1. Introducción

Sea E una curva elíptica definida sobre $\mathbb{Q}$:

$$E:\ y^2 + b_1 xy + b_3 y = x^3 + b_2 x^2 + b_4 x + b_6, \qquad b_i \in \mathbb{Z},\ \Delta_E \neq 0$$

Sabemos que $E(\mathbb{Q}) = \{(x,y) \in \mathbb{Q}^2$ que satisfacen la ec. de $E\}$ tiene estructura de gp. abeliano.

Teorema de Mordell: $E(\mathbb{Q})$ es finitamente generado, es decir

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E_{tors} \quad ; \quad \begin{array}{l} E_{tors} := \text{subgrupo de torsión},\ \#E_{tors} < \infty \\ r = \text{rango de } E(\mathbb{Q}) \end{array}$$

- Se saben muchas cosas de E_{tors}:

  1\) Mazur: $E_{tors} \simeq \begin{cases} \mathbb{Z}/n\mathbb{Z}, & 1 \leq n \leq 10,\ \text{ó } n = 12 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & 1 \leq n \leq 4 \end{cases}$ $\Rightarrow$ Controlamos E_{tors} uniformemente para toda E

  2\) Nagell-Lutz: dada una E concreta, nos da un algoritmo muy sencillo para calcular explícitamente E_{tors}.

- El invariante r es mucho más misterioso:

  1\) No se sabe si puede ser arbitrariamente grande (record $r=28$ Elkies)

  2\) No se tiene un algoritmo para, dada E, calcular $P_1, \to P_r \in E(\mathbb{Q})$ puntos independientes.

Se conjetura que r viene dado por el comportamiento de $L(E/\mathbb{Q}, s)$

$$E \text{ curva elíptica } /\mathbb{Q} \rightsquigarrow \underset{\text{función analítica}}{L(E/\mathbb{Q}, s)}$$

$\uparrow$ función L asociada a E; es una función de variable complej

Conjetura de Birch y Swinnerton Dyer: $\operatorname{rango}(E(\mathbb{Q})) = \operatorname{ord}_{s=1} L(E/\mathbb{Q}, s) =: r_{an}(E$

Teorema (Gross-Zagier 84, Kolyvagin 89, Wiles et.al 2001)

$$\text{Si } \operatorname{ord}_{s=1} L(E/\mathbb{Q}, s) \leq 1 \Rightarrow \operatorname{rango}(E(\mathbb{Q})) = \operatorname{ord}_{s=1} L(E/\mathbb{Q}, s)$$

Corolario: Si $\operatorname{ord}_{s=1} L(E/\mathbb{Q}, s) = 1 \Rightarrow E$ tiene un punto de orden infinito

Problema: calcular-lo ; **Solución**: método de los puntos de Heegner.

Estratégia: Teorema de Modularidad $\Rightarrow$ $\pi_E : X_0(N) \longrightarrow E$ morfismo exhausti

$N =$ conductor de E, $N \in \mathbb{Z}_{>0}$

$X_0(N) =$ curva modular de nivel N

$X_0(N)$
- curva definida sobre $\mathbb{Q}$: viene dada por $f_N(X,Y)=0$ $\quad f_N(X,Y) \in \mathbb{Q}[X,Y]$
- interpretación de moduli : $Q \in X_0(N)(\mathbb{C}) \leftrightarrow (A, C)$ $\quad$ A: curva elíptica/ $\quad$ C: subgrupo cíclic de A de orden

Idea: encontrar puntos algebraicos $Q \in X_0(N)(K)$

$$K/\mathbb{Q} \text{ extensión finita}$$

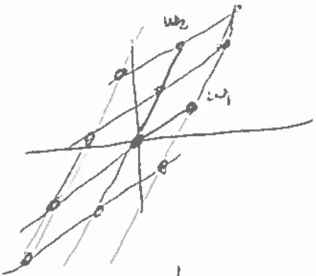
y considerar $P = \pi_E(Q) \in E(K)$

punto de Heegner: veremos que bajo ciertas condiciones $P \in E(\mathbb{Q})$ y tiene orden infinito

$X_0(N)$ tiene unos puntos algebraicos muy naturales a considerar: son los que corresponden con pares (A, C) donde A és lo que se llama una curva elliptica con multiplicación compleja.

2. Curvas elípticas con multiplicación compleja

Recordemos: un lattice complejo $\Lambda \subseteq \mathbb{C}$ es un subgrupo isomorfo a $\mathbb{Z} \times \mathbb{Z}$ tal que $\mathbb{R}\Lambda = \mathbb{C}$. Es decir, $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, $\omega_1, \omega_2 \in \mathbb{C}$ l.i sobre $\mathbb{R}$.



Sabemos que, dado Λ existe una curva elíptica $E_\Lambda / \mathbb{C}$ tal que

$$\Phi \quad \mathbb{C}/\Lambda \xrightarrow{\sim} E_\Lambda(\mathbb{C})$$
$$z \longmapsto (\wp(z), \wp'(z))$$

$$E_\Lambda : y^2 = 4x^3 - g_2 x - g_3$$

$$g_2 = 60 \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{\lambda^4}, \quad g_3 = 140 \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{\lambda^6}$$

$$\wp(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left[\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right]$$

Además:
- •) $\mathrm{End}(E_\Lambda) \simeq \{ \alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda \}$
- •) $\mathbb{C}/\Lambda_1 \cong \mathbb{C}/\Lambda_2 \iff \Lambda_1 = \alpha\Lambda_2$ para algún $\alpha \in \mathbb{C}$.

•) una "fuente natural" de lattices complejos (y por tanto de c.e.) són los cuerpos cuad. imaginarios

Ejemplo: $K = \mathbb{Q}(\sqrt{-7})$, $\omega = \frac{1+\sqrt{-7}}{2}$; $\omega^2 = \omega - 2$

$$\Lambda = \mathbb{Z}[\omega] = \{ a + b\omega \mid a, b \in \mathbb{Z} \} \simeq \mathbb{Z} \oplus \mathbb{Z}\omega \text{ es un lattice}$$

fijaos que, además, es un subanillo de $\mathbb{C} \Rightarrow \mathbb{Z}[\omega] \cdot \Lambda \subseteq \Lambda$

$$\Rightarrow \text{[illegible]} \quad \mathbb{Z}[\omega] \subseteq \mathrm{End}(E_\Lambda)$$

Ejercicio: comprobad que, de hecho, $\mathbb{Z}[\omega] = \mathrm{End}(E_\Lambda)$

Propiedad: $g_2(\Lambda), g_4(\Lambda) \in K \Rightarrow E_\Lambda$ está definida sobre K.

Este ejemplo no as un caso único: esto ocurre más en general.

Sea $K=\mathbb{Q}(\sqrt{D})$, $D\in\mathbb{Z}_{<0}$ un cuerpo cuadrático imaginario

Def/ Un orden de K es un subanillo de K de $\mathbb{Z}$-rango 2 ($\simeq\mathbb{Z}^2$ como gr

Todo K tiene un orden maximal, que se llama el anillo de enteros de K.

Proposición: El anillo de enteros $\mathcal{O}_K$ de K viene dado por $\mathbb{Z}[\omega]$

$$\omega=\begin{cases}\sqrt{D} & \text{si } D\equiv 2,3\ (4) \\ \frac{1+\sqrt{D}}{2} & \text{si } D\equiv 1\ (4)\end{cases}$$

(assumimos $\square\nmid D$)

Proposición: Sea $E/\mathbb{C}$ una curva elíptica. Entonces $\mathrm{End}(E)\simeq\begin{cases}\mathbb{Z} \\ \mathcal{O} \text{ un orden en un cuerpo cuadrático imaginario}\end{cases}$

dem/ $E\simeq\mathbb{C}/\langle\omega_1,\omega_2\rangle\simeq\mathbb{C}/\langle 1,\tau\rangle$, $\tau=\frac{\omega_2}{\omega_1}$

Sea α tal que $\alpha\langle 1,\tau\rangle\subseteq\langle 1,\tau\rangle$: $\begin{cases}\alpha\cdot 1=a+b\tau, & a,b\in \\ \alpha\cdot\tau=c+d\tau, & c,d\in\mathbb{Z}\end{cases}$

$\Rightarrow$ $\alpha\notin\mathbb{Z}$ y $\mathbb{Q}(\alpha)=\mathbb{Q}(\tau)$

$(a+b\tau)\tau=c+d\tau\Rightarrow b\tau^2+(a-d)\tau+c=0\Rightarrow\mathbb{Q}(\tau)$ es un cuerpo cuadrático imaginario

$$\mathbb{Z}\oplus\mathbb{Z}\alpha\subseteq\underset{\substack{\uparrow \\ \text{sabemos que es un subanillo}}}{\mathrm{End}(E)}\subseteq K=\mathbb{Q}(\tau)\Rightarrow\mathrm{End}(E)\text{ es un orden en }\mathbb{Q}(\tau)\qquad\square$$

Def/ $CM(\mathcal{O}_K)=\{E/\mathbb{C}:\ \mathrm{End}(E)=\mathcal{O}_K\}/\simeq$

Obs: $\mathbb{C}/\mathcal{O}_K\in CM(\mathcal{O}_K)$; pero también $\mathbb{C}/I$ para cualquier ideal fraccion $I\subseteq K$

def/ Un ideal fraccionario es un $\mathcal{O}_K$-módulo $I\subseteq K$ de rango 2

$Cl(K)=\{\text{ideales fraccionarios}\}/\sim$, $I\sim I'\Leftrightarrow I=\lambda I'$, $\lambda\in$

Teorema: $Cl(K)$ es un conjunto finito

Teorema: Sea K un cuerpo cuadrático imaginario tal que $\# Cl(K)=1$. Sea $E \in CM(\mathcal{O}_K)$. Entonces E admite una ecuación $y^2=x^3+ax+b$ con $a,b \in K$.

Obs 1: Si $\# Cl(K)=h$, entonces lo que podemos decir es que $a,b \in H$ con $[H:K]=h$; este H se llama el Hilbert class field de K.

Obs 2: $K=\mathbb{Q}(\sqrt{D})$, $\# Cl(K)=1 \Leftrightarrow D=-1,-2,-3,-7,-11,-19,-43,-67,163.$

•) A partir de ahora supongamos, para simplificar, que $h(K)=1$ (pero todo generaliza correctamente)

Puntos CM en $X_0(N)$

Def/ Dado $\tau \in \mathcal{H}=\{z \in \mathbb{C} : \mathrm{Im}(z)>0\}$, ~~sea~~ denotamos $A_\tau = \mathbb{C}/\Lambda_\tau$, $\Lambda_\tau = \langle 1,$

$$X_0(N)=\left\{ (A,B) \;\middle|\; \begin{array}{l} A/\mathbb{C}, B/\mathbb{C} \text{ curvas elípticas} \\ \text{con } A \xrightarrow{\phi} B \text{ isogenia, } \ker\phi \simeq \mathbb{Z}/N\mathbb{Z} \end{array} \right\} \Big/ \simeq$$

$$\Gamma_0(N)\backslash\mathcal{H} \simeq X_0(N)(\mathbb{C}) \simeq \{(X,Y) \in \mathbb{C}\times\mathbb{C} \mid f_N(X,Y)=0$$

$$\tau \xleftrightarrow{1:1} (A_\tau, A_{N\tau}) \longleftrightarrow (j(A_\tau), j(A_{N\tau}))\,)$$

$$\mathbb{C}/\langle 1,\tau\rangle \xrightarrow{\cdot N} \mathbb{C}/\langle 1,N\tau\rangle$$

$$x \longmapsto Nx$$

Por lo tanto: si A_τ y $A_{N\tau} \in CM(\mathcal{O}_K)$, K = cuad. imag., $\# Cl(K$

$\Rightarrow A_\tau$ y $A_{N\tau}$ estan def /K $\Rightarrow j(A_\tau), j(A_{N\tau}) \in K$

$\Rightarrow$ τ nos da un punto en $X_0(N)(K)$

Siguiente paso: dado K cuerpo cuadrático imaginario y $N\in\mathbb{N}$, cómo encontramos $\tau \in \mathcal{H}$ tal que $\mathrm{End}(A_\tau) \simeq \mathrm{End}(A_{N\tau}) \simeq \mathcal{O}_K$?

def/ $$\mathcal{O}_\tau = \{ \underset{\substack{\uparrow \\ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ \gamma\cdot\tau = \frac{a\tau+b}{c\tau+d}}}{\gamma \in M_2(\mathbb{Z}) \mid \gamma\cdot\tau = \tau} \} \cup \{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\} \subseteq M_2(\mathbb{Z})$$

Ejercicio: $\mathrm{End}(A_\tau) \simeq \mathcal{O}_\tau$

def/ $$\mathcal{O}_\tau^{(N)} = \{ \underset{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}{\gamma} \in M_2(\mathbb{Z}) \mid N|c \} \cup \{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\} \subseteq M_2(\mathbb{Z})$$

$$\mathcal{O}_\tau^{(N)} \cong \{ \alpha \in \mathbb{C} : \alpha\Lambda_\tau \subseteq \Lambda_\tau,\ \alpha\Lambda_{N\tau} \subseteq \Lambda_{N\tau} \} \simeq \mathrm{End}(A_\tau) \cap \mathrm{End}(A_{N\tau}$$

Hipótesis: todo primo $\ell | N$ es split en $K/\mathbb{Q}$ (i.e.

Entonces existe lo que se denomina un embedding optimal:

$$\iota : K \longrightarrow M_0(N) = \{\gamma \in M_2(\mathbb{Z}) \mid N|c\}$$

tal que $\iota(w) \in M_2(\mathbb{Z})$, $\mathcal{O}_K = \mathbb{Z}[w]$

Proposición: Sea $\iota : K \hookrightarrow M_0(N)$ un embedding optimal, ~~entonces~~
y sea $\gamma = \iota(w)$ con $\mathcal{O}_K = \mathbb{Z}[w]$.
Entonces existe un único $\tau \in \mathcal{H}$ tal que $\gamma\cdot\tau = \tau$ y además

$$\mathcal{O}_\tau^{(N)} \simeq \mathcal{O}_K .$$

Ejercicios:

Teorema de Modularidad

$E/\mathbb{Q}$ curva elíptica, $N = \text{cond}(E)$.

Vamos a dar varios enunciados equivalentes del teorema de modularidad

(Wiles, Taylor-Wiles, Breuil-Diamond-Conrad-Taylor, 2001)

Teorema: existe un morfismo exaustivo y definido sobre $\mathbb{Q}$

$$\phi : X_0(N) \longrightarrow E$$

Para hacerlo explícito, necesitamos hablar de la forma modular asociada a E:

- p primo, $a_p = p+1-\#E(\mathbb{Z}/p\mathbb{Z})$ ← número de soluciones de la ec. que define E "módulo p"
- definimos a_n, para todo n mediante:

$$L(E,s) := \prod_{p\nmid N} \frac{1}{1-a_p p^{-s}+p^{1-2s}} \prod_{p\mid N} \frac{1}{1-a_p p^{-s}} = \sum_{n\geq 1} a_n n^{-s}$$

- $a_{r\cdot s} = a_r \cdot a_s$ si $(r,s)=1$
- $a_{p^{r+1}} = \begin{cases} a_{p^r}\cdot a_p - p\, a_{p^{r-1}} & \text{si } p\nmid N \\ a_p^{r+1} & \text{si } p\mid N \end{cases}$
- $f_E(z) := \sum_{n\geq 1} a_n e^{2\pi i n z}$, $(a_1=1)$

Teorema: La función $f_E(z) : \mathcal{H} \longrightarrow \mathbb{C}$ es una forma modular de nivel N. Es decir:

$$f_E(\gamma\cdot z)(cz+d)^{-2} = f(z) \quad \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

tal que $N \mid c$.

Consecuencia: la diferencial $\omega_{f_E} = (2\pi i) f_E(z)\,dz$ es invariante por la acción de $\Gamma_0(N)$: $(2\pi i) f(\gamma\cdot z)\, d(\gamma\cdot z) = (2\pi i) f(z)$

$\Rightarrow$ ω_{f_E} es una diferencial en $\Gamma_0(N)\backslash\mathcal{H}^* \simeq X_0(N)$

__Teorema__: Sea $\Lambda_{f_E} = \{ \int_\gamma \omega_{f_E} \mid \gamma \in H_1(X_0(N), \mathbb{Z}) \} \subseteq \mathbb{C}$.

Entonces Λ_{f_E} es un lattice y $\mathbb{C}/\Lambda_{f_E}$ es isógena a E.

__Obs__: podemos, cambiando E por una curva isógena, suponer que $\mathbb{C}/\Lambda_{f_E} \cong E$.

Entonces ϕ viene dada por:

$$\begin{tikzcd} X_0(N) \simeq \mathcal{H}^*/\Gamma_0(N) \arrow[r] & \mathbb{C}/\Lambda_{f_E} \arrow[r, "\simeq"] & E \\ \tau \arrow[r, mapsto] & J_\tau = \int_{i\infty}^{\tau} \omega_{f_E} \arrow[r, leftrightarrow] & (\wp(J_\tau), \wp'(J_\tau)) = \end{tikzcd}$$

__Rmk__: $J_\tau = \int_{i\infty}^{\tau} \omega_{f_E} = \int_{i\infty}^{\tau} 2\pi i \sum_{n\geq 1} a_n e^{2\pi i n z} dz = \sum_{n \geq 1} \frac{a_n}{n} e^{2\pi i n \tau}$ converge para $\tau \in$

Por lo tanto, si hemos encontrado $\tau \in K \cap \mathcal{H}$ tal que

$\mathcal{O}_\tau^{(N)} \simeq \mathcal{O}_K$ (ie. tal que $\mathrm{End}(\mathbb{C}/\langle 1,\tau\rangle) \cong \mathrm{End}(\mathbb{C}/\langle 1, N\tau\rangle) \cong \mathcal{O}_K$)

el punto P_τ pertenece a $E(K)$.

__Teorema__ (Gross – Zagier) $P_\tau \in E(K)$ es de orden infinito

si y sólo si $\mathrm{ord}_{s=1} L(E/K, s) = 1$.

Además, si $\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) = 1 \Rightarrow P_\tau \in E(\mathbb{Q})$

Metodo de los puntos de Heegner

$E/\mathbb{Q}$, conductor N

$$X_0(N) \underset{\Gamma_0(N)}{\simeq} \mathcal{H}^* \longrightarrow \mathbb{C}/\Lambda_{g_E} \xrightarrow{\sim} E(\mathbb{C})$$

$$\tau \longmapsto J_\tau = \sum_{n\geq 1} \frac{a_n}{n} e^{2\pi i n\tau} \mapsto (\wp(J_\tau), \wp'(J_\tau))$$

$$a_p = p+1-\#E(\mathbb{Z}/p\mathbb{Z})$$

$K \subset \mathbb{C}$ cuadrático imaginário y $\tau \in K \cap \mathcal{H}$ tal que

$$\mathrm{End}(\mathbb{C}/\langle 1,\tau\rangle) \simeq \mathrm{End}(\mathbb{C}/\langle 1,N\tau\rangle) \simeq \mathcal{O}_K$$

Entonces $P_\tau \in E(K)$ y es de orden ∞ si y sólo si $\mathrm{ord}_{s=1} L(E/K,s)=1$

Si $\mathrm{ord}_{s=1} L(E/\mathbb{Q},s) = 1 \Rightarrow P_\tau \in E(\mathbb{Q})$.

Algoritmo

1. $E/\mathbb{Q}$ curva ellíptica, conductor N
2. Buscar cuadrático imaginario $K=\mathbb{Q}(\sqrt{D})$ tal que
   - $(d_K, N)=1$, donde $d_K = \begin{cases} 4D & \text{si } D\equiv 2,3\ (4) \\ D & \text{si } D \equiv 1\ (4) \end{cases}$
   - para todo primo l con $l \mid N$ entonces
     - $\left(\frac{D}{l}\right)=1$ si $l \neq 2$
     - $D \equiv 1\ (8)$ si $l=2$

Rk: - esto garantiza que existan embeddings optimales $K \hookrightarrow M_0(N)$

- nos vamos a restringir a K's con $h(K)=1$.
- si $\mathrm{ord}_{s=1} L(E/\mathbb{Q},s)=1$, un teorema asegura que siempre podemos encontrar K (quizá $h(K)>1$) tal que $\mathrm{ord}_{s=1} L(E/K,s) = 1$,

3. Calcular un embedding optimal $K \hookrightarrow M_0(N)$

- Sea $\mathcal{N} = a + c\omega$ un elemento de norma N, $\mathcal{O}_K = \mathbb{Z}[\omega]$.

- existen $b, d \in \mathbb{Z}$ tales que $\mathcal{O}_K = \mathbb{Z}\cdot(a+c\omega) + \mathbb{Z}\cdot(b+d\omega)$,

  es decir, tale que $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ tiene det 1

- sea M la matriz de "multiplicar por ω" en la base $\langle e_1, e_2 \rangle = \langle a+c\omega,\ b+d\omega \rangle$.

- $M \in M_0(N)$ y $\iota : \omega \mapsto M$ nos da un embedding optimal.

4. Calcular el punto fijo $\tau \in \mathcal{H}$ tal que $M \cdot \tau = \tau$

5. Calculamos $J_\tau = \sum \frac{c_n}{n} e^{\pi i n \tau}$

6. $P_\tau = (\wp(J_\tau), \wp'(J_\tau)) \in E(K)$