Puntos de Darmon, motivación

GdT puntos de Darmon, motivación.

- Sistemas de Heegner, teoría CM
- Signo de la ec. funcional
- Teoría p-ádica

Uniformización de c.e:

$A/_{\mathbb{C}}$ una curva elíptica. Entonces $\exists\ \Lambda \subseteq \mathbb{C}$, reticulado, tal que $A(\mathbb{C}) \simeq \mathbb{C}/_{\Lambda}$. Además, podemos suponer $\Lambda = \Lambda_\tau := \mathbb{Z} + \tau.\mathbb{Z}$, con $\tau \in \mathbb{H} = \{ z \in \mathbb{C} : \operatorname{Im} z > 0 \}$.

A: $z, z' \in \mathbb{H}$, $\Lambda_z = \Lambda_{z'} \iff \tau' = \dfrac{a\tau + b}{c\tau + d}$; $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Sl_2(\mathbb{Z})$.

$$Sl_2(\mathbb{Z})\backslash \mathbb{H} \xrightarrow{\sim} \{ A/_{\mathbb{C}},\ \text{curva elíptica} \}/\sim$$
$$(\tau) \longmapsto A_\tau : \quad A_\tau(\mathbb{C}) \simeq \mathbb{C}/_{\mathbb{Z}+\tau.\mathbb{Z}}$$

Más generalmente, $N \geq 1$, $\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Sl_2(\mathbb{Z}) : c \equiv 0 \bmod N \right\}$

$$Y_0(N) := \Gamma_0(N)\backslash \mathbb{H} \xrightarrow{\sim} \{ (A, C) : A \text{ c.e. } C \subseteq A \text{ subgrupo cíclico de orden } N \}/\sim$$
$$(\tau) \longmapsto (A_\tau, \langle 1, \tfrac{\tau}{N} \rangle)$$

$Y_0(N)$ es una superficie de Riemann no compacta. Agregando un nº finito de puntos, obtenemos $X_0(N) = Y_0(N) \cup \{\text{cúspides}\}$, s. R. compacta.

Teorema de modularidad (Wiles, BCDT)

Sea $E/_{\mathbb{Q}}$ una curva elíptica de conductor N. Entonces existe una aplicación holomorfa no constante $\Phi_N : X_0(N) \longrightarrow E(\mathbb{C})$, con "propiedades aritméticas"

Teoría CM

$A = \mathbb{C}/\Lambda$; $\operatorname{End} A = \{\lambda \in \mathbb{C} : \lambda \cdot \Lambda \subseteq \Lambda\}$

$\operatorname{End} A$ es un anillo conmutativo. Además, $\mathbb{Z} \subseteq \operatorname{End} A$

Teorema: $\operatorname{End} A = \begin{cases} \mathbb{Z} \\ \left.\begin{array}{l}\text{orden dentro de} \\ \text{un cuerpo cuadrático imaginario}\end{array}\right\} \text{ caso CM} \end{cases}$

Ej: $A = \mathbb{C}/\mathbb{Z}[i]$; $\operatorname{End} A = \mathbb{Z}[i]$

En general, A_τ es CM $\iff [\mathbb{Q}(\tau) : \mathbb{Q}] = 2$.

$K/\mathbb{Q}$ cuerpo cuadrático imaginario. $K = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$, $d < 0$, sin factores cuadrados.

$\mathcal{O}_K = \{\text{enteros algebraicos en } K\} = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{si } d \equiv 2,3 \ (4) \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{si } d \equiv 1 \ (4) \end{cases}$

Un <u>orden</u> es un subanillo $\mathcal{O} \subseteq \mathcal{O}_K$ tal que $\operatorname{Frac} \mathcal{O} = K$.

($\mathcal{O}_K$ es el orden maximal).

$\mathcal{O}$ tiene la forma $\mathcal{O} = \mathbb{Z} + c \cdot \mathcal{O}_K$; $c \geq 1$, $c \in \mathbb{Z}$.

c se dice el conductor de $\mathcal{O}$.

$\operatorname{Pic} \mathcal{O} = \{\mathcal{O}\text{-ideales} \subseteq K, \text{propios}\}/\sim \; = \{\mathcal{O}\text{-módulos proyectivos de rango } 1\}/\sim$

Si $\mathcal{O} = \mathcal{O}_K$, $\operatorname{Pic} \mathcal{O}_K = Cl(K)$.

$\operatorname{Pic} \mathcal{O}$ es un grupo abeliano finito.

TCC $\Rightarrow$

Teorema $\forall\ \mathcal{O} \subseteq K$, orden de conductor c, existe una extensión finita y Galois H/K tal que

i) $\mathrm{Gal}(H_c/K) \simeq \mathrm{Pic}(\mathcal{O})$ (en particular abeliano)

ii) H/K es no ramificada fuera de c.

H es el "ring class field" asociado a $\mathcal{O}$.

Puntos de Heegner

$$N \geq 1 \ ; \quad M_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) : c \equiv 0 \bmod N \right\}$$

$$\begin{array}{c} M_0(N) \\ \cup \\ \Gamma_0(N) \end{array}$$

$\tau \in \mathbb{H}$; suponemos $K := \mathbb{Q}(\tau)$ es una ext. cuadrática de $\mathbb{Q}$.

$$\mathcal{O}_\tau^{(N)} := \{ \gamma \in M_0(N) : a\tau + b = \tau(c\tau + d) \}, \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Hecho: $\mathcal{O}_\tau^{(N)}$ es un anillo isomorfo a un orden de K.

Teorema (milagro CM) $E/\mathbb{Q}$ de conductor N.

$$\Phi : \mathbb{H} \longrightarrow \Gamma_0(N)\backslash\mathbb{H} = Y_0(N) \xrightarrow{\Phi_N} E$$

Si $\tau \in \mathbb{H} \cap K$; H/K el ring class field asociado a $\mathcal{O}_\tau^{(N)}$.

Entonces $\Phi(\tau) \in E(H)$.

Complementos

$\mathcal{O} \subseteq K$, K cuadrático imaginario.

$$CM(\mathcal{O}) := \{ [z] \in \Gamma_0(N) \backslash \mathbb{H} : \mathcal{O}_z^{(N)} \simeq \mathcal{O} \}$$

Ley de reciprocidad de Shimura: si $z \in CM(\mathcal{O})$ y $\alpha \in \operatorname{Pic} \mathcal{O}$, entonces $\Phi(\alpha * z) = \operatorname{rec}(\alpha^{-1}) \Phi(z)$

Condición de Heegner

sea $\mathcal{O} \subseteq K$ (cuad. imaginario) un orden de discriminante primo a N. Entonces

$CM(\mathcal{O}) \neq \emptyset \iff$ todos los divisores primos de N se escinden en K.

Sistemas de Heegner

Fijamos $F/\mathbb{Q}$ extensión finita. Sea $E/_F$ curva elíptica semiestable de conductor N. Sea $K/_F$ una extensión cuadrática.

$$S_{E/K} := \{ v \in \mathcal{M}_K : v | \infty \text{ v } E_v \text{ tiene reducción multiplicativa escindida} \}.$$

$$= \{ v : E(K_v) \text{ admite una uniformización} \}$$

Sea $\operatorname{sgn}(E, K) = (-1)^{\# S_{E,K}}$.

Para cada $n \in \mathbb{N}$, $(n, N) = 1$, sea $\mathcal{O}_n \subseteq \mathcal{O}_K$ el orden de conductor n y $H_n/_K$ el ring class field correspondiente.

Def: Un sistema de Heegner asociado a (E, K) es una colección de puntos algebraicos $P(n) \subseteq E(H_n)$ con $(n, N) = 1$, tales que para todo primo $\ell \nmid N$ y todo $P_{n\ell} \in P(n\ell)$, existen $P_n \in P(n)$ y $P_{\frac{n}{\ell}} \in P\left(\frac{n}{\ell}\right)$ (cuando $\ell | n$) tales que

$$\mathrm{Tr}_{H_{M\ell}/H_M}(P_{M\ell}) = \begin{cases} a_\ell \cdot P_M & \text{si } \ell \nmid M \text{ es inerte en } K \\ (a_\ell - \sigma_\lambda - \sigma_\lambda^{-1}) P_M & \text{si } \ell = \lambda\bar\lambda \nmid M \text{ se escinde en } K \\ (a_\ell - \sigma_\lambda) P_M & \text{si } \ell = \lambda^2 \text{ es ram. en } K \\ a_\ell P_M - P_{\frac{M}{\ell}} & \text{si } \ell \mid M \end{cases}$$

Además, $\forall\ \sigma \in \mathrm{Gal}(H_M/\mathbb{Q})$ con $\sigma^2 = id$, $\exists\ \sigma' \in \mathrm{Gal}(H_M/K)$ tal que $\sigma(P_M) = -\mathrm{Sign}(E, \mathbb{Q}) \cdot \sigma'(P_M) \mod E(H_M)_{tors}$

<u>Conjetura</u> Si $\mathrm{sgn}(E, K) = -1$, entonces $\exists$ un sistema de Heegner asociado a (E, K).
(motivada por BSD)

Ej: K cuad. imaginaria que satisface la hip. de Heegner,

$$S_{E,K} = \underbrace{\{\lambda : \lambda \mid \ell \mid N \text{ y } E/\mathbb{Q}_\ell \text{ tiene red. mult.}\}}\cup\{\infty\}$$

ℓ escinde $\Rightarrow$ card. par

$\therefore\ (-1)^{S_{E,K}} = -1.$

El sistema de Heegner se construye usando los puntos de Heegner

<u>K cuadrático real</u>

Si $\mathrm{sgn}(E, K) = -1$, ¿cómo construir un sist. de Heegner sin la ayuda de la teoría CM?

Obs: $\mathrm{sgn}(E, K) = -1 \Rightarrow \exists\ p \mid N$ que es inerte o ramificado en K

Idea básica: $p \leftrightarrow \infty$

$\mathbb{Q}_p$, números p-ádicos.

$\mathbb{C}_p$ = completación de $\overline{\mathbb{Q}}_p$

$\mathbb{H}_p = \mathbb{C}_p - \mathbb{Q}_p$.

p inerte o ram. en $K \Rightarrow K \not\subseteq \mathbb{Q}_p$.

$\Rightarrow z \in \mathbb{H}_p \cap K$ puede jugar el rol de z CM.

¿Cómo construir $\Phi(z) \in E(H)$?