1341b

Wednesday, 23 October, 2024 9:55

Aritmetică în Z_n

$Z_n = \{0, 1, \dots, n-1\}$ → clase de resturi modulo n
= resturi posibile la împărțirea cu n

$(Z_n, +, \cdot)$ - inel comutativ:

→ $(Z_n, +)$ grup comutativ:

0 = el. neutru

pt orice $x \in Z_n$, notez $-x$ „simetricul" lui x față de „+"

$-x$ s.n. opusul lui x.

Adică: $x + (-x) = 0$.

→ $(Z_n - \{0\}, \cdot)$ monoid comutativ:

1 = element neutru

Nu orice $x \in Z_n$ are „simetric" față de „·"

Dacă există, notez cu x^{-1} acest „simetric", numit inversul lui x.

Adică: $x \cdot (x^{-1}) = 1$.

Def: $U(Z_n) = \{x \in Z_n \mid \text{există } x^{-1}\}$; $x \in U(Z_n)$ s.n. unitate.

Teoremă $x \in U(Z_n) \iff \text{cmmdc}(x, n) = 1$.

$U(Z_n) = \{x \in Z_n \mid \text{cmmdc}(x, n) = 1\}$

Corolar: Dacă n este nr. prim $\Rightarrow U(Z_n) = Z_n^*$.

Ex: $(Z_{11}, +, \cdot)$; $Z_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ → reprezentanți

$7 + 8 = 15 = \overset{0}{11} + 4 = 4$.

$7 + 8 = 15 = \underset{0}{11} + 4 = 4.$

$4 \cdot 7 = 28 = \underset{0}{22} + 6 = 6.$

$7 = \{$ toate nr. întregi care dau restul 7 la împ. cu 11 $\}$

$= \{11K + 7 \mid K \in \mathbb{Z}\} = \{7, 18, 29, 40, \ldots\}$

$4 = \{11K + 4 \mid K \in \mathbb{Z}\} = \{4, 15, 26, 37, \ldots\}$

$\mathbb{Z}_{11} : 4 \cdot 7 = 6 \iff 40 \cdot 15 = 17$

$-2 = y \iff y + 2 = 0 \Rightarrow y = 9$ pt că $9 + 2 = 11 = 0.$

$-7 = 4$ pt că $7 + 4 = 11 = 0.$

$-7 = 0 - 7 = 11 - 7 = 4$

11 nr prim $\Rightarrow U(\mathbb{Z}_{11}) = \mathbb{Z}_{11}^{*} = \{1, 2, 3, \ldots, 10\}$

$2^{-1} = y \iff 2y = 1 \Rightarrow y = 6$ pt că $2 \cdot 6 = 12 = \underset{0}{11} + 1 = 1$

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

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

$6^{-1} = 2$ și $9^{-1} = 5$ și $8^{-1} = 7.$

Ecuații de gradul I

Ex: $5X + 7 = 2$ în $\mathbb{Z}_{13}$

$5X = 2 - 7 = -5 = 8 \mid \cdot 5^{-1} = 8$ (pt că $5 \cdot 8 = 40 = \underset{0}{39} + 1$)

$8 \cdot 5 \cdot X = 8 \cdot 8$

$X = 64 = 12 \Rightarrow \underline{X = 12}.$

Verificare: $5 \cdot 12 + 7 = 60 + 7 = (\underset{0}{52} + 8) + 7 = 15 = 2.$ $\underline{OK}.$

Verificare: $5\cdot 12+7 = 60+7 = (52+8)+7 = 15 = 2$. ok.

Ex: $7x+3=1$ în $\mathbb{Z}_9$

$7x = 1-3 = -2 = 7 \Rightarrow x = 1$.

Ex: $3x+5=4$ în $\mathbb{Z}_{12}$ $\quad U(\mathbb{Z}_{12}) = \{1,5,7,11\} \not\ni 3$

$3x = -1 = 11 \mid \cdot 3^{-1}$ NU EXISTĂ!

Rezolv prin încercări

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

Ec. nu are soluții.

Ec. de gradul II

Ex: $3x^2-5x+1=0$ în $\mathbb{Z}_7$.

$\Delta = 25-4\cdot 3 = 25-12 = 13 = 6$.

Există $\sqrt{\Delta}$? Dacă da, $\sqrt{6} = y \Rightarrow y^2 = 6$

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

$\not\ni 6 \Rightarrow \nexists \sqrt{6}$ în $\mathbb{Z}_7$

$\Rightarrow$ Ec. nu are soluții.

Ex: $x^2-5x+6=0$ în $\mathbb{Z}_{13}$

$\Delta = 25-4\cdot 6 = 1$

$\sqrt{1} = 1$ ok.

$\sqrt{1} = 1$ ok.

$x_1 = (5+1)\cdot 2^{-1} = 6\cdot 7 = 42 = 39+3 = 3$

$x_2 = (5-1)\cdot 2^{-1} = 4\cdot 7 = 28 = 26+2 = 2$

Dacă calculam $\sqrt{1}$:

y	0	1	2	3	4	....	12
y^2	0	1	4	9	3	....	1

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

$12 = -1$ și $(-1)^2 = 1$

În plus, $x_1 = (5+12)\cdot 2^{-1} = \underset{4}{\underset{\parallel}{17}}\cdot 7 = 4\cdot 7 = 28 = 2$

$x_2 = (5-12)\cdot 2^{-1} = (-7)\cdot 7 = -49 = -39-10 = -10 = 3.$

Sisteme liniare (2×2)

Ex: $\begin{cases} 2x - y = 3 \\ 5x + 3y = 1 \end{cases}$ în $\mathbb{Z}_7$

! Calculez det matricei sist. Dacă $=0$ sau neinversabil $\Rightarrow$ rezolv prin încercări.

$A = \begin{pmatrix} 2 & -1 \\ 5 & 3 \end{pmatrix}$; $\det A = 11 = 4$ ok.

Substituție: $y = 2x - 3 \Rightarrow 5x + 3(2x-3) = 1$

$11x - 9 = 1$

$4x - 2 = 1 \Rightarrow 4x = 3 \mid \cdot 4^{-1} = 2$

$\underline{x = 6}$

$\underline{y = 2\cdot 6 - 3 = 9 = 2}$

inverse matriceale

În $\mathbb{R}$: $A \in \mathcal{M}_n(\mathbb{R})$ este inversabilă $\Leftrightarrow$ $\det A \neq 0$.

În $\mathbb{Z}_n$: $A \in \mathcal{M}_t(\mathbb{Z}_n)$ este inversabilă $\Leftrightarrow$ $\det A \in U(\mathbb{Z}_n)$

(ca să existe $(\det A)^{-1}$).

Ex: $A = \begin{pmatrix} 2 & -5 \\ 3 & 1 \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}_{11})$

$\det A = 17 = 6 \in U(\mathbb{Z}_{11})$; $6^{-1} = 2 \Rightarrow (\det A)^{-1} = 2$

$A \to A^t = \begin{pmatrix} 2 & 3 \\ -5 & 1 \end{pmatrix} \to A^* = \begin{pmatrix} 1 & +5 \\ -3 & 2 \end{pmatrix}$

$A^{-1} = (\det A)^{-1} \cdot A^* = 2 \cdot \begin{pmatrix} 1 & 5 \\ -3 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 10 \\ -6 & 4 \end{pmatrix}$

$\Rightarrow A^{-1} = \begin{pmatrix} 2 & 10 \\ 5 & 4 \end{pmatrix}$

Verificare: $A \cdot A^{-1} = A^{-1} \cdot A = I_2$.