük modulo p, ha az $x^k \equiv a \pmod p$ kongruencia megoldható. Ellenkező esetben nem k-adik hatványmaradéknak nevezzük modulo p.

Tétel: Legyen $p \nmid a$. Az $a \in \mathbb{Z} \Leftrightarrow$ k-adik hatványmaradék modulo p, ha $(k, p-1) \mid \operatorname{ind} a$, vagy ami ezzel ekvivalens: $a^{\frac{p-1}{(k,p-1)}} \equiv 1 \pmod p$.

Az inkongruens hatványmaradékok száma modulo p:

$$\frac{p-1}{(k, p-1)}$$

Def.: Ha az $a \in \mathbb{Z}$-nek $\varphi(m)$ modulo m, $\Rightarrow a$-t primitív gyökének nevezzük.

Tétel: Legyen $a \in \mathbb{Z}$ rendje ε modulo m.

I.) Ha $a^u \equiv 1 \pmod m$, $\Rightarrow \varepsilon \mid u \quad (u \in \mathbb{N})$

II.) $\varepsilon \mid \varphi(m)$

III.) Ha $i, j \in \mathbb{N}$, $\Rightarrow a^i \equiv a^j \pmod m \Rightarrow i \equiv j \pmod \varepsilon$

Kvadratikus kongruenciák:

Legyenek $c, d, e \in \mathbb{Z}$ és tekintsük

$$cx^2 + dx + e \equiv 0 \pmod p$$ prímmodulusú kongruenciát,

ahol $p \nmid c$. $4c$-vel szorozva:

$$4c^2x^2 + 4cdx + 4ce \equiv 0 \pmod p$$

$$(2cx + d)^2 \equiv d^2 - 4ce \pmod p$$

$$y = 2cx + d \qquad b = d^2 - 4ce$$

$$y^2 \equiv b \pmod p$$

Kongruencia mindig visszavezethető egy másodfokú binom kongruenciára és egy lineáris kongruenciára.

Elegendő az $x^2 \equiv a \pmod p$ alakú kongruenciák megoldásával foglalkozni.

Def: A $cx^2 + dx + e \equiv 0 \pmod p$ kongruenciát (prímmodulusú) kvadratikus kongruenciának nevezzük. Ha megoldható, akkor a-t kvadratikus maradéknak nevezzük modulo p, ellenkező esetben a nem kvadratikus maradék modulo p.

Tétel: Az $x^2 \equiv a \pmod p$ $(p \nmid a, p > 2)$ kongruencia $\Leftrightarrow$ oldható meg, azaz $a \Leftrightarrow$ kvadratikus maradék modulo p, ha $a^{\frac{p-1}{2}} \equiv 1 \pmod p$, vagy ami ezzel ekvivalens, ha $2 \mid \operatorname{ind}_g a$.

Tétel: (Euler-lemma)

Legyen $p>2$, $p \nmid a$. Ekkor

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 \pmod p, & \text{ha } a \text{ kvadratikus maradék modulo } p \\ -1 \pmod p, & \text{ha } a \text{ nem kvadratikus maradék mod } p. \end{cases}$$

Biz: Tudjuk, h:

$x^{p-1} \equiv 1 \pmod p$ kongruenciának $p-1$ inkongruens megoldása van, amelyek:

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

miatt vagy

$$x^{\frac{p-1}{2}} \equiv 1 \pmod p$$

vagy

$$x^{\frac{p-1}{2}} \equiv -1 \pmod p$$

kongruencia megoldásai. A tételt a kvadratikus maradékok elégítik ki.

A bizonyításból adódik, h. a kvadratikus és a nem kvadratikus maradékok száma $\frac{p-1}{2}$, hiszen az inkongruens megoldások száma: $\left(\frac{p-1}{2}, p-1\right) = \frac{p-1}{2}$

Definíció: (Legendre-szimbólum)

Legyen $p>2$ prím és $p \nmid a$. Ekkor

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ha } a \text{ kv. maradék modulo } p \\ -1, & \text{ha } a \text{ nem kv. maradék modulo } p. \end{cases}$$

definiáljuk $\left(\frac{a}{p}\right)$ számot Legendre-szimbólumnak nevezzük.

Tétel: Legyen $p>2$, $p \nmid a$, $p \nmid b$.

I.) Ha $a \equiv b \pmod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

II.) $\left(\frac{a^2}{p}\right) = 1$, így $\left(\frac{1}{p}\right) = 1$.

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

IV.) $\left(\frac{-1}{p}\right) = \begin{cases} 1, \text{ ha } p \equiv 1 \pmod 4 \\ -1, \text{ ha } p \equiv -1 \pmod 4 \end{cases}$

Tétel: (Gauss-lemma)

Legyen $p>2$, $p \nmid a$.

Tekintsük az $a, 2a, 3a \dots \frac{p-1}{2}a$ számok modulo p vett legkisebb pozitív maradékait. Legyen ezek között m db, amely nagyobb, mint $\frac{p}{2}$. Ekkor

$$\left(\frac{a}{p}\right) = (-1)^m,$$

azaz m paritása meghatározza a kvadratikus karakterét.

Tétel: Legyen p páratlan prím. Ekkor

$$\left(\frac{2}{p}\right) = \begin{cases} 1, \text{ ha } p \equiv \pm 1 \pmod 8 \\ -1, \text{ ha } p \equiv \pm 3 \pmod 8 \end{cases}$$

Biz.: Gauss-lemmával.

$$2, 2\cdot 2, 3\cdot 2, \dots, \frac{p-1}{2}\cdot 2$$

Az első $\frac{p-1}{2}$ pozitív páros szám, akkor a legnagyobb is kisebb, mint p.

A Gauss-lemmában szereplő m értékét megrapjuk, ha p-nél kisebb pozitív páros számok számából kivonjuk a $\frac{p}{2}$-nél kisebb pozitív páros számok számát.

BF/4

$$u = \left[\frac{p}{2}\right] - \left[\frac{p}{4}\right]$$

A p prímszám $8\ell \pm 1$ és $8\ell \pm 3$ alakjait behelyettesítve látható, hogy u páros, ha $p = 8\ell \pm 1$ alakú, míg u páratlan, ha $p = 8\ell \pm 3$ alakú, azaz

$$\left(\frac{2}{p}\right) = (-1)^u = \begin{cases} 1, \text{ ha } p \equiv \pm 1 \pmod 8 \\ -1, \text{ ha } p \equiv \pm 3 \pmod 8 \end{cases}$$

pl.: $p = 8\ell - 1$ alakú

$$\left[\frac{p}{2}\right] = \left[\frac{8\ell - 1}{2}\right] = \left[\frac{8(\ell-1) + 7}{2}\right] = 4(\ell-1) + 3$$

$$\left[\frac{p}{4}\right] = \left[\frac{8\ell - 1}{4}\right] = \left[\frac{8(\ell-1) + 7}{4}\right] = 2(\ell-1) + 1$$

$$u = \left[\frac{p}{2}\right] - \left[\frac{p}{4}\right] \Rightarrow u = 2(\ell-1) + 2 \rightarrow \underline{\text{páros}}$$

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

Tétel: (Gauss - féle reciprocitás tétele)

Legyen p és q két különböző páratlan prím. Ekkor

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

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), \text{ ha } p \equiv 1 \pmod 4 \text{ v. } q \equiv 1 \pmod 4 \\ -\left(\frac{q}{p}\right), \text{ ha } p \equiv q \equiv -1 \pmod 4 \end{cases}$$

Megj.: $\left(\frac{a}{p}\right)$ Legendre - szimbólum általánosításaként kapható az $\left(\frac{a}{u}\right)$ Jacobi - szimbólum.