Teste de primalitate

Ciurul (sita) lui Eratostene

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

Ex: $n = 23$

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

$\boxed{13}$ $\cancel{14}$ $\cancel{15}$ $\cancel{16}$ $\boxed{17}$ $\cancel{18}$ $\boxed{19}$ $\cancel{20}$ $\cancel{21}$ $\cancel{22}$ $\boxed{23}$

nr prim

$\square$ = nr prime

Testul Fermat

Mica teoremă a lui Fermat

Dacă n 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 $\mathbb{Z}_n^*$ $\Rightarrow n$ compus.

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

$1^{12} = 1$ ✓

$2^{12} = (2^4)^3 = 3^3 = 27 = 1$ ✓

$3^{12} = (3^3)^4 = 1^4 = 1$ ✓

$4^{12} = (2^2)^{12} = (2^{12})^2 = 1$ ✓

$5^{12} = (5^2)^6 = (-1)^6 = 1$ ✓

$5^{12} = (5^2)^6 = (-1)^6 = 1$ ✓

$6^{12} = 2^{12} \cdot 3^{12} = 1$ ✓

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

$8^{12} = (2^3)^{12} = (2^{12})^3 = 1$ ✓

$9^{12} = (3^2)^{12} = (3^{12})^2 = 1$ ✓ $\Rightarrow n = 13$ prim (Fermat)

$10^{12} = 2^{12} \cdot 5^{12} = 1$ ✓

$11^{12} = (-2)^{12} = 2^{12}$ ✓

$12^{12} = (-1)^{12} = 1$ ✓

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

$1^{14} = 1$ ✓

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

Varianta exactă (deterministă) = răspunde sigur

Varianta probabilistă

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

↳ mostre

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

Dacă toate mostrele verifică teorema $\Rightarrow n$ probabil prim

prob $= \frac{t}{n-1}$.

Testul Solovay-Strassen

Simbolul lui Jacobi:

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

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

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

$\left(\frac{2}{7}\right) = 1$ pt că $2 = 3^2 = 4^2$

x	1	2	$\boxed{3}$	$\boxed{4}$	5	6
x^2	1	4	$\boxed{2}$	$\boxed{2}$	4	1

în $\mathbb{Z}_7$

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

$\left(\frac{17}{5}\right) = \left(\frac{2}{5}\right) = -1$

x	1	2	3	4
x^2	1	4	4	1

$\left(\frac{52}{13}\right) = 0$ pt că $13 / 52$.

Teoremă (Solovay-Strassen)

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

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

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

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

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

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

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

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

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

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

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

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

Ex: $n=27 \overset{?}{\Rightarrow} \forall a \in \mathbb{Z}_{27},\ a^{13} = \left(\frac{a}{27}\right)$ 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, $a=2$ martor.

Obs: Testul Solovay-Strassen are și o variantă probabilistă.