13426

Aritmetică în Z_n : $(Z_n,+,\cdot)$ inel comutativ

- $(Z_n,+)$ grup comutativ
- $(Z_n - \{0\}, \cdot)$ monoid
  $\hookrightarrow$ nu orice element este inversabil

Ex: $(Z_7,+,\cdot)$

$2+3=5 \Leftrightarrow 16+17=12 \Leftrightarrow 23+3=5$ etc (în Z_7) modulo 7, mod 7

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

$3=\{7k+3 \mid k\in Z\}=\{3,10,17,24,\dots\}$

$5=\{7k+5 \mid k\in Z\}=\{5,12,19,26,\dots\}$

$Z_7=\{0,1,2,3,4,5,6\}$ → reprezentanți

0 = element neutru la $+$ $\Rightarrow x+0=x, \forall x\in Z_7$

Notez $-x$ simetricul (inversul) lui x față de „+"

$-x$ se mai numește opusul lui x.

Def: $-x=y \Leftrightarrow y+x=0$

$-2=y \Leftrightarrow y+2=0=\{7k \mid k\in Z\} \Rightarrow y=5$

Obs: $\underline{-2=0-2=7-2}=14-2=\dots$ pt că 0 = multipli de 7

Înmulțirea: $2\cdot 3=6 \Leftrightarrow 9\cdot 24=13 \Leftrightarrow 16\cdot 10=34$ etc

Def: x^{-1} = simetricul lui x față de „$\cdot$" = invers

Obs: $(Z_n,+,\cdot)$ inel $\Rightarrow x^{-1}$ nu există pentru orice x.

Def: $U(Z_n)=\{x\in Z_n \mid \text{există } x^{-1}\}$ = unități

Teoremă: x este unitate în $Z_n \Leftrightarrow$ cmmdc $(x,n)=1$

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

Obs: Dacă n este număr prim $\Rightarrow U(\mathbb{Z}_n) = \mathbb{Z}_n - \{0\} = \mathbb{Z}_n^*$

Cum calculez x^{-1}?

Ex: În $\mathbb{Z}_7$, $U(\mathbb{Z}_7) = \mathbb{Z}_7^*$ pt că 7 prim.

$2^{-1} = y \Leftrightarrow 2 \cdot y = 1 \leftarrow$ el. neutru la "$\cdot$"

$\Downarrow$

$y = 4$ pt că $2 \cdot 4 = 8 = 1$.

Ecuații de gradul I

1) $5x + 2 = 1$ în $\mathbb{Z}_7 = \{0, 1, \dots, 6\}$

$\Downarrow$

$5x = 1 - 2 = -1 = 6 \mid \cdot 5^{-1} = 3$

$3 \cdot 5 \cdot x = 6 \cdot 3$

$x = 18 = 4 \quad \Rightarrow x = 4$ este soluție.

2) $3x + 1 = 7$ în $\mathbb{Z}_9 = \{0, 1, 2, \dots, 8\}$

$3x = 7 - 1 = 6 \mid \cdot 3^{-1}$ NU EXISTĂ ÎN $\mathbb{Z}_9$ pt că $\text{cmmdc}(3,9) = 3 \neq 1$ $\Rightarrow 3 \notin U(\mathbb{Z}_9)$

Rezolv prin încercări:

$x = 0$ NU; $x = 1$ NU; $x = 2$: ok; $x = 3$ NU; $x = 4$: NU; $x = 5$: ok;

$x = 6$: NU; $x = 7$ NU; $x = 8$: ok

Ecuații de gradul II

Ex: $2x^2 - 5x + 1 = 0$ în $\mathbb{Z}_7 = \{0, 1, \dots, 6\}$

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

Există $\sqrt{\Delta}$? Dacă $\sqrt{\Delta} = y \Leftrightarrow \Delta = y^2$

Există $\sqrt{3}$ în $\mathbb{Z}_7 \Leftrightarrow$ există $a \in \mathbb{Z}_7$ a.î. $a^2 = 3$.

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

în $\mathbb{Z}_7$

$\Rightarrow$ nu există $\sqrt{3}$ în $\mathbb{Z}_7$ $\Rightarrow$ ec. nu are soluții în $\mathbb{Z}_7$!

Ex: $x^2 - 5x + 6 = 0$ în $\mathbb{Z}_{11}$

$\Delta = 25 - 24 = 1$

Există $\sqrt{1}$ în $\mathbb{Z}_{11}$?

a	0	1	2	3	4	5	6	7	8	9	10
a^2	0	1	4	9	5	3	3	5	9	4	1

$\Rightarrow \sqrt{1} \in \{1, 10\}$ dar $10 = -1$

Aleg $\sqrt{1} = 1$: $x_1 = (5+1) \cdot 2^{-1} = 6 \cdot 6 = 36 = 3$

$x_2 = (5-1) \cdot 2^{-1} = 4 \cdot 6 = 24 = 2$

Dacă lucram cu $\sqrt{1} = 10$: $x_1 = (5+10) \cdot 2^{-1} = 15 \cdot 6 = 90 = 2$

$x_2 = (5-10) \cdot 2^{-1} = (-5) \cdot 6 = 6 \cdot 6 = 36 = 3$

Ex: $3x^2 + x + 4 = 2$ în $\mathbb{Z}_8$

$3x^2 + x + 2 = 0$

$\Delta = 1 - 4 \cdot 2 \cdot 3 = 1 - \overset{0}{\overset{\shortparallel}{24}} = -23 = -\overset{0}{\overset{\shortparallel}{16}} - 7 = -7 = 1$

$\sqrt{1}$ în $\mathbb{Z}_8$ este 1 sau 7

$x_1 = (-1 + 1) \cdot (2 \cdot 3)^{-1}$ $\hookrightarrow 6^{-1}$ NU EXISTĂ în $\mathbb{Z}_8$ (cum dc $(6,8) = 2$)

$\Rightarrow$ Ec. nu are soluții.

Sisteme liniare (2x2)

! Dacă det matricei sistemului **nu** este element inversabil $\Rightarrow$ rezolv prin încercări.

Altfel, aplic reducere sau substituție.

Ex: $\begin{cases} 2x+3y=1 \\ x-5y=2 \end{cases}$ în $\mathbb{Z}_7$ $\quad U(\mathbb{Z}_7)=\mathbb{Z}_7^*$

$A=\begin{pmatrix} 2 & 3 \\ 1 & -5 \end{pmatrix}$ $\det A = -10-3 = -13 = -6 = 1$ ok

Reducere: $\begin{cases} 2x+3y=1 \\ x-5y=2 \mid \cdot 2 \end{cases} \Rightarrow \begin{cases} 2x+3y=1 \\ 2x-10y=4 \end{cases}$

$(-)$

$13y=-3 \Rightarrow 6y=4 \mid \cdot 6^{-1}$
$ \overset{\shortparallel}{6}$

$y=24=3$

$x-5\cdot 3=2$

$x=2\cdot 15=17=3$

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

$4+10y+3y=1$

$13y=-3=4 \Rightarrow y=3$

$x=2+5\cdot 3=3$

Inverse matriceale

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

În $\mathbb{Z}_n$, M este inversabilă $\Leftrightarrow \det M \in U(\mathbb{Z}_n)$

Ex: $A=\begin{pmatrix} 2 & 3 \\ 0 & 5 \end{pmatrix} \in M_2(\mathbb{Z}_7)$ $\quad A^{-1}=?$ dacă există

$\det A = 10 = 3 \in U(\mathbb{Z}_7) \Rightarrow$ există A^{-1}

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

$A \longrightarrow A^t=\begin{pmatrix} 2 & 0 \\ 3 & 5 \end{pmatrix} \longrightarrow A^*=\begin{pmatrix} 5 & -3 \\ 0 & 2 \end{pmatrix}$

$A^{-1}=(\det A)^{-1}\cdot A^* = 3^{-1}\cdot A^* = 5\cdot\begin{pmatrix} 5 & -3 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 25 & -15 \\ 0 & 10 \end{pmatrix}$

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

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

$\shortparallel$

$A^{-1}\cdot A$