

## 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:

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

$0$  = el. neutru

Pt orice  $x \in \mathbb{Z}_n$ , notez  $-x$  „simetric” lui  $x$  față de „+”  
 $-x$  s.n. opusul lui  $x$ .

Adică:  $x + (-x) = 0$ .

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

$1$  = element neutru

Nu orice  $x \in \mathbb{Z}_n$  are „simetric” față de „·”

Dacă există, notez cu  $x^{-1}$  acest „simetric”, numit inverse lui  $x$ .

Adică:  $x \cdot (x^{-1}) = 1$ .

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

Teorema  $x \in U(\mathbb{Z}_n) \Leftrightarrow \text{cmmdc}(x, n) = 1$ .

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

Corolar: Dacă  $n$  este nr. prim  $\Rightarrow U(\mathbb{Z}_n) = \mathbb{Z}_n^*$ .

Ex:  $(\mathbb{Z}_{11}, +, \cdot)$ ;  $\mathbb{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$$7 + 8 = 15 = 11 + 4 = 4,$$

reprenzentanți

$$7+8=15=11+4=4,$$

$$4 \cdot 7=28=22+6=6.$$

... punctuală

$7 = \{$  toate nr. întregi care dau restul 7 la împ. cu 11

$$= \{ 11k+7 \mid k \in \mathbb{Z} \} = \{ 18, 29, 40, \dots \}$$

$$4 = \{ 11k+4 \mid k \in \mathbb{Z} \} = \{ 4, 15, 26, 37, \dots \}$$

$$\mathbb{Z}_{11} : 4 \cdot 7 = 6 \quad ( \Rightarrow 40 \cdot 15 = 17 )$$

$$-2 = y \quad (\Rightarrow) \quad y+2=0 \Rightarrow y=9 \quad \text{pt că } 9+2 < 11=0.$$

$$-7 = 4 \quad \text{pt că } 7+4=11=0.$$

$$-7 = 0 - 7 = 11 - 7 = 4$$

$$11 \text{ nr prim} \Rightarrow U(\mathbb{Z}_{11}) = \mathbb{Z}_{11}^* = \{ 1, 2, 3, \dots, 10 \}$$

$$2^{-1} = y \quad (\Rightarrow) \quad 2y = 1 \Rightarrow y = 6 \quad \text{pt că } 2 \cdot 6 = 12 = 11 + 1 = 1$$

$$5^{-1} = 9 \quad \text{pt că } 5 \cdot 9 = 45 = 4 \cdot 11 + 1 = 1$$

$$7^{-1} = 8 \quad \text{pt că } 7 \cdot 8 = 56 = 5 \cdot 11 + 1 = 1$$

$$6^{-1} = 2 \quad \text{și} \quad 9^{-1} = 5 \quad \text{și} \quad 8^{-1} = 7$$

### Ecuații de gradul I

$$\text{Ex: } 5x+7=2 \text{ în } \mathbb{Z}_{13}$$

$$5x = 2 - 7 = -5 = 8 \quad | \cdot 5^{-1} = 8 \quad \left( \text{pt că } 5 \cdot 8 = 40 = 3 \cdot 11 + 1 \right)$$

$$8 \cdot 5 \cdot x = 8 \cdot 8$$

$$x = 64 = 12 \Rightarrow x = \underline{12}.$$

$$\text{Verificare: } 5 \cdot 12 + 7 = 60 + 7 = (5 \cdot 11 + 5) + 7 = 52 + 8 = 15 = 2 \cdot \underline{12}.$$

Verificare:  $5 \cdot 12 + 7 = 60 + 7 = (52+8) + 7 = 15 = 2 \cdot \underline{OK}$ .

Ex:  $7x + 3 = 1$  în  $\mathbb{Z}_9$

$$\underline{7x} = 1 - 3 = -2 = \underline{7} \Rightarrow 7x = 1.$$

Ex:  $3x + 5 = 4$  în  $\mathbb{Z}_{12}$   $U(\mathbb{Z}_{12}) = \{1, 5, 7, 11\} \not\ni 3$   
 $\underline{3x} = -1 = \underline{11} \mid 3^{-1}$  **NU EXISTĂ!**

Rezolv prin încercări

x	0	1	2	3	4	5	6	7	8	9	10	11
$3x$	0	3	6	9	0	3	6	9	0	3	6	9

Ec. nu are soluții.

Ec. de gradul II

Ex:  $3x^2 - 5x + 1 = 0$  în  $\mathbb{Z}_7$ .

$$\Delta = 25 - 4 \cdot 3 = 25 - 12 = 13 = 6.$$

Există rădăcini? Dacă da,  $\sqrt{6} = y \Rightarrow y^2 = 6$

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

$\Rightarrow$  Ec. nu are soluții.

Ex:  $x^2 - 5x + 6 = 0$  în  $\mathbb{Z}_{13}$

$$\Delta = 25 - 4 \cdot 6 = 1$$

$$\sqrt{1} = 1 \text{ OK.}$$

$$\sqrt{1} = 1 \text{ sfk.}$$

$$x_1 = (5+1) \cdot 2^{-1} = 6 \cdot 7 = 42 = 39 + 3 = 3$$

$$x_2 = (5-1) \cdot 2^{-1} = 4 \cdot 7 = 28 = 26 + 2 = 2$$

Dacă calculăm  $\sqrt{1}$ :

$y$	0	1	2	3	4	$\dots$	12
$y^2$	0	1	4	9	3	$\dots$	1

$$\Rightarrow \sqrt{1} \in \{1, 12\}$$

$$42 = -1 \text{ și } (-1)^2 = 1$$

În plus,  $x_1 = (5+12) \cdot 2^{-1} = 17 \cdot 7 = 4 \cdot 7 = 28 = 2$

$$x_2 = (5-12) \cdot 2^{-1} = (-7) \cdot 7 = -49 = -39 - 10 = -10 = 3.$$

### Sisteme liniare (2x2)

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

! Calculați  $\det$  matricei sist. Dacă  $= 0$  sau neinvertibil  $\Rightarrow$  rezolv prin încercări.

$A = \begin{pmatrix} 2 & -1 \\ 5 & 3 \end{pmatrix}; \det A = 11 = 4 \text{ sfk.}$

Substituție:  $y = 2x - 3 \Rightarrow 5x + 3(2x - 3) = 1$

$$11x - 9 = 1$$

$$4x - 2 = 1 \Rightarrow 4x = 3 \quad | \cdot 4^{-1} = 2$$

$$\begin{array}{l} x = 6 \\ y = 2 \cdot 6 - 3 = 9 = 2 \end{array}$$

## Inversă matricială

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

În  $\mathbb{Z}_n$ :  $A \in M_t(\mathbb{Z}_n)$  este inversabilă ( $\Leftrightarrow \det A \in U(\mathbb{Z}_n)$   
(ca să existe  $(\det A)^{-1}$ )).

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

$$\det A = 17 = 6 \in U(\mathbb{Z}_{11}); \quad 6^{-1} = 2 \Rightarrow (\det A)^{-1} = 2$$

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

$$A^{-1} = (\det A)^{-1} \cdot A^* = 2 \cdot \begin{pmatrix} 1 & 5 \\ -3 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 10 \\ -6 & 4 \end{pmatrix}$$

$$\Rightarrow A^{-1} = \begin{pmatrix} 2 & 10 \\ 5 & 4 \end{pmatrix}$$

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

## Cifruri elementare

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

$\gamma$      $\leftarrow$      $\rightarrow$      $\cdot$      $:$   
 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  $\Rightarrow$  Codurile care folosesc elemente neinvertibile vor fi îndesifrabile.

$\Rightarrow$  Vom lucra în  $\mathbb{Z}_{29} = \{0, 1, 2, \dots, 28\}$

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

### Cifrul Caesar

Varianta flux (stream cipher) : aceeași cheie pt tot mesajul

Ec. de criptare: mesaj + cheie = cod  
 $m + K = c$

Ec. de decriptare:  $c - K = m$

Ex:  $m: COLEG, K=21$

$[C, O, L, E, G] \rightarrow [2, 14, 11, 4, 6] \xrightarrow{+K} [23, 35, 32, 25, 27]$

$\xrightarrow{\text{mod } 29} [23, 6, 3, 25, 27] \rightarrow XGDZ.$

$COLEG \rightarrow XGDZ.$  (Caesar,  $K=21$ )

Decriptare:  $[X, G, D, Z, .] \rightarrow [23, 6, 3, 25, 27] \xrightarrow{-K}$

$\xrightarrow{\text{mod } 29} [2, 14, 11, 4, 6] \rightarrow COLEG$

Variantă pe blocuri (block cipher) { Împărțim textul în blocuri de lungime fixă și folosim  
a) fără padding  
b) cu padding (random)

Ex:  $m: MIERCURI$  blocuri de lungime 5

$b_1: MIERC$   $K_1 = 11$

$b_2: URIRS$   $K_2 = 15$

$$[M, I, E, R, C] \rightarrow [12, 8, 4, 17, 2] \xrightarrow{+K_1 \atop +11} [23, 19, 15, 28, 13]$$

$\rightarrow XTP?N$

$$[U, R, I, R, S] \rightarrow [20, 17, 8, 17, 18] \xrightarrow{+K_2 \atop +15}$$

$$\rightarrow [35, 32, 23, 32, 33] \xrightarrow{\text{mod } 29} [6, 3, 23, 3, 4]$$

$\rightarrow GDXDE$

$MIECURIRIS \rightarrow XTP?NGDXDE$  (Caesar pe blocuri)

(Obs: 1) Caractere identice în blocuri diferite  $\rightarrow$  criptarea diferențială  
 $\rightarrow$  securitate ++

2) Nu există nicio metodă teoretică de a separa padding-ul de textul decriptat.

### Cifrul afin

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

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

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

Varianta flux: 2 chei pt făt mesajul

$$\text{Ex.: } m: \text{MESAJ} \quad K_1 = 6 \quad K_2 = 12$$

$$[M, E, S, A, J] \rightarrow [12, 4, 18, 0, 9] \xrightarrow[\mod 29]{\begin{matrix} \cdot K_1 + K_2 \\ \cdot 6 + 12 \end{matrix}} [84, 36, 120, 12, 66]$$

$$\xrightarrow{\mod 29} [26, 7, 4, 12, 8] \rightarrow \text{HEMI}$$

$$\text{MESAJ} \rightarrow \text{HEMI} \text{ (afin)}$$

$$\text{Decriptarea: } [\text{H, E, M, I}] \rightarrow [26, 7, 4, 12, 8] \xrightarrow[-12 \cdot 6^{-1}]{\begin{matrix} \cdot K_2 \cdot K_1^{-1} \\ \mod 29 \end{matrix}}$$

$$[70, -25, -40, 0, -20] \xrightarrow[\mod 29]{\begin{matrix} \cdot 5 \\ \mod 29 \end{matrix}} [12, 4, 18, 0, 9] \rightarrow \text{MESAJ}$$

Varianta pe blocuri: cite 2 chei pt fiecare bloc

### Cifrul Hill

vectorii-coloană

$$\text{Ec. de criptare: } K \cdot M = C$$

matrice  
(de criptare)

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

$$\text{Ex.: } M = \text{CRÍ} \rightarrow \begin{pmatrix} C \\ R \\ I \end{pmatrix} = \begin{pmatrix} 2 \\ 17 \\ 8 \end{pmatrix}$$

$$K \in U_3(\mathbb{Z}_{29}) = \begin{pmatrix} 1 & -1 & 0 \\ 2 & 0 & 1 \\ -1 & 1 & 2 \end{pmatrix} \quad \det K = 4 \in U(\mathbb{Z}_{29})$$

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

Criptarea:  $\begin{pmatrix} 1 & -1 & 0 \\ 2 & 0 & 1 \\ -1 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 17 \\ 8 \end{pmatrix} = \begin{pmatrix} -15 \\ 12 \\ 31 \end{pmatrix} \pmod{29} = \begin{pmatrix} 14 \\ 12 \\ 2 \end{pmatrix} \begin{matrix} O \\ M \\ C \end{matrix}$

ORI  $\longrightarrow$  OM C (Hill flux)

Decriptarea:  $K \rightarrow K^t = \begin{pmatrix} 1 & 2 & -1 \\ -1 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix} \rightarrow K^* = \begin{pmatrix} -1 & +2 & -1 \\ -5 & 2 & -1 \\ 2 & 0 & 2 \end{pmatrix}$

$$K^{-1} = (\det K)^{-1} \cdot K^* = h^{-1} \cdot K^* = 22 \cdot K^*$$

$$h^{-1} = y \Rightarrow hy = 1 \pmod{29} = \{30, 59, 88, \dots\}$$

$$22 \cdot \begin{pmatrix} -1 & 2 & -1 \\ -5 & 2 & -1 \\ 2 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 14 \\ 12 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \\ 17 \\ 8 \end{pmatrix} = \begin{matrix} C \\ R \\ I \end{matrix}$$

Varianta pe blocuri: cîte o matrice de criptare pt fiecare bloc.

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

$\downarrow \quad \downarrow \quad \swarrow$   
matrice      vector-coborâr

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

Ex:  $m = ROZ$

$$K_1 = \begin{pmatrix} -1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}; K_2 = \begin{pmatrix} 2 \\ 5 \end{pmatrix}$$

$$K_1 = \begin{pmatrix} -1 & 1 & 0 \\ 2 & 1 & 0 \\ -1 & -1 & -2 \end{pmatrix} ; K_2 = \begin{pmatrix} 5 \\ 7 \end{pmatrix}$$

$$\underbrace{T_{\text{uno}}}_{11} =$$