

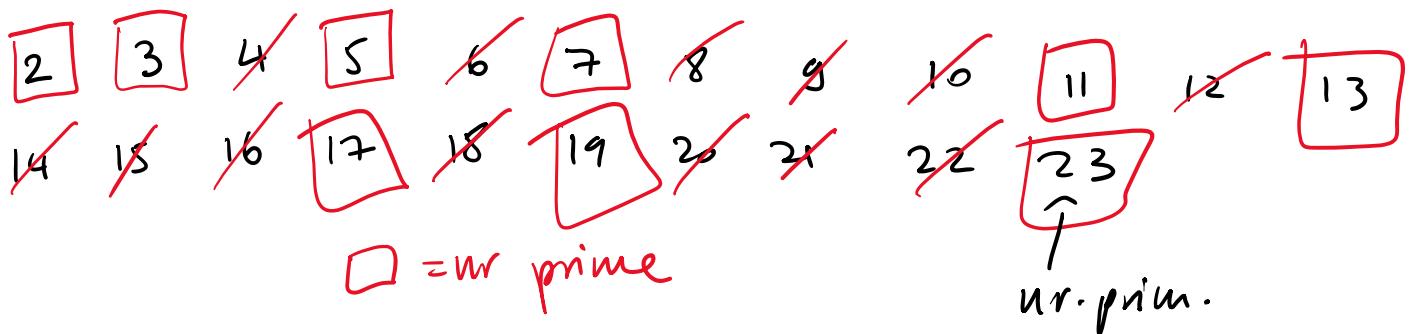
Teste de primalitate

Cișnul (sita) lui Eratostene

Primeste $n \in \mathbb{N}$

Răspunde cu toate nr prime $\leq n$

Ex: $n = 23$



Testul Fermat

Mica Teorema a lui Fermat

Dacă n este nr prim $\Rightarrow a^{n-1} = 1$ în \mathbb{Z}_n^* , $\forall a \in \mathbb{Z}_n^*$.

Negatia: Dacă $\exists a \in \mathbb{Z}_n^*$ a.i. $a^{n-1} \neq 1$ în \mathbb{Z}_n^* $\Rightarrow n$ nu este prim.
 ↑
 a s.n. mărtor (witness)

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

$$1^{10} = 1 \quad \checkmark$$

$$(-1)^{10} = 1$$

$$3^3 = 27$$

$$27 - 1 = 26$$

$$26 - 11 = 15$$

$$15 - 11 = 4$$

$$4 - 1 = 3$$

$$3 - 1 = 2$$

$$2 - 1 = 1$$

$$1^{10} = \left(2^3\right)^3 \cdot 2 = (-3)^3 \cdot 2 = -27 \cdot 2 = (-22-5) \cdot 2 = (-5) \cdot 2 = -10 = 1 \checkmark$$

$$3^{10} = \left(3^2\right)^5 = 9^5 = (-2)^5 = (-2)^3 \cdot (-2)^2 = -8 \cdot 4 = 3 \cdot 4 = 12 = 1 \checkmark$$

$$4^{10} = (2^2)^{10} = (2^1)^2 = 1 \checkmark$$

$$5^{10} = (5^2)^5 = 25^5 = 3^5 = 3^2 \cdot 3^3 = (-2) \cdot 5 = -10 = 1 \checkmark$$

$$6^{10} = 2^{10} \cdot 3^{10} = 1 \checkmark$$

$$7^{10} = (7^2)^5 = 5^5 = (5^2)^2 \cdot 5 = 3^2 \cdot 5 = (-2) \cdot 5 = -10 = 1 \checkmark$$

$$8^{10} = 2^{10} \cdot 4^{10} = 1 \checkmark$$

$$9^{10} = (3^2)^{10} = (3^{10})^2 = 1 \checkmark$$

$$10^{10} = 2^{10} \cdot 5^{10} = 1 \checkmark$$

$\Rightarrow \underline{n=11 \text{ prim (Fermat)}}$

Ex.: $n=21 \Rightarrow \forall a \in \mathbb{Z}_{21}^*, a^{20}=1 \in \mathbb{Z}_{21}^*$?

$$1^{20} = 1 \checkmark$$

$$2^{20} = (2^4)^5 = (-5)^5 = ((-5)^2)^2 \cdot (-5) = 4^2 \cdot (-5) = (-5) \cdot (-5) = 25 = 4$$

$\Rightarrow n=21$ este compus, $a=2$ mărtor.

Varianta probabilistică

Aleg t elemente din \mathbb{Z}_n^* și testează pt fiiceare

Aleg t elemente din \mathbb{Z}_n^* și testează pe fiecare teorema.

Dacă găsești un mărtor \Rightarrow n compus 100%.

Dacă toate mostrele satisfac teorema \Rightarrow

$\Rightarrow n$ probabil prim, cu prob = $\frac{t}{n-1}$.

Ex: $n = 37$

$t = 3$, mostre $\{7, 11, 17\}$? $a^{36} = 1$ în \mathbb{Z}_{37}^* , $\forall a \in \{7, 11, 17\}$

$$7^{36} = (7^2)^{18} = 12^{18} = 2^{36} \cdot 3^{18} = (2^5)^7 \cdot 2 \cdot (3^3)^6$$

$$= (-5)^7 \cdot 2 \cdot (-10)^6 = ((-5)^2)^3 \cdot (-5) \cdot 2 \cdot (-5)^6 \cdot 2^6$$

$$= (-12)^3 \cdot (-5)^7 \cdot 2^7 = -2^6 \cdot 3^3 \cdot (-10)^7 = -2 \cdot 2^5 \cdot 2^7 \cdot (-10) \cdot 100^3$$

$$= -2 \cdot (-5) \cdot \underbrace{(-10) \cdot (-10)}_{-110} \cdot (-11)^3 = \underbrace{10 \cdot (-11) \cdot (-11)^3}_{-110=1} = 1 \cdot (-11) \cdot 121$$

$$= 1 \cdot (-11) \cdot 10 = -110 = 1. \checkmark$$

$a = 11$ OK $\Rightarrow n = 37$ probabil prim, prob = $\frac{3}{36} = \frac{1}{12}$

$a = 17$ OK

Testul Solovay-Strassen

Simbolul lui Jacobi:

Def: Fie $a, n \in \mathbb{N}$, n impar, $a \neq 0$.

$\sim \backslash \sim \backslash \sim$ dacă $n \mid a$

Vezi: în cadrul unui grup de numere.

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

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

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

$$\left(\frac{19}{5}\right) = \left(\frac{4}{5}\right) = 1 \text{ pt că } 4 = 2^2 \text{ în } \mathbb{Z}_5.$$

Teorema (SS)

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

Ez: $n=7 \Rightarrow a^3 = \left(\frac{a}{7}\right)$ în \mathbb{Z}_7 , $\forall a \in \mathbb{Z}_7$

$$a=0 \Rightarrow 0^3=0; \quad \left(\frac{0}{7}\right)=0 \text{ pt că } 7 \mid 0. \checkmark$$

$$a=1 \Rightarrow 1^3=1; \quad \left(\frac{1}{7}\right)=1 \text{ pt că } 1=1^2 \checkmark$$

$$a=2 \Rightarrow 2^3=1; \quad \left(\frac{2}{7}\right)=1 \text{ pt că } 2=3^2 \checkmark$$

$$a=3 \Rightarrow 3^3=-1; \quad \left(\frac{3}{7}\right)=-1$$

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



$$a=3 \Rightarrow 3^3 = -1; \quad \left(\frac{3}{7}\right) = -1$$

$$a=4 \Rightarrow 4^3 = (2^3)^2 = 1 \cdot \left(\frac{4}{7}\right) = 1 \text{ și că } 4=2^2.$$

$$a=5 \Rightarrow 5^3 = 5^2 \cdot 5 = 4 \cdot 5 = 6 = -1; \quad \left(\frac{5}{7}\right) = -1$$

$$a=6 \Rightarrow 6^3 = (-1)^3 = -1; \quad \left(\frac{6}{7}\right) = -1$$

$\Rightarrow n=7$ prim (SS).

Ex: $n=21 \stackrel{?}{\Rightarrow} \nexists a \in \mathbb{Z}_{21}^*, a^{10} = \left(\frac{a}{21}\right)$ in \mathbb{Z}_{21}

$$a=2 \Rightarrow 2^{10} = (2^4)^2 \cdot 2^2 = (-5)^2 \cdot 4 = 25 \cdot 4 = 4 \cdot 4 = 16 \neq \left(\frac{2}{21}\right)$$

$\Rightarrow n=21$ compus, $a=21$ marker.

OBS: Testul Solovay-Strassen are și o variantă probabilistică

Ordinal unui element într-un grup

Def: Fie G un grup, $g \in G$.

$\text{ord } g = n$ dacă $g^n = e$ și n este cel mai mic

$\text{ord } g = n$ dacă $g^n = e$ și n este cel mai mic cu această proprietate.

Dacă nu există $(g^n \neq e, \forall n)$, spunem $\text{ord } g = \infty$.

Ex: Dacă n este un prim $\Rightarrow (\mathbb{Z}_n^*, \cdot)$ grup.

(\mathbb{Z}_7^*, \cdot) $\text{ord } 3 = ?$ $\text{ord } (5) = ?$ $\text{ord } 2 = ?$

\times	1	2	3	4	5	6
$3 \times$	3	2	6	4	5	1

$$\Rightarrow \text{ord } 3 = 6$$

\times	1	2	3	4	5	6
$5 \times$	5	4	6	2	3	1

$$\Rightarrow \text{ord } 5 = 6$$

\times	1	2	3	4	5	6
$2 \times$	2	4	1	2	4	1

$$\Rightarrow \text{ord } 2 = 3.$$

Teorema (Fermat): Dacă n prim $\Rightarrow a^{n-1} = 1 \in \mathbb{Z}_n^*$,

$\forall a \in \mathbb{Z}_n^* \Rightarrow \text{orda} \leq n-1$.

Teorema (Lagrange) Fie G un grup. Numărul

ordinul grupului nr. de elemente ale mulțimii G .

$$\text{ord } G = \# G.$$

Dacă G grup finit $\Rightarrow \text{ord } g | \text{ord } G, \forall g \in G$.

$$x_1 - x \rightarrow \star \quad \text{or } \text{or}$$

$$\text{Ex: } G = \mathbb{Z}_7^*, \text{ ord } G = 6$$

ord 3 = 6 ✓

ord 2 = 3 ✓

Logaritmul discret (folosit în Diffie-Hellman)

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

- Obs:
- 1) Log este scump computațional în \mathbb{Z}_n .
 - 2) Log nu există mereu în \mathbb{Z}_n .

$$\text{Ex: } \log_3 2 \in \mathbb{Z}_7 = x \Leftrightarrow 3^x = 2 \in \mathbb{Z}_7$$

$$3^2 = 9 = 2 \Rightarrow x = 2$$

$$\log_3 2 = 2 \in \mathbb{Z}_7$$

$$\log_5 2 \in \mathbb{Z}_7 = x \Leftrightarrow 5^x = 2 \in \mathbb{Z}_7$$

c.f. calculul anterior, $5^4 = 2$

$$\Rightarrow \log_5 2 = 4 \in \mathbb{Z}_7$$

$$\log_2 3 \in \mathbb{Z}_7 \quad \begin{array}{r} x | 1 & 2 & 3 \\ \hline 2^x | 2 & 4 & 1 & 2 & 4 & 1 & 2 & 4 & \dots \end{array}$$

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

Ex: $\log_3 5 \in \mathbb{Z}_{11}$ $\Rightarrow 3^x = 5 \in \mathbb{Z}_{11}$

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

1 (Fermat)

$$3^3 = 3^2 \cdot 3 = 6 \cdot 3 = 18 \equiv 7 \Rightarrow \log_3 5 = 6 \in \mathbb{Z}_{11}$$

$$3^4 = 3^3 \cdot 3 = 7 \cdot 3 = 21 \equiv 10$$

Grupuri ciclice. Generatori (folosit în El Gamal)

Def: Fie G grup, $g \in G$.

$$\langle g \rangle = \{g, g^2, g^3, g^4, \dots\}$$

Dacă $\text{ord } g = t \Rightarrow \langle g \rangle = \{g, g^t, g^{2t}, \dots, g^{(t-1)t} = e\}$

$\langle g \rangle$ s.n. subgrupul generat de g . (g = generator)

Dacă $\langle g \rangle = G \Rightarrow G$ s.n. grup ciclic,
 g devine generator

Ex: $G = \mathbb{Z}_7^*$, $\langle 2 \rangle = \{2, 2^2, 2^3 = 1\} = \{1, 2, 4\}$

$$\langle 3 \rangle = \{3, 3^2, 3^3, 3^4, 3^5, 3^6 = 1\}$$

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

$\Rightarrow \mathbb{Z}_7^*$ este ciclic, 3 este un generator.

$\Rightarrow \mathbb{Z}_7^*$ este arlic, 3 este un generator.

$\langle 5 \rangle = \mathbb{Z}_7^*$, și 5 este un generator.

Obs: Dacă \mathbb{Z}_7^* este arlic, 2 nu este generator.

$$\langle 2 \rangle = \{1, 2, 4\}.$$

Indicatorul lui Euler (folosit în RSA)

Def: Fie $n \in \mathbb{N}$. $\varphi(n) = \#\left\{x \mid 1 \leq x < n \text{ și } \text{cmmdc}(x, n) = 1\right\}$

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

2) Dacă $(a, b) = 1 \Rightarrow \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

3) În general: $\varphi(n) = \prod_{p|n} p^{\alpha_p} \left(1 - \frac{1}{p}\right)$
peste divizori primi ai n !

Ex: $\varphi(53) = 52$ pt că 53 prim

$$\begin{array}{r} 15 \\ 51 \\ 17 \end{array} \left| \begin{array}{r} 3 \\ 3 \\ 17 \end{array} \right.$$

$$\varphi(153) = \varphi(3^2 \cdot 17) = \varphi(3^2) \varphi(17)$$

pt că cmmdc($3^2, 17$) = 1

$$\varphi(17) = 16$$

$\varphi(3^2) = ?$ $\neq \varphi(3) \cdot \varphi(3)$ nu pt că
cmmdc(3, 3) $\neq 1$

$$\varphi(3) \text{ is } + \text{ if } \text{cmdc}(3,3) = 1 \\ \text{cmdc}(3,3) \neq 1$$

$$\begin{aligned} \varphi(9) &= \#\{1 \leq x < 9 \mid \text{cmdc}(x, 9) = 1\} \\ &= \#\{1, 2, 4, 5, 7, 8\} = 6 \Rightarrow \varphi(9) = 6 \end{aligned}$$

$$\Rightarrow \varphi(153) = 6 \cdot 16 = 96$$

$$\underline{\text{Ex}}: \varphi(100) = ? \quad 100 = 2^2 \cdot 5^2$$

$$\begin{aligned} \varphi(100) &= 100 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) \\ &= 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40. \end{aligned}$$