1343a - Aritmetică modulară (în $\mathbb{Z}_n$)

$\mathbb{Z}_n = \{0, 1, 2, 3, \dots, n-1\}$

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

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

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

Ex: $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$

$-a$ = opusul lui $a \in \mathbb{Z}_7$

= simetricul față de +

$-a = b \Leftrightarrow a + b = 0$

$-3 = x \Leftrightarrow x + 3 = 0$ în $\mathbb{Z}_7 \Rightarrow x = 4$

$\Leftrightarrow -4 = 3$

$-2 = 5$ pt că $2 + 5 = 7 = 0$ în $\mathbb{Z}_7$

a^{-1} = inversul lui $a \in \mathbb{Z}_7$

= simetricul față de $\cdot$

$3^{-1} = x \Leftrightarrow 3 \cdot x = 1$

$x = 5$ pt că $3 \cdot 5 = 15 = 1$

$3^{-1} = 5 \Rightarrow 5^{-1} = 3$

$2^{-1}=4$ pt că $2\cdot 4=8=1$

$1^{-1}=1$

$6^{-1}=6$

$\Rightarrow (\mathbb{Z}_7-\{0\},\cdot)$ grup com.

Teoremă: $U(\mathbb{Z}_n)=\{x\in \mathbb{Z}_n \mid \exists x^{-1}\}$

grupul unităților

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

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

$1^{-1}=1$; $3^{-1}=7 \Rightarrow 7^{-1}=3$; $9^{-1}=9$

$\cdot$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

$(U(\mathbb{Z}_{10}),\cdot)$ grup com.

Ec. de gradul I în $\mathbb{Z}_n$

$3x+2=1$ în $\mathbb{Z}_7$

$3x=-1$

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

$$\underbrace{5\cdot 3}\cdot x=-1\cdot 5$$

$$x=-5=2$$

$$3x=-1=6 \Rightarrow x=2$$

$2x-1=5$ în $\mathbb{Z}_{10}$ $\quad U(\mathbb{Z}_{10})=\{1,3,7,9\}$

$\Updownarrow$

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

<u>obs</u>: $x=3$ din tabla înmulțirii

$\cdot$	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8

Ex. $2x=3$ în $\mathbb{Z}_{10}$ nu are sol.

<u>Ec. de gradul II</u>

- $2x^2-5x+1=3$ în $\mathbb{Z}_7$

$$2x^2-5x-2=0$$

$$\Delta=(-5)^2-4\cdot 2\cdot(-2)=4+2=6$$

$\sqrt{6}$ în $\mathbb{Z}_7 = a \iff a^2 = 6$

$0^2=0;\ 1^2=1;\ 2^2=4;\ 3^2=2;\ 4^2=2;\ 5^2=4;\ 6^2=1$

$\Rightarrow \sqrt{6}$ nu există în $\mathbb{Z}_7 \Rightarrow$ ec. nu are sol.

- $x^2-5x+6=0$ în $\mathbb{Z}_{13}$

$\Delta = 25-24 = 1$

$\sqrt{\Delta} = \sqrt{1} = \{1, 12\} = \{1, -1\}$ $\qquad \overset{0}{\overset{\shortparallel}{-26}}\underset{\shortparallel}{-10}$

$x_1 = (5+1)\cdot 2^{-1} = 6\cdot 7 = 6\cdot(-6) = -36$
$= -10 = 3$

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

4^{100} în $\mathbb{Z}_{11} = ?$

$(4^2)^{50} = 5^{50} = (5^2)^{25} = 3^{25} = (3^5)^5 = 1^5 = 1$

$3^5 = 3^2\cdot \underbrace{3^2\cdot 3}_{5} = 9\cdot 5 = 1$

Logaritmul discret

$$\log_a b = c \iff a^c = b$$

$\log_2 3$ în $\mathbb{Z}_5$ $\Rightarrow \log_2 3$ în $\mathbb{Z}_5 = 3$

$2^0 = 1;\ 2^1 = 2;\ 2^2 = 4;\ \underline{2^3 = 3}$

$\log_2 3$ în $\mathbb{Z}_7$ nu există.

$$\underbrace{2^0 = 1;\ 2^1 = 2;\ 2^2 = 4;}\ \underbrace{2^3 = 1;\ 2^4 = 2, \dots}$$

$\log_a b$ în $\mathbb{Z}_n$

Teorema lui Lagrange pt grupuri

$(G, \cdot)$ grup, $\# G = n$

Fie $g \in G. \Rightarrow g^n = e.$

$(\mathbb{Z}_7^*, \cdot)$, $g^6 = 1, \forall g \in \mathbb{Z}_7^*$

grup.

Inverse matriceale

$A \in \mathcal{M}_n(\mathbb{Z}_t)$ este inversabilă $\Leftrightarrow$

$\det A \in \mathcal{U}(\mathbb{Z}_t) \Leftrightarrow \text{cmmdc}(\det A, t) = 1.$

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

Coduri folosind $\mathbb{Z}_n$

1. Flux (stream cipher): aceeași cheie pt tot mesajul
2. Bloc (block cipher): o cheie / bloc de mesaj

   a) fără padding: ≤ 1 bloc mai scurt

   b) cu padding: toate blocurile au ac. lung.

$\mathbb{Z}_{26}$ | $\boxed{\mathbb{Z}_{29}}$

A	B	C	D	...	Z	␣	.	?
0	1	2	3	...	25	26	27	28

Caesar $c = m + K$

Ec. de criptare: $Cod = Mesaj + cheie$

Ec. de decriptare $m = C - K$

Ex: Flux: Mesaj: ANDREEA

Cheia: 20

$[A, N, D, R, E, E, A] \rightarrow [0, 13, 3, 17, 4, 4, 0]$

$\xrightarrow[+20]{+K} [20, 33, 23, 37, 24, 24, 20] \xrightarrow[\text{mod } 29]{\% 29}$

$[20, 4, 23, 8, 24, 24, 20] \rightarrow$ UEXiYYU

ANDREEA $\rightarrow$ UEXiYYU.

Decriptare:

$[U, E, X, i, Y, Y, U] \rightarrow [20, 4, 23, 8, 24, 24, 20]$

$\xrightarrow[-20]{-K} [0, -16, 3, -12, 4, 4, 0] \xrightarrow{\% 29}$

$\rightarrow [0, 13, 3, 17, 4, 4, 0] \rightarrow$ ANDREEA

Pe blocuri, fără padding

Mesaj: ANDREEA

Bloc: 4 => ANDR K1: 15

EEA K2: 43

$[A, N, D, R] \to [0, 13, 3, 17] \xrightarrow[+15]{+K1} [15, 28, 18, 32]$

$\xrightarrow{\% 29} [15, 28, 18, 3] \to P?SD$

$[E, E, A] \to [4, 4, 0] \xrightarrow[+43]{+K2} [47, 47, 43] \xrightarrow{\% 29}$

$\to [18, 18, 14] \to SSO$

ANDREEA → P?SDSSO

Pe blocuri, cu padding

Mesaj: ANDREEA

Bloc: 5 => ANDRE K1: 10

EAASD K2 = 13

$[A, N, D, R, E] \to [0, 13, 3, 17, 4] \xrightarrow[+10]{+K1}$

$[10, 23, 13, 27, 14] \to KXN.O$

$[E, A, A, S, D] \rightarrow [4, 0, 0, 18, 3] \xrightarrow[+13]{+K2} [17, 13, 13, 31, 16]$

$\xrightarrow{\% 29} [17, 13, 13, 2, 16] \rightarrow$ RNNCQ

$\underbrace{\text{ANDREEA}}\text{,ASD} \rightarrow \underbrace{\text{KXN.ORNNCQ}}$

Cifrul afin

Ec. de criptare: $C = m \cdot K1 + K2$

Ec. de decriptare: $m = (C - K2) \cdot K1^{-1}$

Ex: Mesaj: LUNI flux

Chei: $K1 = 5$; $K2 = 11$

$[L, U, N, i] \rightarrow [11, 20, 13, 8] \xrightarrow[\cdot 5 + 11]{\cdot K1 + K2}$

$\rightarrow [66, 111, 76, 51] \xrightarrow{\% 29} [8, 24, 18, 22]$

$66 = 58 + 8$

$111 = 116 - 5 = -5 = 24$

$76 = 66 + 10$

iYSW

Decriptare: $m = (c - 11) \cdot 5^{-1}$ în $\mathbb{Z}_{29}$

5^{-1} în $\mathbb{Z}_{29} = 6$

$[i, Y, S, W] \to [8, 24, 18, 22] \xrightarrow{-11 \cdot 6}$

$[-18, 78, 42, 66] \xrightarrow{\% 29} [11, 20, 13, 8]$

LUNi

Hill

Ec. de criptare: $\begin{pmatrix} C \\ O \\ D \end{pmatrix} = MC \cdot \begin{pmatrix} M \\ S \\ J \end{pmatrix}$

Ec. de decriptare: $\begin{pmatrix} M \\ S \\ J \end{pmatrix} = MC^{-1} \cdot \begin{pmatrix} C \\ O \\ D \end{pmatrix}$

Ex:

Mesaj: ALO $\to \begin{pmatrix} A \\ L \\ O \end{pmatrix} = \begin{pmatrix} 0 \\ 11 \\ 14 \end{pmatrix}$

$$MC = \begin{pmatrix} -1 & 2 & 0 \\ 1 & -2 & 1 \\ 0 & 1 & -1 \end{pmatrix}$$

$$\begin{pmatrix} C \\ O \\ D \end{pmatrix} = \begin{pmatrix} -1 & 2 & 0 \\ 1 & -2 & 1 \\ 0 & 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 11 \\ 14 \end{pmatrix} = \begin{pmatrix} 22 \\ -8 \\ -3 \end{pmatrix} \% 29$$

$$= \begin{pmatrix} 22 \\ 21 \\ 26 \end{pmatrix} \begin{matrix} W \\ V \\ \sqcup \end{matrix}$$

<u>Decriptare</u>: $\det MC = \begin{vmatrix} -1 & 2 & 0 \\ 1 & -2 & 1 \\ 0 & 1 & -1 \end{vmatrix} = -2+1+2 = \underline{1}$

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

$$\Rightarrow \begin{pmatrix} M \\ S \\ J \end{pmatrix} = 1^{-1} \cdot \begin{pmatrix} 1 & 2 & 2 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 22 \\ 21 \\ 26 \end{pmatrix} = \begin{pmatrix} 0 \\ 11 \\ 14 \end{pmatrix} \begin{matrix} A \\ L \\ O \end{matrix}$$

<u>Hill afin</u>

Ec. de criptare: $\begin{pmatrix} C \\ O \\ D \end{pmatrix} = MC_1 \cdot \begin{pmatrix} M \\ S \\ J \end{pmatrix} + MC_2$

Ec. de decriptare: $\begin{pmatrix} M \\ S \\ J \end{pmatrix} = MC_1^{-1} \left(\begin{pmatrix} C \\ O \\ D \end{pmatrix} - MC_2 \right)$