Aritmetică in $\mathbb{Z}_n$

$\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ clase de resturi modulo n
= resturi posibile la împărțirea cu n

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

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

0 = element neutru

pt orice $x \in \mathbb{Z}_n$, not $-x$ „simetricul" lui x față de +

$-x$ s.n. opusul lui x : $\forall x \in \mathbb{Z}_n, x + (-x) = 0$.

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

1 = element neutru

Nu pt orice $x \in \mathbb{Z}_n - \{0\}$ există un „simetric"

Dacă există, not. x^{-1} și s.n. inversul lui x.

$x \cdot (x^{-1}) = 1$.

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

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

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

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

$2 + 3 = 5$

$2 \cdot 3 = 6$

$5 \cdot 6 = 30 = 28 + 2 = 2$ ($28 = 0$)

$2 = \{x \in \mathbb{Z}_n \mid x \text{ dă restul 2 la imp cu 7}\} = \{7k+2 \mid k \in \mathbb{Z}\}$

$= \{2, 9, 16, 23, 30, \dots\}$

$= \{2, 9, 16, 23, 30, \dots\}$

$5 \cdot 6 = 2 \Leftrightarrow 12 \cdot 34 = 23$ în $\mathbb{Z}_7$.

$-3 = y \Leftrightarrow y + 3 = 0$ în $\mathbb{Z}_7 \Rightarrow y = 4$ pt că $3+4 = 7 = 0$

$-5 = 2$ pt că $-5 = 0 - 5 = 7 - 5 = 2$

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

$5^{-1} = y \Leftrightarrow y \cdot 5 = 1$ în $\mathbb{Z}_7 \Rightarrow y = 3$

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

Obs: Deoarece 7 prim $\Rightarrow U(\mathbb{Z}_7) = \mathbb{Z}_7 - \{0\} = \mathbb{Z}_7^*$

pt că $\text{cmmdc}(x, 7) = 1, \forall x \in \mathbb{Z}_7^*$.

Ecuații de gradul I

Ex: $2x + 5 = 1$ în $\mathbb{Z}_7$

$2x = 1 - 5 = -4 = 3 \mid \cdot 2^{-1} = 4$

$4 \cdot 2 \cdot x = 4 \cdot 3$

$1x = 12 = 5 \Rightarrow \underline{x = 5}$

Verificare:

$2 \cdot 5 + 5 = 15 = 1$ în $\mathbb{Z}_7$ ✓

Ex: $5x + 3 = 7$ în $\mathbb{Z}_{11}$

$5x = 7 - 3 = 4 \mid \cdot 5^{-1} = 9$

$9 \cdot 5 \cdot x = 9 \cdot 4$

$x = 36 = 3 \Rightarrow \underline{x = 3}$

Ex: $6x + 1 = 2$ în $\mathbb{Z}_{10}$ $\quad U(\mathbb{Z}_{10}) = \{1, 3, 7, 9\}$

$6x = 1 \mid \cdot 6^{-1}$ NU EXISTĂ!!

Rezolv prin încercări: $\quad x \mid 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9$

Rezolv prin încercări:

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

Ec. nu are sol.

Obs: Ec. $6x=1$ este echivalentă cu $x=6^{-1}$ nu se poate!

Ec. de gradul II

Ex: $2x^2+5x-1=0$ în $\mathbb{Z}_9$

$\Delta = 25+8 = 33 = 6$

$\sqrt{\Delta} = \sqrt{6} = y \Leftrightarrow y^2=6$ există?

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

$\not\exists\, 6 \Rightarrow \sqrt{6}$ nu există în $\mathbb{Z}_9$!

$\Rightarrow$ Ec. nu are soluții.

Ex: $x^2-5x+6=0$ în $\mathbb{Z}_7$

$\Delta = 25-24 = 1$; $\sqrt{1} = 1$ în $\mathbb{Z}_7$.

$x_1 = (5+1)\cdot 2^{-1} = 6\cdot 4 = 24 = 3$

$x_2 = (5-1)\cdot 2^{-1} = 4\cdot 4 = 16 = 2$

Obs:

y	0	1	2	3	4	5	$6 = -1$
y^2	0	1	4	2	2	4	1

$1 = 1^2 = (-1)^2 = 6^2$

Dacă luam $\sqrt{1} = 6 \Rightarrow x_1 = (5+6)\cdot 2^{-1} = 4\cdot 4 = 2$

$x_2 = (5-6)\cdot 2^{-1} = 6\cdot 4 = 3$

Sisteme liniare (2x2)

Ex: $\begin{cases} 2x - y = 3 \\ 5x + 2y = 1 \end{cases}$ în $\mathbb{Z}_{11}$

Obs Verific dacă det matricei sist = 0 sau element neinversabil.
Dacă da, rezolv prin încercări.

$A = \begin{pmatrix} 2 & -1 \\ 5 & 2 \end{pmatrix}$; $\det A = 4 + 5 = 9 \neq 0$, $9 \in U(\mathbb{Z}_{11})$ ok.

Substituție: $y = 2x - 3$

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

$9x - 6 = 1 \Rightarrow 9x = 7 \;\; | \cdot 9^{-1} = 5$

$\begin{cases} x = 7 \cdot 5 = 35 = 2 \\ y = 2x - 3 = 1. \end{cases}$

Inverse matriceale

În $\mathbb{R}$: $A \in M_n(\mathbb{R})$ este inversabilă dacă $\det A \neq 0$.
În $\mathbb{Z}_n$: $A \in M_t(\mathbb{Z}_n)$ este inversabilă dacă $\det A \in U(\mathbb{Z}_n)$.

Ex: $A = \begin{pmatrix} 1 & 5 \\ 3 & 2 \end{pmatrix}$ în $M_2(\mathbb{Z}_{11})$

$\det A = 2 - 15 = -13 = -\underset{0}{\underbrace{11}} - 2 = -2 = 9 \in U(\mathbb{Z}_{11})$

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

$-22 - 3 = -3 = 8$

$A^{-1} = (\det A)^{-1} \cdot A^* = 5 \cdot \begin{pmatrix} 2 & -5 \\ -3 & 1 \end{pmatrix} = \begin{pmatrix} 10 & -25 \\ -15 & 5 \end{pmatrix}$

$-11 - 4 = -4 = 7$

$= \begin{pmatrix} 10 & 8 \end{pmatrix}$

$$= \begin{pmatrix} 10 & 8 \\ 7 & 5 \end{pmatrix}.$$

<u>Verificare</u>: $A \cdot A^{-1} = A^{-1} \cdot A = I_2$.