$(a,p)=1$; a é resíduo quadrático de p se (r.q.)

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

<u>SÍMBOLO DE LEGENDRE</u>: $\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{se } (a,p)\neq 1 \\ 1 & \text{se } a \text{ é r.q.} \\ -1 & \text{se } a \text{ é n-r.q.} \end{cases}$

<u>CRITÉRIO DE EULER</u>: $(a,p)=1$, $2\neq p$ primo

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

$\nexists x \in \mathbb{Z}_7^* : x^2 \equiv 3 \mod 7$

$$\left(\frac{3}{7}\right) \equiv 3^{\frac{7-1}{2}} \mod 7 \equiv 3^3 \mod 7 \equiv \underbrace{3^2}_{\equiv 2}\cdot 3 \mod 7$$

$$\equiv 6 \mod 7 \equiv -1$$

$\left(\frac{3}{7}\right) = -1$

$\left(\frac{\cdot}{p}\right) : \mathbb{Z}_p^* \to \{-1;+1\}$

$a \mapsto \left(\frac{a}{p}\right)$

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

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

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

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

L.R.Q. p, q primos $\neq$'s ímpares

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

Símbolo de Jacobi $n = \prod p_i^{\alpha_i}$, $p_i \neq 2$

$(a,n) = 1$; $\left(\frac{a}{n}\right) = \prod \left(\frac{a}{p_i}\right)^{\alpha_i}$

$$\left(\frac{5}{21}\right) = \left(\frac{5}{3\cdot 7}\right) = \left(\frac{5}{3}\right)\left(\frac{5}{7}\right) = \underbrace{\left(\frac{2}{3}\right)}_{=-1} \underbrace{(-1)^{\frac{5-1}{2}\cdot\frac{7-1}{2}}}_{=1} \underbrace{\left(\frac{7}{5}\right)}_{=\underbrace{\left(\frac{2}{5}\right)}_{-1}} = 1$$

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

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

L.R.Q. m, n ímpares $(m,n) = 1$

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

Teste de Primalidade SOLOVAY-STRASSEN

n passa o teste S-S na base b, $(b,n) = 1$

se $\left(\frac{b}{n}\right) \equiv b^{\frac{n-1}{2}} \mod n$

A probabilidade de n passar o teste p/ k bases, sendo n composto, é $< \frac{1}{2^k}$

Como calcular x: $x^2 \equiv a \mod p$, c/ $\left(\frac{a}{p}\right)=1$

$\rightarrow$ $p \equiv 3 \mod 4$ $\qquad b := a^{\frac{p+1}{4}} \mod p$

mostra-se que $b^2 \equiv a \mod p$ (usar C. Euler)

$\rightarrow$ $p \equiv 1 \mod 4$ $\qquad$ não se conhece algoritmo P determinista

$\left(\frac{a}{p}\right)=1$

$$\mathbb{Z}_p[x] / (x^2-a) = \{ \alpha x + \beta : \alpha, \beta \in \mathbb{Z}_p \}$$

$$(\alpha_1 x + \beta_1) + (\alpha_2 x + \beta_2) = (\alpha_1 + \alpha_2) x + (\beta_1 + \beta_2)$$

$$(\alpha_1 x + \beta_1)(\alpha_2 x + \beta_2) = (\alpha_1 \beta_2 + \alpha_2 \beta_1) x + (\beta_1 \beta_2 + \alpha_1 \alpha_2 a)$$

$\alpha_1 \alpha_2 \underset{a}{\underset{\shortparallel}{x^2}} = \alpha_1 \alpha_2 a$

$x^2 - a = 0 \Rightarrow x^2 = a$

Sejam $b, c \in \mathbb{Z}_p^*$ t.q. $b^2 \equiv a \equiv c^2 \mod p$

$f, g : R = \mathbb{Z}_p[x] / (x^2-a) \longrightarrow \mathbb{Z}_p$ $\qquad$ homomorfismo de anéis

$\mu x + \nu \longmapsto f(\mu x + \nu) = \mu b + \nu$

$g(\mu x + \nu) = \mu c + \nu$

$\varphi : R \longrightarrow \mathbb{Z}_p \times \mathbb{Z}_p$ $\qquad$ hom. de anéis

$\mu x + \nu \longmapsto (f(\mu x + \nu), g(\mu x + \nu)) = (\mu b + \nu, \mu c + \nu)$

$\to z \in \mathbb{Z}_p^*$ fg. $\quad \exists\, u, v \in \mathbb{Z}_p$:

$$(1+zx)^{\frac{p-1}{2}} = ux+v$$

Se $u=0$,

Vamos então supor que $(1+zx)^{\frac{p-1}{2}} = ux+v$ c/ $u \neq 0$

Substituindo x por b,

$$(1+zb)^{\frac{p-1}{2}} \equiv ub+v \mod p$$

$$\Rightarrow \left((1+zb)^{\frac{p-1}{2}}\right)^2 \equiv (ub+v)^2 \mod p$$

$$\Rightarrow (ub+v)^2 \equiv (1+zb)^{p-1} \mod p$$

$$\Rightarrow \begin{cases} 1+zb \equiv 0 \mod p \\ ub+v \equiv \pm 1 \mod p \end{cases} \Rightarrow \begin{cases} ub+v \equiv 0 \mod p \\ ub+v \equiv \pm 1 \mod p \end{cases}$$

Teor. EULER

$(a,n)=1 \Rightarrow a^{\varphi(n)} \equiv 1 \mod n$

$\left.\begin{array}{l} p \text{ primo} \\ p \nmid a \end{array}\right| \Rightarrow a^{p-1} \equiv 1 \mod p$

$ub+v=0$ em $\mathbb{Z}_p \Rightarrow b = -\frac{v}{u}$

$ub+v=1$ em $\mathbb{Z}_p \Rightarrow b = \frac{1-v}{u}$

$ub+v=-1$ em $\mathbb{Z}_p \Rightarrow b = \frac{-1-v}{u}$

testamos qual b satisfaz $b^2 \equiv a \mod p$

Curvas Elípticas

Defn. Uma curva elíptica sobre $\mathbb{F}$ corpo é uma curva definida por uma equação da forma

$$y^2 = x^3 + ax + b \quad , \quad a, b \in \mathbb{F}$$

$$-16(4a^3 + 27b^2) \neq 0$$

$$E_{a,b} = \{ (x,y) \in \mathbb{F} \times \mathbb{F} : y^2 = x^3 + ax + b \} \cup \{ \mathcal{O} \}$$

"Soma" de $P, Q \in E$

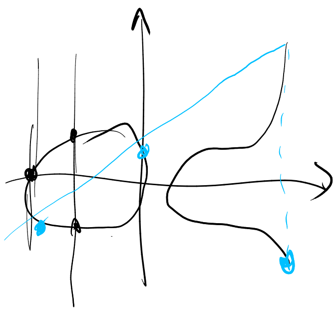
Se $P = \mathcal{O}$ então $P + Q = Q$

Se $Q = \mathcal{O}$ então $P + Q = P$

Se $P \neq \mathcal{O}$ e $Q \neq \mathcal{O}$ então $P = (p_1, p_2)$

$Q = (q_1, q_2)$

Se $p_1 = q_1$ e $p_2 = -q_2$ então $P + Q = \mathcal{O}$



Seja
$$\lambda = \begin{cases} \dfrac{3p_1^2 + a}{2p_2} & \text{se } P = Q \\[2ex] \dfrac{p_2 - q_2}{p_1 - q_1} & \text{se } P \neq Q \end{cases}$$

Então $P + Q = (\lambda^2 - p_1 - q_1, -\lambda\mu - \nu)$

Com $\nu = p_2 - \lambda p_1$, $\mu = \lambda^2 - p_1 - q_1$

Teor. $(E_{a,b}, +)$ é um grupo abeliano c/ id. $\mathcal{O}$

Defn. $\mathbb{F}$ corpo

se $\operatorname{car} \mathbb{F} \neq 2, 3$ (i.e. $1+1 \neq 0$; $1+1+1 \neq 0$)

$$E(\mathbb{F}) = \{(x,y) \in \mathbb{F} \times \mathbb{F} : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

$$-16(4a^3 + 27b^2) \neq 0$$

$\mathbb{F} = \mathbb{Z}_p$

$p \neq 2, 3$

$p \nmid (4a^3 + 27b^2)$

Curva Elíptica sobre $\mathbb{Z}_n$ $(n, 6) = 1$

$$(n, 4a^3 + 27b^2) = 1$$