35. tétel

Lineáris kongruenciák, illetve kongruenciarendszerek. Magasabb fokú algebrai kongruenciák.

Def.: Legyen $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$. Az $f(x)$ polinom modulo m foka n, ha $a_n \not\equiv 0 \pmod m$. Ha $a_n \equiv a_{n-1} \equiv \dots \equiv a_0 \equiv 0 \pmod m$, $\Rightarrow$ az $f(x)$ polinomnak nem tulajdonítunk modulo m fokot.

Def.: Legyen $f(x)$ egy modulo m n-edfokú ($n \geq 1$) egész együtthatós polinom. Az $f(x) \equiv 0 \pmod m$ kongruenciát n-edfokú egyismeretlenes algebrai kongruenciának nevezzük.

Def.: Az $x_0 \in \mathbb{Z}$-t az $f(x) \equiv 0 \pmod m$ megoldásának nevezzük, ha $f(x_0) \equiv 0 \pmod m$

Def.: Az $f(x) \equiv 0 \pmod m$ kongruencia x_1 és x_2 megoldását különbözőnek nevezzük, ha $x_1 \not\equiv x_2 \pmod m$. Az $f(x) \equiv 0 \pmod m$ kongruencia megoldásainak számán az inkongruens megoldások számát értjük.

Def.: Az $f(x) \equiv 0 \pmod{m_1}$ és $g(x) \equiv 0 \pmod{m_2}$ algebrai kongruenciákat ekvivalensnek nevezzük, ha ugyanazon egész számok a megoldásaik (persze más-más maradékosztályba tartoznak mod m_1, illetve mod m_2 szerint.)

Jatsf. 35

Def.: Az $ax \equiv b \pmod m$ algebrai kongruenciát, ahol $a \not\equiv 0 \pmod m$ lineáris kongruenciának nevezzük.

Tétel: Az $ax \equiv b \pmod m$ lin. kongruencia $\Leftrightarrow$ oldható meg, ha $(a,m) = d \mid b$, továbbá ha megoldható, akkor az inkongruens megoldások száma d.
Ha x_0 egy konkrét megoldás, $\Rightarrow$ az összes különböző (inkongruens) megoldás:

$$x_0,\ x_0 + \frac{m}{d},\ x_0 + 2\frac{m}{d},\ \ldots,\ x_0 + (d-1)\frac{m}{d}$$

BIZ.:

I. ! $(a,m) = d = 1$ Euler-F. tétel miatt

$$x_0 = b\, a^{\varphi(m)-1}$$

$$ax \equiv b \pmod m$$

$$\boxed{a^{\varphi(m)} \equiv 1 \pmod m}$$

$$\Downarrow$$

$$a x_0 = a\, b\, a^{\varphi(m)-1} = b a^{\varphi(m)} \equiv b \pmod m$$

mo. egyértelmű:

indirekt. x_1, x_2

$$ax_1 \equiv b \pmod m \ \wedge\ ax_2 \equiv b \pmod m \qquad x_1 \not\equiv x_2 \pmod m$$

$$ax_1 \equiv ax_2 \pmod m \text{, mivel } (a,m) = 1 \Rightarrow x_1 \equiv x_2 \pmod m \ \lightning$$

II. $!(a,m) = d > 1$

felt. szükséges: x_0 megp. $\rightarrow ax_0 \equiv b \pmod m \Rightarrow \exists\, y_0 \in \mathbb{Z}$

$$ax_0 + my_0 = b$$

$$d \mid a \quad d \mid m \Rightarrow d \mid b$$

elégséges:

① $ax \equiv b \pmod m$ ekvivalens

② $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$

x_0 megp. ①-ből : $ax_0 \equiv b \pmod m$ $\quad : d$

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

x_0' megp ② -ből : $\frac{a}{d}x_0' \equiv \frac{b}{d} \pmod{\frac{m}{d}}$ $\quad c \in \mathbb{Z}$-vel

$$\frac{a}{d}x_0' - \frac{b}{d} = c\frac{m}{d} \qquad \cdot d$$

$$ax_0' - b = cm \quad \text{ekv.: } ax_0' \equiv b \pmod m$$

$\left(\frac{a}{d}, \frac{m}{d}\right) = 1$ miatt: 1 kongruens megoldása van $\pmod{\frac{m}{d}}$

összes megp. számai $x \in \mathbb{Z}$-re:

$$x = x_0 + t\frac{m}{d} \qquad t \in \mathbb{Z}$$

③ $x_0,\ x_0 + \frac{m}{d},\ x_0 + 2\frac{m}{d},\ \dots,\ x_0 + (d-1)\frac{m}{d}$

t-t osztva maradékosan d-vel.

$$t = dq + r \qquad (0 \le r \le d-1)$$

$$x = x_0 + t\frac{m}{d} = x_0 + (dq+r)\frac{m}{d} = x_0 + qm + r\frac{m}{d} \equiv x_0 + r\frac{m}{d} \pmod m$$

③-beli egészek páronként inkongruensek $\pmod m$:

Tfh: $\exists\, i, j \quad 0 \le i < j \le d-1$ és $x_0 + i\frac{m}{d} \equiv x_0 + j\frac{m}{d} \pmod m$

$$\Downarrow$$

$$m \mid \frac{m}{d}(j-i)$$

$1 \le j - i \le d-1$ miatt ellentétben. ✓

Def.: Legyen $n \geq 1$ és tekintsük az

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

kongruenciákat. A kongruenciák egy rendszerét lineáris kongruenciarendszernek (röv. rendszernek kongruenciáknak) nevezzük. Egy x_0 egész számot a kongruenciarendszer megoldásának nevezünk, ha $a_i x_0 \equiv b_i \pmod{m_i}$ $\forall\ 1 \leq i \leq n$ esetén. A megoldásokat szokás rendszerben megoldásoknak nevezni.

Tétel: az előző def.-ból $\Rightarrow$ $x \equiv c_i \pmod{m_i}$ alakúakat kapunk, ha egyenként megoldjuk a kongr.-kat.

$$\left.\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_n \pmod{m_n} \end{aligned}\right\} \quad *$$

A $*$ lineáris kongruenciarendszernek pontosan akkor van megoldása, ha $(m_i, m_j) \mid c_i - c_j$ minden $1 \leq i < j \leq n$-re. Ha megoldható, akkor a megoldás modulo $[m_1, m_2 \ldots m_n]$-re nézve egyértelmű.

Tétel: (Kínai maradéktétel)
Ha a lin. kongruenciarendszerben az $m_1, m_2 \ldots m_n$ modulusok párosával relatív prímek, továbbá $(a_i, m_i) = 1$ minden $1 \leq i \leq n$-re, $\Rightarrow$ a kongruenciarendszer tetszőleges b_i $(1 \leq i \leq n)$ egészek esetén megoldható, és a megoldás modulo $m_1 m_2 \ldots m_n$-re nézve egyértelmű.

Biz.: (egy része)

$$\left.\begin{aligned} a_1 m_1' y &\equiv b_1 \pmod{m_1} \\ a_2 m_2' y &\equiv b_2 \pmod{m_2} \\ &\vdots \\ a_n m_n' y &\equiv b_n \pmod{m_n} \end{aligned}\right\}$$

$(a_i, m_i) = 1 \quad (1 \le i \le n)$ mindegyiknek egy megoldása van

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

ahol $m_i' = \dfrac{\prod_{j=1}^{n} m_j}{m_i} \quad (i = 1, 2 \dots n)$

összeszorzok az összes modulust, kivéve amiről szó van.

teljesülnek a megoldások:

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

$\vdots$

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

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

Magasabb fokú kongruenciák:

1., Az együtthatók redukciója:

Az $f(x) \equiv 0 \pmod m$-ben valamennyi együtthatót helyettesítjük a vele kongruens legkisebb abszolút értékű egésszel.

Így előállítjuk:

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

kongruenciában az a_i együtthatóra $|a_i| \le \frac{m}{2} \quad (0 \le i \le n)$

II., A modulus redukciója:

$f(x) = a_n x^n + \dots + a_0 \equiv 0 \pmod m$ 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

$1 \le \alpha_i \quad (1 \le i \le n)$ p_i: prímek

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

$$\left.\begin{aligned} f(x_0) &\equiv 0 \pmod{p_1^{\alpha_1}} \\ f(x_0) &\equiv 0 \pmod{p_2^{\alpha_2}} \\ &\vdots \\ f(x_0) &\equiv 0 \pmod{p_r^{\alpha_r}} \end{aligned}\right\} \rightarrow \text{ekvivalensek} \quad (\text{mert } p_1^{\alpha_1} \mid m \dots)$$

$$x \equiv c_{1j_1} \pmod{p_1^{\alpha_1}}$$

$$x \equiv c_{rj_r} \pmod{p_r^{\alpha_r}}$$

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

↓

Csak a modulus, mert 1 prímnek a hatványa.

Vezessük prímhatványra, aztán ha megoldható a prímhatvány modulusú kongr. $\Rightarrow$ kapunk lin. kong.-rendszert.

Megoldás: $x = x_0 + p x_1 + p^2 x_2 + \dots p^{\alpha-1} x_{\alpha-1}$ alakú

III. Forszám redukciója:

Forszámlánc segítségével. (lsd. 36. tétel)