Aritmetică în $\mathbb{Z}_n$

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

$\hat{a} = \{$ nr. întregi care dau restul a la împărțirea cu $n\}$

$$\hat{a} = \{nk + a, k \in \mathbb{Z}\}$$

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

$\hat{0}$ = multipli de 7 $= \{0, 7, 14, 21, 28, \dots\}$

$\cup \{-7, -14, -21, -28, \dots\}$

$$\hat{1} = \{7k + 1 \mid k \in \mathbb{Z}\} = \{1, 8, 15, 22, 29, \dots\}$$

$$2 \in \mathbb{Z}_7 = \{2, 9, 16, 23, \dots\}$$

Structura algebrică a $\mathbb{Z}_n$:

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

$\rightarrow (\mathbb{Z}_n, +)$ grup com.

el. neutru : 0

simetricul lui $a \in \mathbb{Z}_n$ este $-a$

= opusul lui a

$\rightarrow (\mathbb{Z}_n - \{0\}, \cdot)$ monoid comutativ

el. neutru 1

nu orice element este simetrizabil față de „$\cdot$"

$$U(\mathbb{Z}_n) = \{ x \in \mathbb{Z}_n \mid x \text{ este simetrizabil față de } \cdot \}$$

Dacă $x \in U(\mathbb{Z}_n)$, x s.n. unitate

Simetricul lui x f. de „$\cdot$" se notează x^{-1} (inversul)

Teoremă: $U(\mathbb{Z}_n) = \{x \in \mathbb{Z}_n \mid \text{cmmdc}(x, n) = 1\}$

Ex: $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

$(\mathbb{Z}_8, +)$ grup comutativ

$(\mathbb{Z}_8 - \{0\}, \cdot)$ monoid comutativ.

$\hat{2} + \hat{3} = \widehat{2+3} = \hat{5}$

$\hat{5} + \hat{7} = \hat{12} = \hat{4}$

$-3 = ?$ opusul lui 3 = simetricul față de +

$-3 = a \Leftrightarrow a + 3 = 0 \Rightarrow a = 5$

$U(\mathbb{Z}_8) = \{x \in \mathbb{Z}_8 \mid \text{cmmdc}(x, 8) = 1\}$

$= \{1, 3, 5, 7\}$

$3^{-1} = ?$ inversul lui 3 = simetricul față de $\cdot$

$3^{-1} = a \Leftrightarrow a \cdot 3 = 1 \Rightarrow a = 3$

$\bar{1}^{-1} = \bar{1}$; $\bar{5}^{-1} = \bar{5}$ pt că $\bar{5}\cdot\bar{5} = \bar{25} = \bar{1}$ în Z_8

$\bar{7}^{-1} = \bar{7}$ pt că $\bar{7}\cdot\bar{7} = \bar{49} = \bar{1}$ în Z_8

Ecuații de gradul I în Z_n

1. $\bar{2}x + \bar{5} = \bar{3}$ în $Z_{11} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{10}\}$

$\bar{2}x = \bar{3} - \bar{5} = \bar{-2}$

$\bar{x} = \bar{-1} = \bar{10}$ SAU $\bar{2}x = \bar{9} \mid \cdot \bar{2}^{-1} = \bar{6}$

$\bar{6}\cdot\bar{2}\cdot x = \bar{9}\cdot\bar{6}$

$\bar{1}x = \bar{54} = \underbrace{\bar{44}}_{\bar{0}} + \bar{10} = \bar{10} = x$

2. $\bar{5}x + \bar{3} = \bar{1}$ în Z_{13}

$\bar{5}x = \bar{-2} = \bar{11} \mid \cdot \bar{5}^{-1}$ $\quad$ $\bar{e}$

$x = \bar{11}\cdot\bar{5}^{-1} = \bar{11}\cdot\bar{8} = \bar{88} = \bar{78} + \bar{10} = \bar{10}$

$= (\bar{-2})\cdot(\bar{-5}) = \bar{10}$

3. $3x+5=1$ în $\mathbb{Z}_{17}$

$3x=-4 \mid \cdot 3^{-1} \Rightarrow x=-4\cdot 3^{-1}=-4\cdot 6$

$\Rightarrow x=-24=\underbrace{-17}_{0}-7=-7=10$

4. $6x+3=1$ în $\mathbb{Z}_{10}$

$6x=-2=8 \mid \cdot 6^{-1}$ ~~$\cdot 6^{-1}$~~ nu există în $\mathbb{Z}_{10}$

$U(\mathbb{Z}_{10})=\{1,3,7,9\}$

$\text{cmmdc}(6,10)=2\neq 1$

$6x=8$ rezolv prin încercări

Obs. $x=3 \Rightarrow 6\cdot 3=18=8 \Rightarrow x=3$ soluție

Ec. de gradul al 2-lea în $\mathbb{Z}_n$

1) $x^2-3x+1=0$ în $\mathbb{Z}_7$

$\Delta=9-4=5$

$\sqrt{5}$ în $\mathbb{Z}_7=?$

$\sqrt{5} = a \Rightarrow a^2 = 5$ în $\mathbb{Z}_7$

$1^2 = 1;\ 2^2 = 4;\ 3^2 = 2;\ 4^2 = 2;\ 5^2 = 4;\ 6^2 = 1;\ 0^2 = 0$

$\Rightarrow \sqrt{5}$ nu există în $\mathbb{Z}_7 \Rightarrow$ ec. nu are sol. în $\mathbb{Z}_7$

2) $x^2 - 5x + 6 = 0$ în $\mathbb{Z}_{13}$

$\Delta = 25 - 24 = 1$

$\sqrt{\Delta} = \sqrt{1} = \{1, 12\} = \{1, -1\}$

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

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

$\overset{\parallel}{0}$

~~$x_3 = (5-1) \cdot 2^{-1}$~~

~~$x_4 = (5+1) \cdot 2^{-1}$~~

Inverse matriceale

$A \in \mathcal{M}_3(\mathbb{Z}_n)$ este inversabilă $\Leftrightarrow$

$\det A \in \mathcal{U}(\mathbb{Z}_n) \Leftrightarrow \text{cmmdc}(\det A, \mathbb{Z}_n) = 1$

În $\mathbb{R}$: $A^{-1} = \frac{1}{\det A} \cdot A^*$ | În $\mathbb{Z}_n$: $A^{-1} = (\det A)^{-1} \cdot A^*$

Ex: $A = \begin{pmatrix} 2 & 1 & -1 \\ 0 & 2 & 0 \\ -1 & 2 & 3 \end{pmatrix} \in \mathcal{M}_3(\mathbb{Z}_7)$

$A^{-1} = ?$ dacă există

$$\det A = \begin{vmatrix} 2 & 1 & -1 \\ 0 & 2 & 0 \\ -1 & 2 & 3 \end{vmatrix} = 12 - 2 = 10 = 3 \text{ în } \mathbb{Z}_7$$

3^{-1} în $\mathbb{Z}_7 = 5$

$(-1)^{\text{lin+col}}$

$$A \to A^t = \begin{pmatrix} 2 & 0 & -1 \\ 1 & 2 & 2 \\ -1 & 0 & 3 \end{pmatrix} \to A^* = \begin{pmatrix} 6 & -5 & 2 \\ 0 & 5 & 0 \\ 2 & -5 & 4 \end{pmatrix}$$

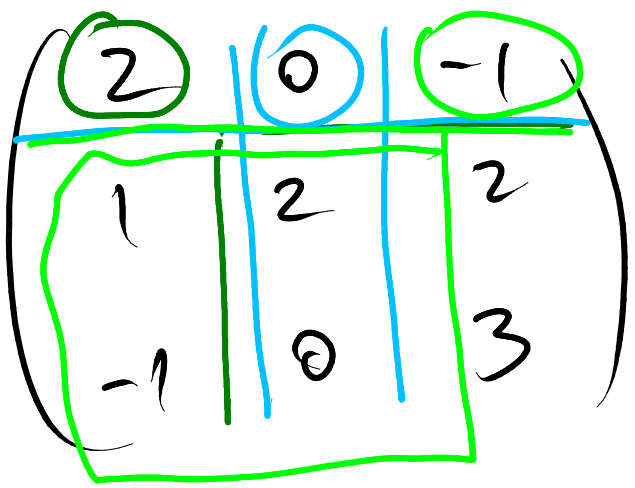
$$A^* = \begin{pmatrix} -1 & 2 & 2 \\ 0 & -2 & 0 \\ 2 & 2 & -3 \end{pmatrix}$$

$$A^{-1} = (\det A)^{-1} \cdot A^* = 5 \cdot A^* =$$

$$= 5 \cdot \begin{pmatrix} -1 & 2 & 2 \\ 0 & -2 & 0 \\ 2 & 2 & -3 \end{pmatrix} = \begin{pmatrix} -5 & 10 & 10 \\ 0 & -10 & 0 \\ 10 & 10 & -15 \end{pmatrix}$$

$$= \begin{pmatrix} 2 & 3 & 3 \\ 0 & 4 & 0 \\ 3 & 3 & 6 \end{pmatrix} = A^{-1}$$

Obs: $A \cdot A^{-1} = A^{-1} \cdot A = I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$



$2 \rightarrow \begin{vmatrix} 2 & 2 \\ 0 & 3 \end{vmatrix} = 6$

$0 \rightarrow \begin{vmatrix} 1 & 2 \\ -1 & 3 \end{vmatrix} = 5$

$-1 \rightarrow \begin{vmatrix} 1 & 2 \\ -1 & 0 \end{vmatrix} = 2$

Sisteme liniare

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

$\Leftrightarrow$

$y = 5x - 3$

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

$3x + 10x - 6 = 1$

$13x = 7 \Rightarrow 0 \Rightarrow 1x = 0$

$y = 5 \cdot 0 - 3 = -3 = 4$

$\Rightarrow S = \{(0, 4)\}$

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

$A = \begin{pmatrix} 5 & 2 \\ -2 & 2 \end{pmatrix}$

$\det A = 14 = 0$

⇒) S/St. nu mai are sol. unică

⇒) { are sol. cu parametri sau
nu are sol.