No.

Date

Fermat (n)
sorteia $x \in \{1, \dots, n-1\}$
aleat. com probabilidade uniforme
se $x^{n-1} \not\equiv 1 \pmod{n}$
então devolva "composto"
senão devolva "provavelmente primo"

⇝ Pequeno Teorema de Fermat
$x^{n-1} \equiv 1 \pmod{n} \iff n$ é primo
$\forall x \in \{1, \dots, n-1\}$

$n$ composto, ímpar
se $\exists\ x$ t.q. $mdc(x, n) = 1$
e $x^{n-1} \not\equiv 1 \pmod{n}$
$\#$ testemunhas $\geq \frac{n-1}{2}$

. Miller - Rabin (1980)
$x, n$ inteiros positivos
$x \not\equiv \pm 1 \pmod{n}$ $\Rightarrow n$ composto
$\underbrace{x^2 \equiv}_{\text{raiz falsa de } 1} 1 \pmod{n}$
$n$ primo:
$x+1 \equiv a \pmod{n}$ $\quad a \in \{1, \dots, n-1\}$
$x-1 \equiv b \pmod{n}$

$\underbrace{(x+1)(x-1)}_{x^2-1} \equiv ab \pmod{n}$

$x^2 - 1 \equiv 0 \pmod{n}$
$ab \equiv 0 \pmod{n}$ ; $1 \leq ab \leq (n-1)^2$

$ab = n.m$
$a = n.ma$ ou $b = n.ma$
$b = mb$ $\quad a = mb$
$\triangleright\ a \equiv 0 \bmod n$ $(\rightarrow\leftarrow)$ $\quad \triangleright\ b \equiv 0 \bmod n$ $(\rightarrow\leftarrow)$

Scanned by CamScanner

Miller - Rabin (n)

Se $n$ é par e $n > 2$ devolva "composto"

Sorteie $x \in \{1, \dots, n-1\}$ aleatoriamente com prob. uniforme

(fermat) se $x^{n-1} \not\equiv 1 \bmod n$
devolva "composto"

Encontre $s$ e $t$, $s$ o maior possível
t.q. $\underbrace{n-1}_{par} = 2^s \cdot t \to t$ é ímpar

Calcula $x^t, x^{2t}, x^{4t}, \dots, x^{2^s t} = x^{n-1}$

para $i$ de $0$ a $s-1$
verifique se $x^{2^i t}$ é uma raiz falsa de 1
$\hookrightarrow \begin{cases} x^{2^i t} \not\equiv \pm 1 \\ x^{2^{i+1} t} \equiv 1 \end{cases}$

devolva "provavelmente primo"

$n$ composto ímpar

$x$ é liar
$\hookrightarrow$ algoritmo retorna prov. primo com este $x$

\# liars $\leq \frac{n-1}{2}$

$L$ = conj de liars

$a \equiv q \pmod{bc}$
$\Rightarrow a \equiv q \pmod{c}$

$a \not\equiv q \pmod{c}$
$\Rightarrow a \not\equiv q \pmod{bc}$

(A)

$\mathbb{Z}_n^* = \{ x \in \{1, \dots, n-1\} : mdc(x, n) = 1 \}$

$(\mathbb{Z}_n^*, \cdot)$ é um grupo

- $\forall a, b \in \mathbb{Z}_n^* \quad a \cdot b \in \mathbb{Z}_n^*$
- $\forall a, b, c : a(b \cdot c) = (a \cdot b) \cdot c$
- $\exists 1 \in \mathbb{Z}_n^* : a \cdot 1 = 1 \cdot a = a$
- $\forall a \in \mathbb{Z}_n^* \ \exists a^{-1} \in \mathbb{Z}_n^*$ t.q $a \cdot a^{-1} = 1 = a^{-1} \cdot a$

No.
Date

$B \subseteq \mathbb{Z}_n^*$ é subgrupo se $(B, \cdot)$ é grupo

$B$ é subgrupo próprio se $B \neq \mathbb{Z}_n^*$

- Lagrange : $|B| = \dfrac{|\mathbb{Z}_n^*|}{b \text{ nº inteiro}}$

Ideia : $B$ subgrupo de $\mathbb{Z}_n^*$ proprio
$L \subseteq B$
$|L| \leq |B| \leq n-1/2$

(I) $B = \{ b \in \mathbb{Z}_n^* : b^{n-1} \equiv 1 \pmod n \}$
é subgrupo
é próprio : $x \in \mathbb{Z}_n^*$ e $x^{n-1} \not\equiv 1 \pmod n$
$x \notin B$

(II) Se $n$ é de Carmichael

Fato : Se $p$ é primo, $p^2 \nmid n$

Teorema do resto chines: (TRC)
Sistema
$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$
$mdc(n_i, n_j) = 1$
$i \neq j$

$\exists\, x$ satisfazendo o sistema
se $x_1, x_2$ soluções $x_1 \equiv x_2 \pmod{n_1 \dots n_k}$

Suponha $p^2 | n \Rightarrow n = p^k \cdot q$ e $mdc(p, q) = 1$

$$\begin{cases} x \equiv p+1 \pmod{p^k} \\ x \equiv 1 \pmod q \end{cases} \Rightarrow \exists\, x \text{ pelo TRC}$$

Scanned by CamScanner

$(p+1)^p = \sum_{i=0}^{p} \binom{p}{i} p^i \equiv 1 \pmod{p^2}$ ; $(mdc(x,n)=1)$

$\vdash x^{n-1} \equiv (p+1)^{n-1} \not\equiv 1 \mod (p^k)$

$\overset{*}{\Rightarrow} x^{n-1} \not\equiv 1 \mod n$

$((p+1)^p)^{n/p} \equiv 1 \mod (p^2)$

$p \mid n$

$(p+1)^n \equiv 1 \pmod{p^2}$

$mdc(p+1, p^2) = 1$

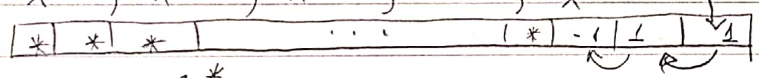
$(p+1)^{n-1} \equiv (p+1)^{-1} \pmod{p^2}$

$\not\equiv 1 \mod p^2$

$(p+1)^{n-1} \not\equiv 1 \pmod{p^k}$ por ⊛

---

$x^t, x^{2t}, x^{4t}, \dots, x^{2^s t = n-1}$




$x \in \mathbb{Z}_n^*$

liar

$j = \max\{ i \in \{0,\dots,s-1\} \mid \exists v \in \mathbb{Z}_n^*, v^{2^i t} \equiv -1 \pmod n \}$

$(n-1)^{2^0 t} \equiv 1 \pmod n$

$B = \{ x \in \mathbb{Z}_n^* \mid x^{2^j t} \equiv \pm 1 \pmod n \}$

∘ $L \subseteq B$ ∘ $B$ grupo

$x$ liar

∘ $B$ é próprio

$n = n_1 . n_2$ ; coprimos

$w = v \pmod{n_1}$

$w = 1 \pmod{n_2}$

TRC $\rightsquigarrow \exists w$

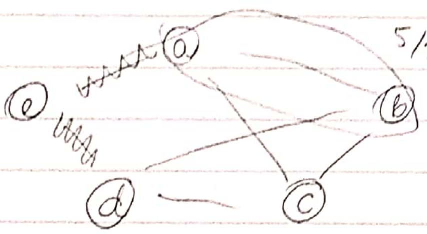
$$w^{2^j t} \equiv v^{2^j t} \pmod{n_1} \equiv -1$$
$$w^{2^j t} \equiv 1 \pmod{n_2}$$

$\vdash \; v^{2^j t} \equiv -1 \pmod{n_1}$ Ⓐ
sei : $v^{2^j t} \equiv -1 \pmod{n}$

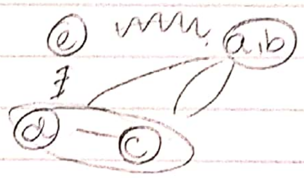
$\vdash \; w \notin B$
$w \in \mathbb{Z}_n^*$ (fácil)

Suponha $w^{2^j t} \equiv 1 \pmod{n}$
$\equiv -1 \pmod{n}$ $(\rightarrow\leftarrow)$

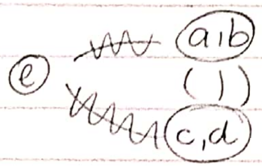
$w^{2^j t} \equiv -1 \bmod n$
$\equiv 1 \bmod n_2$ $(\rightarrow\leftarrow)$



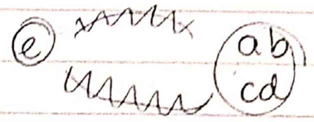
5/7



$\frac{1}{6}$



$\frac{3}{5}$



$$\frac{5 \quad 4 \quad 3}{7 \quad 6 \quad 5} = \frac{2}{7}$$