Teste de primalitate

Ciurul (sita) lui Eratostene

Primește $n \in \mathbb{N}$
Răspunde cu toate nr prime $\leq n$

Ex: $n = 23$

$\boxed{2}$ $\boxed{3}$ $\cancel{4}$ $\boxed{5}$ $\cancel{6}$ $\boxed{7}$ $\cancel{8}$ $\cancel{9}$ $\cancel{10}$ $\boxed{11}$ $\cancel{12}$ $\boxed{13}$
$\cancel{14}$ $\cancel{15}$ $\cancel{16}$ $\boxed{17}$ $\cancel{18}$ $\boxed{19}$ $\cancel{20}$ $\cancel{21}$ $\cancel{22}$ $\boxed{23}$

$\boxed{}$ = nr prime

nr. prim.

Testul Fermat

Mica Teoremă a lui Fermat

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

Negația: Dacă $\exists\, a \in \mathbb{Z}_n^*$ a.î. $a^{n-1} \neq 1$ în $\mathbb{Z}_n^* \Rightarrow n$ nu este prim.

a s.n. martor (witness)

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

$1^{10} = 1$ ✓

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

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

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

$4^{10} = (2^2)^{10} = (2^{10})^2 = 1$ ✓

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

$6^{10} = 2^{10} \cdot 3^{10} = 1$ ✓

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

$8^{10} = 2^{10} \cdot 4^{10} = 1$ ✓

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

$10^{10} = 2^{10} \cdot 5^{10} = 1$ ✓

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

<u>Ex</u>: $n = 21 \Rightarrow \forall a \in \mathbb{Z}_{21}^*,\ a^{20} = 1$ în $\mathbb{Z}_{21}^*$?

$1^{20} = 1$ ✓

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

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

<u>Varianta probabilistă</u>

Aleg t elemente din $\mathbb{Z}_n^*$ și testez pt fiecare teorema.

Dacă găsesc un martor $\Rightarrow$ n compus 100%.

Dacă toate mostrele satisfac teorema $\Rightarrow$

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

Ex: $n = 37$

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

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

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

$$= (-12)^3 \cdot (-5)^7 \cdot 2^7 = -2^6 \cdot 3^3 \cdot (-10)^7 = -2 \cdot 2^5 \cdot 27 \cdot (-10) \cdot 100^3$$

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

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

$a = 11$ 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, $a \neq 0$.

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

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

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

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

| 5 | | 5 |

Teoremă (SS)

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

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

$a = 0 \Rightarrow 0^3 = 0$; $\left(\frac{0}{7}\right) = 0$ pt că $7 | 0$. ✓

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

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

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

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

$a = 4 \Rightarrow 4^3 = (2^3)^2 = 1$; $\left(\frac{4}{7}\right) = 1$ pt că $4 = 2^2$. ✓

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

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

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

<u>Ex</u>: $n = 21 \overset{?}{\Rightarrow} \forall a \in \mathbb{Z}_{21}^*$, $a^{10} = \left(\frac{a}{21}\right)$ în $\mathbb{Z}_{21}$

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

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

<u>Obs</u>: Testul Solovay-Strassen are și o variantă probabilistă.