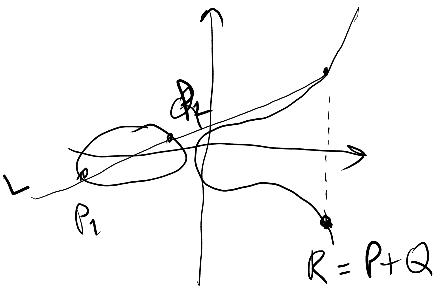
Teorema. $(E; +)$ é um grupo abeliano c/ id $\mathcal{O}$.



$P_1, P_2 \in E$, $P_i \neq \mathcal{O}$, $P_1 \neq P_2$

$P_1 = (x_1, y_1)$ $P_2 = (x_2, y_2)$, $x_1 \neq x_2$

L recta definida por P_1 e P_2

$y = y_1 + (x - x_1)\lambda$, $\lambda \in \mathbb{F}$

$y^2 = x^3 + ax + b \Rightarrow (y_1 + (x-x_1)\lambda)^2 = x^3 + ax + b$

$\Rightarrow f(x) = x^3 - \lambda^2 x^2 + \dots = 0$

Como P_1 e P_2 estão em $L \cap E$ então

$f(x_1) = f(x_2) = 0$

i.e., x_1 e x_2 são raízes de $f(x)$

$(x - x_1) \mid f(x)$; $(x - x_2) \mid f(x)$

$\Rightarrow (x - x_1)(x - x_2) \mid f(x)$

$\Rightarrow \underbrace{f(x)}_{\text{mónico}} = (x - x_1)(x - x_2) g(x) \Rightarrow g(x) = x - x_3$

$(x - x_3) \mid f(x) \Rightarrow x_3$ é raiz de $f(x)$

$f(x) = (x - x_3) h(x) \Rightarrow f(x_3) = (x_3 - x_3) h(x_3) = 0$

$f(x) = (x - x_1)(x - x_2)(x - x_3) = x^3 - x^2(x_1 + x_2 + x_3) + \dots$

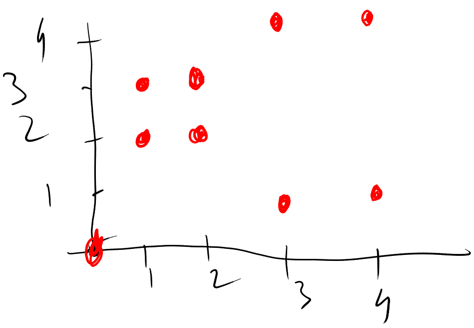
$$\Rightarrow \quad \lambda^2 = x_1 + x_2 + x_3 \quad \Rightarrow \quad x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = -\left(y_1 + (x_3 - x_1)\lambda\right) \qquad P_1 + P_2 = (x_3, y_3)$$

4

$E: \; y^2 = x^3 + 3x$ sobre $\mathbb{Z}_5$

$$E = \{\mathcal{O}, (0,0), (1,2), (1,3), (2,2), (2,3), (3,1), (3,4), (4,1), (4,4)\}$$



$x = 0: \; y^2 = 0 \Rightarrow y = 0$ em $\mathbb{Z}_5$

$x = 1: \; y^2 = 4 \Rightarrow y = 2 \vee y = 3$

$x = 2: \; y^2 = 4 \Rightarrow y = 2 \vee y = 3$

$x = 3: \; y^2 = 2 + 4 = 1 \Rightarrow y = 1 \vee y = 4$

$x = 4 = -1: \; y^2 = -1 - 3 = -4 = 1 \Rightarrow y = 1 \vee y = 4$

$O(E) = \# E = 10$

$E: y^2 = x^3 + x + 2$ em $\mathbb{Z}_5$

$4a^3 + 27b^2 \neq 0$ em $\mathbb{Z}_5$

$a = 1; \; b = 2$

$4 \cdot 1 + \underbrace{2 \cdot 2^2}_{=3} = 2 \neq 0$

$x = 0: \; y^2 = 2$ em $\mathbb{Z}_5$

$$\left(\frac{2}{5}\right) = -1 \qquad \left(\frac{2}{p}\right) = \begin{cases} 1 & \text{se } p \equiv \pm 1 \bmod 8 \\ -1 & \text{se } p \equiv \pm 3 \bmod 8 \end{cases}$$

$x = 1: \; y^2 = 4 \Rightarrow y = 2 \vee y = 3 \qquad (1,2), (1,3) \in E$

$x=2: \quad y^2=2$

$x=3: \quad y^2=2$

$x=4: \quad y^2=0 \Rightarrow y=0 \qquad (4,0)$
$=-1$

<u>Teor.</u> $E: y^2=x^3+ax+b$, sobre $\mathbb{Z}_p$,

$$\#E = 1+p+\underbrace{\sum_{x\in\mathbb{Z}_p}\left(\frac{x^3+ax+b}{p}\right)}_{=\varepsilon} = 1+p+\varepsilon$$

$$\sum_{x\in\mathbb{Z}_p}\left(\left(\frac{x^3+ax+b}{p}\right)+1\right) = \sum_{x\in\mathbb{Z}_p}\left(\frac{x^3+ax+b}{p}\right) + \underbrace{\sum_{x\in\mathbb{Z}_p}1}_{=p}$$

<u>TEOREMA DE HASSE</u> $\quad |\varepsilon| \leq 2\sqrt{p}$

MASSEY-OMURA

1) Alice & Bob escolhem E c.e.

$P \in E$; $\#E = N$

2) Alice escolhe e_A, d_A t.q. $d_A = e_A^{-1} \bmod N$

Bob " e_B, d_B t.q. $d_B = e_B^{-1} \bmod N$

3) Alice quer enviar P a Bob

a) Alice envia $e_A P$

b) Bob envia $e_B(e_A P)$

c) Alice envia $d_A(e_B(e_A P))$

d) Bob calcula $d_B(d_A(e_B(e_A P))) = P$

Menezes - Vanstone

$$\underbrace{(E, P, Q)}_{\text{Ch pub.}} \qquad Q = aP$$

$$a = \text{ch priv.}$$

Alice pretende cifrar $m = (m_1, m_2) \in \mathbb{Z}_p^* \times \mathbb{Z}_p^*$

Escolhe k qq. , calcula $(y_1, y_2) = kQ$

$$C_0 = kP$$

$$C_1 = y_1 m_1 \bmod p \ ; \ C_2 = y_2 m_2 \bmod p$$

Bob recebe $C = (C_0, C_1, C_2)$ e calcula

$$aC_0 = akP = k(aP) = kQ = (y_1, y_2)$$

obtendo

$$\left(C_1 \cdot y_1^{-1}, C_2 \cdot y_2^{-1}\right) = (m_1, m_2) = m$$