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

n passa o teste de Miller na base b se

$b^t \equiv 1 \mod n$ ou $b^{2^j \cdot t} \equiv -1 \mod n$

p/ algum $0 \leq j \leq s-1$

<u>Teorema</u>. Se n é primo então n passa o teste de Miller p/ qq. base

⚠ $n = 2047$ é composto e passa teste de Miller na base $b=2$.

n é pseudo primo forte (pspF) na base b se n é composto e passa o teste de Miller na base b.

<u>Teorema</u>. Existe uma infinidade de pspF na base 2.

<u>dem</u>. Vamos mostrar se n psp-f base 2 então $N = 2^n - 1$ é psp.F base 2.

n ímpar psp. f base 2 i.e.

n é composto e $2^{n-1} \equiv 1 \mod n$

$$2^{n-1} \equiv 1 \mod n \iff \underbrace{2^{n-1}-1}_{\text{ímpar}} = nk \text{ p/ algum } k$$

Logo k é ímpar

$$N = 2^n - 1 \Rightarrow N-1 = 2^n - 2 = 2(\underbrace{2^{n-1}-1}_{nk \text{ ímpar}})$$

i.e. obtemos $s=1$, $t = nk$ no teste de Miller

$$2^t = 2^{nk} = (2^n)^k \equiv 1 \mod N$$

porque $2^n = (2^n-1)+1 \equiv 1 \mod \underbrace{2^n-1}_{=N}$

Ou seja $N = 2^n-1$ passa o teste de Miller na base 2.

Resta mostrar que N é composto.

$$d \mid n \Rightarrow (2^d-1) \mid (2^n-1)$$

$\square$

Teorema de Euler

$\varphi(n) = \# \{ m : (m,n)=1 \text{ e } m \leq n \}$

K s. completo de resíduos (s.c.r)

$K \supseteq S$ é sistema reduzido de resíduos (s.r.r) se $\# S = \varphi(n)$ e

$\forall s \in S, \ (s,n)=1$

$\mathbb{Z}_n = \{0, 1, \dots, n-1\}$

$\mathbb{Z}_n^* = \{ 1 \leq m \leq n-1 : (m,n)=1 \}$

$\mathbb{Z}_8 = \{0, 1, 2, \dots, 7\}$

$\mathbb{Z}_8^* = \{1, 3, 5, 7\} \qquad \varphi(8) = 4$

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

$(\mathbb{Z}_n; +; \cdot)$ anel abeliano

$a \in \mathbb{Z}_n$ é invert. sse $(a,n)=1$

O número de unidades (i.e., invertíveis) em $\mathbb{Z}_n$ é $\varphi(n)$.

$$\mathbb{Z}_n^* = \{ a \in \mathbb{Z}_n : (a,n) = 1 \}$$
$$= \{ a \in \mathbb{Z}_n : a \text{ é invertível} \}$$

$(\mathbb{Z}_n^*; \cdot)$ é um grupo com $\varphi(n)$ elementos

$a \in \mathbb{Z}_n^*$ sse. i.e., $a \in \mathbb{Z}_n$ t.q. $(a,n)=1$

$\mathrm{ord}_n(a)$ é o menor k t.q. $a^k = 1$

Lagrange: $\mathrm{ord}_n a \mid \underbrace{|\mathbb{Z}_n^*|}_{=\varphi(n)}$

$$a^{\varphi(n)} = (a^k)^{\frac{\varphi(n)}{k}} \equiv 1 \mod n$$

Teorema de Euler: $(a,n) = 1$ então
$$a^{\varphi(n)} \equiv 1 \mod n$$

HW. Se $\{r_1, \dots, r_{\varphi(n)}\}$ s.r.r modulo n e $a \in \mathbb{Z}$ t.q. $(a,n)=1$ então $\{ar_1, ar_2, \dots, ar_{\varphi(n)}\}$ é s.r.r. modulo n

$$\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\} \qquad a : (a,n)=1, \quad n=9$$

$a = -2$

$$S = \{-2, -4, -8, -10, -14, -16\} \quad \text{s.r.r mod. } 9$$

Funç multiplicativa

f é f. multiplicativa se $(m,n)=1 \Rightarrow f(m \cdot n) = f(m) f(n)$.

Teor. f funç multiplicativa, $n = \prod_i p_i^{\alpha_i}$ produto de potências de primos $\neq$'s

Então $f(n) = \prod_i f(p_i^{\alpha_i})$

Teor. n primo $\iff \varphi(n) = n-1$

dim "$\Rightarrow$" è banale

"$\Leftarrow$" $\varphi(n) = n-1$ e n è composto

Esiste d t.c. $1 < d < n$ e $d \mid n$

$d \in \mathbb{Z}_n$, $(d, n) \neq 1$ logo $d \notin \mathbb{Z}_n^*$

logo $\underbrace{\# \mathbb{Z}_n^*}_{= \varphi(n) = n-1} \leq n-2$

Isto è $n - 1 \leq n-2$ ↯

$\square$

$n = 5^7$ $\quad \mathbb{Z}_n^* = \{ s \in \mathbb{Z}_n : (s, 5) = 1 \}$

$1 \leq m \leq 5^7$, $(m, 5^7) \neq 1$ significa

que $m = k \cdot 5$, $1 \leq k \leq 5^6$

$\# \mathbb{Z}_n^* = 5^7 - 5^6$

Teor. p primo. $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$

$\varphi(9) = \varphi(3^2) = 3^2 - 3^1 = 6$

Teor. φ e' multiplicativa

Corolario.

p, q primos $\neq$'s.

$\varphi(pq) = (p-1)(q-1)$

$$\varphi(144) = \varphi(12^2) = \varphi(2^4 \cdot 3^2) = \varphi(2^4)\varphi(3^2)$$
$$= (2^4 - 2^3)(3^2 - 3) = 8 \cdot 6 = 48$$

$\varphi(42) = \varphi(2 \cdot 3 \cdot 7) = 2 \cdot 6 = 12$

$\varphi(35) = \varphi(5 \cdot 7) = 4 \cdot 6$ $\qquad \varphi(5^2 \cdot 7^3) = (5^2 - 5) \cdot (7^3 - 7^2)$

Teor. $n > 2$, $\varphi(n)$ e' par.

dem. Sup. $n = \prod_i p_i^{\alpha_i}$ c/ p_j impar

$\varphi(n) = \prod \varphi(p_i^{\alpha_i}) = \varphi(p_j^{\alpha_j}) \prod_{i \neq j} \varphi(p_i^{\alpha_i})$

$$= \underbrace{\left(p_j^{\alpha_j} - p_j^{\alpha_j - 1}\right)}_{\text{par}} \prod_{i \neq j} \varphi(p_i^{\alpha_i})$$

$$n = 2^\alpha, \ \alpha \geq 2$$

$$\varphi(n) = \varphi(2^\alpha) = \underbrace{2^\alpha}_{\text{par}} - \underbrace{2^{\overbrace{\alpha - 1}^{\geq 1}}}_{\text{par}} \text{ é par} \quad \square$$

Rivest Shamir Adlemann

$n = pq$

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

$e \in \mathbb{Z}_m^*$

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

Ch. Pub. (n, e)

Ch. Priv. d

Cifrar $x \in \mathbb{Z}_n$: $c = x^e \bmod n$

Decifrar $y \in \mathbb{Z}_n$: $z = y^d \bmod n$

$$z = y^d = \left(x^e\right)^d \bmod n$$

$$ed \equiv 1 \bmod \varphi(n) \Rightarrow \varphi(n) \mid (ed-1)$$

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

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

$$z \equiv x^{ed} \bmod n \Rightarrow z \equiv \left(x^{\varphi(n)}\right)^k \cdot x \bmod n$$

$$\Rightarrow z \equiv x \bmod n$$

Teorema Euler