Aritmetică în $\mathbb{Z}_n$

$(\mathbb{Z}_n, +, \cdot)$ - inel comutativ
- $\hookrightarrow (\mathbb{Z}_n, +)$ grup comutativ
- $\hookrightarrow (\mathbb{Z}_n, \cdot)$ monoid comutativ
  - $\hookrightarrow$ nu orice element este inv. față de „$\cdot$"

$\mathbb{Z}_n$ = resturile posibile la împărțirea cu n

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

Ex: $(\mathbb{Z}_7, +, \cdot)$, $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ ← reprezentanți

$2 + 4 = 6 \Leftrightarrow 16 + 11 = 6 \Leftrightarrow 23 + 25 = 13$ etc

$2 = \{7k+2 \mid k \in \mathbb{Z}\} = \{2, 9, 16, 23, \dots\}$

$4 = \{7k+4 \mid k \in \mathbb{Z}\} = \{4, 11, 18, 25, \dots\}$

$6 = \{7k+6 \mid k \in \mathbb{Z}\} = \{6, 13, 20, 27, 34, \dots\}$

Pt $x \in \mathbb{Z}_n$, notez cu $-x$ simetricul față de „$+$" = <u>opusul</u> lui x

<u>Def</u>: $-x = y \Leftrightarrow x + y = 0$, elem. neutru.

Ex: În $\mathbb{Z}_7$, $-3 = y \Leftrightarrow 3 + y = 0 \Rightarrow y = 4$

<u>Sau</u>: $-3 = 0 - 3 = 7 - 3 = 4$.

Notez cu x^{-1} simetricul față de „$\cdot$" = <u>inversul</u> lui x.

Pt că $(\mathbb{Z}_n, \cdot)$ monoid $\Rightarrow x^{-1}$ nu există pt orice x.

<u>Def</u>: $x^{-1} = y \Leftrightarrow x \cdot y = 1$, elem. neutru

Ex: În $\mathbb{Z}_7$, $3^{-1} = y \Leftrightarrow 3 \cdot y = 1 \Rightarrow y = 5$ pt că $3 \cdot 5 = 15 = \overset{0}{14} + 1 = 1$.

$6^{-1} = y \Leftrightarrow 6 \cdot y = 1 \Rightarrow y = 6$ pt că $6 \cdot 6 = 36 = \overset{0}{35} + 1 = 1$

$6^{-1} = \hat{y} \Leftrightarrow 6 \cdot y = 1 \Rightarrow \hat{y} = 6$ pt că $6 \cdot 6 = 36 = \hat{35} + 1 = 1$

Not. $U(\mathbb{Z}_n) = \{ x \in \mathbb{Z}_n \mid \text{există } x^{-1} \} =$ unitățile

Teoremă: În $\mathbb{Z}_n$, $\hat{x}$ este unitate $\Leftrightarrow$ cmmdc$(x, n) = 1$

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

În particular, dacă n nr prim $\Rightarrow U(\mathbb{Z}_n) = \mathbb{Z}_n - \{\hat{0}\} = \mathbb{Z}_n^*$

De ex, $U(\mathbb{Z}_7) = \mathbb{Z}_7^* = \{\hat{1}, \hat{2}, \hat{3}, \hat{4}, \hat{5}, \hat{6}\}$

Ecuații de gradul I în $\mathbb{Z}_n$

1) $5\hat{x} + \hat{1} = \hat{3}$ în $\mathbb{Z}_{11}$

$5\hat{x} = \hat{3} - \hat{1} = \hat{2} \quad | \cdot 5^{-1} = \hat{9}$

$\hat{9} \cdot \hat{5} \cdot \hat{x} = \hat{2} \cdot \hat{9}$

$\hat{1} \cdot \hat{x} = \hat{18} = \hat{7} \Rightarrow \hat{x} = \hat{7}$

2) $6\hat{x} + \hat{5} = \hat{2}$ în $\mathbb{Z}_{10}$

$6\hat{x} = \hat{2} - \hat{5} = -\hat{3} = \hat{7} \quad | \cdot 6^{-1}$

NU EXISTĂ pt că cmmdc$(6, 10) = 2 \neq 1$

Rezolv prin încercări

$\hat{x}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$	$\hat{6}$	$\hat{7}$	$\hat{8}$	$\hat{9}$
$6\hat{x}$	$\hat{0}$	$\hat{6}$	$\hat{2}$	$\hat{8}$	$\hat{4}$	$\hat{0}$	$\hat{6}$	$\hat{2}$	$\hat{8}$	$\hat{4}$

$\Rightarrow$ ec. nu are sol.

3) $4x+7=2$ în $\mathbb{Z}_{10}$

$4x = 2-7 = -5 = 5 \mid \cdot 4^{-1}$ NU EXISTĂ

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

$\Rightarrow$ nu are sol.

Ec. de gradul al II-lea

Ex: 1) $2x^2 - 5x + 1 = 0$ în $\mathbb{Z}_7$

$\Delta = (-5)^2 - 4 \cdot 1 \cdot 2 = 25 - 8 = 17 = 3$

Există $\sqrt{3}$? Dacă $\sqrt{3} = y \Rightarrow 3 = y^2$

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

$\Rightarrow \nexists \sqrt{3}$ în $\mathbb{Z}_7$

$\Rightarrow$ ec. nu are sol.

2) $x^2 - 5x + 6 = 0$ în $\mathbb{Z}_9$

$\Delta = 25 - 24 = 1$

y	0	1	2	3	4	5	6	7	8
y^2	0	1	4	0	7	7	0	4	1

$\Rightarrow \sqrt{1} \in \{1, 8\}$ $\quad 8 = -1$

Iau $\sqrt{1} = 1 \Rightarrow x_1 = (5+1) \cdot 2^{-1} = 6 \cdot 5 = 30 = 3$

$x_2 = (5-1) \cdot 2^{-1} = 4 \cdot 5 = 20 = 2$

Dacă luam $\sqrt{7}=8 \Rightarrow x_1=(5+8)\cdot 2^{-1}=13\cdot 5=4\cdot 5=20=2$

$x_2=(5-8)\cdot 2^{-1}=(-3)\cdot 5=-15=-9-6$

$=-6=3$

Ex: $4x^2+x+5=2$ în $\mathbb{Z}_{10}$

$4x^2+x+3=0$ în $\mathbb{Z}_{10}$

$\Delta=1-4\cdot 3\cdot 4=-47=-40-7=-7=3$

$\exists\sqrt{3}$ în $\mathbb{Z}_{10}$? NU $\Rightarrow$ nu are sol.

Sisteme liniare (2x2)

Obs: Dacă $\det$(mat. sist.) $=0$ (sau neinversabil) $\Rightarrow$ rezolv prin încercări

Altfel, pot aplica reducere sau substituție.

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

$A=\begin{pmatrix} 3 & 1 \\ 2 & -5 \end{pmatrix}$; $\det A=-15-2=-17=-14-3=-3=4$ ok.

Reducere: $\begin{cases} 3x+y=2 \mid\cdot 5 \\ 2x-5y=1 \end{cases} \Rightarrow \begin{cases} 15x+5y=10 \\ 2x-5y=1 \end{cases}$ (+)

$17x=11 \Rightarrow 3x=4 \mid\cdot 3^{-1}=5$

$x=20=6$.

$2\cdot 6-5y=1$

$5y=11=4 \mid\cdot 5^{-1}=3$

$y=12=5$

Substituție: $\begin{cases} 3x+y=2 \Rightarrow y=2-3x \\ 2x-5y=1 \end{cases}$

$2x-5(2-3x)=1$

$2x-10+15x=1$

$2x - 5(2-3x) = 1$

$2x - 10 + 15x = 1$

$17x = 11 \Rightarrow 3x = 4 \Rightarrow x = 6$

$y = 2 - 3 \cdot 6 = -16$

$= -14 - 2 = -2 = 5$

Inverse matriceale

În $\mathbb{R}$, matricea M este inversabilă $\Leftrightarrow \det M \neq 0$.

În $\mathbb{Z}_n$, matricea M este inversabilă $\Leftrightarrow$ există $(\det M)^{-1}$

Ex: $A = \begin{pmatrix} 2 & 3 \\ -1 & 4 \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}_5)$

$\det A = 8 + 3 = 11 = 1$ OK $\Rightarrow$ există A^{-1}

$A \to A^t = \begin{pmatrix} 2 & -1 \\ 3 & 4 \end{pmatrix} \longrightarrow A^* = \begin{pmatrix} 4 & -3 \\ +1 & 2 \end{pmatrix}$ $(-1)^{\text{linie + col.}}$

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

Verificare: $A \cdot A^{-1} = A^{-1} \cdot A = I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$