

Aritmetică în \mathbb{Z}_n

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

↪ $(\mathbb{Z}_n, +)$ grup comutativ

↪ (\mathbb{Z}_n, \cdot) monoid comutativ

↪ 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

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

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

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

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

Pf $x \in \mathbb{Z}_n$, notiz $u - x$ simetricul față de „ $+$ ” = oposul lui x

Def: $-x = y \Leftrightarrow x+y=0$, elem. neutr.

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

$$\underline{\text{Stiu}}: -3 = 0-3 = 7-3 = 4.$$

Notez $u \ x^{-1}$ simetricul față de „ \cdot ” = inversul lui x .

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

Def: $x^{-1} = y \Leftrightarrow x \cdot y = 1$, elem. neutr.

Ex: în \mathbb{Z}_7 , $3^{-1} = y \Leftrightarrow 3 \cdot y = 1 \Rightarrow y = 5$ pt că $3 \cdot 5 = 15 = 14 + 1 = 1$.
 $6^{-1} = y \Leftrightarrow 6 \cdot y = 1 \Rightarrow y = 6$ pt că $6 \cdot 6 = 36 = 35 + 1 = 1$.

$$6^{-1} = \bar{y} (\Rightarrow 6 \cdot \bar{y} = 1 \Rightarrow \bar{y} = 6) \text{ pt că } 6 \cdot 6 = 36 = \bar{3} + 1 = 1$$

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

Teorema: În \mathbb{Z}_n , x este unitate ($\Leftrightarrow \text{cumndc}(x, n) = 1$)
 $\Rightarrow U(\mathbb{Z}_n) = \{x \in \mathbb{Z}_n \mid \text{cumndc}(x, n) = 1\}$

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

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

Ecuatii de gradul I în \mathbb{Z}_n

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

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

$$\begin{aligned} 9 \cdot 5 \cdot x &= 2 \cdot 9 \\ 1 \cdot x &= 18 = 7 \quad \Rightarrow \underline{x = 7} \end{aligned}$$

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

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

NU EXISTĂ

pt că $\text{cumndc}(6, 10) = 2 \neq 1$

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

\Rightarrow ec. nu are sol.

$$3) 4x + 7 = 2 \text{ în } \mathbb{Z}_{10}$$

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

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.

Sr. do ambele alături

Ecu. 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	$\Rightarrow \exists \sqrt{3} \text{ în } \mathbb{Z}_7$
y^2	0	1	4	2	2	4	1	

\Rightarrow ec. cu une pat.

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

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

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

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

Dacă luăm $\sqrt{1} = 8 \Rightarrow x_1 = (5+8) \cdot 2^{-1} = 13 \cdot 5 = 65 = 20 = 2$
 $x_2 = (5-8) \cdot 2^{-1} = (-3) \cdot 5 = -15 = -9 = 6$
 $= -6 = 3$

Ex: $4x^2 + x + 5 = 2$ în \mathbb{Z}_{10}

$$4x^2 + x + 3 = 0$$
 în \mathbb{Z}_{10}

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

- - - ? .. . "

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

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

Sisteme liniare (2x2)

| obs: Dacă $\det(\text{mat. sist.}) = 0 \checkmark$ ^{sau neinvertibil} \Rightarrow rezolv puțin incertă

Altfel, pot aplica reducere sau substituții.

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

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

Reducere:

$$\begin{cases} 3x + y = 2 | \cdot 5 \\ 2x - 5y = 1 \end{cases} \Rightarrow \left\{ \begin{array}{l} 15x + 5y = 10 \\ 2x - 5y = 1 \\ (+) \end{array} \right. \quad 17x = 11 \Rightarrow 3x = 4 | \cdot 3^{-1} = 5$$

$$\begin{aligned} 2 \cdot 6 - 5y &= 1 \\ 5y &= 11 = 4 | \cdot 5^{-1} = 3 \\ y &= 12 = 5 \end{aligned} \quad \underline{x = 20 = 6.}$$

Substituție:

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

$$\begin{aligned} 2x - 5(2 - 3x) &= 1 \\ 2x - 10 + 15x &= 1 \\ 17x = 11 &\Rightarrow 3x = 4 \Rightarrow \begin{aligned} x &= 6 \\ y &= 2 - 3 \cdot 6 = -16 \\ &= -14 - 2 = -2 = 5 \end{aligned} \end{aligned}$$

Inverse matriceale

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

$\uparrow \rightarrow \dots \Leftarrow \dots M$ este inversabilă (\Rightarrow există $(\det M)^{-1}$)

In \mathbb{R} , matricea $|M|$ are inversabilită $\Leftrightarrow \det M \neq 0$.

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

Ex: $A = \begin{pmatrix} 2 & 3 \\ -1 & 4 \end{pmatrix} \in M_2(\mathbb{Z}_5)$

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

$$A \rightarrow A^t = \begin{pmatrix} 2 & -1 \\ 3 & 4 \end{pmatrix} \rightarrow A^* = \begin{pmatrix} 4 & -3 \\ -1 & 2 \end{pmatrix}$$

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

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

Coduri elementare

Setup:

A	B	C	D	E	F	G	H	I	J
O	1	2	3	4	5	6	7	8	g
K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19
U	V	W	X	Y	Z				?
20	21	22	23	24	25	26	27	28	

Alfabetul englezesc conduce la lucrul în $\mathbb{Z}_{26} = \{0, \dots, 25\}$

DAR: $U(\mathbb{Z}_{26}) = \{x \in \mathbb{Z}_{26} \mid \text{cmmdc}(x, 26) = 1\} \neq \text{nr. par}$
 \Rightarrow unele litere vor fi indescifrabile

... . + ... restul cu 3 simboluri \Rightarrow 29 prim

\Rightarrow urmăruim
 \Rightarrow Comptăm efectul cu 3 simboluri $\Rightarrow \mathbb{Z}_{2^9}$, 2^9 prim
 $\Rightarrow U(\mathbb{Z}_{2^9}) = \mathbb{Z}_{2^9}^*$

Cifrul Caesar

Varianta flux (stream cipher)

\hookrightarrow aceeași cheie pt tot mesajul

Ecuția de criptare: mesaj + cheie = cod
 $m + k = c$

Ecuția de decriptare: $c - k = m$
 $cod - cheie = mesaj$

Ex: mesaj: CIFRU, cheia: 19

$[C, I, F, R, U] \rightarrow [2, 8, 5, 17, 20] \xrightarrow[\text{mod } 29]{+ \text{cheia} + 19} [21, 27, 24, 36, 39]$
 $\xrightarrow{\text{mod } 29} [21, 27, 24, 7, 10] \rightarrow V. YHK$

CIFRU \rightarrow V. YHK (Caesar)

Decriptare: $[V, Y, H, K] \rightarrow [21, 27, 24, 7, 10] \xrightarrow[-K - 19]{} [2, 8, 5, 17, 20] \rightarrow$ CIFRU.
 $\xrightarrow[\text{mod } 29]{} [2, 8, 5, 17, 20] \rightarrow$ CIFRU.

Varianta pe blocuri (block cipher): cite o cheie pt fiecare bloc

a) fără padding

b) cu padding

Ex: $m = STICKY$, blocuri de lungime 4
 $K_1 = 10$

Ex: $m = STICLA$, blouri de lungime 4

$\Rightarrow b_1 : STIC$

$b_2 : LA?S \leftarrow \text{padding random}$

$K_1 = 10$

$K_2 = 20$

$$[S, T, I, C] \rightarrow [18, 19, 8, 2] \xrightarrow[\substack{+K_1 \\ +10}]{} [28, 29, 18, 12] \xrightarrow[\substack{\text{mod } 29}]{} [28, 0, 18, 12]$$

$$\rightarrow [28, 0, 18, 12] \rightarrow [?, A, S, M]$$

$$[L, A, ?, S] \rightarrow [11, 0, 28, 18] \xrightarrow[\substack{+K_2 \\ +20}]{} [31, 20, 48, 38]$$

$$\xrightarrow[\substack{\text{mod } 29}]{} [2, 20, 19, 9] \rightarrow [C, U, T, J]$$

$STICLA?S \rightarrow ?ASMCUTJ$ (Caesar pe blouri cu padding)

Ohs 1) Două caractere identice în blouri diferite se criptază diferit
 \Rightarrow securitate ++

2) Nu există metode de a separa padding-ul de mesaj
 (după decriptare).

Cifrul afin

Varianta flux:

Ec. de criptare: $m \cdot K_1 + K_2 = c$

Ec. de decriptare: $(c - K_2) K_1^{-1} = m$

Ex: $m = AFIN$, $K_1 = 3$, $K_2 = 17$

$$[A, F, I, N] \rightarrow [0, 5, 8, 13] \xrightarrow[\substack{\cdot K_1 + K_2 \\ \cdot 3 + 17}]{} [17, 32, 41, 56]$$

$$\xrightarrow[\substack{\text{mod } 29}]{} [17, 3, 12, 27] \rightarrow RDM.$$

$\wedge \tau : m \rightarrow \alpha M \quad r \in \{0, \dots, 1\}$

$\text{mod } 29 \quad L^1 \cdot 1 - 1 \cdot 1 - 1 \rightarrow 111.$

$\text{AFIN} \rightarrow \text{RDM. (afin)}$

$$\begin{array}{l} \text{Decriptarea: } [R, D, M, \cdot] \rightarrow [17, 3, 12, 27] \\ \qquad\qquad\qquad \xrightarrow{-K_2 \cdot K_1^{-1}} \\ \qquad\qquad\qquad \xrightarrow{-17 \cdot 3^{-1}} \\ \qquad\qquad\qquad \xrightarrow{-17 \cdot 10} \\ \qquad\qquad\qquad \xrightarrow{+12} \\ \rightarrow [0, -140, -50, 100] \end{array}$$

$$\xrightarrow{\text{mod } 29} [0, 5, 8, 13] \rightarrow \text{AFIN}$$

$$-140 = -116 - 24 = -24 = 5$$

$$29 \cdot 4 = 116$$

$$-50 = -29 - 21 = -21 = 8$$

$$100 = 87 + 13 = 13$$

Varianta pe blocuri

- cite 2 chei pt fiecare bloc
etc

Cifrul Hill

Ecuatia de criptare: $\underset{\substack{\uparrow \\ \text{matrice}}}{\text{cheie} \cdot \text{mesaj}} = \text{cod}$ Vectori

Ecuatia de decriptare: $\text{mesaj} = \underset{\substack{\uparrow \\ \text{matrice}}}{\text{cheie}^{-1} \cdot \text{cod}}$

$$\text{Ex: mesaj: ROZ} \rightarrow \begin{pmatrix} R \\ O \\ Z \end{pmatrix} \rightarrow \begin{pmatrix} 17 \\ 14 \\ 25 \end{pmatrix}$$

$$\text{cheie} \in M_3(\mathbb{Z}_{29}) \quad K = \begin{pmatrix} 1 & -1 & 0 \\ 2 & -2 & 1 \\ 0 & -1 & 1 \end{pmatrix}$$

$$\det K = -2 + 1 + 2 = 1 \Rightarrow K \text{ inversabil}$$

$$\det K = -2 + 1 + 2 = 1 \Rightarrow K \text{ invertible}$$

Criptarea: $\begin{pmatrix} 1 & -1 & 0 \\ 2 & -2 & 1 \\ 0 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 17 \\ 14 \\ 25 \end{pmatrix} = \begin{pmatrix} 3 \\ 31 \\ 11 \end{pmatrix} \pmod{29} = \begin{pmatrix} 3 \\ 2 \\ 11 \end{pmatrix} = \begin{pmatrix} D \\ C \\ L \end{pmatrix}$

R02 \rightarrow DCL (Hill)

Decriptarea $\det K = 1 \Rightarrow (\det K)^{-1} = 1$

$$K \rightarrow K^t = \begin{pmatrix} 1 & 2 & 0 \\ -1 & -2 & -1 \\ 0 & 1 & 1 \end{pmatrix} \rightarrow K^* = \begin{pmatrix} -1 & +1 & -1 \\ -2 & 1 & -1 \\ -2 & +1 & 0 \end{pmatrix}$$

$$K^{-1} = (\det K)^{-1} \cdot K^* = \begin{pmatrix} -1 & 1 & -1 \\ -2 & 1 & -1 \\ -2 & 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} -1 & 1 & -1 \\ -2 & 1 & -1 \\ -2 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 2 \\ 11 \end{pmatrix} = \begin{pmatrix} 17 \\ 14 \\ 25 \end{pmatrix} = \begin{pmatrix} R \\ O \\ Z \end{pmatrix}$$