33. tétel

A kongruencia fogalma, tulajdonságai. Maradékosztályok. Teljes, illetve redukált reprezentáns rendszer. A $(\mathbb{Z}/m; +; \cdot)$ gyűrű, illetve $(\mathbb{Z}/p; +; \cdot)$ test. Wilson-tétel.

Def.: Legyen $a, b, m \in \mathbb{Z}$, ahol m rögzített. Az a egész számot kongruensnek nevezzük b-vel, az m modulusra nézve, ha $m \mid (a-b)$.

jel.: $a \equiv b \pmod{m}$, $a \not\equiv b \pmod{m}$

Tétel: $\forall\ a, b, c, d \in \mathbb{Z}$ számra:
*

a) $a \equiv a \pmod{m}$

b) $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$

c) $a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

d) $a \equiv b \pmod{m} \wedge c \equiv d \pmod{m} \Rightarrow a + c \equiv b + d \pmod{m}$
$ac \equiv bd \pmod{m}$

Biz.:

a) $m \mid (a-a)$

b) ha $m \mid (a-b) \Rightarrow m \mid (b-a)$

c) ha $m \mid (a-b) \wedge m \mid (b-c) \Rightarrow m \mid (a-c)$

d) ha $m \mid (a-b) \wedge m \mid (c-d) \Rightarrow m \mid ((a+c)-(b+d)) \wedge$
$m \mid (ac - bd)$

pl.: $m \mid (a-b)$ és $m \mid (c-d)$

$m \mid (a-b)c \wedge m \mid b(c-d)$

$\Downarrow$

$m \mid ((ac-bc)+(bc-bd)) = ac-bd$ ✓

33. tétel

Tétel: $\forall\, a, b, c \in \mathbb{Z}$-re

a.; ha $a \equiv b \pmod{m} \wedge m_1 \mid m \Rightarrow a \equiv b \pmod{m_1}$;

b.; ha $ac \equiv bc \pmod{m} \Rightarrow a \equiv b \left(\bmod \frac{m}{(m,c)}\right)$;

c.; ha $a \equiv b \pmod{m_1}$ és $a \equiv b \pmod{m_2} \Rightarrow$

$a \equiv b \pmod{[m_1, m_2]}$;

BIZ.:

b.; $m \mid (ac - bc) \Rightarrow c(a-b) = mk \quad (k \in \mathbb{Z})$

(m, c)-vel osztva: $\frac{c}{(m,c)}(a-b) = \frac{m}{(m,c)}k$

$$\frac{m}{(m,c)} \;\Big|\; \frac{c}{(m,c)}(a-b)$$

$$\Downarrow$$

$$\frac{m}{(m,c)} \;\Big|\; (a-b) \Rightarrow a \equiv b \left(\bmod \frac{m}{(m,c)}\right)$$

Tétel: Legyen $a, b \in \mathbb{Z}$. $a \equiv b \pmod{m} \Leftrightarrow$, ha a és b m-mel osztva ugyanazt a legkisebb nemnegatív maradékot adja.

pl.; $\overline{0} = \{ n \mid n = mq + 0 \;,\; q \in \mathbb{Z} \}$

$\overline{1} = \{ n \mid n = mq + 1 \;,\; q \in \mathbb{Z} \}$

faktorhalmaz: $\mathbb{Z}/(m) = \{ \overline{0}, \overline{1}, \overline{2} \ldots \overline{m-1} \}$

Def.: Ha $a \in \bar{a}$, $\Rightarrow$ az a egész számot az $\bar{a}$ reprezentánsának nevezzük. Ha minden modulo m maradékosztályból pontosan egy reprezentánst választunk, akkor e reprezentánsok halmazát modulo m teljes reprezentánsrendszernek (v. maradékrendszernek) nevezzük.

Tétel: Az $a_1, a_2 \dots a_k$ egész számok $\Leftrightarrow$ alkotnak modulo m teljes reprezentánsrendszert, ha $k = m \wedge a_i \not\equiv a_j \pmod{m}$ minden $1 \le i < j \le m$-re.

Tétel: Legyen $\{a_1, a_2 \dots a_m\}$ egy teljes reprezentánsrendszer modulo m. Ha $c, b \in \mathbb{Z}$ és $(c,m) = 1$ akkor

$$\{ca_1 + b, ca_2 + b, \dots, ca_m + b\}$$

szintén teljes reprezentánsrendszer modulo m.

BIZ.: A $ca_i + b$ $(i = 1, 2 \dots m)$ számok száma nyilván m, ezért csak a páronkénti inkongruenciát kell bizonyítani.

Tfh.: $ca_i + b \equiv ca_j + b \pmod{m}$ $\quad i < j$-re.

A * tétel szerint:

$$ca_i \equiv ca_j \pmod{m}$$

$$\Downarrow$$

$(c,m) = 1$ miatt $\underbrace{a_i \equiv a_j \pmod{m}}$

↯ $a_1, a_2 \dots a_m$ egészek teljes reprezentánsrendszert alkotnak modulo m.

Tétel: Legyen $\bar{a} \in \mathbb{Z}/(m)$. $\forall\, a_1, a_2 \in \bar{a}$ egészre:

$$(a_1, m) = (a_2, m)$$

Def.: Azokat a modulo m maradékosztályokat, amelyeknek az elemei m-hez relatív prímek, redukált (v. prím) maradékosztályoknak nevezzük. Ezen osztályok halmazát $P(m)$-mel jelöljük.

Def.: Ha minden modulo m redukált maradékosztályból pontosan egy reprezentánst választunk, akkor e reprezentánsok halmazát redukált reprezentánsrendszernek (ill. redukált maradékrendszernek) nevezzük modulo m.

$(\mathbb{Z}/_{m}; +; \cdot)$ tulajdonságai:

Tétel: $(\mathbb{Z}; +; \cdot)$ integritástartomány

$f: \mathbb{Z} \to \mathbb{Z}/_{(m)}$ $\quad (a \mapsto \bar{a})$

↳ term. homomorfizmus

$\forall a, b \in \mathbb{Z}$

- $f(a+b) = f(a) + f(b)$ ✓
- $f(a \cdot b) = f(a) \cdot f(b)$ ✓

$(\mathbb{Z}/_{(m)}; +; \cdot)$

kommutatív, egységelemes gyűrű (zérusosztómentes!)

faktorstruktúra

De: zérusosztóság külön vizsgálandó:

pl.: $m = 4 \Rightarrow \bar{2} \cdot \bar{2} = \bar{0}$ $\quad (\mathbb{Z}/_4; +; \cdot)$ zérusosztós

$m = 5$ $\quad \bar{a}, \bar{b} \in \mathbb{Z}/_5 \setminus \{\bar{0}\}$ $\quad \bar{a}\bar{b} \neq \bar{0}$

$(\mathbb{Z}/_5; +; \cdot)$ zérusosztómentes

Sőt, a zéruselem kivételével minden elemnek van inverze. $\Rightarrow (\mathbb{Z}/_5; +; \cdot)$ test

Tétel: $(\mathbb{Z}/_{(m)}; +; \cdot)$ test $\Leftrightarrow$ ha m prímszám.

BIZ.:

1., Legyen n összetett $(n = n_1 \cdot n_2; \ 2 \le n_1 \le n_2 \le n)$

állítjuk: $\overline{n_1}$-nek $\nexists$ multiplikatív inverze $\Rightarrow (\mathbb{Z}/(n); +; \cdot)$ nem test.

indirekt:

Tfh: $\overline{n_1} \cdot \overline{x} = \overline{1} \Leftrightarrow \quad n_1 \cdot x \equiv 1 \pmod n$

$$n_1 \cdot x - 1 = -n y \qquad y \in \mathbb{Z}$$

$$\underbrace{n_1 x}_{n_1 | ?} + \underbrace{n y}_{n_1 | ?} = 1$$

$n_1 | n \qquad n_1 | 1 \quad \lightning \quad 2 \le n_1$

n_1, n_2 zérusosztók.

2., $n = p$ prímszám

$\mathbb{Z}/(p) \setminus \{\overline{0}\} = \{\overline{1}, \overline{2} \ldots \overline{p-1}\} = P_p$ - redukált maradékosztály $\Rightarrow$

$\Rightarrow (P_p; \cdot)$ csoport ✓

$(\mathbb{Z}/(p); +; \cdot)$ <u>test</u>

A legszűkebb test: $(\mathbb{Z}/(2))$

Tétel: (Wilson-tétel)

$n \ge 2$ egész $\Leftrightarrow$ prímszám, ha $(n-1)! \equiv -1 \pmod n$

BIZ.:

1, n összetett $\qquad n = n_1 \cdot n_2 \quad (2 \le n_1 \le n_2 \le n)$

ind.

$(n-1)! \equiv -1 \pmod n \Rightarrow (n-1)! \equiv -1 \pmod{n_1}$

de $(n-1)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n_1 \cdots (n-1) \equiv 0 \pmod{n_1}$

$\Downarrow$

benne van n_1.

$1 \equiv 0 \pmod{n_1} \Rightarrow n_1 | 1 \quad \lightning \quad 2 \le n_1$

2., $n = p$ prímszám

$n = p = 2$ $\quad (2-1)! \equiv -1 \pmod 2$

$1 \equiv -1 \pmod 2$

$2 \equiv 0 \pmod 2$ ✓

$n = p = 3$ $\quad (3-1)! \equiv 1 \pmod 3$

$3 \equiv 0 \pmod 3$ ✓

$n = p \geq 5$:

$\overline{(p-1)!} = \bar{1} \cdot \bar{2} \cdot \bar{3} \cdot \ldots \overline{(p-1)}$

$\bar{1} \cdot \bar{1} = \bar{1}$ ✓

$\left.\begin{array}{l} \\ \overline{(p-1)} \cdot \overline{(p-1)} = \overline{p^2 - 2p + 1} = \bar{1} \end{array}\right\} \left(\mathbb{Z}_{/(p)} \setminus \{\bar{0}\}\right)$ $\quad \bar{1}$ inv $= \bar{1}$

$\overline{(p-1)}$ inv $\overline{(p-1)}$

Segédtétel:

$2 \leq n_1 \leq \underset{p-2}{(p-1)-1}$ $\qquad \overline{n_1} \cdot \overline{n_1} \neq \bar{1}$

BIZ.: indirekt

$\overline{n_1} \cdot \overline{n_1} = \bar{1}$

$n_1^2 \equiv 1 \pmod p$

$p \mid (n_1^2 - 1) = (n_1 + 1)(n_1 - 1)$

Mivel p prím $\Rightarrow p \mid \underbrace{n_1 + 1}_{3 \leq \quad \leq p-1} \vee p \mid \underbrace{n_1 - 1}_{1 \leq \quad \leq p-3}$

ell ↯ ezek között nincsenek

p-vel osztható számok.

$\overline{(p-1)!} = \bar{1} \cdot \bar{2} \cdot \bar{3} \ldots \overline{p-1} = \overline{p-1}$

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

ha prím -1 -gyel kongruens :

$$(n-1)! = \begin{cases} 2, & \text{ha } n = 4 \\ 0, & \text{ha } n > 4 \text{ összetett} \\ -1, & \text{ha } n = p \text{ prímszám} \end{cases}$$