# SÍMBOLO DE LEGENDRE

mdc $(a, p) = 1$

$2 \neq p$ primo

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

$a$ é resíduo quadrático se

$$\exists x \in \mathbb{Z}_p : \quad x^2 \equiv a \pmod{p}$$

- $a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
- $\left(\frac{a^2}{p}\right) = 1$
- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Critério de Euler $\qquad a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$

LRQ $\qquad p, q$ primos $\neq$s, ímpares

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

- $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{se } p \equiv 1 \pmod{4} \\ -1 & \text{se } p \equiv -1 \pmod{4} \end{cases}$
- $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{se } p \equiv \pm 1 \pmod{8} \\ -1 & \text{se } p \equiv \pm 3 \pmod{8} \end{cases}$

## SÍMBOLO DE JACOBI

$n$ ímpar

$n = \prod_{i=1}^{k} p_i^{\alpha_i}$

$a$ t.q. mdc $(a, n) = 1$ $\qquad \left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{\alpha_i}$

LRQ $\qquad m, n$ ímpares, mdc $(m, n) = 1$ $\qquad \left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\times\frac{n-1}{2}} \left(\frac{n}{m}\right)$