Teste de primalidade de

Miller-Rabin de base b

n ímpar ; $n-1 = 2^s \cdot t$, t ímpar, $s \geq 1$

n passa o teste de Miller na base b

se $b^t \equiv 1 \bmod n$ ou

$b^{2^j \cdot t} \equiv -1 \bmod n$ p/ algum $0 \leq j \leq s-1$

Teorema: n primo ímpar, $b \in \mathbb{Z}_n \setminus \{0\}$ (i.e., $n \nmid b$)

Então n passa o teste de Miller.

dem.

$n-1 = 2^s \cdot t$, $s \geq 1$, t ímpar

Seja $(x_k)_k$ com $x_k = b^{\frac{n-1}{2^k}} = b^{2^{s-k} \cdot t} \bmod n$

com $k = 0, \ldots, s$

Sendo n primo,

$x_0 = b^{2^s \cdot t} = b^{n-1} \equiv 1 \bmod n$ pelo PTF

$$x_1 = b^{2^{s-1}\cdot t} \bmod n \Rightarrow x_1^2 = b^{2\cdot 2^{s-1}\cdot t} = b^{2^s\cdot t} = x_0 \equiv 1 \bmod n$$

I.e. $x_1^2 \equiv 1 \bmod n \overset{n \text{ primo}}{\Longrightarrow} x_1^2 - 1 \equiv 0 \bmod n$

$\Rightarrow (x_1-1)(x_1+1) \equiv 0 \bmod n$

$\Rightarrow x_1 - 1 \equiv 0 \bmod n$ ou $x_1 + 1 \equiv 0 \bmod n$

$\overset{n \text{ primo}}{\Longrightarrow} x_1 \equiv 1 \bmod n$ ou $x_1 \equiv -1 \bmod n$

$x_1 \equiv -1 \bmod n \Rightarrow b^{2^{s-1}\cdot t} \equiv -1 \bmod n$

Basta tomar $j = s-1$ no teste

I.e., passa o teste.

Sup. agora que $x_1 \equiv 1 \bmod n$

$$(x_2)^2 = \left(b^{2^{s-2}\cdot t}\right)^2 \bmod n$$

$$= b^{2^{s-1}\cdot t} = x_1 \equiv 1 \bmod n$$

$\Rightarrow x_2^2 \equiv 1 \bmod n \Rightarrow x_2 \equiv 1 \bmod n$ ou $x_2 \equiv -1 \bmod n$

$x_2 \equiv -1 \bmod n \Rightarrow b^{2^j\cdot t} \equiv -1 \bmod n$

Com $j = s-2$ i.e., passa o teste.

Se $x_2 \equiv 1 \mod n$, repetimos o raciocínio

Se $x_0 \equiv x_1 \equiv x_2 \equiv \cdots \equiv x_s \equiv 1 \mod n$

$x_0 \equiv b^{2^0 \cdot t} = b^t \equiv 1 \mod n$ ie

n passa o teste

Se n passa o teste de Miller na base b $\square$

então $b^{n-1} \equiv 1 \mod n$

Sup n passa o teste de Miller

$n-1 = 2^s \cdot t$

- $b^t \equiv 1 \mod n$

$b^t \equiv 1 \mod n \Rightarrow (b^t)^{2^s} \equiv 1 \mod n$

$\Rightarrow b^{2^s \cdot t} \equiv 1 \mod n$

$\Rightarrow b^{n-1} \equiv 1 \mod n$

- $b^{2^j\cdot t} \equiv -1 \mod n$ para algum $0 \leq j \leq s-1$

$$b^{2^j\cdot t} \equiv -1 \mod n \Rightarrow \left(b^{2^j\cdot t}\right)^{2^{s-j}} \equiv 1 \mod n$$

$$\Rightarrow b^{n-1} \equiv 1 \mod n$$

$\overline{b \in \mathbb{Z}_n \qquad n-1 = 2^s\cdot t}$ $\qquad x_k = b^{2^{s-k}\cdot t} \mod n$

Sequência - B

$$(x_s, \dots, x_2, x_1, x_0)$$

$$\left(b^t, \dots, b^{2^{s-2}\cdot t}, b^{2^{s-1}\cdot t}, b^{n-1}\right)$$

$$\xleftarrow{\ \sqrt{\ }\ }$$

$$\xrightarrow{\ \hat{}\,2\ }$$

n primo: $(\dots, ?, ?, -1, 1, \dots, 1, 1)$

$$(1, \dots, 1, 1, 1)$$

n ímpar é pseudoprimo Forte

pspF na base b se

n é composto e passa o teste de Miller na base b

n = 2047 é pspF base 2

Teorema. $\exists \infty$ psp F base 2

Teorema (RABIN) n ímpar

Dadas $b_k \in \mathbb{Z}_n$ ...

A probabilidade de n passar o teste de Miller p/ os b_i bases e n ser composto é $< \frac{1}{4^k}$

TEOREMA DE EULER $\quad n \in \mathbb{N}$

$$\varphi(n) = \# \{ m \leq n ; \ (m,n) = 1 \}$$

$$= \sum_{\substack{k \\ 1 \leq k \leq n \\ (k,n)=1}} 1$$

S s.r.r. sistema reduzido de resíduos

é um subconjunto de um s.c.r.

t.q. $\#S = \varphi(n)$ e $\forall_{s \in S}, (n,s)=1$

$n = 7 \qquad \mathbb{Z}_7$ s.c.r.

s.r.r. $\mathbb{Z}_7^* = \{ 1, 2, 3, 4, 5, 6 \}$

$\varphi(7) = 6$

p primo $\Rightarrow \varphi(p) = p-1$

n primo $\Leftrightarrow \varphi(n) = n-1$

$n = 15$ $\quad \mathbb{Z}_{15}$

$\varphi(15) = 8$ $\quad \mathbb{Z}_{15}^{*} = \{ \quad \}$

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

$$\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1} \quad ; \quad \varphi(p) = p-1$$

$$(m,n) = 1 \Rightarrow \varphi(m \cdot n) = \varphi(m)\,\varphi(n)$$

$$\varphi(15) = \varphi(3 \cdot 5) = \varphi(3)\,\varphi(5)$$

$$\varphi(2^2 \cdot 3^4 \cdot 7 \cdot 11^3) = (2^2 - 2^1)(3^4 - 3^3)(7-1)(11^3 - 11^2)$$

Teorema. $(a,n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \bmod n$

RSA

p, q primos $\neq$'s

$$n = p \cdot q$$

$$m = \varphi(n) = (p-1)(q-1)$$

$$e \in \mathbb{Z}_m^* \quad \text{i.e. } e \in \mathbb{Z}_m \text{ t.q. } (e, m) = 1$$

$$d = e^{-1} \bmod m$$

Chave pública (n, e)

Chave privada d

Alice pretende enviar $x \in \mathbb{Z}_n$ para Bob

$$c = x^e \bmod n$$ ← esquema de cifração

Bob:

$$z = c^d \bmod n$$ ← esquema de decifração

$$ed \equiv 1 \bmod \varphi(n) \Rightarrow ed - 1 = k \cdot \varphi(n)$$

$$\Rightarrow ed = k\varphi(n) + 1$$

$$z = c^d = (x^e)^d = x^{ed} = x^{\varphi(n)\cdot k+1}$$

$$= \underbrace{\left(x^{\varphi(n)}\right)^k}_{\equiv 1 \bmod n} \cdot x \bmod n = x \bmod n$$