13.12.2020

Aritmetică în $\mathbb{Z}_n$

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

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

$\hat{k} = \{x \in \mathbb{Z} \mid x \text{ dă restul } k \text{ la împărțirea cu } n\}$

$= \{x \in \mathbb{Z} \mid x = nq + k, q \in \mathbb{Z}\}$

→ $(\mathbb{Z}_n, +)$ grup comutativ, $\hat{0}$ elementul neutru: $\hat{a} + \hat{0} = \hat{a}, \forall \hat{a} \in \mathbb{Z}_n$

$\forall \hat{a} \in \mathbb{Z}_n$, $\exists -\hat{a}$ opusul (cls XI: simetricul) lui $\hat{a}$, adică $-\hat{a} + \hat{a} = \hat{0}$.

→ $(\mathbb{Z}_n - \{\hat{0}\}, \cdot)$ monoid comutativ
↳ nu toate elementele au invers față de „·"

$\hat{1}$ = elem. neutru

Dacă există, $\hat{a}^{-1}$ inversul lui $\hat{a}$, adică $\hat{a}^{-1} \cdot \hat{a} = \hat{1}$

Def: $\hat{a} + \hat{b} = \widehat{a+b}$

$\hat{a} \cdot \hat{b} = \widehat{a \cdot b}$ ← reprezentanți

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

$\hat{2} + \hat{4} = \hat{6}$

$\hat{4} + \hat{6} = \hat{10} = \hat{3} = \{3, 10, 17, 24, 31, \dots\}$

$-\hat{5} = \hat{a} \Leftrightarrow \hat{a} + \hat{5} = \hat{0} \Rightarrow \hat{a} = \hat{2}$.

$-\hat{3} = \hat{6} \Leftrightarrow \hat{6} + \hat{3} = \hat{0} \Rightarrow \hat{b} = \hat{4}$

$\hat{3}^{-1} = \hat{c} \Leftrightarrow \hat{3} \cdot \hat{c} = \hat{1} \Rightarrow \hat{c} = \hat{5}$

$\hat{4}^{-1} = \hat{2}$ pt că $\hat{4} \cdot \hat{2} = \hat{8} = \hat{7} + \hat{1} = \hat{1}$
(0)

Ex: $\mathbb{Z}_{11} = \{0, 1, 2, \dots, 10\}$

$-5 = 6$; $-7 = 4$ (0)

$3^{-1} = 4$ pt că $3 \cdot 4 = 12 = 11 + 1 = 1$ (0)

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

$7^{-1} = 8$ pt că $7 \cdot 8 = 56 = 55 + 1$ (0)

Ex: $\mathbb{Z}_{13} = \{0, 1, \dots, 12\}$

$2^{-1} = 7$ pt că $2 \cdot 7 = 14 = 13 + 1 = 1$ (0) $\Rightarrow 7^{-1} = 2$

$5^{-1} = 8$

Ex: $\mathbb{Z}_{12} = \{0, \dots, 11\}$ 4^{-1} nu există, 6^{-1} nu există, 3^{-1} nu există

Teoremă $x \in \mathbb{Z}_n$ este inversabil $\Leftrightarrow$ cmmdc$(x, n) = 1$

În particular, dacă n este un prim, toate elem. $\neq 0$ din $\mathbb{Z}_n$ au invers.

Ecuații de gradul I în $\mathbb{Z}_n$

Ex: $2x + 5 = 3$ în $\mathbb{Z}_{11}$

$2x = 3 - 5 = -2 = 9$ (0)

$x = 9 \cdot 2^{-1} = 9 \cdot 6 = 54 = 44 + 10 = 10$ (0)

Ex: $5x - 3 = 7$ în $\mathbb{Z}_{13}$

$5x = 10$ (0) $\cdot 5^{-1} = 8$ (0) $\Rightarrow x = 10 \cdot 8 = -3 \cdot 8 = -24 = -13 - 11 = -11 = 2$.
(0)

Ex: $4x + 1 = 5$ în $\mathbb{Z}_8$

$4x = 4$ 4^{-1} nu există în $\mathbb{Z}_8^*$.

Rezolv prin încercări: $\Rightarrow x \in \{1, 3, 5, 7\}$

x	0	**1**	2	**3**	4	**5**	6	**7**
$4x$	0	**4**	0	**4**	0	**4**	0	**4**

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

Ex: $x^2 - 3x + 6 = 0$ în $\mathbb{Z}_7$

$\Delta = 9 - 4 \cdot 6 = 2 - 4 \cdot (-1) = 6$

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

$\sqrt{6} = ?$ în $\mathbb{Z}_7$ $\sqrt{6} = a \Leftrightarrow a^2 = 6 \Rightarrow$ nu există $\sqrt{\Delta} = 1$, $S = \emptyset$

Ex: $x^2 - 5x + 7 = 1$ în $\mathbb{Z}_{11}$

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

$\Delta = 25 - 24 = 1 = 1 \Rightarrow \sqrt{\Delta} \in \{1, 10\}$

- Dacă iau $\sqrt{\Delta} = 1 \Rightarrow x_1 = (5+1) \cdot 2^{-1} = 6 \cdot 6 = 36 = 33 + 3 = 3$.
  $x_2 = (5-1) \cdot 2^{-1} = 4 \cdot 6 = 24 = 22 + 2 = 2$

- Dacă iau $\sqrt{\Delta} = 10 \Rightarrow x_1 = (5+10) \cdot 6 = 15 \cdot 6 = 4 \cdot 6 = 24 = 2$
  $x_2 = (5-10) \cdot 6 = -5 \cdot 6 = -30 = -22 - 8 = -8 = 3$.