36. tétel

Prímmodulusú kongruenciák. Fokszám-tétel, König-Rados tétel. Binom kongruenciák, rendi illetve primitív kongruenciagyök. Index.

Biz: (35/5, 35/6.)

(Fokszámtétel)

Tétel: Az $f(x) \equiv 0 \pmod{p}$ prímmodulusú n-edfokú kongruenciának legfeljebb n inkongruens megoldása van. (ellenkező esetben $f(x)$ azonosan nulla polinom modulo p)

__BIZ.__: Fokszámra vonatkozó teljes indukció:

$ax + b \equiv 0 \pmod{p}$ $\quad a \not\equiv 0 \pmod{p}$

1 inkongruens mego. $\quad n = 1$-re igaz.

Tfh: legfeljebb $n-1$ $(n \geq 1)$ prímmodulusú kongruenciának legfeljebb $n-1$ inkongruens megoldása van.

Biz. n-re!

$f(x) \equiv 0 \pmod{p}$ ha nem oldható meg $\Rightarrow$ igaz az állítás

$f(x) \equiv 0 \pmod{p}$ ha megoldható $\exists\, x_1 \in \mathbb{Z}$

$$f(x_1) \equiv 0 \pmod{p}$$

$$f(x) - f(x_1) = a_n(x^n - x_1^n) + a_{n-1}(x^{n-1} - x_1^{n-1}) + \ldots + a_1(x - x_1)$$

$f(x) - f(x_1) = (x - x_1)\, g(x)$ $\quad g(x)$ $n-1$-edfokú

$f(x_1) \equiv 0 \pmod p$ miatt

$$f(x) \equiv (x - x_1)\, g(x) \pmod p$$

ha $f(x) \equiv 0 \pmod p$ $n+1$ inK. megoldás $\Rightarrow$ p prím miatt

$g(x) \equiv 0 \pmod p$ n inK. mego.

de: $g(x) \equiv 0 \pmod p$ $n-1$-edfokú $\lightning$ ind. feltevés

Tétel: (König Gyula - Rados Gusztáv)

Legyen $f(x) = a_{p-2}x^{p-2} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$, ahol $a_0 \not\equiv 0 \pmod p$, $p > 2$ prím és M jelöli az alábbi ciklikus mátrixot:

$$M := \begin{pmatrix} a_{p-2} & a_{p-3} & a_{p-4} & \dots & a_1 & a_0 \\ a_0 & a_{p-2} & a_{p-3} & \dots & a_2 & a_1 \\ \vdots & & & & & \\ a_{p-3} & a_{p-4} & \dots & & a_0 & a_{p-2} \end{pmatrix}$$

amelynek a rangja r.

Az $f(x) \equiv 0 \pmod p$ kongruencia $\Leftrightarrow$ oldható meg, ha $\det(M) \equiv 0 \pmod p$ és ha megoldható $\Rightarrow$ az inkongruens megoldások száma $p-1-r$.

Prímmodulusú binom kongruenciák:

Def.: Az $ax^k \equiv b \pmod m$ kongruenciát, ahol $a \not\equiv 0 \pmod m$ és $k \in \mathbb{N}^+$, k-adfokú binom kongruenciának nevezzük.

A legegyszerűbben az $m = p$ és $y_0 = 1$ esetben kapott: $x^k \equiv 1 \pmod p$, ahol $1 \le k \le p-1$.

Def.: Legyen $(a,p)=1$ és p prímszám. Azt a legkisebb pozitív t egész számot, amelyre $a^t \equiv 1 \pmod p$ az $a \in \mathbb{Z}$ rendjének nevezzük modulo p.

Tétel: Legyen a rendje t modulo p.

1.) Ha $a^u \equiv 1 \pmod p$, $\Rightarrow$ $t \mid u$ $(u \in \mathbb{N})$

II.) $t \mid (p-1)$

III.) ha $i, j \in \mathbb{N}$, úgy $a^i \equiv a^j \pmod p \Rightarrow i \equiv j \pmod t$

Tétel: Ha $a \equiv b \pmod p$ és a rendje t mod $p \Rightarrow$ b rendje is t modulo p.

BIZ.: Tfh: b rendje t és $t < t$.

$a \equiv b \pmod p \rightarrow a^t \equiv b^t \pmod p$, így $a^t \equiv 1 \pmod p$

miatt $b^t \equiv 1 \pmod p$. ↯ b rendje t.

$t < t$ feltételnél is ellentmondásra jutunk $\Rightarrow t = t$.

Tétel: Létezik olyan $g \in \mathbb{Z}$, amelyre $(g,p)=1$, és g rendje $p-1$ modulo p.

Def.: A $g \in \mathbb{Z}$-t primitív gyöknek nevezzük modulo p, ha $(g,p)=1$, és g rendje $p-1$ mod p.

Tétel: Ha g primitív gyök modulo p $\Rightarrow$ $g^0, g^1 \dots g^{p-2}$ egész számok redukált maradékrendszert alkotnak modulo p.

BIZ.: $p=2$ esetén triviális.

$! \, p \geq 3$: modulo m redukált reprezentánsrendszerre vonatkozó tétel miatt (3A/2 2. tétel) igaz az állítás a $g^0, g^1 \dots g^{p-2}$ -beli egészek száma $p-1$, relatív prímek p-hez, páronként inkongruensek modulo p.

indirekt

Tfh.: $\exists\ 0 \le i < j \le p-2$, amelyre $g^j \equiv g^i \pmod{p}$.

$\Downarrow$

$j \equiv i \pmod{p-1}$, azaz $(p-1) \mid (j-i)$ ↯ $1 \le j-i \le p-2$.

Def.: Legyen g primitív gyök modulo p és $(a,p)=1$. Az $a \in \mathbb{Z}$ g alapú modulo p indexének nevezzük, és $\operatorname{ind}_g a$-val jelöljük azt a legkisebb természetes számot, melyre
$$g^{\operatorname{ind}_g a} \equiv a \pmod{p}.$$

Tétel: Legyenek g, q primitív gyökök modulo p, $(a,p)=(b,p)=1$ és $k \in \mathbb{N}$.

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

II.) $\operatorname{ind}_g(a^k) \equiv k \operatorname{ind}_g a \pmod{p-1}$

III.) $\operatorname{ind}_g a \equiv (\operatorname{ind}_q a)(\operatorname{ind}_g q) \pmod{p-1}$