Kongruenciák és aritmetika modulo m

Legyen $m \in \mathbb{N}$. $\varrho_m = (\mathbb{Z}, \mathbb{Z}, R_{\varrho_m})$, $x, y \in \mathbb{Z}$

$x \, \varrho_m \, y \iff m \mid x - y$

$\varrho_m \in E(\mathbb{Z})$

Ezek:

- $\boxed{m = 0}$: a ϱ_0 reláció az egyenlőség
- $\boxed{m = 1}$: a ϱ_1 az univerzális reláció $\mathbb{Z}$-n
- $\boxed{m > 1}$: $\mathbb{Z}/_{\varrho_m} = \{ \underbrace{\{\ldots, -2m, -m, 0, m, 2m, \ldots\}}_{\hat{0}}, \underbrace{\{\ldots, -m+1, 1, m+1, \ldots\}}_{\hat{1}}, \ldots$
  $\underbrace{\{\ldots, -m+2, 2, m+2, \ldots\}}_{\hat{2}}, \ldots \underbrace{\{\ldots, -m+(m-1), m-1, m+(m-1), \ldots\}}_{\widehat{m-1}} \}$

Def: Legyen $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$, $n > 1$. Azt mondjuk, hogy „a kongruens b-vel modulo n", ha $n \mid a - b$.

Jelölés: $a \equiv b \pmod{n}$.

Tétel: A kongruencia modulo n egy ekvivalenciareláció $\mathbb{Z}$-n, és a faktorhalmaz $\mathbb{Z}/_{\equiv} = \{ x + n\mathbb{Z} \mid x \in \mathbb{Z} \} =$

$$= \{ \hat{0}, \hat{1}, \dots, \widehat{n-1} \} \stackrel{\text{jel}}{=} \mathbb{Z}_n$$

Tétel: Legyen $n \in \mathbb{N}$, $n > 1$. Akkor a $(\mathbb{Z}_n, +, \cdot)$ struktúra gyűrű, ahol $\hat{x} + \hat{y} = \widehat{x+y}$ és $\hat{x} \cdot \hat{y} = \widehat{x \cdot y}$, $\forall\, \hat{x}, \hat{y} \in \mathbb{Z}_n$.

Megj.: $a \equiv b \pmod{n} \iff \hat{a} = \hat{b}$, ahol $\hat{a}, \hat{b} \in \mathbb{Z}_n$.

Tétel (maradékos osztás tétele)

a.) Legyen $a, b \in \mathbb{N}$, $b \neq 0$. Akkor $\exists!\, q, r \in \mathbb{N}$: $a = bq + r$, $0 \leq r < b$.

b.) Legyen $a, b \in \mathbb{Z}$, $b \neq 0$. Akkor $\exists!\, q, r \in \mathbb{Z}$: $a = bq + r$, $0 \leq r < |b|$.

Pl: „-7 div 3" $= \begin{cases} -7 = (-3)\cdot 3 + 2 & \text{Tétel} \\ -7 = (-3)\cdot 2 + (-1) & \text{„DIV"} \end{cases}$

Tétel: Legyen $a, b \in \mathbb{N}^*$. Akkor a két szám legnagyobb közös osztójára igaz, hogy

$$\boxed{\text{lnko}(a, b) = \min\{ax + by \mid x, y \in \mathbb{Z},\ ax + by > 0\}.}$$

Pl: $\text{lnko}(12,18) = 6 = \overset{a}{12}\cdot\overset{x}{(-1)} + \overset{b}{18}\cdot\overset{y}{1}$

Biz: Legyen $D = \{ax+by \mid x,y\in\mathbb{Z},\ ax+by>0\}$.

$D \neq \emptyset \Rightarrow \exists\, d\in\mathbb{N}^*,\ d=\min D$. Azt kell bizonyítani, hogy $d = \text{lnko}(a,b)$. $d\in D \Rightarrow \exists\, x,y\in\mathbb{Z}:\ d = ax+by$.

$\exists!\, q,r\in\mathbb{N}:\ a = d\cdot q + r$, ahol $0\le r<d$.

$r = a - d\cdot q = a - (ax+by)q = a - axq - byq = a\underbrace{(1-xq)}_{\in\mathbb{Z}} + b\underbrace{(-yq)}_{\in\mathbb{Z}}$.

Ha $0<r$, akkor $r = ax'+by'$ alakú is emiatt $r\in D$ és $r<d=\min D$, ami ellentmondás.

Tehát $r=0$ és emiatt $d\mid a$. Hasonlóan $d\mid b$, tehát közös osztó.

Legyen $d' \in \mathbb{N}^*$ ú.h. $d' \mid a$ és $d' \mid b$. $\Rightarrow d' \mid ax$ és $d' \mid by$

$\Rightarrow d' \mid ax+by \Rightarrow d' \mid d \Rightarrow d' \leq d \Rightarrow d = \text{lnko}(a,b)$.

<u>Következmény</u>: Legyen $a, b \in \mathbb{N}^*$.

$$\text{lnko}(a,b) = 1 \iff \exists\, x, y \in \mathbb{Z} : \; ax + by = 1.$$

Ha $\text{lnko}(a,b) = d$, akkor az $x, y \in \mathbb{Z}$ értékek kiszámítására (ahol $d = ax+by$) az ún. bővített euklideszi algoritmust lehet használni.

<u>Megj</u>: $\text{lnko}(a,b) = \text{lnko}(a \bmod b, a)$, $\text{lnko}(0,a) = a$.

Példa: $\text{lnko}(1547, 560) = ?$

$$1547 = 2 \cdot 560 + 427$$
$$560 = 1 \cdot 427 + 133$$
$$427 = 3 \cdot 133 + 28$$
$$133 = 4 \cdot 28 + 21$$
$$28 = 1 \cdot 21 + \boxed{7} = \text{lnko}(1547, 560)$$
$$21 = 3 \cdot 7 + 0$$

euklideszi algoritmus

$\Rightarrow \exists\, x, y \in \mathbb{Z} : \; 7 = 1547 \cdot x + 560 \cdot y$. Ezeket az értékeket a köv. módon határozzuk meg:

$$7 = 28 - 1\cdot 21 = 28 - 1\cdot(133 - 4\cdot 28) = -133 + 5\cdot 28 =$$

$$= -133 + 5(427 - 3\cdot 133) = 5\cdot 427 - 16\cdot 133 =$$

$$= 5\cdot 427 - 16\cdot(560 - 427) = -16\cdot 560 + 21\cdot 427 =$$

$$= -16\cdot 560 + 21(1547 - 2\cdot 560) =$$

$$= 21\cdot 1547 - 58\cdot 560$$

$$\Rightarrow \overset{d}{7} = \overset{a}{1547}\cdot \overset{x}{21} + \overset{b}{560}\cdot(\overset{y}{-58})$$

bővített euklideszi alg.

Tétel: Legyen $n \in \mathbb{N}$, $n > 1$ és $\hat{a} \in \mathbb{Z}_n^*$. Akkor a $(\mathbb{Z}_n, +, \cdot)$ gyűrűben igaz, hogy

$$\boxed{\hat{a} \text{ invertálható} \iff \text{lnko}(a, n) = 1}$$

Biz: $\boxed{\Leftarrow}$ $\text{lnko}(a, n) = 1 \Rightarrow \exists\, x, y \in \mathbb{Z}: ax + ny = 1$.

$\Rightarrow \widehat{ax + ny} = \hat{1} \Rightarrow \widehat{ax} + \widehat{ny} = \hat{1} \Rightarrow \hat{a}\hat{x} + \hat{n}\hat{y} = \hat{1} \Rightarrow$

$\Rightarrow \hat{a}\hat{x} + \hat{0} \cdot \hat{y} = \hat{1} \Rightarrow \hat{a} \cdot \hat{x} = \hat{1} \Rightarrow \hat{a}$ invertálható és $\hat{a}^{-1} = \hat{x}$.

$\boxed{\Rightarrow}$ $\hat{a}$ invertálható $\Rightarrow \exists\, \hat{x} \in \mathbb{Z}_n : \hat{a} \cdot \hat{x} = \hat{1}$. $\Rightarrow n \mid ax - 1$

$\Rightarrow \exists\, k \in \mathbb{Z} : ax - 1 = nk \Rightarrow 1 = ax + n(-k) \Rightarrow \text{lnko}(a, n) = 1$.

Tétel: Legyen $n \in \mathbb{N}$, $n > 1$. A $(\mathbb{Z}_n, +, \cdot)$ gyűrű akkor és csak akkor test, ha n prímszám.

Biz: $(\mathbb{Z}_n, +, \cdot)$ test $\iff \forall \hat{a} \in \mathbb{Z}_n^*$: $\hat{a}$ invertálható $\iff$

$\iff \forall a \in \mathbb{Z}$, $0 < a < n$: lnko$(a, n) = 1 \iff$

$\iff n$ prímszám.

Pl: $(\mathbb{Z}_7, +, \cdot)$ kommutatív test.

Tétel

Legyen $a, a', b, b' \in \mathbb{Z}$, $n, m \in \mathbb{N}$, $n \geq 2$, $m \geq 2$. *Igazak a következők:*

(i) *Ha* $a \equiv b \pmod{n}$ *és* $a' \equiv b' \pmod{n}$, *akkor* $a \pm a' \equiv b \pm b' \pmod{n}$, $aa' \equiv bb' \pmod{n}$ *és* $a^k \equiv b^k \pmod{n}$, $\forall k \in \mathbb{N}$;

(ii) *Ha* $k \in \mathbb{N}$ *úgy, hogy* $\mathit{lnko}(k, n) = 1$ *és* $ka \equiv kb \pmod{n}$, *akkor* $a \equiv b \pmod{n}$;

(iii) *Ha* $a \equiv b \pmod{n}$ *és* $d \mid n$, *akkor* $a \equiv b \pmod{d}$;

(iv) *Ha* $d \in \mathbb{N}$ *úgy, hogy* $d \mid n$, $d \mid a$ *és* $d \mid b$, *akkor* $a \equiv b \pmod{n} \iff \frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}}$;

(v) *Ha* $a \equiv b \pmod{n}$, $a \equiv b \pmod{m}$ *és* $\mathit{lnko}(m, n) = 1$, *akkor* $a \equiv b \pmod{mn}$.

bizonyítás

(i) Mivel $a \equiv b \pmod{n}$ és $a' \equiv b' \pmod{n}$, következik, hogy $n \mid a - b$ és $n \mid a' - b'$. Ezeket összeadva illetve kivonva kapjuk, hogy $n \mid (a-b) \pm (a'-b')$, vagyis $n \mid (a \pm a') - (b \pm b')$, vagyis $a \pm a' \equiv b \pm b' \pmod{n}$. Ugyanezekből következik az is, hogy $n \mid (a-b)a'$ és $n \mid (a'-b')b$, tehát $n \mid aa' - ba' + a'b - bb'$ és $n \mid aa' - bb'$, vagyis $aa' \equiv bb' \pmod{n}$. Az utolsó állítás indukcióval igazolható.

(ii) Mivel $ka \equiv kb \pmod{n}$, $n \mid k(a-b)$. De $lnko(k,n) = 1$, tehát $n \mid a - b$, vagyis $a \equiv b \pmod{n}$.

(iii) Mivel $a \equiv b \pmod{n}$, $n \mid a - b$ és ha $d \mid n$, akkor $d \mid a - b$, ami azt jelenti, hogy $a \equiv b \pmod{d}$.

(iv) Mivel $d \mid n$, $d \mid a$ és $d \mid b$ akkor léteznek $n', a', b' \in \mathbb{Z}$ úgy, hogy $n = dn'$, $a = da'$ és $b = db'$. Ezekkel írhatjuk, hogy $a \equiv b \pmod{n} \iff n \mid a - b \iff dn' \mid da' - db'$ $\iff dn' \mid d(a'-b') \iff n' \mid a' - b' \iff \frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}}$.

(v) Mivel $a \equiv b \pmod{n}$ és $a \equiv b \pmod{m}$, következik, hogy $n \mid a - b$ és $m \mid a - b$ és mivel $lnko(m,n) = 1$, következik, hogy $mn \mid a - b$, vagyis $a \equiv b \pmod{mn}$.

Tétel

Tekintsük az $ax \equiv b \pmod{n}$ *egyenletet, ahol* $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$, $n \geq 2$.

(i) *Ha* $\text{lnko}(a, n) = 1$, *akkor az egyenletnek van megoldása:*

$$x \equiv a^{-1}b \pmod{n},$$

vagyis $x = a^{-1}b + n\mathbb{Z}$, *ahol* a^{-1} *az a inverze modulo n.*

(ii) *Ha* $\text{lnko}(a, n) = d > 1$, *az egyenletnek akkor és csakis akkor van megoldása, ha* $d \mid b$. *Ebben az esetben az egyenletnek ugyanaz a megoldása lesz, mint az*

$$a'x \equiv b' \pmod{n'}$$

egyenletnek, ahol $a' = \frac{a}{d}$, $b' = \frac{b}{d}$ *és* $n' = \frac{n}{d}$.

Példa:

1.) $26x \equiv 29 \pmod{18}$

$8x \equiv 11 \pmod{18}$

lnko$(8, 18) = 2$, de $2 \nmid 11$ $\Rightarrow$ az egyenletnek nincs megoldása

2.) $8x \equiv 48 \pmod{18}$

$8x \equiv 12 \pmod{18}$

lnko$(8, 18) = 2$ és $2 \mid 12$ $\Rightarrow$ áttérünk a $\frac{8}{2}x \equiv \frac{12}{2} \left(\mathrm{mod}\ \frac{18}{2}\right)$ egyenletre

$4x \equiv 6 \pmod{9}$, $4^{-1} \equiv 7 \pmod{9}$, $4 \cdot 7 = 28 = 3 \cdot 9 + 1$

$x \equiv 4^{-1} \cdot 6 \equiv 7 \cdot 6 \equiv 42 \equiv 6 \pmod{9}$

$\Rightarrow x \in 6 + 9\mathbb{Z}$ a megoldáshalmaz

Tétel (Kínai maradéktétel) :

$(\mathbb{Z}_N, +, \cdot) \cong (\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_r}, +, \cdot)$

Legyenek $n_1, n_2, \dots, n_r > 0$ *páronként relatív prímek,* $a_1, a_2, \dots, a_r$ *pedig tetszőleges egészek. Akkor a*

$\hat{x} \in \mathbb{Z}_N$

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \quad \vdots \\ x \equiv a_r \pmod{n_r} \end{cases}$$

$(\hat{a}_1, \hat{a}_2, \dots, \hat{a}_r) \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_r}$

rendszer megoldható, és megoldása egyetlen maradékosztály lesz modulo $N = n_1 n_2 \dots n_r$, *nevezetesen*

$$x \equiv \sum_{i=1}^{r} a_i N_i K_i \pmod{N},$$

ahol $N_i = \frac{N}{n_i}$ *és* $K_i = N_i^{-1} \pmod{n_i}$, $\forall i \in \{1, \dots, r\}$.

Biz: Tfh. x_1 és x_2 megoldások. $\Rightarrow$ $\underline{x_1 \equiv x_2} \equiv a_i \ (\underline{\text{mod } m_i})$, $\forall i \in \{1, \dots, n\}$

$\Rightarrow x = x_1 - x_2 \equiv 0 \ (\text{mod } m_i)$. $\Rightarrow x \equiv 0 \ (\text{mod } N)$ - mert lnko$(m_i, m_j) = 1$ $(i \neq j)$. $\Rightarrow x_1 \equiv x_2 \ (\text{mod } N)$.

Mivel $N_i = \frac{N}{m_i}$ és lnko$(m_i, m_j) = 1$ $(i \neq j)$ $\Rightarrow$ lnko$(N_i, m_i) = 1$ $\Rightarrow$

$\exists\, k_i, K_i \in \mathbb{Z} : 1 = m_i k_i + N_i K_i \Rightarrow N_i K_i \equiv 1 \ (\text{mod } m_i)$.

$$x \equiv \sum_{i=1}^{n} a_i N_i K_i \equiv a_1 N_1 K_1 + a_2 N_2 K_2 + \dots + a_i N_i K_i + \dots + a_n N_n K_n$$

$$\equiv 0 + 0 + \dots a_i \cdot 1 + \dots + 0 \quad (\text{mod } m_i)$$

$$\equiv a_i \ (\text{mod } m_i) \quad \forall i \in \{1, \dots, n\}$$

A megoldáshalmaz: $x \in \sum_{i=1}^{n} a_i N_i K_i + N\mathbb{Z}$

Példa

Oldjuk meg a következő egyenletrendszert:

$$\begin{cases} x \equiv 4 \pmod{9} \\ x \equiv 8 \pmod{11} \\ x \equiv 1 \pmod{2} \end{cases}.$$

A Tétel jelöléseit használva: $N = 9 \cdot 11 \cdot 2 = 198$, és a 9, 11 illetve 2 értékek páronként relatív prímek.

$$\begin{aligned}
N_1 &= \tfrac{198}{9} = 22 &&\Longrightarrow && K_1 = N_1^{-1} = 22^{-1} \equiv 4^{-1} \equiv 7 \pmod{9} \\
N_2 &= \tfrac{198}{11} = 18 &&\Longrightarrow && K_2 = N_2^{-1} = 18^{-1} \equiv 7^{-1} \equiv 8 \pmod{11} \\
N_3 &= \tfrac{198}{2} = 99 &&\Longrightarrow && K_3 = N_3^{-1} = 99^{-1} \equiv 1^{-1} \equiv 1 \pmod{2}
\end{aligned}$$

$$x \equiv \sum_{i=1}^{3} a_i N_i K_i = 4 \cdot 22 \cdot 7 + 8 \cdot 18 \cdot 8 + 1 \cdot 99 \cdot 1 = 1867 \equiv 85 \pmod{198}.$$

Ezért a megoldás $x \in 85 + 198\mathbb{Z}$.