# Curvas elípticas y el grupo 2-Selmer

Gonzalo Tornaría

Universidad de la República
Uruguay

LATeN
Seminario Latinoamericano de Teoría de Números

23 de abril, 2020

Trabajo conjunto con Daniel Barrera y Ariel Pacetti

arXiv:2001.02263

(1) Descenso de Fermat $x^4+y^4=z^2$

No tiene puntos racionales con $xyz\neq 0$

P con coordenadas enteras ⟶ P' "más pequeño" ⇒ $y^2=x^3+x$

Curvas elípticas $E: y^2=F(x)$ F cúbico, mónico sin R.R.

$K=\mathbb{Q}$

$E(\mathbb{Q})=\{P\in E$ con coordenadas en $\mathbb{Q}\}\cup\{\mathcal{O}\}$

es un grupo abeliano.

$h: E(\mathbb{Q})\to\mathbb{R}$ "altura"

(A) $\{P : h(P)<k\}$ es finito $\forall k\in\mathbb{R}$

(B) "Asintóticamente" $h$ crece cuadráticamente.

$h((x,y))=\log(\max(|p|,|q|))$ $x=\frac{p}{q}$

Supongamos: $E(Q) = 2E(Q)$

Sea $P = \mathcal{O}$ $\quad P = 2P_1$, $P_1 = 2P_2$, .....

$$h(P_1) \leq \frac{1}{4} h(P) + C$$

$$h(P_2) < \frac{1}{4} h(P_1) + C < \frac{1}{16} h(P) + \left(1 + \frac{1}{4}\right) C$$

$$\vdots$$

$$h(P_t) < \frac{1}{4^t} h(P) + 2C$$

$\{P : h(P) \leq 2C + \xi\}$ genera $E(Q)$

es finitamente generado.

Teorema de Mordell (Weil) $\quad K$ $\quad E(Q)$ es f.g.

$\Rightarrow$ ① $E(Q)/2E(Q)$ es finito (M-W débil)

② argumento del descenso funciona.

$$E(Q) = T \oplus \mathbb{Z}^r$$

$$E(Q)/2E(Q) = T/2T \oplus \left(\mathbb{Z}/2\mathbb{Z}\right)^r$$

Thm de Mordell-Weil débil

$$y^2 = x(x-a)(x-b) \qquad a, b \in \mathbb{Z}$$

$$\delta : E(\mathbb{Q}) \longrightarrow \left(\frac{\mathbb{Q}^\times}{\mathbb{Q}^{\times 2}} \times \frac{\mathbb{Q}^\times}{\mathbb{Q}^{\times 2}} \times \frac{\mathbb{Q}^\times}{\mathbb{Q}^{\times 2}}\right) \square$$

$$(x,y) \longmapsto (x-a,\ x-b,\ x)$$

$$(a,0) \longmapsto (\ ?\ ,\ a-b\ ,\ a)$$

$$(b,0) \longmapsto (b-a\ ,\ ?\ ,\ b)$$

$$(0,0) \longmapsto (-a\ ,\ -b\ ,\ ?\ )$$

$$\mathcal{O} \longmapsto (1\ ,\ 1\ ,\ 1)$$

**Prop** $\delta$ es un homomorfismo de grupos

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

$$\delta : \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \hookrightarrow \left(\frac{\mathbb{Q}^\times}{\mathbb{Q}^{\times 2}}\right)^3 \square$$

$$\text{"}\supseteq\text{"} \quad \operatorname{Im}(\delta) = \delta(E)$$

Sup. $(\alpha, \beta, \alpha\beta) \in \delta(E)$ $\qquad \alpha, \beta \in \mathbb{Z}$ libres de $\square$

$\delta(x,y)$ "$=$"

$$\begin{cases} x - a = \alpha u^2 \\ x - b = \beta v^2 \\ x = \alpha\beta w^2 \\ y = \alpha\beta uvw \end{cases}$$

$$\mathcal{C}_{\alpha,\beta} : \begin{cases} \alpha\beta w^2 = \alpha u^2 + a \\ \alpha\beta w^2 = \beta v^2 + b \end{cases}$$

**Obs** Si $p \nmid 2ab(a-b) \Rightarrow \mathcal{C}_{\alpha,\beta}$ no tiene solución en $\mathbb{Q}_p$ $\Rightarrow \mathcal{C}_{\alpha,\beta}$ no tiene sol en $\mathbb{Q}$

$p \mid \alpha$ ó $p \mid \beta$

Corolario: $\exists\ p \mid \alpha\beta \Rightarrow p \mid 2ab(a-b)$

$\delta(E) \subseteq \{(\alpha, \beta, \alpha\beta) : \text{los primos que dividen a } \alpha, \beta \text{ son finitos}\}$

finito

finito

---

## El mapa de Kummer.

$K$ cuerpo $(\operatorname{car} K \neq 2)$

$y^2 = F(x) \qquad F(x) \in K[x]$

$A_K := K[T]/F(T)$ álgebra cúbica/$K$

$N \downarrow$

$K$

$\left(A_K^\times / A_K^{\times 2}\right)_{\square} = \{[\alpha] \in A_K^\times / A_K^{\times 2} : N(\alpha) \in (K^\times)^2\}$

Prop $\exists!$ un homomorfismo de grupos

$\delta_K : E(K)/2E(K) \hookrightarrow \left(A_K^\times / A_K^{\times 2}\right)_{\square}$ $\quad H^1(G_K, E[2]) \simeq$

$(x, y) \longmapsto x - T$

siempre que $x - T \in A_K^\times$

Mapa de Kummer

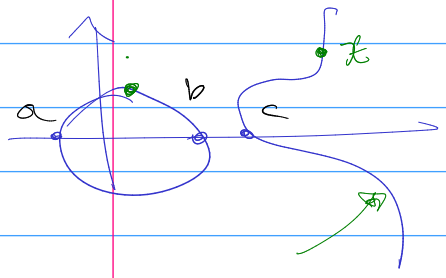
Corolario $E(K)/2E(K) \simeq \delta_K(E)$

Ejemplo 1 $F(x) = x(x-a)(x-b)$

$A_{\mathbb{Q}} \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}$

$T \mapsto (a, b, 0)$ y $S_{\mathbb{Q}}$ es el trivial

(2) $E/\mathbb{R}$ $\Delta(E) > 0$ $\quad A_{\mathbb{R}} \cong \mathbb{R} \times \mathbb{R} \times \mathbb{R}$




$T \mapsto a \quad b \quad c$

$\mathbb{R}^\times / \mathbb{R}^{\times 2} = \{+1, -1\}$

$S_{\mathbb{R}}(E) = \langle (+1, -1, -1) \rangle$

$2E(\mathbb{R})$

$\#E(\mathbb{R})/2E(\mathbb{R}) = 2$

---

(3) $k = \mathbb{Q}_p$ $\quad \mathcal{O} = \mathbb{Z}_p$

$F(x)$ irreducible/$\mathbb{Q}_p$

$A_k$ representación de $k$

$A_{\mathcal{O}}$ anillo enteros

$$\left( A_{\mathcal{O}}^\times / (A_{\mathcal{O}}^\times)^2 \right)_\square \subseteq A_k^\times / (A_k^\times)_\square$$

Prop $\quad S_{\mathbb{Q}_p}(E) \subseteq \left( A_{\mathcal{O}}^\times / (A_{\mathcal{O}}^\times)^2 \right)_\square$

Contar elementos

$p \neq 2$ es un $=$

$p = 2$ es una inclusión de índice 2.

## (3) El grupo 2-Selmer.

$K = \mathbb{Q}$

$\delta_{\mathbb{Q}} : E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow \left(A_{\mathbb{Q}}^{\times}/(A_{\mathbb{Q}}^{\times})^2\right)[2]$

$\delta(P)$

$\mathbb{Q} \subset \mathbb{Q}_p$

$A_{\mathbb{Q}} \subset A_{\mathbb{Q}_p}$

$P \in E(\mathbb{Q})$

$\delta_v : E(\mathbb{Q}_p)/2E(\mathbb{Q}_p) \longrightarrow \left(A_{\mathbb{Q}_p}^{\times}/(A_{\mathbb{Q}_p}^{\times})^2\right)[2]$

$P \in E(\mathbb{Q}_p)$

$\delta(P)$

$res_p$

$$Sel_2(E) := \left\{ c \in \left(A_{\mathbb{Q}}^{\times}/(A_{\mathbb{Q}}^{\times})^2\right)[2] : res_p(c) \in \delta_p(E_p) \ \forall p \text{ finito} \cdot \infty \right\}$$

$\delta$ : es finito

$$\delta_{\mathbb{Q}}(E) \subseteq Sel_2(E)$$

Nota

$$1 \to E(\mathbb{Q})/2E(\mathbb{Q}) \xrightarrow{\delta} Sel_2(E) \longrightarrow Ш(E)[2] \to 1$$

$E(\mathbb{Q})/2E(\mathbb{Q})$ — computable

$Sel_2(E)$ — computable

misterioso

Cotas para $\#Sel_2(E)$

$F(x)$ irreducible en $\mathbb{Q}$ $\quad \Delta(F) > 0$.

$A_{\mathbb{Q}}/\mathbb{Q}$ cúbica totalmente real

$v_1, v_2, v_3 \mid \infty$

$v_1(T) < v_2(T) < v_3(T)$

---

$H^1(G_m, E[m])$

$$C_*(E) := \{[\alpha] : (A_k^\times/(A_k^\times)^2)_{\mathfrak{P}} : A_k(\sqrt{\alpha})/A_k$$

no ramifica en lugares finitos,
no ramifica en $v_1$
ramifica en $v_2 \Leftrightarrow$ ramifica en $v_3$ $\}$

$$\tilde{C}(E) := \{[\alpha] : N(\alpha) = \square,\ v(\alpha) \text{ par para todo lugar finito},\ y\ v_1(\alpha) > 0\}$$

---

**Prop** $\quad C_*(E) \subseteq Sel_2(E) \subseteq \tilde{C}(E)$

---

**Relación con grupos de clases**

$$\mathrm{Frac}(A_k) \supseteq P \supseteq P^+ = \{(\alpha) : \alpha \gg 0\}.$$

$$Cl(A_k) = \frac{\mathrm{Frac}(A_k)}{P}$$

$$Cl^+(A_k) = \frac{\mathrm{Frac}(A_k)}{P^+}$$

$$P_*(E) = \{(\alpha) : v_1(\alpha) > 0,\ v_2(\alpha) \cdot v_3(\alpha) > 0\}$$

$$Cl_*(A_K, E) = \mathrm{Frac}(A_K) / P_*(E)$$

**Teorema** ① $C_*(E) \cong Cl_*(A_K, E)$ [2]

② $\left[\widetilde{C}(E) : C_*(E)\right] = 2$ [K:Q]

**Corolario**

$h_2 = 2$-rango de $Cl_*$

$s_2 = 2$-rango de $Sel_2(E)$

$\Rightarrow \quad h_2 \leq s_2 \leq h_2 + 1$ [K:Q]