13.03

Aritmetica modulară (în $\mathbb{Z}_n$) $\quad \mathbb{Z}_n = \{\hat{0}, \hat{1}, \hat{2}, \dots, \widehat{n-1}\}$

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

- $(\mathbb{Z}_n, +)$ grup comutativ
  - $\hat{a} + \hat{b} = \widehat{a+b}$
- $(\mathbb{Z}_n, \cdot)$ monoid com.
  - $\hat{a} \cdot \hat{b} = \widehat{a \cdot b}$

$\hat{x} \in \{x \in \mathbb{Z} \mid x \text{ este inversabil în } \mathbb{Z}_n\}$ (mulțimea lui $\hat{x}$)

Ly nu mai pot scrie $\frac{1}{x}$ (în $\mathbb{Z}_n$) din cauza inversabilitate

Ex: $\mathbb{Z}_3 = \{\hat{0}, \hat{1}, \hat{2}\}$

$\hat{1} + \hat{2} = \hat{0}$; $\hat{2} + \hat{2} = \hat{1}$

$\hat{1} \cdot \hat{2} = \hat{2}$; $\hat{2} \cdot \hat{2} = \hat{1}$

reprezentanți

$\hat{2} \cdot \hat{3} = \hat{6} = \hat{1}$; $\hat{4} \cdot \hat{4} = \hat{16} = \hat{1}$; $\hat{2} \cdot \hat{4} = \hat{8} = \hat{2}$

$\hat{a}^{-1}$ = inversul multiplicativ al lui $\hat{a}$ din $\mathbb{Z}_n$

$= \hat{a}$ — " — additiv

Def: $\hat{a}^{-1} = \hat{b}$ în $\mathbb{Z}_n$ (=) $\widehat{ab} = \hat{1} \in \mathbb{Z}_n$

$-\hat{a} = \hat{b}$ în $\mathbb{Z}_n$ (=) $\widehat{a+b} = \hat{0} \in \mathbb{Z}_n$

Ex: $\mathbb{Z}_{12}$

$-7 + a$ (=) $7 + a = 0 \Rightarrow a = 5$

$-11 = a$ (=) $11 + b = 0 \Rightarrow b = 1$

$5^{-1} = c$ (=) $5c = 1 \Rightarrow c = 5$

$7^{-1} = d$ (=) $7d = 1 \Rightarrow d = 7$ pt că $7 \cdot 7 = 49 = \overset{0}{48} + 1$

$11^{-1} = 11$ pt că $11 \cdot 11 = 121 = 120 + 1$

8^{-1} nu există pt că $8 \times 1 \in \mathbb{Z}_{12}$ nu are inv.

10^{-1} nu $\Rightarrow$ $\hat{0}$ $\quad 2^{-1}, 4^{-1}, 5^{-1}, 6^{-1}$

Def: $U(\mathbb{Z}_n) = \{x \in \mathbb{Z}_n \mid \text{există } x^{-1} \text{ în } \mathbb{Z}_n\}$ (= grupul multiplicativ al lui $\mathbb{Z}_n$

$x \in U(\mathbb{Z}_n)$ s.n. unitate

Obs: $(U(\mathbb{Z}_n), \cdot)$ grup comutativ.

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

Obs 1: Dacă n nr prim $\Rightarrow U(\mathbb{Z}_n) = \mathbb{Z}_n - \{0\}$

Obs 2: Dacă $x \notin U(\mathbb{Z}_n)$ $\exists y \in \mathbb{Z}_n$ a.î. $xy = 0$, $y \neq 0$

$\hookrightarrow$ x, y s.n. divizori ai lui zero

Ex: În $\mathbb{Z}_{12}$, 4 este divizor al lui zero pt că $4 \cdot 3 = 0$

10 — " — pt că $10 \cdot 6 = 60 = 0 \cdot 5 + 0$.

Ex: $U(\mathbb{Z}_{10}) = \{3, 7, 9, 1\}$

3^{-1} în $\mathbb{Z}_{10}$, $7^{-1} = 3$, $9^{-1} = 9$

Cuadru de grupul $\hat{5}$ în $\mathbb{Z}_n$

Ex: $5x + 5 = 1$ în $\mathbb{Z}_7$

$5x = 1 - 5 = -4 = 3 \Rightarrow \underline{x = 6}$

Ex: $3x + 7 = 2$ în $\mathbb{Z}_{13}$

$3x = 2 - 7 = -5 = 8$

$3x = 8 \mid \cdot 3^{-1} \Rightarrow x = 8 \cdot 9 = 72 = \overset{0}{65} + 7 = 7$

$\underline{x = 7}$

Ex: $5x - 3 = 7$ în $\mathbb{Z}_9$

$5x = 7 + 3 = 10 \mid \cdot 4^{-1} = 9 \Rightarrow x = 10 \cdot 9 = 90 = 88 + 2 = 2$

$\underline{x = 2}$

Ex: $4x + 1 = 3$ în $\mathbb{Z}_{10}$ Rezolvăm prin inversiune

$4x = 2$ în $\mathbb{Z}_{10}$

4^{-1} nu există!

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

$\Rightarrow x \in \{3, 8\}$

Ecuație de gradul 2

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

$\Delta = 9 - 4 = 5$

$\sqrt{5}$ în $\mathbb{Z}_7$ $\quad \sqrt{5} = a$ (=) $a^2 = 5$ nu se găsește $\Rightarrow \sqrt{\Delta} \notin \mathbb{Z}_7$

S.i.p.

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

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

$\Delta = 25 - 24 = 1$

$\sqrt{1} \in \{1, 12\}$ pt că $12^2 = 144 = 11 \cdot 13 + 1 = 1$

$(12 = -1)$

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

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

Dacă iau $\sqrt{1} = 12$: $x_1 = (5 + 12) \cdot 7 = 17 \cdot 7 = \underline{2}$

$x_2 = (5 - 12) \cdot 7 = (-7) \cdot 7 = 6 \cdot 7 = 42 = \underline{3}$

Cifruri simple: Cesar, afin, Hill

Cifruri: flux (stream cipher) = asociază cheie pt fiet mesajul pe biți (block cipher) = o cheie / bloc de mesaj

cu padding: toate literele de aceeași lungime [salted hash]

fără padding: ultimul bloc este mai scurt

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

Lucrez în $\mathbb{Z}_{26} = \{0, 1, 2, \dots, 25\}$, ori de câte ori pot, mă ajut de ex. nr par, nu am inverse!

Atenș: L, O, 26, 27, 28 $\Rightarrow$ lucrez în $\mathbb{Z}_{29}$, 29 prim!

Cifrul Cesar

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

Ecuația de decriptare: mesaj = cod - cheie (în $\mathbb{Z}_{29}$)

Ex: MARTI $\rightarrow [M, A, R, T, I] \rightarrow [12, 0, 17, 19, 8] \xrightarrow{+k, +21}$

Cheia: $k = 21$

$\rightarrow [33, 21, 38, 40, 29] \xrightarrow{\bmod 29} [4, 21, 9, 11, 0] \rightarrow$

$\rightarrow$ EVJLA

Decriptare: EVJLA $\rightarrow [4, 21, 9, 11, 0] \xrightarrow{-k, -21} [-17, 0, -12, -10, -21]$

$\xrightarrow{+29} [12, 0, 17, 19, 8] \rightarrow$ MARTI

Variantă pt biți / block

Cu padding random

Ex: MARTI = mesaj $\quad$ MARTI $\rightarrow$ MAR

b_1 = lungimea blocurilor = 3 $\quad$ TIS

Cu padding random

$k_1 = 15$, $k_2 = 6$

MAR $\rightarrow [12, 0, 17] \xrightarrow{+15} [27, 15, 32] \rightarrow [27, 15, 3] \rightarrow$ PD

TIS $\rightarrow [19, 8, 18] \xrightarrow{+k_2} [25, 14, 24] \rightarrow$ ZOY

MARTIIS $\rightarrow$ PDZOY

Cifrul afin

Flux: Ecuația de criptare: cod = mesaj · cheie1 + cheie2

Ecuația de decriptare: mesaj = (cod - cheie2) · cheie1^{-1}

Ex: MARTI = mesaj

$k_1 = 4$; $k_2 = 11$

$[MARTI] \rightarrow [12, 0, 17, 19, 8] \xrightarrow{\cdot 4, +11} [59, 11, 79, 87, 43]$

$\xrightarrow{\bmod 29} [1, 11, 21, 0, 14] \rightarrow$ BLVAO

Decriptare: BLVAO $\rightarrow [1, 11, 21, 0, 14] \xrightarrow{-11, \cdot 4^{-1}} [-220, 0, 220, -242, 66]$

$\rightarrow [12, 0, 17, 19, 8] \rightarrow$ MARTI

$-220 = -280 + 60 \Rightarrow -220 = 58 + 12$

$220 = 280 - 60 \Rightarrow 220 = 58 - 12 = -12 = 17$

$-242 = -280 + 38 \Rightarrow -242 = 58 - 10 = -10 = 19$

$66 = 58 + 8 = 8$

Hill

La matrice de criptare drept cheie

Ec de criptare: $\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} M \\ T \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \end{pmatrix}$

Ec de decriptare: $\begin{pmatrix} M \\ T \end{pmatrix} = M^{-1} \cdot \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$

Ex: $A\hat{z}i$ = mesaj $= \begin{pmatrix} 25 \\ 8 \end{pmatrix}$

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

$\begin{pmatrix} 1 & -1 & 0 \\ 2 & 1 & -1 \\ -2 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 25 \\ 8 \end{pmatrix} = \begin{pmatrix} -25 \\ 17 \\ 8 \end{pmatrix} \bmod 29 = \begin{pmatrix} 4 \\ 17 \\ 8 \end{pmatrix} = \begin{pmatrix} E \\ R \\ I \end{pmatrix} = cod.$

Decriptare: $A = \begin{pmatrix} 1 & -1 & 0 \\ 2 & 1 & -1 \\ -2 & 0 & 1 \end{pmatrix}$; $\det A = 1 - 2 + 2 = 1 \in U(\mathbb{Z}_{29})$

$\Rightarrow \exists A^{-1}$

$A \rightarrow A^T = \begin{pmatrix} 1 & 2 & -2 \\ -1 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix} \longrightarrow A^* = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 2 & 2 & 3 \end{pmatrix}$

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

$\begin{pmatrix} M \\ T \\ I \end{pmatrix} = A^{-1} \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 2 & 2 & 3 \end{pmatrix} \begin{pmatrix} 4 \\ 17 \\ 8 \end{pmatrix} = \begin{pmatrix} 0 \\ 25 \\ 8 \end{pmatrix}$