13416

Aritmetică în $\mathbb{Z}_n$

$(\mathbb{Z}_n, +, \cdot)$ inel comutativ

$\mathbb{Z}_n = \{\hat{0}, \hat{1}, \hat{2}, \dots, \widehat{n-1}\}$

$\hat{k} = \{x \in \mathbb{Z} \mid x \text{ dă restul } k \text{ la împărțirea cu } n\}$
$= \{x \in \mathbb{Z} \mid n \mid (x-k) \Leftrightarrow x = nq + k,\ q \in \mathbb{Z}\}$

$\hat{a} + \hat{b} = \widehat{a+b}$
$\hat{a} \cdot \hat{b} = \widehat{ab}$

$(\mathbb{Z}_n, +)$ grup comutativ, $\hat{0}$ element neutru
pt $x \in \mathbb{Z}_n$, not $-x$ opusul lui x, adică
$-x = y \Leftrightarrow x + y = \hat{0}$.

$(\mathbb{Z}_n \setminus \{\hat{0}\}, \cdot)$ monoid comutativ, $\hat{1}$ element neutru
↳ nu toate elementele au invers față de $\cdot$
Dacă există inversul lui x se notează x^{-1}
$x^{-1} = y \Leftrightarrow xy = \hat{1}$.
↳ reprezentanți

Ex: $\mathbb{Z}_7 = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}, \hat{4}, \hat{5}, \hat{6}\}$

$\hat{3} = \{3, 10, 17, 24, 31, 38, \dots\} = \{7k+3 \mid k \in \mathbb{Z}\}$

$\hat{52}$ în $\mathbb{Z}_7$ $= 7 \cdot 7 + 3 = \hat{3}$
(7 ≡ 0)

$-\hat{3} = \hat{a} \Leftrightarrow a + \hat{3} = \hat{0}$ în $\mathbb{Z}_7 \Rightarrow a = \hat{4}$.
$-\hat{5} = \hat{b} \Leftrightarrow 6 + \hat{5} = \hat{0} \Rightarrow b = \hat{2}$.
$-\hat{47} = -\hat{49} + \hat{2} = \hat{2}$.
(49 ≡ 0)

$\hat{3}^{-1} = \hat{a} \Leftrightarrow a \cdot \hat{3} = \hat{1}$ în $\mathbb{Z}_7$
$a = \hat{5}$ pt că $\hat{15} = \hat{14} + \hat{1} = \hat{1}$
$\hat{3}^{-1} = \hat{5} \Rightarrow \hat{5}^{-1} = \hat{3}$.
$\hat{4}^{-1} = \hat{2}$ $\hat{4} \cdot \hat{2} = \hat{8} = \hat{7} + \hat{1} = \hat{1}$
(7 ≡ 0)

Ex: $\mathbb{Z}_{11} = \{\hat{0}, \dots, \hat{10}\}$

$-\hat{3} = \hat{8}$; $-\hat{56} = -\hat{55} - \hat{1} = -\hat{1} = \hat{10}$.
(55 ≡ 0)

$\hat{5}^{-1} = \hat{9}$ pt că $\hat{9} \cdot \hat{5} = \hat{45} = \hat{44} + \hat{1} = \hat{1}$
(44 ≡ 0)

$\hat{7}^{-1} = \hat{8}$

Ex: $\mathbb{Z}_{12}$ $\hat{3}^{-1} = ?$ nu există

$3X = 12k + 1 \mid \cdot 4 \Rightarrow 12X = 12 \cdot (4k) + 4$

Teoremă $\hat{x}$ este inversabil în $\mathbb{Z}_n \Leftrightarrow \text{cmmdc}(x, n) = 1$
În particular, dacă n este nr prim $\Rightarrow$ toate elem lui $\mathbb{Z}_n \setminus \{\hat{0}\}$ au invers.

Ecuații de gradul I în $\mathbb{Z}_n$

Ex: $5x + 2 = 1$ în $\mathbb{Z}_{13}$

$5x = 1 - 2 = -1 = 12 \mid \cdot 5^{-1} = 8$

$\Rightarrow x = 12 \cdot 8 = -1 \cdot 8 = -8 = 5$.

Ex: $7x + 3 = 2$ în $\mathbb{Z}_{11}$

$7x = -1 = 10 \mid \cdot 7^{-1} = 8 \Rightarrow x = 10 \cdot 8 = (-1) \cdot 8 = -8 = 3$.

Ex: $4x + 5 = 3$ în $\mathbb{Z}_{12}$

$4x = -2 = 10$

4^{-1} nu există!

Rezolv prin încercări

x	0	1	2	3	4	5	6	7	8	9	10	11
$4x$	0	4	8	0	4	8	0	4	8	0	4	8

$\Rightarrow 4x = 10$ nu se poate $\Rightarrow S = \emptyset$.

Ecuații de gradul II în $\mathbb{Z}_n$

Ex: $x^2 - 3x + 1 = 0$ în $\mathbb{Z}_7$

$\Delta = 9 - 4 = 5$

$\sqrt{5} = ?$ $\sqrt{5} = a \Leftrightarrow a^2 = 5$

x	0	1	2	3	4	5	6
x^2	0	1	4	2	2	4	1

↳ nu se poate $\Rightarrow S = \emptyset$.

Ex: $x^2 - 5x + 7 = 1$ în $\mathbb{Z}_{13}$

$x^2 - 5x + 6 = 0$ $[(x-2)(x-3)]$

$\Delta = 25 - 24 = 1$

$\sqrt{1} \in \{1, 12\}$

Dacă $\sqrt{1} = 1 \Rightarrow x_1 = (5+1) \cdot 2^{-1} = 6 \cdot 7 = 42 = 39 + 3 = 3$
$x_2 = (5-1) \cdot 2^{-1} = 4 \cdot 7 = 28 = 26 + 2 = 2$.

Dacă $\sqrt{1} = 12 \Rightarrow x_1 = (5+12) \cdot 2^{-1} = 17 \cdot 7 = 4 \cdot 7 = 28 = 2$
$x_2 = (5-12) \cdot 2^{-1} = -7 \cdot 7 = -49 = -10 = 3$.