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

pt orice $x \in \mathbb{Z}_n$, not $-x$ „simetricul" 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 pt orice $x \in \mathbb{Z}_n - \{0\}$ există un „simetric"

Dacă există, not. x^{-1} și s.n. inversul lui x.

$x \cdot (x^{-1}) = 1$.

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

Teoremă $x \in \mathbb{Z}_n$ unitate $\Leftrightarrow$ 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

$2 + 3 = 5$

$2 \cdot 3 = 6$

$5 \cdot 6 = 30 = \overset{0}{28} + 2 = 2$

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

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

[illegible] $\Leftrightarrow$ $12 \cdot 34 = 2 \cdot 3$ în $\mathbb{Z}$[illegible]

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

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

$-5 = 2$ pt că $-5 = 0-5 = 7-5 = 2$

$3^{-1} = y \Leftrightarrow y\cdot 3 = 1$ în $\mathbb{Z}_7 \Rightarrow y = 5$ pt că $3\cdot 5 = 15 = \underset{0}{14}+1 = 1$

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

$4^{-1} = 2$ pt că $4\cdot 2 = 8 = \underset{0}{7}+1 = 1$

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

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

Ecuații de gradul I

Ex: $2x+5=1$ în $\mathbb{Z}_7$

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

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

$1x = 12 = 5 \Rightarrow \underline{x=5}$

Verificare:

$2\cdot 5 + 5 = 15 = 1$ în $\mathbb{Z}_7$ ✓

Ex: $5x+3=7$ în $\mathbb{Z}_{11}$

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

$\underbrace{9\cdot 5}_{1}\cdot x = 9\cdot 4$

$x = 36 = 3 \Rightarrow \underline{x=3}$

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

$6x = 1 \quad |\cdot 6^{-1}$ NU EXISTĂ!!

Rezolv prin încercări:

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

Ec. nu are sol.

Ec. nu are sol.

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

Ec. de gradul II

Ex: $2x^2+5x-1=0$ în $\mathbb{Z}_9$

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

$\sqrt{\Delta}=\sqrt{6}=y \Leftrightarrow y^2=6$ există?

y	0	1	2	3	4	5	6	7	8
y^2	0	1	4	0	7	7	0	4	1

$\not\ni 6 \Rightarrow \sqrt{6}$ nu există în $\mathbb{Z}_9$!

$\Rightarrow$ Ec. nu are soluții.

Ex: $x^2-5x+6=0$ în $\mathbb{Z}_7$

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

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

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

Obs:

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

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

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

$x_2=(5-6)\cdot 2^{-1}=6\cdot 4=3$

Sisteme liniare (2x2)

Ex: $\begin{cases} 2x-y=3 \\ 5x+2y=1 \end{cases}$ în $\mathbb{Z}_{11}$

det matricei sist $=0$ sau element neinversabil.

Obs Verific dacă det matricei este $=0$ sau element neinversabil.
Dacă da, rezolv prin încercări.

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

Substituție: $y=2x-3$

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

Inverse matriceale

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

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

$$\det A = 2-15=-13=\underset{\overset{\parallel}{0}}{-11}-2=-2=9\in U(\mathbb{Z}_{11})$$

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

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

$-22-3=-3=8$

$-11-4=-4=7$

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

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

Coduri elementare

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 indescifrabile.

$\Rightarrow$ 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, $K = 18$

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

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

$\rightarrow$ SHISO␣

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

<u>Decriptare</u> $[S, H, I, S, O, ␣] \rightarrow [18, 7, 8, 18, 14, 26]$

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

$\rightarrow$ ASTAZI

2) Varianta pe blocuri
a) fără padding
b) cu padding (random)

} Împart mesajul în blocuri de lungime dată și folosesc câte o cheie pt fiecare bloc.

<u>Ex</u>: $m = \text{ASTAZI}$ blocuri de lungime 3

b_1: AST $K_1 = 15$

b_2: AZI $K_2 = 20$

$[A, S, T] \rightarrow [0, 18, 19] \xrightarrow[+15]{+K1} [15, 33, 34] \xrightarrow[\text{mod } 29]{} [15, 4, 5] \rightarrow \text{PEF}$

$[A, Z, I] \rightarrow [0, 25, 8] \xrightarrow[+20]{+K2} [20, 45, 28] \xrightarrow[\text{mod } 29]{} [20, 16, 28]$

$\rightarrow$ UQ?

ASTAZI $\rightarrow$ PEFUQ? (Caesar pe blocuri fără padding)

<u>Obs</u>: Caractere identice în blocuri diferite vor fi criptate diferit $\Rightarrow$ securitate ++.

Ex: m = ASTAZI   blocuri de lungime 4 cu padding random

b_1 : ASTA $K1 = 15$

b_2 : ZIX. $K2 = 20$

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

$\xrightarrow[\text{mod } 29]{} [15, 4, 5, 15] \to$ PEFP

$[Z, I, X, .] \to [25, 8, 23, 27] \xrightarrow[+20]{+K2} [45, 28, 43, 47]$

$\xrightarrow[\text{mod } 29]{} [16, 28, 14, 18] \to$ Q?OS

ASTAZIX. $\to$ PEFPQ?OS

dec.

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

---

Cifrul afin

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

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

Varianta flux: aceleași 2 chei pt tot mesajul

Ex: m = TRUMP , $K1 = 6$, $K2 = 12$ $(K1^{-1} = 6^{-1} = 5)$

$[T, R, U, M, P] \to [19, 17, 20, 12, 15] \xrightarrow[\cdot 6, +12]{\cdot K1 + K2} [126, 114, 132, 84, 102]$

$\xrightarrow[\text{mod } 29]{} [10, 27, 16, 26, 15] \to$ K.Q␣P

$\xrightarrow[\text{mod } 29]{} [10, 27, 16, 26, 15] \to K \cdot Q \sqcup P$

decriptarea: $[K, \cdot, Q, \sqcup, P] \to [10, 27, 16, 26, 15]$

$\xrightarrow[-12 \cdot 5]{-K2 \cdot K1^{-1}} [-10, 75, 20, 70, 15] \xrightarrow[\text{mod } 29]{} [19, 17, 20, 12, 15]$

$\to$ TRUMP

Varianta pe blocuri: câte 2 chei pt fiecare bloc

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

b_1: HARRI, $K1 = 10$, $K2 = 13$ | $K1^{-1} = 10^{-1} = 3$

b_2: S, $K3 = 15$, $K4 = 20$ | $K3^{-1} = 15^{-1} = 2$

$[H, A, R, R, I] \to [7, 0, 17, 17, 8] \xrightarrow[\cdot 10 + 13]{\cdot K1 + K2}$

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

$\to$ ZNJJG

$S \to 18 \xrightarrow[\cdot 15 + 20]{\cdot K3 + K4} 290 \xrightarrow[\text{mod } 29]{} 0 \to A$

HARRIS $\to$ ZNJJGA

Cifrul Hill

Ec. de criptare: $K \cdot m = c$

vectori

matrice de criptare

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

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

Ex: m: ION $\longrightarrow \begin{pmatrix} I \\ O \\ N \end{pmatrix}$

$K: \begin{pmatrix} 1 & -1 & 0 \\ 2 & 0 & 1 \\ -1 & -1 & 1 \end{pmatrix} \in \mathcal{M}_3(\mathbb{Z}_{29})$ $\quad \det K = 1 + 1 + 2 = 4$

$\begin{pmatrix} I \\ O \\ N \end{pmatrix} = \begin{pmatrix} 8 \\ 14 \\ 13 \end{pmatrix}$; $\begin{pmatrix} 1 & -1 & 0 \\ 2 & 0 & 1 \\ -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} 8 \\ 14 \\ 13 \end{pmatrix} = \begin{pmatrix} -6 \\ 29 \\ -9 \end{pmatrix} \bmod 29$

$= \begin{pmatrix} 23 \\ 0 \\ 20 \end{pmatrix}$ $\begin{matrix} X \\ A \\ U \end{matrix}$

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

$4 \cdot y = 1 \bmod 29 = \{30, 59, 88, \ldots\}$

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

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

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

Decriptarea: $22 \cdot \begin{pmatrix} 1 & 1 & -1 \\ -3 & 1 & -1 \\ -2 & 2 & 2 \end{pmatrix} \cdot \begin{pmatrix} 23 \\ 0 \\ 20 \end{pmatrix} = \begin{pmatrix} 8 \\ 14 \\ 13 \end{pmatrix} \pmod{29}$

Teste de primalitate

1) Ciurul (sita) lui Eratostene (Grecia antică)

Ex: $n = 27$

$\boxed{2}$ $\boxed{3}$ $\cancel{4}$ $\boxed{5}$ $\cancel{6}$ $\boxed{7}$ $\cancel{8}$ $\cancel{9}$ $\cancel{10}$ $\boxed{11}$ $\cancel{12}$ $\boxed{13}$ $\cancel{14}$

$\cancel{15}$ $\cancel{16}$ $\boxed{17}$ $\cancel{18}$ $\boxed{19}$ $\cancel{20}$ $\cancel{21}$ $\cancel{22}$ $\boxed{23}$ $\cancel{24}$ $\cancel{25}$ $\cancel{26}$ $\cancel{27}$

$n = 27$ compus

$\Rightarrow \{2, 3, 5, 7, 11, 13, 17, 19, 23\}$ nr prime ≤ 27

2) Testul Fermat (sec. XVII)

Teoremă (Mica Teoremă a lui Fermat)

Dacă n nr. prim $\Rightarrow \forall a \in \{1, 2, \dots, n-1\}$, $a^{n-1} = 1 \bmod n$.

Echivalent: $\forall a \in \mathbb{Z}_n^*$, $a^{n-1} = 1$.

Ex: $n = 11 \overset{?}{\Rightarrow} \forall a \in \mathbb{Z}_{11}^*$, $a^{10} = 1$ în $\mathbb{Z}_{11}^*$.

$a = 1 \Rightarrow 1^{10} = 1$ ok

$a = 2 \Rightarrow 2^{10} = (2^3)^3 \cdot 2 = (-3)^3 \cdot 2 = -27 \cdot 2 = -5 \cdot 2 = -10 = 1$ ok

$a = 3 \Rightarrow 3^{10} = (3^2)^5 = (-2)^5 = (-2)^3 \cdot 2^2 = -8 \cdot 4 = 3 \cdot 4 = 12 = 1$ ok

$a = 4 \Rightarrow 4^{10} = (2^2)^{10} = (2^{10})^2 = 1^2 = 1$ ok

$a = 5 \Rightarrow 5^{10} = (5^2)^5 = 3^5 = (3^2)^2 \cdot 3 = (-2)^2 \cdot 3 = 4 \cdot 3 = 12 = 1$ ok

$a = 6 \Rightarrow 6^{10} = 2^{10} \cdot 3^{10} = 1 \cdot 1 = 1$ ok

$a = 7 \Rightarrow 7^{10} = (-4)^{10} = 4^{10} = 1$ ok

$a=7 \Rightarrow 7^{10} = (-4)^{10} = 4^{10} = 1$ ok

$a=8 \Rightarrow 8^{10} = 2^{10}\cdot 4^{10} = 1\cdot 1 = 1$ ok

$a=9 \Rightarrow 9^{10} = (3^2)^{10} = (3^{10})^2 = 1$ ok

$a=10 \Rightarrow 10^{10} = 2^{10}\cdot 5^{10} = 1\cdot 1 = 1$ ok

$\Rightarrow n = 11$ prim (Fermat).

Ex: $n=15 \overset{?}{\Rightarrow} \forall a \in \mathbb{Z}_{15}^*,\ a^{14} = 1$ în $\mathbb{Z}_{15}^*$.

$a=1 \Rightarrow 1^{14} = 1$ ok

$a=2 \Rightarrow 2^{14} = (2^4)^3 \cdot 2^2 = 4 \neq 1$

$\Rightarrow n=15$ compus cf. Fermat ($a=2$ s.n. martor (witness))

Testul Solovay-Strassen (~ sec XIX)

Simbolul Jacobi

Def: $b, n \in \mathbb{N}^*$, n impar

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

$\Updownarrow$ $\exists \sqrt{b \bmod n}$ în $\mathbb{Z}_n^*$

Ex: $\left(\frac{15}{3}\right) = 0$ pt că $3 \mid 15$

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

				(-3)	(-2)	(-1)
x	1	2	3	4	5	6
x^2	1	4	2	2	4	1

1

$$\left(\frac{4}{19}\right) = 1 \quad \text{pt că} \quad 4 = 2^2 \text{ în } \mathbb{Z}_{19}^*$$

Teoremă (Solovay-Strassen)

n prim $\Rightarrow \forall a \in \{1, \dots, n-1\}$, $a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right) \bmod n$.

Echivalent, $\forall a \in \mathbb{Z}_n^*$, $a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right)$ în $\mathbb{Z}_n^*$.

Ex: $n = 9 \overset{?}{\Rightarrow} \forall a \in \mathbb{Z}_9^*$, $a^4 = \left(\frac{a}{9}\right)$ în $\mathbb{Z}_9^*$.

$a = 1 \Rightarrow 1^4 = 1$; $\left(\frac{1}{9}\right) = 1$ pt că $1 = 1^2$ ✓

$a = 2 \Rightarrow 2^4 = 2^3 \cdot 2 = (-1) \cdot 2 = -2 = 7 \neq \left(\frac{2}{9}\right) \Rightarrow$

$\Rightarrow n = 9$ compus ($a = 2$ martor)

Ex: $n = 11 \overset{?}{\Rightarrow} \forall a \in \mathbb{Z}_{11}^*$, $a^5 = \left(\frac{a}{11}\right)$ în $\mathbb{Z}_{11}^*$.

$a = 1$ ✓

$a = 2 \Rightarrow 2^5 = 32 = -1$; $\left(\frac{2}{11}\right) = -1$ ✓

x	1	2	3	4	5
x^2	1	4	9	5	3

$a = 3 \Rightarrow 3^5 = (3^2)^2 \cdot 3 = (-2)^2 \cdot 3 = 4 \cdot 3 = 12 = 1$

$\left(\frac{3}{11}\right) = 1$ pt că $3 = 5^2$ ✓

$a = 4 \Rightarrow 4^5 = (2^2)^5 = (2^5)^2 = (-1)^2 = 1$; $\left(\frac{4}{11}\right) = 1$ pt că $4 = 2^2$ ✓

$a = 5 \Rightarrow 5^5 = (5^2)^2 \cdot 5 = 3^2 \cdot 5 = (-2) \cdot 5 = -10 = 1$

$a=4 \Rightarrow 4 = ($

$a=5 \Rightarrow 5^5 = (5^2)^2 \cdot 5 = 3^2 \cdot 5 = (-2)\cdot 5 = -10 = 1$

$\left(\frac{5}{11}\right) = 1$ pt că $5 = 4^2$ ✓

$a=6 \Rightarrow 6^5 = 2^5 \cdot 3^5 = (-1)\cdot 1 = -1$; $\left(\frac{6}{11}\right) = -1$ ✓

$a=7 \Rightarrow 7^5 = (-4)^5 = -4^5 = -1$; $\left(\frac{7}{11}\right) = -1$ ✓

$a=8 \Rightarrow 8^5 = 2^5 \cdot 4^5 = (-1)\cdot 1 = -1$; $\left(\frac{8}{11}\right) = -1$ ✓

$a=9 \Rightarrow 9^5 = (3^2)^5 = (3^5)^2 = 1$; $\left(\frac{9}{11}\right) = 1$ pt că $9 = 3^2$ ✓

$a=10 \Rightarrow 10^5 = 2^5 \cdot 5^5 = (-1)\cdot 1 = -1$; $\left(\frac{10}{11}\right) = -1$ ✓

$\Rightarrow n = 11$ prim (Solovay-Strassen).

Variantele probabiliste

Fermat
Solovay-Strassen } Aleg t mostre (nr. din $\mathbb{Z}_n^*$) și testez teoremele doar cu ele.
Rezultatul va avea prob $= \frac{t}{n-1}$.

Ex: Fermat probabilist, $t=3$, $n=41$

Mostre: $a \in \{23, 36, 40\} \overset{?}{\Rightarrow} a^{40} = 1$ în $\mathbb{Z}_{41}^*$

$23^{40} = (-18)^{40} = 18^{40} = 2^{40} \cdot 3^{80} = 1 \cdot 1 = 1$ ✓

$3^{80} = (3^4)^{20} = 81^{20} = (-1)^{20} = 1$

$2^{40} = (2^5)^8 = 32^8 = (-9)^8 = 9^8 = (9^2)^4 = (-1)^4 = 1$

$2^{40} = (2^5)^8 = 32^8 = (-9)^8 = 9^8 = (9^2)^4 = (-1)^4 = 1$

$36^{40} = (-5)^{40} = 5^{40} = (5^2)^{20} = (-16)^{20} = 2^{80} = (2^{40})^2 = 1.$

$40^{40} = (-1)^{40} = 1.$

$\Rightarrow n = 41$ probabil prim, prob $= \frac{3}{40}$.

Logaritmul discret (în $\mathbb{Z}_n$)

Def: $\log_a b = c \Leftrightarrow a^c = b$ (în $\mathbb{R}_+$, în $\mathbb{Z}_n$)

Obs: Există valori pt a, b a.î. $\log_a b$ nu există în $\mathbb{Z}_n$.

Ex: $\log_2 3$ în $\mathbb{Z}_{11}$ $\qquad \log_2 3 = x \Leftrightarrow 2^x = 3$ în $\mathbb{Z}_{11}$

x	1	2	3	4	5	6	7	$\boxed{8}$	9	$\boxed{10}$
2^x	2	4	8	5	10	9	7	$\boxed{3}$	6	$\boxed{1}$

$\Rightarrow \text{ord}\, 2 = 10$ în $\mathbb{Z}_{11}$

$2^6 = 2^5 \cdot 2 = 10 \cdot 2 = 20 = 9$; $\quad 2^7 = 2^6 \cdot 2 = 9 \cdot 2 = 18 = 7$

$2^8 = 2^7 \cdot 2 = 7 \cdot 2 = 14 = 3$

$\Rightarrow \log_2 3 = 8$ în $\mathbb{Z}_{11}$. (pt că $2^8 = 3$ în $\mathbb{Z}_{11}$).

Ex: $\log_3 5$ în $\mathbb{Z}_{13}$ dacă există

$\log_3 5 = x \Leftrightarrow 3^x = 5$ în $\mathbb{Z}_{13}$

x | 1 2 3 4 5 $\cancel{6}$ 7 8 $\cancel{9}$ 10 $\cancel{11}$ 12

x	1	2	3	4	5	6	7	8	9	10	11	12
3^x	3	9	1	3	9	1	3	9	1	3	9	1

$\Rightarrow \log_3 5$ nu există în $\mathbb{Z}_{13}$.

Obs: Cf. Fermat, dacă n nr prim $\Rightarrow a^{n-1} = 1$ în $\mathbb{Z}_n^*$, $\forall a \in \mathbb{Z}_n^*$.

Ex: $\log_3 4$ în $\mathbb{Z}_{17} = x \Leftrightarrow 3^x = 4$ în $\mathbb{Z}_{17}$

x	1	2	3	4	5	6	7	8	9 (-8)	10 (-7)	11 (-6)	12 (-5)
3^x	3	9	10	13	5	15	11	16	14	8	7	4

$3^4 = 3^3 \cdot 3 = 10 \cdot 3 = 30 = 13$; $3^5 = 3^4 \cdot 3 = 3 \cdot 13 = 39 = 5$

$3^6 = 3^5 \cdot 3 = 5 \cdot 3 = 15$; $3^7 = 3^6 \cdot 3 = 15 \cdot 3 = (-2) \cdot 3 = -6 = 11$

$3^8 = 3^7 \cdot 3 = 11 \cdot 3 = (-6) \cdot 3 = -18 = -1 = 16$

$3^9 = 3^8 \cdot 3 = 16 \cdot 3 = (-1) \cdot 3 = -3 = 14$

3^{-8} în $\mathbb{Z}_{17} = ?$ $\quad 3^{-8} = (3^8)^{-1} =$ inversul lui $3^8 = 16 = (-1)$

$(-1)^{-1} = -1$ pt că $(-1) \cdot (-1) = 1$

$3^{10} = 3^9 \cdot 3 = 14 \cdot 3 = (-3) \cdot 3 = -9 = 8$

$3^{10} = 3^{-7} = (3^7)^{-1} = 11^{-1}$

$3^{11} = 3^{10} \cdot 3 = 8 \cdot 3 = 7$

$3^{12} = 3^{11} \cdot 3 = 7 \cdot 3 = 21 = 4$

$\Rightarrow 3^{12} = 4 \Rightarrow \log_3 4 = 12$ în $\mathbb{Z}_{17}$.

Ordinul unui element în $\mathbb{Z}_n$

Def: $ord(x \in \mathbb{Z}_n) = t \Leftrightarrow x^t = 1$ și t este cea mai mică putere

Dacă nu există ($x^t \neq 1, \forall t$), punem $ord(x) = \infty$.

Ex: $3^3 = 1$ în $\mathbb{Z}_{13} \Rightarrow ord(3) = 3$ în $\mathbb{Z}_{13}$.

Obs: Dacă n este prim și folosim Fermat $\Rightarrow x^{n-1} = 1$, dar asta nu înseamnă mereu că $ord(x) = n-1$.

Teoremă (Lagrange)

Ordinul oricărui element din $\mathbb{Z}_n$ este divizor al lui $n-1$.

Ex: $ord\, 3 = 3$ în $\mathbb{Z}_{13}$ (OK)

Ex: $\mathbb{Z}_7$:

x	1	2	3	4	5	6	
2^x	2	4	$\boxed{1}$	2	4	1	$\Rightarrow ord\, 2 = 3$
3^x	3	2	6	4	5	1	$\Rightarrow ord\, 3 = 6$
4^x	4	2	1				$\Rightarrow ord\, 4 = 3$
5^x	5	4	6	2	3	1	$\Rightarrow ord\, 5 = 6$
6^x	6	1					$\Rightarrow ord\, 6 = 2$

Def: Dacă $ord(x) = n-1$ în $\mathbb{Z}_n$, spunem că x este **generator** pt $\mathbb{Z}_n$, iar $\mathbb{Z}_n$ s.n. **ciclic**.

Ex: $\mathbb{Z}_7$ este ciclic, generat de 3 sau 5

$$\mathbb{Z}_7 = \langle 3 \rangle = \langle 5 \rangle$$

Indicatorul lui Euler (TOTIENT function)

Def: $n \in \mathbb{N}$, $\varphi(n) = \# \{ 1 \le x \le n \mid cmmdc(x,n) = 1 \}$

Obs: $\varphi(n) = \# U(\mathbb{Z}_n)$

Ex: $n = 10$, $\{ 1 \le x \le 10 \mid cmmdc(x,10) = 1 \} = \{1, 3, 7, 9\}$

$\Rightarrow \varphi(10) = 4$. ($\# U(\mathbb{Z}_{10}) = 4$, adică $1, 3, 7, 9$ inversabile în $\mathbb{Z}_{10}$)

Proprietăți: 1) Dacă p prim $\Rightarrow \varphi(p) = p - 1$

2) $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$

3) $\varphi(n) = n \cdot \prod_{\substack{p \mid n \\ p \text{ prim}}} \left(1 - \frac{1}{p}\right), \forall n.$

Formulă generală

Ex: $n = 97 \Rightarrow \varphi(97) = 96$.

$n = 582 = 2 \cdot 3 \cdot 97$

582	2
291	3
97	97

$n = 582 = 2\cdot 3\cdot 97$

$97 \mid 97$

$\varphi(582) = \varphi(2)\cdot\varphi(3)\cdot\varphi(97)$

$= 1\cdot 2\cdot 96 = 192$ (propr 1&2)

$\varphi(582) = 582\cdot\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{3}\right)\cdot\left(1-\frac{1}{97}\right)$

$= \cancel{582}\cdot\frac{1}{\cancel{2}}\cdot\frac{2}{\cancel{3}}\cdot\frac{96}{\cancel{97}} = 192$

$\varphi(1000) = 1000\cdot\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{5}\right) = 100\cancel{0}\cdot\frac{1}{\cancel{2}}\cdot\frac{4}{\cancel{5}} = 400.$

$1000 = 10^3 = 2^3\cdot 5^3$

$\varphi(2^3) = 2^3\cdot\left(1-\frac{1}{2}\right)$; $\varphi(5^3) = 5^3\cdot\left(1-\frac{1}{5}\right)$