$\mathbb{Z}_n = \{0, \ldots, n-1\}$ ; $a \in \mathbb{Z}_n$.

$\exists x \in \mathbb{Z}_n \cdot ax \equiv 1 \mod n$

$\iff (a,n) = 1$

$\varphi(n) = \#\{a \in \mathbb{Z}_n : (a,n) = 1\}$

<u>Teorema Euler</u>: $(a,n)=1$. Então $a^{\varphi(n)} \equiv 1 \mod n$

$\varphi$ é multiplicativa, i.e., $(m,n) = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$

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

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

$p, q$ primos $\Rightarrow \varphi(pq) = (p-1)(q-1)$

<u>Ex</u>: $\varphi(2^4 \cdot 3^2 \cdot 5 \cdot 7^8) = \varphi(2^4)\varphi(3^2)\varphi(5)\varphi(7^8)$

$= (2^4 - 2^3)(3^2 - 3)(5-1)(7^8 - 7^7)$

<u>Teor</u>. $n = pq$. Calcular $\varphi(n)$ é equivalente a factorizar $n$

$\boxed{\text{RSA}}$

$p, q$ primos $\neq$'s

$n = pq$

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

$e \in \mathbb{Z}_m^* = \{k \in \mathbb{Z}_m : (k,m) = 1\}$

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

$(n, e)$ chave pública

$d$ chave privada

<u>Cifração</u>: $c(x) = x^e \mod n$

<u>Decifração</u>: $dec(y) = y^d \mod n$

<u>Motivação:</u> $n=7$ $\mathbb{Z}_7 = \{0,1,2,3,4,5,6\}$

$$\mathbb{Z}_7^* = \underbrace{\{a \in \mathbb{Z}_7 : (a,7)=1\}}_{\text{grupo dos elementos de } \mathbb{Z}_7 \text{ invertíveis}} = \{1,2,3,4,5,6\}$$

grupo cíclico gerado por $g$

$\langle g \rangle := \{g^\alpha\}_{\alpha=0}$

$\langle 1 \rangle = \{1\}$

$\langle 2 \rangle = \{1,2,4\}$

$o(2) = 3$

O menor $k>0$ t.q. $g^k=1$ chama-se a ordem de $g$ $o(g)$

<u>Teorema de LAGRANGE</u>: $o(g) \mid \#G$

$$\langle 3 \rangle = \{\underset{3^0}{1}, \underset{3^1}{3}, \underset{3^2}{2}, \underset{3^3}{6}, \underset{3^4}{4}, \underset{3^5}{5}\}$$

$$\forall b \in \mathbb{Z}_7^*, \exists!\, 0 \le k < \varphi(7) : b \equiv 3^k \mod 7$$

$k$ é o índice ou logaritmo discreto

Encontrar $k$ é o PLD (Problema do logaritmo discreto)

<u>Outro exemplo:</u> $\mathbb{Z}_8 = \{0,1,\dots,7\}$ $\varphi(8) = \varphi(2^3) = 2^3 - 2^2 = 4$

$\mathbb{Z}_8^* = \{1,3,5,7\}$

$\langle 3 \rangle = \{3,1\}$ $o(3) = 2$

$\langle 5 \rangle = \{5,1\}$

$\langle 7 \rangle = \{7,1\}$

$n \in \mathbb{N}$. Dizemos que $r \in \mathbb{Z}_n^* = \{\alpha \in \mathbb{Z}_n : (\alpha, n) = 1\}$

é raiz primitiva de $n$ se $\langle r \rangle = \mathbb{Z}_n^*$

onde $\langle r \rangle = \{ r^i : i = 1, \dots, \varphi(n) \}$

$b \in \mathbb{Z}_n^*$, $b \equiv r^k \bmod n$

$k = \operatorname{ind}_r b$ índice de $b$ na base $r$

$= \log_r b$ logaritmo

TEOREMA: Todo o primo tem raiz primitiva

Isto é, $p$ primo, $\exists r \in \mathbb{Z}_p^* : \langle r \rangle = \mathbb{Z}_p^*$

## Protocolo de troca de Chaves Diffie - Hellman

$p$ primo, $r$ r.p. de $p$

Alice escolhe $1 < a < p-1$

Bob escolhe $1 < b < p-1$

Alice envia $r^a$ a Bob

Bob envia $r^b$ a Alice

Alice calcula $(r^b)^a \mod p$
$\qquad\qquad\qquad\qquad\;\; \shortparallel$
Bob calcula $(r^a)^b \mod p$

---

# RESÍDUOS QUADRÁTICOS

$p$ primo $\qquad a$ t.q. $p \nmid a$

$a$ é resíduo quadrático de $p$ se

$$\exists x : x^2 \equiv a \mod p$$

<u>SÍMBOLO DE LEGENDRE</u>: $p$ primo, $a \in \mathbb{Z}$

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{se } p \mid a \\ 1 & \text{se } a \text{ é r.q. de } p \\ -1 & \text{se } a \text{ é n-r.q. de } p \end{cases}$$

<u>LEI DA RECIPROCIDADE QUADRÁTICA</u> $\quad p, q$ primos ímpares $\neq$'s

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \qquad \left(\frac{2}{p}\right) = \begin{cases} 1 & \text{se } p \equiv \pm 1 \mod 8 \\ -1 & \text{se } p \equiv \pm 3 \mod 8 \end{cases}$$

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{q}{p}\right)$$

<u>Lema</u>. $p \neq 2$, $\begin{aligned} \varphi : \mathbb{Z}_p^* &\longrightarrow \{\pm 1\} \\ a &\longmapsto \left(\frac{a}{p}\right) \end{aligned}$ é um epimorfismo de grupos

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \quad ; \quad a \equiv b \mod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

# CRITÉRIO DE EULER

$p$ primo ímpar

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \mod p$$

# SÍMBOLO DE JACOBI

$n = \prod p_i^{\alpha_i}$ ímpar

$$\left(\frac{a}{n}\right) = \prod \left(\frac{a}{p_i}\right)^{\alpha_i}$$

$$\left(\frac{7}{15}\right) = \left(\frac{7}{3 \cdot 5}\right) = \left(\frac{7}{3}\right)\left(\frac{7}{5}\right)$$

# LRQ.

$(m, n) = 1$, $m, n$ ímpares

$$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}} \left(\frac{n}{m}\right)$$

$a \equiv b \mod n \Rightarrow \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$

$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$