KONGRUENCIÁK

Waldhauser Tamás

SZTE Bolyai Intézet

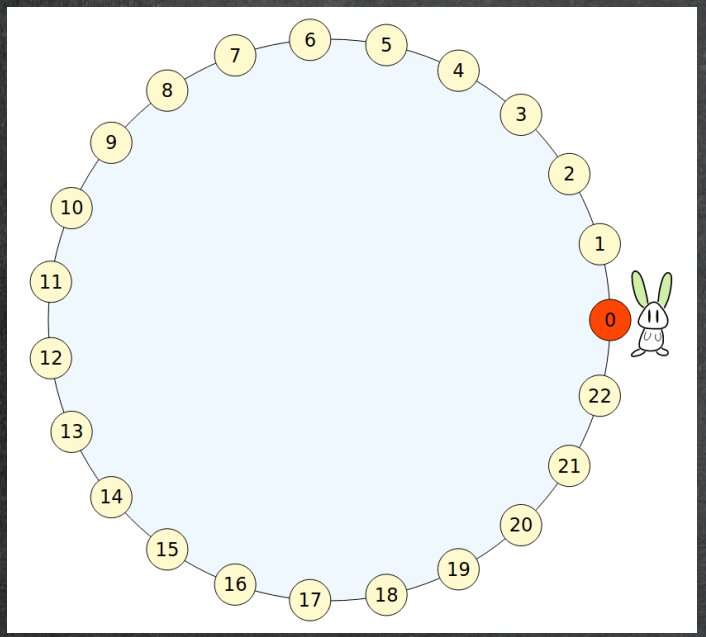
Tartalom

Bemelegítő feladat

Egy nyúl ugrál egy szabályos 23 oldalú sokszög csúcsain.

(a) Hol lesz 2312 ugrás után?

(b) Ugyanoda jut-e 72 364 783 ugrás után, mint akkor, ha 72 594 783-at ugrik?



(a) $2312 = 100 \cdot 23 + 12$

$12 \equiv 12$

$2312 \equiv 12 \pmod{23}$

(b) $230\,000 +$

$+72\,364\,783 =$

$= 72\,594\,783$

Igen.

$72\,364\,783 \equiv 72\,594\,783 \pmod{23}$

Definíció

Tetszőleges a, b egész számok és $m \geq 2$ természetes szám esetén azt mondjuk, hogy a kongruens b-vel modulo m, ha $m \mid a - b$. Az m számot a kongruencia modulusának nevezzük. Jelölés: $a \equiv b \pmod{m}$.

Tétel (alternatív def.)

Két egész szám akkor és csak akkor kongruens modulo m, ha ugyanazt a maradékot adják m-mel osztva.

Példák

(a) $1367 \overset{?}{\not\equiv} 1581 \pmod{10}$

(b) $-14 \overset{?}{\equiv} 46 \pmod{10}$ ✓

(c) $1111 \overset{?}{\equiv} 22222 \pmod{3}$ ✓

(d) $1210 \overset{?}{\not\equiv} 1264 \pmod{7}$

(a) $1367 = 136 \cdot 10 + 7$, $1581 = 158 \cdot 10 + 1$

(b) $-14 = (-2) \cdot 10 + 6$ $46 = 4 \cdot 10 + 6$

$10 \mid -14 - 46 = -60$

(c) $1111 \equiv 4 \equiv 1 \pmod{3} \Rightarrow 1111 \equiv 1$

$22222 \equiv 10 \equiv 1 \pmod{3} \Rightarrow 22222 \equiv 1$

(d) $7 \nmid 1210 - 1264 = -54$

Tétel (a kongruencia tulajdonságai)

Tetszőleges a, a_1, a_2, b, b_1, b_2 egész számok és $m \geq 2$ modulus esetén teljesülnek a következők:

1. $a \equiv a \pmod{m}$;
2. $(a \equiv b \pmod{m}$ és $b \equiv c \pmod{m}) \implies a \equiv c \pmod{m}$;
3. $a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$;
4. $\left.\begin{array}{l} a_1 \equiv b_1 \pmod{m} \\ a_2 \equiv b_2 \pmod{m} \end{array}\right\} \implies \begin{array}{l} a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m} \text{ és} \\ a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}. \end{array}$

(4.) Tfh. $m \mid a_1 - b_1$ és $m \mid a_2 - b_2$. Ekk. $m \mid a_1 a_2 - b_1 b_2$.

$$a_1 a_2 - b_1 b_2 = \underbrace{a_1 a_2 - b_1 a_2}_{m \mid} + \underbrace{b_1 a_2 - b_1 b_2}_{m \mid} = (a_1 - b_1) \cdot a_2 + b_1 \cdot (a_2 - b_2) \quad \checkmark \quad \blacksquare$$

Következmény

A modulo m kongruencia ekvivalenciareláció az egész számok halmazán (és kompatibilis az első három alapművelettel). A megfelelő ekvivalenciaosztályokat modulo m maradékosztályoknak nevezzük.

Példa

Milyen nap lesz 699^{1001} nap múlva?

$699^{1001} \equiv ? \pmod 7$

$699 \equiv -1 \pmod 7$

$\vdots$

$699 \equiv -1 \pmod 7$

$699^{1001} \equiv (-1)^{1001} \pmod 7$

$\| $

-1

Ugyanúgy megy, mint fent.

$699^{1001} \equiv (-1)^{1001} \equiv -1 \pmod 7$

$699 \equiv -1$

$12 \equiv 24 \pmod 6$

$2 \equiv 8 \pmod 6$

$12/2 \equiv 24/8 \pmod 6$

Példa

$\overline{a_n \cdots a_2 a_1 a_0} \equiv a_0 - a_1 + a_2 - \cdots + (-1)^n a_n \pmod{11}$

$\|$

$a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \ldots + a_n \cdot 10^n \equiv$ ← $10 \equiv -1 \pmod{11}$

$\equiv a_0 + a_1 \cdot (-1) + a_2 \cdot (-1)^2 + \ldots + a_n \cdot (-1)^n \equiv$

$\equiv a_0 - a_1 + a_2 - \ldots + (-1)^n a_n \pmod{11}$

Példa

Mit ad 7-tel osztva maradékul $2^{102} + 3^{201}$?

(1)

n	0	1	2	3	4	5	6	7	8	9	...	102
$2^n \pmod 7$	1	2	4	1	2	4	1	2	4	1	...	1

$\cdot 2 \quad \cdot 2 \quad \cdot 2 \quad \cdot 2 \quad \cdot 2 \quad \cdot 2 \quad \cdot 2 \quad \cdot 2 \quad \cdot 2$

$2^{u_1} \equiv 2^{u_2} \pmod 7 \iff u_1 \equiv u_2 \pmod 3$

$2^{102} \equiv 1 \pmod 7$

n	0	1	2	3	4	5	6	7	8	9	...	201
$3^n \pmod 7$	1	3	2	6	4	5	1	3	2	6	...	6

$\cdot 3 \quad \cdot 3 \quad \cdot 3 \quad \cdot 3 \quad \cdot 3 \quad \cdot 3 \quad \cdot 3 \quad \cdot 3 \quad \cdot 3$

$3^{u_1} \equiv 3^{u_2} \pmod 7 \iff u_1 \equiv u_2 \pmod 6$

$3^{201} \equiv 6 \pmod 7$

$2^{102} + 3^{201} \equiv 1 + 6 \equiv 7 \equiv 0 \pmod 7$

Példa

Mit ad 7-tel osztva maradékul $2^{102} + 3^{201}$?

(2.)

$$2^{102} + 3^{201} \equiv 2^2 \cdot 2^{100} + 3^1 \cdot (3^2)^{100} \equiv$$

$$\equiv 4 \cdot 2^{100} + 3 \cdot 2^{100} \equiv$$

$9 \equiv 2 \pmod 7$

$$\equiv 7 \cdot 2^{100} \equiv 0 \pmod 7$$

$$\forall n: 7 \mid 2^{n+2} + 3^{2n+1}$$

Tartalom

Példa

Egy nyúl ugrál egy szabályos 28 oldalú sokszög csúcsain. Mekkorákat ugorjon, hogy a 10. ugrással a 26-os csúcsba jusson?

$10x \equiv 26 \pmod{28} \Leftrightarrow 28 \mid 10x-26$

$\Leftrightarrow \exists y \in \mathbb{Z}: 10x-26 = 28y$

$10x-28y=26$

$10 \cdot \underbrace{3}_{\dots} - 28 \cdot \underbrace{1}_{\dots} = 2 = \text{lnko}(10,28)$

$\cdot 13$

$10 \cdot \underbrace{39}_{x_0} - 28 \cdot \underbrace{13}_{y_0} = 26$

$x_t = 39 + 14t \quad t \in \mathbb{Z}$

$y_t = 13 + 5t$

$x_t = 39+14t \Leftrightarrow 14 \mid x_t - 39$

$\Leftrightarrow x_t \equiv 39 \pmod{14}$

$x \equiv 11 \pmod{14}$

$M = \{\dots, -3, \boxed{11, 25}, 39, \dots\}$

Definíció

Lineáris kongruencián $ax \equiv b \pmod{m}$ alakú „egyenletet” értünk, ahol $a, b, m\,(a \neq 0, m \geq 2)$ adott egész számok, és az x ismeretlent is az egész számok körében keressük.

$ax \equiv b \pmod{m} \iff m \mid ax - b \iff \exists y \in \mathbb{Z} : ax - b = my$

$ax - my = b$

van m.o. $\iff$ ha $(a, m) \mid b$

Ha (x_0, y_0) m.o. Az összes m.o.: $x_t = x_0 + \frac{m}{(a,m)} t \quad (t \in \mathbb{Z})$

$x \equiv x_0 \pmod{\frac{m}{(a,m)}}$

Tétel

Tekintsük az $ax \equiv b \pmod{m}$ lineáris kongruenciát.

- A kongruenciának akkor és csak akkor van megoldása, ha $\text{lnko}(a, m) \mid b$.
- Ha van megoldás, akkor a megoldások egyetlen maradékosztályt alkotnak modulo $\frac{m}{\text{lnko}(a,m)}$. Tehát ha x_0 egy megoldás, akkor az általános megoldás így fest:

$$x \equiv x_0 \pmod{\frac{m}{\text{lnko}(a, m)}}.$$

Példa

$2x \equiv 6 \pmod{10}$ $/:2$

$x \equiv 3 \pmod{10}$

$M = \{\ldots, -7, 3, 13, 23, \ldots\}$

$2 \cdot 8 \equiv 6 \pmod{10}$

$2x \equiv 6 \pmod{10} \Leftrightarrow 10 \mid 2x-6$

$\Leftrightarrow 10 \mid 2(x-3)$

E.L. $\rightarrow$ $\Leftrightarrow 5 \mid x-3$

$\Leftrightarrow x \equiv 3 \pmod{5}$

$M = \{\ldots, -2, 3, 8, 13, \ldots\}$

Tétel (a kongruencia tulajdonságai)

Tetszőleges a, b, c egész számok és $m \geq 2$ modulus esetén teljesülnek a következők:

5. Ha $c \neq 0$, akkor $ac \equiv bc \pmod{m} \iff a \equiv b \pmod{\frac{m}{\text{lnko}(m,c)}}$.
6. Ha c és m relatív prímek, akkor
   $ac \equiv bc \pmod{m} \iff a \equiv b \pmod{m}$.

Biz.

5. $ac \equiv bc \pmod{m} \iff m \mid c(a-b)$

E.L. $\iff \frac{m}{(m,c)} \mid a-b$

$\iff a \equiv b \pmod{\frac{m}{(m,c)}}$ ∎

Példa

$3x \equiv 4 \pmod 5$

$3x = 4 \quad /:3$

$x = \frac{4}{3}$

$3x = 4 \quad /\cdot \frac{1}{3}$

$x = 3 \cdot \frac{1}{3} x = \frac{4}{3}$

① $3x \equiv 4 \pmod 5$

$\| \quad$

$3x \equiv 9 \pmod 5 \quad /:3 \quad (3,5) = 1$

$x \equiv 3 \pmod 5$

② $3x \equiv 4 \pmod 5$

$\| \quad$

$-2x \equiv 4 \pmod 5 \quad /:-2 \quad (-2,5) = 1$

$x \equiv -2 \pmod 5$

③ $3x \equiv 4 \pmod 5 \quad /\cdot 2$

$6x \equiv 8 \pmod 5 \quad (2,5) = 1$

$x \equiv 8 \pmod 5$

Példa

$10x \equiv 26 \pmod{28}$

(1) $10x \equiv 26 \pmod{28}$

$\|$

$10x \equiv -30 \pmod{28} \quad /:10 \quad (10,28)=2$

$x \equiv -3 \pmod{14}$

(2) $10x \equiv 26 \pmod{28} \quad /:2 \quad (2,28)=2$

$5x \equiv 13 \pmod{14}$

$\|$

$-9x \equiv 27 \pmod{14} \quad /:-9 \quad (-9,14)=1$

$x \equiv -3 \pmod{14}$

(3) $5x \equiv 13 \pmod{14} \quad /\cdot 3 \quad (3,14)=1$

$x \equiv 39 \pmod{14}$

$x \equiv 11 \pmod{14}$

Tartalom

Definíció

Adott a_i, b_i, n_i $(i = 1, 2, \ldots, k)$ egész számok esetén az alábbi alakú „egyenletrendszereket” lineáris kongruenciarendszereknek nevezzük (az x ismeretlent természetesen az egész számok körében keressük):

$$\left.\begin{array}{rcl} a_1 x & \equiv & b_1 \pmod{n_1} \\ & \vdots & \\ a_k x & \equiv & b_k \pmod{n_k} \end{array}\right\}$$

Megjegyzés

A továbbiakban feltesszük, hogy a kongruenciarendszer ilyen alakú:

$$\left.\begin{array}{rcl} x & \equiv & c_1 \pmod{m_1} \\ & \vdots & \\ x & \equiv & c_k \pmod{m_k} \end{array}\right\} \qquad (*)$$

Példa

$$\left.\begin{aligned} x &\equiv 1 \pmod{14} \\ x &\equiv 7 \pmod{10} \end{aligned}\right\} \Leftrightarrow \exists y \in \mathbb{Z}: x = 14y + 1 \Leftrightarrow \exists z \in \mathbb{Z}: x = 10z + 7$$

$$x = 14y + 1 = 10z + 7$$

$$14y - 10z = 6$$

$$14 \cdot 3 - 10 \cdot 4 = 2 = (14, 10) \quad \downarrow \cdot 3$$

$$14 \cdot \underbrace{9}_{y_0} - 10 \cdot \underbrace{12}_{z_0} = 6$$

$[14, 10]$

$x \equiv 57 \pmod{70}$

$x \equiv 127 \pmod{70}$

$$y = 9 + 5t \Rightarrow x = 14y + 1 = 14 \cdot \overbrace{(9 + 5t)}^{y} + 1 = 127 + 70t$$

$$z = 12 + 7t \Rightarrow x = 10z + 7 = 10 \cdot \underbrace{(12 + 7t)}_{z} + 7 = 127 + 70t$$

$x \equiv c_1 \pmod{m_1} \iff x = m_1 y + c_1$

$x \equiv c_2 \pmod{m_2} \iff x = m_2 z + c_2$

$x = m_1 y + c_1 = m_2 z + c_2$

$m_1 y - m_2 z = c_2 - c_1$

$\exists$ Lsg. $\iff (m_1, m_2) \mid c_2 - c_1$

$x \equiv x_0 \pmod{[m_1, m_2]}$

Sei (y_0, z_0) eine Lsg.

Alle Lsg: $y = y_0 + \frac{m_2}{(m_1, m_2)} \cdot t \Rightarrow x = m_1 \cdot \underbrace{\left(y_0 + \frac{m_2}{(m_1, m_2)} t\right)}_{y} + c_1$

$z = z_0 + \frac{m_1}{(m_1, m_2)} \cdot t$

$= \underbrace{m_1 y_0 + c_1}_{x_0} + \underbrace{\frac{m_1 \cdot m_2}{(m_1, m_2)}}_{[m_1, m_2]} t$

$x = x_0 + [m_1, m_2] \cdot t \quad (t \in \mathbb{Z})$

Tétel

Tekintsük az alábbi kongruenciarendszert.

$$\left.\begin{array}{rcl} x & \equiv & c_1 \pmod{m_1} \\ & \vdots & \\ x & \equiv & c_k \pmod{m_k} \end{array}\right\}$$

- A kongruenciarendszernek akkor és csak akkor van megoldása, ha minden i, j esetén $\mathrm{lnko}(m_i, m_j) \mid c_i - c_j$.
- Ha van megoldás, akkor a megoldások egyetlen maradékosztályt alkotnak modulo $\mathrm{lkkt}(m_1, \ldots, m_k)$. Tehát ha x_0 egy megoldás, akkor az általános megoldás így fest:

$$x \equiv x_0 \pmod{\mathrm{lkkt}(m_1, \ldots, m_k)}.$$

Tétel (a kongruencia tulajdonságai)

Tetszőleges a, b egész számok és $m \geq 2$ modulus esetén

7. $\left.\begin{array}{l} a \equiv b \pmod{m_1} \\ a \equiv b \pmod{m_2} \end{array}\right\} \iff a \equiv b \pmod{\text{lkkt}(m_1, m_2)}.$

Biz.

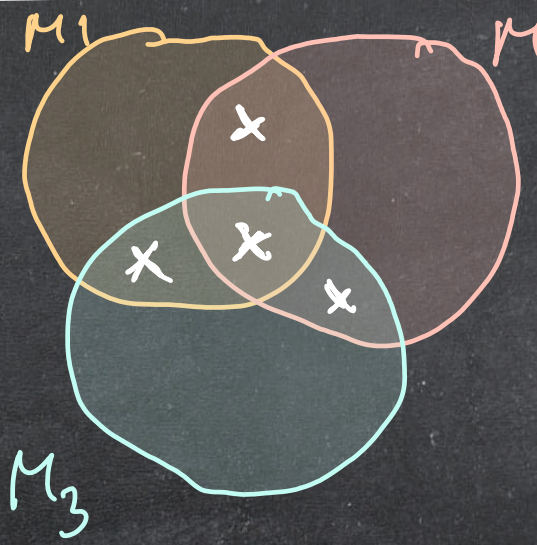
$$\left.\begin{array}{l} a \equiv b \pmod{m_1} \iff m_1 \mid a-b \\ a \equiv b \pmod{m_2} \iff m_2 \mid a-b \end{array}\right\} \overset{\text{lkkt. def.}}{\iff} [m_1, m_2] \mid a-b \iff a \equiv b \pmod{[m_1,m_2]}$$

□

$x \equiv c_1 \pmod{m_1} \iff x \in M_1$

$x \equiv c_2 \pmod{m_2} \iff x \in M_2$

$x \equiv c_3 \pmod{m_3} \iff x \in M_3$



$(m_1, m_2) \mid c_1 - c_2$

$(m_1, m_3) \mid c_1 - c_3$

$(m_2, m_3) \mid c_2 - c_3$

Tétel (kínai maradéktétel)

Ha a $(*)$ kongruenciarendszerben a modulusok páronként relatív prímek (azaz $i \neq j$ esetén $\text{lnko}(m_i, m_j) = 1$), akkor mindig van megoldás, és a megoldás megkapható a következő módon. Tekintsük azt a kongruenciarendszert, amelyet úgy kapunk $(*)$-ból, hogy az i-edik sorban a jobb oldalra 1-et írunk, a többi sorban pedig 0-t:

$$\left.\begin{array}{rcl} x & \equiv & 0 \pmod{m_1} \\ & \vdots & \\ x & \equiv & 1 \pmod{m_i} \\ & \vdots & \\ x & \equiv & 0 \pmod{m_k} \end{array}\right\}$$

$$\left.\begin{array}{l} x \equiv c_1 \pmod{m_1} \\ \vdots \\ x \equiv c_k \pmod{m_k} \end{array}\right\} (*)$$

Legyen e_i egy tetszőleges megoldása ennek a kongruenciarendszernek $(k = 1, \ldots, k)$. Ekkor az eredeti $(*)$ kongruenciarendszer általános megoldása:

$$x \equiv c_1 e_1 + \cdots + c_k e_k \pmod{m_1 \cdots m_k}.$$

$$[m_1, \ldots, m_k]$$

0	1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20	21
22	23	24	25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40	41	42	43
44	45	46	47	48	49	50	51	52	53	54
55	56	57	58	59	60	61	62	63	64	65

$$\left.\begin{aligned} x &\equiv 1 \pmod{11} \\ x &\equiv 0 \pmod{6} \end{aligned}\right\}$$

$$e_1 = 12$$

$$\left.\begin{aligned} x &\equiv 0 \pmod{11} \\ x &\equiv 1 \pmod{6} \end{aligned}\right\}$$

$$e_2 = 55$$

$$\left.\begin{aligned} x &\equiv c_1 \pmod{11} \\ x &\equiv c_2 \pmod{6} \end{aligned}\right\}$$

$$x \equiv c_1 e_1 + c_2 e_2 \equiv 12c_1 + 55c_2 \pmod{66}$$

$(11,6) \mid c_1 - c_2$, where $(11,6) = 1$

$\Rightarrow$ van mo.

Ell. $12c_1 + 55c_2 \equiv 1 \cdot c_1 + 0 \cdot c_2 \equiv c_1 \pmod{11}$ (since $12 \equiv 1$, $55 \equiv 0$)

$12c_1 + 55c_2 \equiv 0 \cdot c_1 + 1 \cdot c_2 \equiv c_2 \pmod{6}$ (since $12 \equiv 0$, $55 \equiv 1$)

e_2 ↑ → e_1