1342a - Aritmetică modulară (în Z_n)

$Z_n = \{0, 1, 2, \ldots, n-1\}$

$(Z_n, +, \cdot)$ inel comutativ

$\rightarrow (Z_n, +)$ grup comutativ

$\rightarrow (Z_n, \cdot)$ monoid comutativ

Ex: $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$

$0 = \{0, \pm 7, \pm 14, \pm 21, \pm 28, \ldots\} = \{7k \mid k \in Z\}$

$1 = \{1, 8, 15, 22, 29, \ldots\} = \{7k+1 \mid k \in Z\}$

$-a$ = opusul elementului a

= simetricul față de +

$-3 = x \Leftrightarrow x + 3 = 0 \Rightarrow -3 = 4$

a^{-1} = inversul el. a

= simetricul față de $\cdot$

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

$2^{-1} = 4$; $6^{-1} = 6$

$U(\mathbb{Z}_n) = \{ x \in \mathbb{Z}_n \mid \text{există } x^{-1} \}$

↑ grupul unităților $(U(\mathbb{Z}_n), \cdot)$ grup com.

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

Ex: $U(\mathbb{Z}_7) = \mathbb{Z}_7^* = \mathbb{Z}_7 - \{0\}$

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

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

Ec. de gradul I

$2x + 5 = 1$ în $\mathbb{Z}_7$

$2x = 1 - 5 = -4 \longrightarrow x = -2 = 5$

↓

$2x = 3 \mid \cdot 2^{-1} \Leftrightarrow \underbrace{2^{-1} \cdot 2} \cdot x = 2^{-1} \cdot 3$

$1 \cdot x = x = 4 \cdot 3 = 12 = 5$

$\boxed{2}x + 5 = 1$ în $\mathbb{Z}_6$ nu are soluții.

$U(\mathbb{Z}_6) = \{1, 5\} \not\ni 2$

Ec. de gradul al ii-lea

$3x^2-2x+4=1$ în $\mathbb{Z}_7$

$3x^2-2x+3=0$

$\Delta = 4-4\cdot3\cdot3 = 4-36=-32=-\overset{0}{\overset{\shortparallel}{28}}-4$

$=-4=3$

$\sqrt{a}=b \Rightarrow a=b^2$

$\sqrt{3}=a$ în $\mathbb{Z}_7 \Leftrightarrow a^2=3$ în $\mathbb{Z}_7$

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

$\Rightarrow \sqrt{3}$ nu există în $\mathbb{Z}_7 \Rightarrow$ ec. nu are sol.

$x^2-5x+6=0$ în $\mathbb{Z}_{11}$

$\Delta=25-4\cdot6=1$

$\sqrt{1}\in\{1,10\}=\{1,-1\}$

$x_{1,2}=(5\pm\sqrt{1})\cdot2^{-1}=(5\pm1)\cdot6$

$x_1=6\cdot6=3;\ x_2=4\cdot6=2$

$x\in\{2,3\}$

Logaritmul discret

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

$\log_2 3$ în $\mathbb{Z}_5$ $= x \iff 2^x = 3$ în $\mathbb{Z}_5$

$2^0 = 1;\ 2^1 = 2;\ 2^2 = 4;\ 2^3 = 3 \Rightarrow \log_2 3 = 3$ în $\mathbb{Z}_5$

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

$$\underbrace{2^0 = 1;\ 2^1 = 2;\ 2^2 = 4}\ ;\ \underbrace{2^3 = 1;\ 2^4 = 2;\ 2^5 = 4}$$

Teorema lui Lagrange (pt grupuri)

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

$\forall g \in G,\ g^n = e.$

Obs: $(\mathbb{Z}_p^*, \cdot)$ grup

p nr prim

În part, $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

În $\mathbb{Z}_{11}$, $4^{50} = ?$

$$4^{50} = (4^2)^{25} = 16^{25} = 5^{25} = (5^5)^5 = 1^5 = 1.$$

$$5^5 = 5^2 \cdot 5^2 \cdot 5 = 3 \cdot \underbrace{3 \cdot 5}_{4} = 1$$

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

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

cmmdc$(\det A, t) = 1$.

$\iff \det A \in U(\mathbb{Z}_t)$.

Algoritmi criptografici bazați pe $\mathbb{Z}_n$

1. Flux (stream cipher): o cheie pt tot msj.

2. Pe blocuri (block cipher): o cheie pt 1 bloc

   a) fără padding: ≤1 bloc mai scurt

   b) cu padding: toate blocurile au ac. lungime

$\mathbb{Z}_{29}$

$\mathbb{Z}_{26}$						$\mathbb{Z}_{29}$		
A	B	C	D	...	Z	␣	.	?
0	1	2	3	...	25	26	27	28

Cifrul Caesar

- Ec. de criptare: Cod = Mesaj + Cheie

  $c = m + K$ în $\mathbb{Z}_{29}$

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

Flux: Mesaj: ANDREEA

cheia: 15

$[ANDREEA] \rightarrow [A, N, D, R, E, E, A] \rightarrow$

$\rightarrow [0, 13, 3, 17, 4, 4, 0] \xrightarrow[+15]{+K}$

$\rightarrow [15, 28, 18, \underline{\underline{32}}, 19, 19, 15] \xrightarrow{\%29}$

$[15, 28, 18, 3, 19, 19, 15] \rightarrow \underline{P}?SD\underline{T}\underline{T}\underline{P}$

Decriptare:

$P?SDTTP \rightarrow [15, 28, 18, 3, 19, 19, 15] \xrightarrow[-15]{-K}$

$\rightarrow [0, 13, 3, \underline{-12}, 4, 4, 0] \xrightarrow{\% 29}$

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

Pe blocuri: Mesaj: ANDREEA

fără padding Bloc: $b = 5 \Rightarrow$ ANDRE $K1 = 20$

EA $K2 = 9$

$[A, N, D, R, E] \rightarrow [0, 13, 3, 17, 4] \xrightarrow[+20]{+K1}$

$\rightarrow [20, 33, 23, 37, 24] \xrightarrow{\% 29}$

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

$[E, A] \rightarrow [4, 0] \xrightarrow[+9]{+K2} [13, 9] \rightarrow$ NJ

UEXIY | NJ

Pe blocuri cu padding: Mesaj: ANDREEA

Bloc: $b=5 \Rightarrow$ ANDRE , $K1=20$

$\text{EA}\underbrace{\text{TID}}$, $K2=9$

$$[A,N,D,R,E] \rightarrow [0,13,3,17,4] \xrightarrow[+20]{+K}$$

$$[20,33,23,37,24] \xrightarrow{\%29} [20,4,23,8,24] \rightarrow$$

$\rightarrow$ UEXIY

$$[E,A,T,I,D] \rightarrow [4,0,19,8,3] \xrightarrow[+9]{+K2}$$

$$[13,9,28,17,12] \rightarrow NJ?RM$$

$\text{ANDREEA}\underbrace{\text{TID}} \rightarrow \text{UEXIYNJ}\underbrace{\text{?RM}}$

ANDREEA , $b=5$

$\text{ANDR}\underbrace{\text{X}}$ $\text{EEA}\underbrace{\text{YT}}$

Cifrul afin

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

Ex: Mesaj: AZi   Flux.

$K1 : 5 ; K2 : 12$

$[A, Z, i] \rightarrow [0, 25, 8] \xrightarrow[\cdot 5+12]{\cdot K1+K2} [12, 137, 52]$

$\xrightarrow{\% 29} [12, 21, 23] \longrightarrow MVX.$

$137 = 145 - 8 \ \% \ 29 = -8 = 21$

$52 = 58 - 6 \ \% \ 29 = -6 = 23$

Decriptarea: $c = m \cdot 5 + 12 \Rightarrow m = (c-12) \cdot 5^{-1}$

5^{-1} în $\mathbb{Z}_{29} = 6$ $m = (c-12) \cdot 6$

$[M, V, X] \rightarrow [12, 21, 23] \xrightarrow{-12 \cdot 6} [0, 54, 66]$

$\xrightarrow{\% 29} [0, 25, 8] \rightarrow AZi$

Hill:

Ec. de criptare: $\begin{pmatrix} c \\ o \\ \Delta \end{pmatrix} = MC \cdot \begin{pmatrix} M \\ s \\ j \end{pmatrix}$

Ec. de decriptare: $\begin{pmatrix} M \\ s \\ j \end{pmatrix} = MC^{-1} \cdot \begin{pmatrix} c \\ o \\ \Delta \end{pmatrix}$

Ex: Mesaj: Joi $\rightarrow \begin{pmatrix} J \\ o \\ i \end{pmatrix} = \begin{pmatrix} 9 \\ 14 \\ 8 \end{pmatrix}$

$$MC = \begin{pmatrix} -2 & 0 & 1 \\ 1 & -1 & 1 \\ 0 & 2 & -3 \end{pmatrix}$$

$$\begin{pmatrix} c \\ o \\ D \end{pmatrix} = \begin{pmatrix} -2 & 0 & 1 \\ 1 & -1 & 1 \\ 0 & 2 & -3 \end{pmatrix} \cdot \begin{pmatrix} 9 \\ 14 \\ 8 \end{pmatrix} = \begin{pmatrix} -10 \\ 3 \\ 4 \end{pmatrix} \% 29$$

$$\begin{pmatrix} 19 \\ 3 \\ 4 \end{pmatrix} = \begin{pmatrix} T \\ D \\ E \end{pmatrix}$$

Decriptare: $\det MC = -6 + 2 + 4 = 0$

$\Rightarrow$ MC nu este inversabilă!

$\Rightarrow$ Mesajul nu se poate decripta

Mesaj: AZi $\rightarrow \begin{pmatrix} 0 \\ 25 \\ 8 \end{pmatrix}$

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

$$= -5 = 24$$

Criptarea: $\begin{pmatrix} C \\ o \\ D \end{pmatrix} = \begin{pmatrix} 0 & 1 & -1 \\ 2 & 0 & 1 \\ -1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 25 \\ 8 \end{pmatrix}$

$$= \begin{pmatrix} 17 \\ 8 \\ 33 \end{pmatrix} \% 29 = \begin{pmatrix} 17 \\ 8 \\ 4 \end{pmatrix} = \begin{pmatrix} R \\ i \\ E \end{pmatrix}$$

<u>Decriptarea</u> : $MC^{-1} = 24^{-1} \cdot MC^{*}$

$$24^{-1} \text{ în } \mathbb{Z}_{29} = x \Leftrightarrow \underline{24x = 1 \text{ în } \mathbb{Z}_{29}}$$

$$1 \text{ în } \mathbb{Z}_{29} = \{1, 30, 59, 88, 117, 146, 175, 204, 233, 262, 291, 320, 349, 378, 407, 436, 465, 494, 523, \underset{24\cdot 23}{\underset{\parallel}{552}}$$

$$\Rightarrow \underline{x = 23}$$

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

$$\Rightarrow MC^{-1} = 23 \cdot \begin{pmatrix} -1 & -2 & 1 \\ -3 & -1 & -2 \\ 2 & -1 & -2 \end{pmatrix}$$

$$\begin{pmatrix} M \\ S \\ J \end{pmatrix} = 23 \cdot \begin{pmatrix} -1 & -2 & 1 \\ -3 & -1 & -2 \\ 2 & -1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 17 \\ 8 \\ 4 \end{pmatrix}$$

$$= \begin{pmatrix} 0 \\ 25 \\ 8 \end{pmatrix} = \begin{pmatrix} A \\ Z \\ i \end{pmatrix}$$

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

Testi de primalitate

1) Sigure (deterministe) = cu certitudine, ineficient

2) Probabiliste = probabil da/sigur nu, eficiente

Algoritmi:

INPUT: $n \in \mathbb{N}$

OUTPUT: A dacă n este prim

F dacă n este compus, eventual afișez un <u>martor</u>

(= „motiv" pt care n este compus)

---

1. <u>Verificarea directă:</u>

- Pentru $d \in \{2, \dots, n-1\}$, verific dacă $d | n$.

↑ Verificarea sigură (deterministă)

- Verificarea probabilistă: Aleg t mostre $d \in \{2, \ldots, n-1\}$ și verific doar pe acelea.

Răspunsul are prob $= \frac{t}{n-2}$

Ex: $n = 17$

- Sigur: iau $d \in \{2, \ldots, 16\}$
- Prob: $t = 5$ și $d \in \{7, 13, 11, 10, 2\}$

$\Rightarrow n = 17$ prim cu prob. $\frac{5}{15} = \frac{1}{3}$.

---

2. Ciurul (Sita) lui Eratostene

Ex: $n = 25$

$\boxed{2}$ $\boxed{3}$ $\cancel{4}$ $\boxed{5}$ $\cancel{6}$ $\boxed{7}$ $\cancel{8}$ $\cancel{9}$

$\cancel{10}$ $\boxed{11}$ $\cancel{12}$ $\boxed{13}$ $\cancel{14}$ $\cancel{15}$ $\cancel{16}$ $\boxed{17}$

$\cancel{18}$ $\boxed{19}$ $\cancel{20}$ $\cancel{21}$ $\cancel{22}$ $\boxed{23}$ $\cancel{24}$ $\cancel{25}$

3. Testul Fermat

Teoremă: n prim $\Rightarrow a^{n-1} = 1$ în $\mathbb{Z}_p^*$,

$\forall a \in \mathbb{Z}_p^*$.

Ex: Var. deterministă:

$n = 7 \Rightarrow \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

$\forall a \in \{1, 2, 3, 4, 5, 6\}$, $a^6 = 1$ în $\mathbb{Z}_7^*$?

$1^6 = 1$; $2^6 = 64 = 1$; $3^6 = (3^2)^3 = 2^3 = 1$;

$4^6 = (2^2)^6 = 2^{12} = (2^3)^4 = 1$;

$5^6 = (-2)^6 = 2^6 = 1$; $6^6 = 2^6 \cdot 3^6 = 1$

$\Rightarrow n = 7$ prim (sigur)

Ex: $n = 9 \Rightarrow \mathbb{Z}_9^* = \{1, 2, 3, 4, 5, 6, 7, 8\}$

$1^8 = 1$; $2^8 = (2^3)^2 \cdot 2^2 = (-1)^2 \cdot 2^2 = 4 \neq 1$

$\Rightarrow n = 9$ compus, $a = 2$ martor

Var. probabilistă: Aleg t elem. din $\mathbb{Z}_n^*$.

Ex: $n = 27409$, $t = 20$ mostre aleatorii

$a = 9731 \Rightarrow$ $9731^{27408} = 1$ în $\mathbb{Z}_{27409}^*$

$9731^{27408} = ?$ în $\mathbb{Z}_{27409}^*$

$a = 9731 \to a^2 = 9731^2 \% 27409$

$= 21675 \in \mathbb{Z}_{27409}^*$

$a^3 = a^2 \cdot a = 21675 \cdot 9731 \% 27409$

$= 7170$

$a^4 = a^3 \cdot a = 7170 \cdot 9731 \% 27409$

etc.

4. Simbolul Jacobi

$n, b \in \mathbb{N}$, n impar

$$\left(\frac{b}{n}\right) = \begin{cases} 0 & \text{dacă } n \mid b \\ 1 & \text{dacă } b \text{ este pătrat în } \mathbb{Z}_n^* \\ -1 & \text{altfel} \end{cases}$$

Ex: $\left(\frac{5}{7}\right) = ?$

$7 \nmid 5$; 5 este pătrat în $\mathbb{Z}_7^*$?

Pătratele din $\mathbb{Z}_7^* = P(\mathbb{Z}_7^*) = \{1, 4, 2\} \not\ni 5$

$\Rightarrow \left(\frac{5}{7}\right) = -1$

Ex : $\left(\frac{13}{5}\right) = ?$ $\quad 5 \nmid 13$

$P(\mathbb{Z}_5^*) = \{1, 4\}$

$\left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = -1$

Teoremă : n prim $\Rightarrow$ $b^{\frac{n-1}{2}} = \left(\frac{b}{n}\right)$ în $\mathbb{Z}_n$, $\forall b \in \mathbb{Z}_n^*$.

Ex : $n = 7 \Rightarrow \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

$\forall b \in \mathbb{Z}_7^*$, $b^{\frac{7-1}{2}} = \left(\frac{b}{7}\right)$ în $\mathbb{Z}_7$?

$b=1 \Rightarrow 1^3 = 1 ; \left(\frac{1}{7}\right) = 1$ OK

$P(\mathbb{Z}_7^*) = \{1,2,4\}$

$b=2 \Rightarrow 2^3 = 1 ; \left(\frac{2}{7}\right) = 1$ pt că $2 \in P(\mathbb{Z}_7^*)$ OK

$b=3 \Rightarrow 3^3 = 3^2 \cdot 3 = 6 = -1$ OK

$\left(\frac{3}{7}\right) = -1$

$b=4 \Rightarrow 4^3 = 2^6 = (2^3)^2 = 1 ; \left(\frac{4}{7}\right) = 1$ OK

$b=5 \Rightarrow 5^3 = (-2)^3 = -8 = -1 = 6 ; \left(\frac{5}{7}\right) = -1$ OK

$b=6 \Rightarrow 6^3 = 2^3 \cdot 3^3 = 1 \cdot 6 = 6 = -1 ; \left(\frac{6}{7}\right) = -1$ OK

$\Rightarrow n = 7$ prim.

↑ Var. deterministă (sigură)

Var. probabilistă: Aleg t martori pt. $b \in \mathbb{Z}_n^*$