

Aritmetică în \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

pătiorice $x \in \mathbb{Z}_n$, not $-x$ „simetric” 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 pătiorice $x \in \mathbb{Z}_n - \{0\}$ există un „simetric”
 Dacă există, not. x^{-1} și s.n. inversul lui x .
 $x \cdot (x^{-1}) = 1$.

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

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

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

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

$$2 + 3 = 5$$

$$2 \cdot 3 = 6$$

$$5 \cdot 6 = 30 = 28 + 2 = 2$$

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

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

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

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

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

$$-5 = 2 \text{ pt că } -5 = 0 - 5 = 7 - 5 = 2$$

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

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

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

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

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

Ecuatii de gradul I

Ex: $2x + 5 = 1$ în \mathbb{Z}_7

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

$$\begin{array}{l} 4 \cdot 2 \cdot x = 4 \cdot 3 \\ \hline 1 \cdot x = 12 = 5 \Rightarrow x = \underline{\underline{5}} \end{array}$$

Verificare:

$$2 \cdot 5 + 5 = 15 = 1 \text{ în } \mathbb{Z}_7 \quad \checkmark$$

Ex: $5x + 3 = 7$ în \mathbb{Z}_{11}

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

$$\begin{array}{l} 9 \cdot 5 \cdot x = 9 \cdot 4 \\ \hline x = 36 = 3 \Rightarrow x = \underline{\underline{3}} \end{array}$$

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

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

Rezolv prin incercari;

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

$$6x \mid 0 \ 6 \ 2 \ 8 \ 4 \ 0 \ 6 \ 2 \ 8 \ 4$$

$\Sigma c.$ nu are sol.

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

$\Sigma c.$ de gradul II

$$\text{Ex: } 2x^2 + 5x - 1 = 0 \text{ în } \mathbb{Z}_9$$

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

$$\sqrt{\Delta} = \sqrt{6} = y \ (\Rightarrow) \ y = 6 \text{ există?}$$

$$\begin{array}{c|cccccccc} y & | & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \hline y^2 & | & 0 & 1 & 4 & 0 & 7 & 7 & 0 & 4 & 1 \end{array} \quad \not\exists 6 \Rightarrow \sqrt{6} \text{ nu există în } \mathbb{Z}_9!$$

$\Rightarrow \Sigma c.$ nu are soluții.

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

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

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

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

$$\text{Obs: } \begin{array}{c|cccccc} y & | & 0 & 1 & 2 & 3 & 4 & 5 & 6 = -1 \\ \hline y^2 & | & 0 & 1 & 4 & 2 & 2 & 4 & 1 \end{array}$$

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

$$\text{Dacă luăm } \sqrt{1} = 6 \Rightarrow x_1 = (5+6) \cdot 2^{-1} = 4 \cdot 4 = 2 \\ x_2 = (5-6) \cdot 2^{-1} = 6 \cdot 4 = 3$$

Sisteme liniare (2x2)

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

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

Obs Verifică dacă $\det \text{matricei} \neq 0$ sau element neversabil.
Dacă da, rezolv prin încercări.

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

$$\text{Substituție: } y = 2x - 3$$

$$\begin{aligned} 5x + 2(2x - 3) &= 1 \\ 9x - 6 &= 1 \Rightarrow 9x \equiv 7 \quad | \cdot 9^{-1} \equiv 5 \\ x &\equiv 7 \cdot 5 \equiv 35 \equiv 2 \\ y &= 2x - 3 = 1. \end{aligned}$$

Inverse matriciale

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

În \mathbb{Z}_n : $A \in M_2(\mathbb{Z}_n)$ este inversabilă dacă $\det A \in U(\mathbb{Z}_n)$.

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

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

$$A \rightarrow A^t = \begin{pmatrix} 1 & 3 \\ 5 & 2 \end{pmatrix} \rightarrow A^* = \begin{pmatrix} 2 & -5 \\ -3 & 1 \end{pmatrix} \quad \begin{matrix} -22-3=-3=8 \\ 11 \\ \end{matrix}$$

$$A^{-1} = (\det A)^{-1} \cdot A^* = 5 \cdot \begin{pmatrix} 2 & -5 \\ -3 & 1 \end{pmatrix} = \begin{pmatrix} 10 & -25 \\ -15 & 5 \end{pmatrix} \quad \begin{matrix} -11+7=-4=7 \\ \end{matrix}$$

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

$$\text{Verificare: } A \cdot A^{-1} = A^{-1} \cdot A = I_2.$$

Coduri elementare

Setup

A	B	C	D	E	F	G	H	I	J	K
0	1	2	3	4	5	6	7	8	9	10
L	M	N	O	P	Q	R	S	T	U	V
11	12	13	14	15	16	17	18	19	20	21
W	X	Y	Z	?	.					
22	23	24	25	26	27	28				

Ar trebui să lucrăm în $\mathbb{Z}_{26} = \{0, 1, 2, \dots, 25\}$

DAR 26 nu este prim $\Rightarrow U(\mathbb{Z}_{26})$ nu conține (de ex.) niciun număr par \Rightarrow vor exista coduri indiscripționabile.

\Rightarrow Vom lucra în $\mathbb{Z}_{29} = \{0, 1, \dots, 28\}$, 29 prim \Rightarrow

$$\Rightarrow U(\mathbb{Z}_{29}) = \mathbb{Z}_{29}^*$$

Cifrul Caesar

Ecuația de criptare: mesaj + cheie = cod (în \mathbb{Z}_{29})
 $m + k = c$

Ecuația de decriptare: Cod - cheie = mesaj
 $c - k = m$

1) Varianta flux (stream cipher) = aceeași cheie pt tot mesajul

Ex: $m = ASTAZI$, $k = 18$

Ex: $m = ASTAZI$, $K = 18$

$$[A, S, T, A, Z, I] \rightarrow [0, 18, 19, 0, 25, 8] \xrightarrow[\mod 29]{+K \atop +18}$$

$$\rightarrow [18, 36, 37, 18, 43, 26] \xrightarrow{\mod 29} [18, 7, 8, 18, 14, 26]$$

$\rightarrow SHISO\cup$

$$ASTAZI \xrightarrow[\text{Caesar}]{+18} SHISO\cup$$

Decriptare $[S, H, I, S, O, \cup] \rightarrow [18, 7, 8, 18, 14, 26]$

$$\xrightarrow[-K \atop -18]{} [0, -11, -10, 0, -4, 8] \xrightarrow{\mod 29} [0, 18, 19, 0, 25, 8]$$

$\rightarrow ASTAZI$

2) Varianta pe blocuri

a) fără padding

b) cu padding (random)

} Împart mesajul în blocuri de lungime fixă și folosesc cîte o cheie pt fiecare bloc.

Ex: $m = ASTAZI$ blocuri de lungime 3

$$b_1: AST \quad K_1 = 15$$

$$b_2: AZI \quad K_2 = 20$$

$$[A, S, T] \rightarrow [0, 18, 19] \xrightarrow[\mod 29]{+K_1 \atop +15} [15, 33, 34] \xrightarrow{\mod 29} [15, 4, 5] \rightarrow PEF$$

$$[A, Z, I] \rightarrow [0, 25, 8] \xrightarrow[\mod 29]{+K_2 \atop +20} [20, 45, 28] \xrightarrow{\mod 29} [20, 16, 28]$$

$\rightarrow UQ?$

$\rightarrow UQ'$

$A S T A Z i \rightarrow P E F U Q?$ (Caesar pe blocuri fără padding)

Ols: Caractere identice în blocuri diferite vor fi criptate
diferit \Rightarrow securitate ++.

Ex: $m = ASTAZi$ blocuri de lungime 4 cu padding random

$$b_1 : ASTA \quad K_1 = 15$$

$$b_2 : zix. \quad K_2 = 20$$

$$\{A, S, T, A\} \rightarrow [0, 18, 19, 0] \xrightarrow[+15]{+K_1} [15, 33, 34, 15]$$

$$\xrightarrow[\text{mod } 29]{} [15, 45, 15] \rightarrow PEFP$$

$$\{z, i, x, .\} \rightarrow [25, 8, 23, 27] \xrightarrow[+20]{+K_2} [45, 28, 43, 47]$$

$$\xrightarrow[\text{mod } 29]{} [16, 28, 19, 18] \rightarrow Q?OS$$

$ASTAZiX. \rightarrow PEFPQ?OS$

dec.

Ols: Nu există metodă teoretică de eliminare a padding-ului
după decriptare

Cifrul afin

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

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

Varianta flux: aceeași 2 chei pt tot mesajul

Varianta flux: acelasi 2 chei pt tot mesajul

Ex: $m = \text{TRUMP}$, $K_1 = 6$, $K_2 = 12$ ($K_1^{-1} = 6^{-1} = 5$)

$$[T, R, U, M, P] \rightarrow [19, 17, 20, 12, 15] \xrightarrow[\mod 29]{\cdot K_1 + K_2 \atop \cdot 6 + 12} [126, 114, 132, 84, 102]$$

$$\xrightarrow{\mod 29} [10, 27, 16, 26, 15] \rightarrow K \cdot Q \llcorner P$$

Decriptarea: $[K, ., Q, \llcorner, P] \rightarrow [10, 27, 16, 26, 15]$

$$\xrightarrow[-K_2 \cdot K_1^{-1} \atop -12 \cdot 5]{} [-10, 75, 20, 70, 15] \xrightarrow{\mod 29} [19, 17, 20, 12, 15]$$

$$\rightarrow \text{TRUMP}$$

Varianta pc idiomii: cite 2 chei pt fiecare bloc

Ex: HARRIS = m, blocuri de lungime 5, fara padding

$$b_1: \text{HARRI}, K_1 = 10, K_2 = 13 \quad | \quad K_1^{-1} = 10^{-1} = 3$$

$$b_2: S, K_3 = 15, K_4 = 20 \quad | \quad K_3^{-1} = 15^{-1} = 2$$

$$[H, A, R, R, I] \rightarrow [7, 0, 17, 17, 8] \xrightarrow[\cdot 10 + 13]{\cdot K_1 + K_2}$$

$$[83, 13, 183, 183, 93] \xrightarrow{\mod 29} [25, 13, 9, 9, 6]$$

$\rightarrow \text{ZNJJG}$

$$S \rightarrow 18 \xrightarrow[\cdot 15 + 20]{\cdot K_3 + K_4} 290 \xrightarrow{\mod 29} 0 \rightarrow A$$

HARRIS $\rightarrow \text{ZNJJG A}$

Cifrul Hill

$$\text{Ec. de criptare : } \underset{\substack{\uparrow \\ \text{matrice} \\ \text{de criptare}}}{K} \cdot \underset{\substack{\nearrow \text{vectori} \\ \downarrow}}{m} = c$$

$$\text{Ec. de decriptare : } m = K^{-1} \cdot c$$

$$\text{Ex: } m: \{0, N\} \rightarrow \begin{pmatrix} 1 \\ 0 \\ N \end{pmatrix}$$

$$K : \begin{pmatrix} 1 & -1 & 0 \\ 2 & 0 & 1 \\ -1 & -1 & 1 \end{pmatrix} \in M_3(\mathbb{Z}_{29}) \quad \det K = 1 + 1 + 2 = 4$$

$$\begin{pmatrix} 1 \\ 0 \\ N \end{pmatrix} = \begin{pmatrix} 8 \\ 14 \\ 13 \end{pmatrix} ; \quad \begin{pmatrix} 1 & -1 & 0 \\ 2 & 0 & 1 \\ -1 & -1 & 1 \end{pmatrix} \left| \begin{array}{c|c} 8 \\ 14 \\ 13 \end{array} \right| = \begin{pmatrix} -6 \\ 29 \\ -9 \end{pmatrix} \text{ mod } 29$$

$$= \begin{pmatrix} 2 & 3 \\ 0 & 1 \\ 2 & 0 \end{pmatrix} \begin{matrix} X \\ A \\ U \end{matrix}$$

$$\text{Decriptare: } K^{-1} = (\det K)^{-1} \cdot K^* = 4^{-1} \cdot K^* = 22 \cdot$$

$$4 \cdot y = 1 \text{ mod } 29 = \{30, 59, 88, \dots\}$$

$$4^{-1} = 22 \text{ pt că } 4 \cdot 22 = 88 = 87 + 1 = 1$$

$$K \rightarrow K^t = \begin{pmatrix} 1 & 2 & -1 \\ -1 & 0 & -1 \\ 0 & 1 & 1 \end{pmatrix} \rightarrow K^* = \begin{pmatrix} 1 & +1 & -1 \\ -3 & 1 & -1 \\ -2 & +2 & 2 \end{pmatrix}$$

$$K^{-1} = 22 \cdot \begin{pmatrix} 1 & 1 & -1 \\ -3 & 1 & -1 \end{pmatrix}$$

$$K^{-1} = 22 \cdot \begin{pmatrix} 1 & 1 & -1 \\ -3 & 1 & -1 \\ -2 & 2 & 2 \end{pmatrix}$$

Decryption : $22 \cdot \begin{pmatrix} 1 & 1 & -1 \\ -3 & 1 & -1 \\ -2 & 2 & 2 \end{pmatrix} \cdot \begin{pmatrix} 23 \\ 0 \\ 20 \end{pmatrix} = \begin{pmatrix} 8 \\ 14 \\ 13 \end{pmatrix} \text{ (mod 29)}$