Hola!

alvaro@uconn.edu

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^{R_{E/\mathbb{Q}}}$$

(puntos en $E(\mathbb{Q})$ + geometrica)

grupo abeliano

ej $y^2 = x^3 + 1$

$$E(\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z}$$

$$E(\mathbb{Q}) \xrightarrow{\cong} \mathbb{Z}/6\mathbb{Z}$$

$$P \longmapsto 1 \bmod 6$$

Ej $y^2 = x^3 + 2x^2 - 3x$

$$E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$$

$$\cong \langle (0,0), (3,6) \rangle$$

P $\quad$ Q

$P, 2P = O, Q, 2Q, 3Q, 4Q = O$

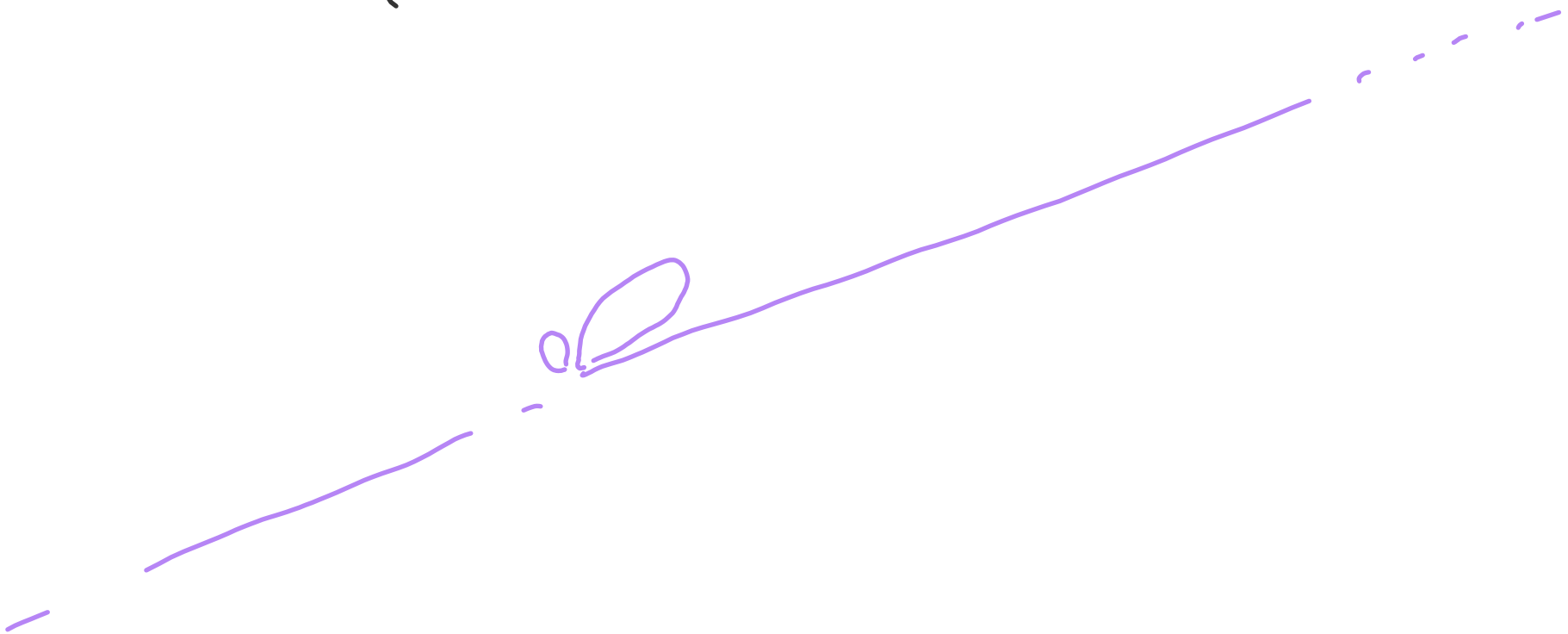
$P+Q, P+2Q, P+3Q$

$T = P+Q, \; 2T = 2Q, \; 3T = P+3Q$

$4T = O$

Ej

$$E(\mathbb{Q}) \cong \mathbb{Z}/2 \oplus \mathbb{Z}/4 \oplus \mathbb{Z}$$



Ej $(1,0), (0,1), (1,1) \in \mathbb{R}^2$

$(1,0) + (0,1) - (1,1) = (0,0)$

$\langle (1,0), (0,1), (1,1) \rangle = \langle (1,0), (0,1) \rangle$

Ej $(3,2), (4,3), (5,-7) \in \mathbb{Z}^2$

Ej $y^2 + y = x^3 - 7x + 6$

$P = (2, 0)$, $Q = (0, -3)$, $R = (8, -22)$

(2) son independientes ???

$$\{ n \cdot P \oplus m Q : n, m \in \mathbb{Z} \} \overset{?}{\ni} R$$

(Respuesta: sí! $E(\mathbb{Q}) \cong \mathbb{Z}^3$)

Def La altura simple o ingenua de $\frac{m}{n} \in \mathbb{Q}$

$\gcd(m,n) = 1$

- $h\left(\frac{m}{n}\right) = \log\left(\max(|m|, |n|)\right)$

ej $h\left(\frac{2}{5}\right) = \log(5)$

- La altura simple de $P = (x_0, y_0) \in E(\mathbb{Q})$

$$H(P) = h(x_0)$$

Ex $y^2 + y = x^3 - 7x + 6$

$P = (2, 0)$, $3P = \left(\frac{913}{361}, \dots\right)$

$$H(P) = \log(2)$$

$$H(3P) = \log(\max(19931, 13611))$$

$$= \log(913)$$

Def La altura canónica de $E(\mathbb{Q})$

$$\hat{h}(P) = \frac{1}{2} \cdot \lim_{N \to \infty} \frac{H(2^N \cdot P)}{4^N}$$

Prop (Neron-Tate)

(1) $\forall P, Q \in E(\mathbb{Q})$

$$\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$$

(2) $\forall P \in E(\mathbb{Q}) \quad \forall m \in \mathbb{Z} \quad \hat{h}(mP) = m^2 \cdot \hat{h}(P)$

(3) $\hat{h}(P) \geq 0$, $\hat{h}(P) = 0 \iff P$ es de torsión

Def Emparejamiento de Neron-Tate.

$$\langle \cdot, \cdot \rangle : E(\mathbb{Q}) \times E(\mathbb{Q}) \longrightarrow \mathbb{R}$$

$$\langle P, Q \rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$$

Matriz del emparej:

$$\mathcal{H}(\{P_i\}_{i=1}^r) = \begin{pmatrix} \langle P_1, P_1 \rangle & \langle P_1, P_2 \rangle & \cdots \\ \langle P_2, P_1 \rangle & & \\ & \ddots & \\ & & \ddots \\ & & \langle P_r, P_r \rangle \end{pmatrix} \left(\frac{E(\mathbb{Q})}{E(\mathbb{Q})_{tors}} \right)$$

TEOREMA

$\det(\mathcal{H}(\{P_i\})) = 0$

si y solo si los puntos $P_1, \ldots, P_r$ son dependientes!

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^R$$

$$\frac{E(\mathbb{Q})}{E(\mathbb{Q})_{tors}} \cong \mathbb{Z}^R$$

Teorema Sea $E/\mathbb{Q}$ una curva elíptica dada por

$$y^2 = x^3 + Ax^2 + Bx \quad , \quad A, B \in \mathbb{Z}$$

Sea R_E el rango de $E(\mathbb{Q})$. Entonces

$$R_E \leq \nu(A^2 - 4B) + \nu(B) - 1$$

donde $\nu(N)$ = Número de divisores primos de N.

$\nu(4) = 1$

(ej. $\nu(5) = 1$, $\nu(15) = 2$

Ej $y^2 = x(x+1)(x+2) = x^3 + 3x^2 + 2x$

$\Rightarrow R_E \leq \nu(1) + \nu(2) - 1 = 0 + 1 - 1 = 0$

$\Rightarrow \boxed{R_E = 0}$

$$y^2 = x(x+1)(x+2)$$

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^0$$

$$\cong E(\mathbb{Q})_{tors}$$

y $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

$$\| \quad \langle (0,0), (-1,0) \rangle$$

$$\Rightarrow E(\mathbb{Q}) = \{ \mathcal{O}, (0,0), (-1,0), (-2,0) \}$$

Ej $y^2 = x(x+5)(x+10)$

$= x^3 + 15x^2 + 50x$

$R_E \leq \nu(A^2 - 4B) + \nu(B) - 1$

$= \nu(25) + \nu(50) - 1$

$= 1 + 2 - 1 = 2$

$$\boxed{R_E \leq 2}$$

Busco puntos. $(-9, 6)$, $(40, 300)$ $\Longrightarrow R_E \geq 1$

$(-9,6)$: orden ∞

$(40, 300)$: no es indep.

Conjetura de Birch y Swinnerton-Dyer ($1M)

Función L de Hasse y Weil. $(E/\mathbb{Q})$

$$L(E,s) \quad s \in \mathbb{C}$$

$$L(E,s) = \prod_p \left(L_p(E,p^{-s})\right)^{-1}$$

$$L_p(E,T) = \begin{cases} 1 - a_p T + p T^2 \\ 1 - a_p T \\ 1 \end{cases}$$

$a_p = p + 1 - \#E(\mathbb{F}_p)$

- p buena reducción
- p mala reducción multiplicativa
- p mala red aditiva.

BSD

Taylor en $s=1$

(1) $L(E,s) = \lambda_E (s-1)^{R_{E/\mathbb{Q}}} + \frac{1}{2}(s-1)^{R_{E/\mathbb{Q}}+1} + \cdots$

tiene un zero en $s=1$

de orden igual al rango de $E/\mathbb{Q}$

(2) λ_E = formula que depende

de invariantes especificos de $E/\mathbb{Q}$.

Método de Descenso (completo)

$$y^2 = (x - e_1)(x - e_2)(x - e_3)$$

$$y_0^2 = (x_0 - e_1)(x_0 - e_2)(x_0 - e_3)$$

$$\begin{cases} x_0 - e_1 = a \cdot u^2 \\ x_0 - e_2 = b \cdot v^2 \\ x_0 - e_3 = c \cdot w^2 \end{cases}$$

$$a \cdot b \cdot c = \square = \frac{y_0^2}{(uvw)^2}$$

Ej $y^2 = x^3 - 556x + 3120$

$e_1 = 6, \quad e_2 = 20, \quad e_3 = -26$

$P = (-8, 84), \quad Q = (24, 60)$

$S = P + Q = \left(-\frac{247}{16}, -\frac{5733}{64}\right)$

$X(P) - e_1 = -14 \cdot 1^2$

$X(P) - e_2 = -7 \cdot 4^2$

$X(P) - e_3 = 2 \cdot 3^2$

$-14 \cdot -7 \; 2 = 14^2$

$X(Q) - e_1 = 2 \cdot 3^2$

$X(Q) - e_2 = 2^2$

$X(Q) - e_3 = 2 \cdot 5^2$

$2 \cdot 1 \cdot 2 = 4 = 2^2$

$$X(P) - e_1 = -14 \cdot 1^2$$
$$X(P) - e_2 = -7 \cdot 4^2$$
$$X(P) - e_3 = 2 \cdot 3^2$$
$$-14 \cdot -7 \; 2 = 14^2$$

$$X(Q) - e_1 = 2 \cdot 3^2$$
$$X(Q) - e_2 = 2^2$$
$$X(Q) - e_3 = 2 \cdot 5^2$$
$$2 \cdot 1 \cdot 2 = 4 = 2^2$$

$$S = P + Q$$

$$X(S) - e_1 = -7 \cdot (7/4)^2$$
$$X(S) - e_2 = -7 \cdot (9/4)^2$$
$$X(S) - e_3 = \left(\frac{13}{4}\right)^2$$

	P	Q	S
a	-14	2	-7
b	-7	1	-7
c	2	2	1



Teorema Sea $E/\mathbb{Q}$ c. ell.

$$y^2 = x^3 + Ax + B = (x-e_1)(x-e_2)(x-e_3). \quad e_i \neq e_j$$

$$e_1 + e_2 + e_3 = 0$$

Entonces, existe un homomorfismo de grupos:

$$\delta : E(\mathbb{Q}) \longrightarrow \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$$

tal que $\delta(P) = \delta((x_0, y_0))$

$$\delta(P) = \begin{cases} (1,1,1) & \text{si } P = \mathcal{O} \\ (x_0 - e_1,\ x_0 - e_2,\ x_0 - e_3) & \text{si } y_0 \neq 0 \\ ((e_1-e_1)(e_1-e_3),\ (e_1-e_1),\ e_1-e_3) & \text{si: } P = (e_1, 0) \\ (e_2-e_1,\ (e_2-e_1)(e_2-e_3),\ e_2-e_3) & \text{si: } P = (e_2, 0) \\ (e_3-e_1,\ e_3-e_2,\ (e_3-e_1)(e_3-e_2)) & \text{si: } P = (e_3, 0) \end{cases}$$

Adem's:

- $\delta(P) = (\delta_1, \delta_2, \delta_3)$

  tiene $\delta_1 \cdot \delta_2 \cdot \delta_3 = 1$ $\quad (\in \mathbb{Q}^\times / (\mathbb{Q}^\times)^2)$

- $\ker(\delta) = 2 \cdot E(\mathbb{Q})$

  $= \{ 2P : P \in E(\mathbb{Q}) \}$

$\left(\delta(Q) = 0 \Longrightarrow Q = 2P \right)$

Ej $y^2 = x^3 - 556x + 3170$

$e_1 = 6$

$e_2 = 20$

$e_3 = -26$

$E(\mathbb{Q}) \simeq \mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}^2$

$= \langle T_1 = (6,0),\ T_2 = (20,0),$

$P = (-8,84),\ Q = (24,60) \rangle$

$\delta(T_1) = (-7,-14,2)$

$\delta(T_2) = (14,161,46)$

$\delta(P) = (-14,-7,2)$

$\delta(Q) = (2,1,2)$

$\Rightarrow \#\delta\left(\frac{E(\mathbb{Q})}{2E(\mathbb{Q})}\right) = 16$

Prop Si $\delta(P) = (\delta_1, \delta_2, \delta_3)$

$\delta_i \in \mathbb{Q}^\times / (\mathbb{Q}^\times)^2$

y si: $p \mid \delta_i$

entonces $p \mid (e_1 - e_2)(e_1 - e_3)(e_2 - e_3) \stackrel{=}{:} \Delta$.

$$\Rightarrow \quad \int : E(\mathbb{Q}) / 2E(\mathbb{Q}) \hookrightarrow \Gamma \subseteq \mathbb{Q}^\times / (\mathbb{Q}^\times)^2$$

$\Rightarrow$ COTAS DEL RANGO.

(f_1, f_2, f_3) t.q. si $p \mid \delta_i \Rightarrow p \mid \Delta$.

$$\begin{cases} y^2 = (x-e_1)(x-e_2)(x-e_3) \\ x - e_1 = \delta_1 \cdot u^2 \\ x - e_2 = \delta_2 \cdot v^2 \\ x - e_3 = \delta_3 \cdot w^2 \end{cases}$$

$$\Longrightarrow C = \mathbb{C}(\delta_1, \delta_2)$$

$$\begin{cases} e_1 - e_2 = \delta_2 Y^2 - \delta_1 X^2 \\ e_3 - e_2 = \delta_2 Y^2 - \delta_1 \delta_2 Z^2 \end{cases}$$