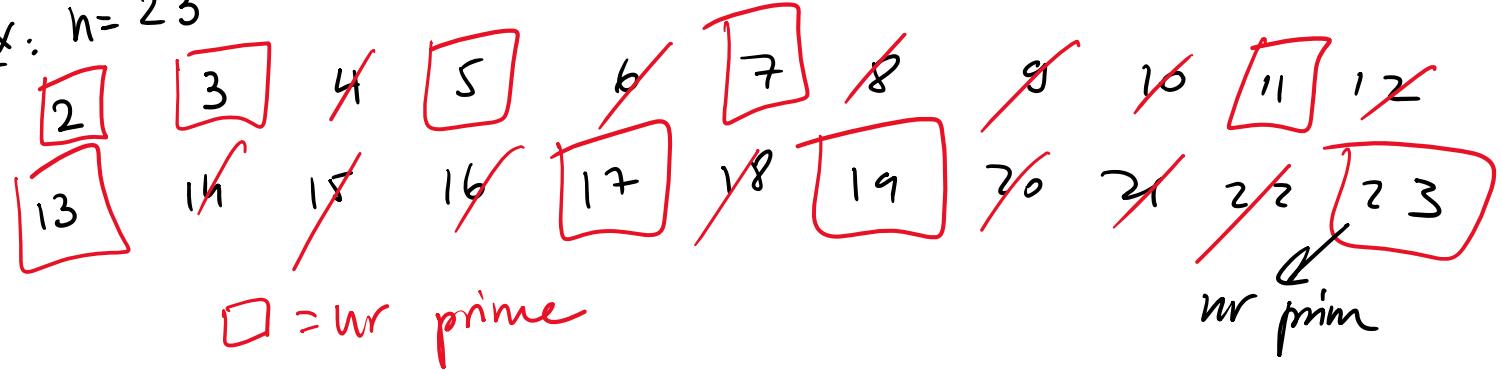


Teste de primalitateCiurul (sita) lui Eratostene

Dacă  $n \in \mathbb{N}$ , returnează toate nr prime  $\leq n$ .

Ex:  $n = 23$

Testul FermatMica teorema a lui Fermat

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

Negativă: Dacă  $\exists a \in \mathbb{Z}_n^*$  așa că  $a^{n-1} \neq 1$  în  $\mathbb{Z}_n^*$   $\Rightarrow n$  compus.

Ex:  $n = 13 \stackrel{?}{\Rightarrow} \forall a \in \mathbb{Z}_{13}^*, a^{12} = 1$ .

$$1^{12} = 1 \quad \checkmark$$

$$2^{12} = (2^4)^3 = 3^3 = 27 = 1 \quad \checkmark$$

$$3^{12} = (3^3)^4 = 1^4 = 1 \quad \checkmark$$

$$4^{12} = (2^2)^{12} = (2^4)^2 = 1 \quad \checkmark$$

$$4^{12} = \overline{(2^2)^{12}} = (2^{12})^2 = 1 \quad \checkmark$$

$$5^{12} = (5^2)^6 = (-1)^6 = 1 \quad \checkmark$$

$$6^{12} = 2^{12} \cdot 3^{12} = 1 \quad \checkmark$$

$$7^{12} = (7^2)^6 = 10^6 = (-3)^6 = 3^6 = 3^3 \cdot 3^3 = 1 \quad \checkmark$$

$$8^{12} = (2^3)^{12} = (2^{12})^3 = 1 \quad \checkmark$$

$$9^{12} = (3^2)^{12} = (3^{12})^2 = 1 \quad \checkmark$$

$\Rightarrow n=13$  prim  
(Fermat)

$$10^{12} = 2^{12} \cdot 5^{12} = 1 \quad \checkmark$$

$$11^{12} = (-2)^{12} = 2^{12} \quad \checkmark$$

$$12^{12} = (-1)^{12} = 1 \quad \checkmark$$

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

$$1^{14} = 1 \quad \checkmark$$

$$a=2 \Rightarrow 2^{14} = (2^4)^3 \cdot 2^2 = 1 \cdot 2^2 = 4 \neq 1 \quad \xrightarrow{n=15 \text{ compus.}} \text{a=2 martor (witness)}$$



Varianta exactă (deterministică) = să spună dacă și cum

Varianta probabilistă

Aleg  $t$  elemente  $a \in \mathbb{Z}_n^*$  și testează teorema doar cu ele.  
↳ măstăre

... măstăre mintre măstăre  $\Rightarrow n=\text{compus } 100$

↪ măstrelor

Dacă găsești un martor printre măstrelor  $\Rightarrow n = \text{componen}^{\text{t}} 100^{\text{t}}$ .  
 Dacă toate măstrelor beneficiază teorema  $\Rightarrow n \frac{\text{probabil prim}}{\text{prob}} = \frac{t}{n-1}$ .

## Testul Solovay - Strassen

Simbolul lui Jacobi:

Def: Fie  $a, n \in \mathbb{N}^+$ ,  $n$  impar.

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

$$\text{Ex: } \left( \frac{4}{13} \right) = 1 \quad \text{pt că } 4 = 2^2 \in \mathbb{Z}_{13}$$

$$\left( \frac{2}{7} \right) = 1 \quad \text{pt că } 2 = 3^2 = 4^2 \quad \begin{array}{c|ccccc} x & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline x^2 & 1 & 4 & 2 & 2 & 4 & 1 \end{array} \in \mathbb{Z}_7$$

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

$$\left( \frac{17}{5} \right) = \left( \frac{2}{5} \right) = -1 \quad \begin{array}{c|cccc} x & 1 & 2 & 3 & 4 \\ \hline x^2 & 1 & 4 & 4 & 1 \end{array}$$

$$\left( \frac{52}{12} \right) = 0 \quad \text{pt că } 13 \mid 52.$$

$$\left( \begin{array}{c} 52 \\ 13 \end{array} \right) = 0 \quad \text{pt că } 13 | 52.$$

Teorema (Solvay - Strassen)

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

Ex:  $n=7 \Rightarrow \forall a \in \mathbb{Z}_7, a^3 = \left( \begin{array}{c} a \\ 7 \end{array} \right) \in \mathbb{Z}_7$

$$a=0 \Rightarrow 0^3=0; \quad \left( \begin{array}{c} 0 \\ 7 \end{array} \right) = 0 \quad \text{pt că } 7|0$$

$$a=1 \Rightarrow 1^3=1; \quad \left( \begin{array}{c} 1 \\ 7 \end{array} \right) = 1 \quad \text{pt că } 1=1^2$$

$$a=2 \Rightarrow 2^3=1; \quad \left( \begin{array}{c} 2 \\ 7 \end{array} \right) = 1 \quad \text{pt că } 2=3^2=4^2$$

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

$$a=3 \Rightarrow 3^3=3^2 \cdot 3=2 \cdot 3=6=-1; \quad \left( \begin{array}{c} 3 \\ 7 \end{array} \right) = -1$$

$$a=4 \Rightarrow 4^3=(2^2)^3=(2^3)^2=1; \quad \left( \begin{array}{c} 4 \\ 7 \end{array} \right) = 1 \quad \text{pt că } 4=2^2$$

$$a=5 \Rightarrow 5^3=(-2)^3=-2=-1; \quad \left( \begin{array}{c} 5 \\ 7 \end{array} \right) = -1$$

$$a=6 \Rightarrow 6^3=2^3 \cdot 3^3=-1; \quad \left( \begin{array}{c} 6 \\ 7 \end{array} \right) = -1$$

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

Ex:  $n=27 \Rightarrow \exists a \in \mathbb{Z}_{27}, a = \left(\frac{a}{27}\right) \text{ în } \mathbb{Z}_{27}$ .

$$a=2 : 2^{13} = (2^5)^2 \cdot 2^3 = 5^2 \cdot 2^3 = (-2) \cdot 2^3 = -16 = 11 \neq \left(\frac{2}{27}\right)$$

$\Rightarrow n=27$  compus,  $a=2$  neutră.

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 cu această proprietate.

Dacă nu există  $(g^n \neq e, \forall n \in \mathbb{N})$ , se pune

$$\text{ord } g = \infty.$$

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

$$2^1 = 2; 2^2 = 4; \boxed{2^3 = 8 = 1 \Rightarrow \text{ord } 2 = 3}$$

$$2^4 = 2^3 \cdot 2 = 1 \cdot 2 = 2; 2^5 = 2^4 \cdot 2 = 2 \cdot 2 = 4;$$

$$2^6 = 2^5 \cdot 2 = 4 \cdot 2 = 8 = 1$$

x	1	2	3	4	5	6
$3x$	3	2	6	4	5	1
$-3$	$-2$	$-1$	$-2$	$-4$	$-5$	$-1$

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

$$3^1 = 3 \quad 3^2 = 9 \quad 3^3 = 27 \quad 3^4 = 81 \quad \dots$$

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

$$3^3 = 3 \cdot 3 = 2 \cdot 3 = 6$$

$$3^4 = 3^3 \cdot 3 = 6 \cdot 3 = 18 = 4$$

Ex:  $(\mathbb{Z}_7, +)$   $\text{ord } 2 = ?$

$$2+2=4; \quad 2+2+2=6; \quad 2+2+2+2=8=1$$

$$\text{ord } 2 = 4$$

$(\mathbb{Z}, +)$   $\text{ord } 2 = ?$

$$2+2=4; \quad 2+2+2=6; \quad 2+2+2+2=8$$

$$\text{etc } 2+2+\dots+2 = 2k+1$$

$k \in \mathbb{N}$

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

Teorema (Fermat): Dacă  $n$  este prim  $\Rightarrow$

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

$$\Rightarrow \text{ord } a \leq n-1$$

Ex:  $(\mathbb{Z}_{19}^*, \cdot)$

$2^{18} = 1$	$3^{18} = 1$	$4^{18} = 1$
--------------	--------------	--------------

$\not\Rightarrow \text{ord } 2 = \text{ord } 3 = \text{ord } 4 = 18$

$x$	1	2	3	4	5	6	7	8	9	10	11	12	13
$x^2$	1	4	8	16	13	7	14	9	18	17	11	15	3

$\frac{1}{2}$	2	4	8	16	13	7	14	9	18	17	15	19	1
$2^x$									$\frac{1}{1}$	$\frac{1}{1}$	$\frac{1}{4}$		

$x$	14	15	16	17	$\overline{18}$								
$2^x$	6	12	5	10	$\overline{1}$ (Fermat)								
$x$	1	2	3	4	5	6	7	8	$\overline{9}$				

$\Rightarrow \text{ord } 2 = 18$

$x$	1	2	3	4	5	6	7	8	$\overline{9}$				
$4^x$	4	16	7	9	$\frac{17}{1}$	11	6	5	$\overline{1}$				
		$\frac{1}{1}$			$\frac{-2}{-2}$								

$\Rightarrow \text{ord } 4 = 9$

$(\mathbb{Z}_{19}^*)$

$\text{ord } \mathbb{Z}_{19}^* = 18$

$18 | 18$

$9 | 18$

### Teorema (Lagrange)

Fie  $G$  un grup.  $\text{ord}(G) = \# G$ .

Dacă  $G$  este finit  $\Rightarrow \text{ord } g \mid \text{ord } G$ ,  $\forall g \in G$ .

În particular,  $\text{ord } g \mid n-1$ ,  $\forall g \in \mathbb{Z}_n^*$ .

Obs: De exemplu, este imposibil ca

$\text{ord } 3 > 5$  în  $\mathbb{Z}_{13}^*$  ( $\text{ord } \mathbb{Z}_{13}^* = 12, 5 \nmid 12$ )

### Aplicații logaritmul discret (folosit în Diffie-Hellman)

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

Obs 1)  $\log$  pe  $\mathbb{Z}_n$  este scump computațional.

2)  $\log_3 5 \in \mathbb{Z}_7$  nu există mereu.

Ex.:  $\log_3 5 \in \mathbb{Z}_7 = x \Leftrightarrow 3^x = 5 \in \mathbb{Z}_7$

x	1	2	3	4	5	6
$3^x$	3	2	6	4	5	1 (Fermat)

$$\Rightarrow \log_3 5 = 5 \notin \mathbb{Z}_7$$

$\log_2 3 \in \mathbb{Z}_7 = x \Leftrightarrow 2^x = 3 \in \mathbb{Z}_7$

x	1	2	3	4	5	6
$2^x$	2	4	1	2	4	1 (Fermat)

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

---

Apliabilitate: Grup ciclic. Generatori (El Gamal)

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

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

Dacă  $\text{ord } g = t \Rightarrow \langle g \rangle = \{g, g^2, g^3, \dots, g^{t-1} = e\}$

$\langle g \rangle$  s.n. subgrupul generat de  $g$

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

Ex:

x	1	2	3	4	5	6
$3x$	3	2	6	4	5	1

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

$\Rightarrow \mathbb{Z}_7^*$  group cuhic 13 este un generator.

JAR:

x	1	2	3
$2x$	2	4	1

$$\subseteq \mathbb{Z}_7^*$$

$$\Rightarrow \langle 2 \rangle = \{1, 2, 4\} \not\subseteq \mathbb{Z}_7^* \text{ nu este cihic}$$

Rezultă doar că 2 nu este generator.

obs: Spunem că  $G$  nu este cihic doar dacă nu există element al său nu este generator.

Ex: Din calculul anterior:  $\langle 2 \rangle = \mathbb{Z}_{19}^*$

$\Rightarrow \mathbb{Z}_{19}^*$  este cihic, și 2 este generator

$$\langle 4 \rangle = \{1, 4, 5, 6, 7, 9, 11, 16, 17\} \Rightarrow$$

$\Rightarrow 4$  este generator.

Indicațional în Euler (folosit în RSA)

Def: În neal.  $\varphi(n) = \#\{1 \leq x < n \mid \text{cmmdc}(x, n) = 1\}$

Proprietăți:

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

2) Dacă  $\text{cmmdc}(a, b) = 1 \Rightarrow \varphi(ab) = \varphi(a)\varphi(b)$

3)  $\varphi(n) = \prod_{p|n} n \left(1 - \frac{1}{p}\right)$ , unde  $p$  este divizor prim al lui  $n$ .

Ex:  $\varphi(51) = \varphi(3 \cdot 17) \stackrel{2)}{=} \varphi(3) \cdot \varphi(17) \stackrel{1)}{=} 2 \cdot 16 = 32$   
 $51 = 3 \cdot 17$

$$\varphi(153) = \varphi(3^2 \cdot 17) = \varphi(9 \cdot 17) \stackrel{2)}{=} \varphi(9) \cdot \varphi(17) \stackrel{1)}{=} \varphi(9) \cdot 16$$

$\text{cmmdc}(9, 17) = 1 \quad = 6 \cdot 16 = 96.$

$$\begin{array}{r} 153 \\ 51 \\ 17 \end{array} \left| \begin{array}{r} 3 \\ 3 \\ 17 \end{array} \right.$$

$$\varphi(9) = \#\left\{1 \leq x < 9 \mid \text{cmmdc}(x, 9) = 1\right\}$$
$$= \#\{1, 2, 4, 5, 7, 8\} = 6$$

$$\varphi(100) = \varphi(2^2 \cdot 5^2) \stackrel{3)}{=} \prod_{p|100} 100 \left(1 - \frac{1}{p}\right) = 100 \cdot \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right)$$

$2, 5 - \text{divizori primi} \uparrow$   
ai lui 100

$$= 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40$$

$$\Rightarrow \varphi(100) = 40.$$