Distribución p-ádica de puntos CM y aplicaciones diofantinas, parte 1

Ricardo Menares

Pontificia Universidad Católica de Chile (Santiago)

Colaboración con Sebastián Herrero (PUCV, Valparaíso)

y Juan Rivera-Letelier (Rochester)

El caso complejo

$Y(\mathbb{C}) = \{E_{/\mathbb{C}} \text{ curva elíptica }\}_{/\sim_{\mathbb{C}}} \simeq SL_2(\mathbb{Z})\backslash\mathbb{H}$
$D \in \mathbb{Z}_{<0}$ un discriminante (i.e. $D \equiv 0, 1 \mod 4$).
$\mathcal{O}_D$: el único orden de discriminante D en $\mathbb{Q}(\sqrt{D})$.

$$\mathcal{H}_D = \{E \in Y(\mathbb{C}) : \mathrm{End}(E) \simeq \mathcal{O}_D\}.$$

$\mathcal{H}_D$ es un conjunto finito de $|Pic(\mathcal{O}_D)|$ elementos.
Un *punto CM* es un elemento de $\mathcal{H}_D$ para algún D.

Teorema (Duke '88, Clozel-Ullmo '04)

Los conjuntos $\mathcal{H}_D$ se equidistribuyen sobre $Y(\mathbb{C})$, cuando $D \to -\infty$, según la medida hiperbólica.

i.e. para toda $f : Y(\mathbb{C}) \to \mathbb{R}$ continua y de soporte compacto,

$$\lim_{\substack{D\to-\infty \\ D \text{ discriminante}}} \frac{1}{|\mathcal{H}_D|} \sum_{E\in\mathcal{H}_D} f(E) = \frac{3}{\pi} \int_{SL_2(\mathbb{Z})\backslash\mathbb{H}} f(x+iy)\frac{dxdy}{y^2}.$$

El caso p-ádico

Fijamos un número primo p.

$$\mathbb{C}_p := \text{ completación de } \overline{\mathbb{Q}}_p \text{ (cuerpo completo y alg. cerrado)}$$

Fijamos una incrustación $\overline{\mathbb{Q}} \to \mathbb{C}_p$. Podemos considerar

$$\mathcal{H}_D \subset Y(\overline{\mathbb{Q}}) \subset Y(\mathbb{C}_p).$$

Pregunta

Sea $(D_n)_{n\geq 0}$ una sucesión de discriminantes tales que $\lim_{n\to\infty} D_n = -\infty$. ¿Cómo se distribuyen los conjuntos $\mathcal{H}_{D_n}$ en $Y(\mathbb{C}_p)$ cuando $n \to \infty$?

A diferencia del caso complejo, la respuesta depende de la secuencia (D_n).

El caso transiente

Definición: los conjuntos $\{\mathcal{H}_{D_n}\}_n$ se distribuyen de manera *transiente* si para todo $P \in Y(\mathbb{C}_p)$, existe una vecindad U tal que

$$\lim_{n\to\infty} \frac{|\mathcal{H}_{D_n} \cap U|}{|\mathcal{H}_{D_n}|} = 0.$$

Todo $E \in \mathcal{H}_D$ tiene buena reducción potencial $\tilde{E}_{/\overline{\mathbb{F}}_p}$. Sea

$$\mathrm{ord}_{p\text{-ss}}(D) := \begin{cases} +\infty & \text{si } \tilde{E} \text{ es una curva elíptica ordinaria} \\ \mathrm{ord}_p(D) & \text{si } \tilde{E} \text{ es una curva elíptica supersingular} \end{cases}$$

Teorema transiente (Herrero, M., Rivera-Letelier)

Los conjuntos $\{\mathcal{H}_{D_n}\}_n$ se distribuyen de manera transiente si y solamente si

$$\lim_{n\to\infty} ord_{p\text{-}ss}(D_n) = +\infty.$$

El caso supersingular

A partir de aquí supondremos que **cada $E \in \mathcal{H}_{D_n}$ tiene reducción supersingular** y $\mathrm{ord}_p(D_n)$ **se mantiene acotado cuando n varía**. En particular,

$$\mathcal{O}_{D_n} \otimes \mathbb{Z}_p \text{ is un orden en una extensión cuadrática de } \mathbb{Q}_p.$$

Supondremos también que $\mathcal{O}_{D_n} \otimes \mathbb{Z}_p$ no cambia cuando n varía. Esto implica que $\mathrm{ord}_p(D_n)$ no cambia cuando n varía.
Sea $\mathcal{O}$ un orden en una extensión cuadrática de $\mathbb{Q}_p$. Sea

$$\Lambda_{\mathcal{O}} := \overline{\{E_{/\mathbb{C}_p} : \mathrm{End}(E) \otimes \mathbb{Z}_p \simeq \mathcal{O}\}}^{|\cdot|_p}.$$

Toda medida límite posible debe estar soportada en este conjunto.

$$\Lambda_{\mathcal{O}} := \overline{\{E_{/\mathbb{C}_p} : \mathrm{End}(E) \otimes \mathbb{Z}_p \simeq \mathcal{O}\}}^{|\cdot|_p}.$$

Teorema supersingular (HMR-L)

1. *$\Lambda_{\mathcal{O}}$ is un conjunto compacto*
2. *Si $\mathcal{O} \neq \mathcal{O}'$, entonces $\Lambda_{\mathcal{O}} \cap \Lambda_{\mathcal{O}'} = \emptyset$*
3. *Supongamos $p \equiv 1 \mod 4$. Entonces, existe una medida $\nu_{\mathcal{O}}$ con soporte igual a $\Lambda_{\mathcal{O}}$, tal que la sucesión de conjuntos*

$$\{\mathcal{H}_{D_n} : \mathcal{O}_{D_n} \otimes \mathbb{Z}_p \simeq \mathcal{O}\}_{n \geq 1}$$

se equidistribuye, cuando $D_n \to -\infty$, según la medida $\nu_{\mathcal{O}}$.

Observación. Si $p = 2$ o $p \equiv 3 \mod 4$, hay un enunciado más complicado.

Aplicación: módulos singulares que son S-unidades

El invariante j de una curva elíptica CM se dice un *módulo singular*. Los módulos singulares son enteros algebraicos.

Teorema (S-unidades, HMR-L)

Sea S un conjunto finito de números primos. Sea j_0 un módulo singular. Entonces, el conjunto

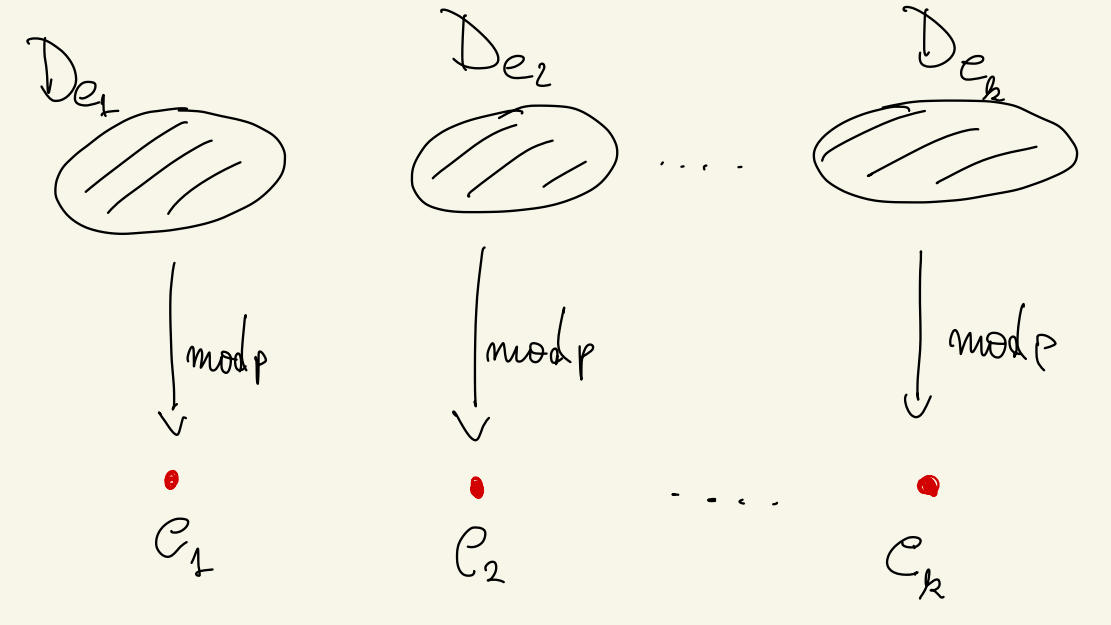
$$C(S, \mathrm{j}_0) = \{\mathrm{j}\ módulo\ singular\ : \mathrm{j} - \mathrm{j}_0\ es\ una\ S - unidad\}$$

es finito.

Habegger: $C(\emptyset, \mathrm{j}_0)$ is finito. Su método usa la equidistribución compleja de puntos CM.
Bilu-Habegger-Kuhne: $C(\emptyset, 0)$ is vacío
Yingkun Li : $C(\emptyset, \mathrm{j}_0)$ es vacío
Campagna: $C(S_{ord}, 0)$ is vacío para $S_{ord} = \{$ primos de reducción ordinaria de $\mathrm{j}_0 = 0\}$ (resultado similar para 1728).

Ideas de la demostración del Teorema supersingular

Sean $e_1, e_2, \ldots, e_k$ las curvas elípticas supersingulares sobre $\overline{\mathbb{F}}_p$.
Sea $D_{e_j} = \{E_{/\mathbb{C}_p} : \tilde{E} \simeq e_j\}$. Es un disco.



Fijamos una curva elíptica supersingular e y buscamos entender la distribución asintótica de $(\mathcal{H}_{d_n} \cap D_e)_n$.

Hipótesis simplificadoras

A partir de aquí, supondremos que los elementos de $\mathcal{H}_{d_n}$ tienen reducción supersingular. Fijamos un order $\mathcal{O}$ en una extensión cuadrática de $\mathbb{Q}_p$ y una curva elíptica supersingular $e_{/\overline{\mathbb{F}}_p}$.
Supondremos también las siguientes **hipótesis simplificadoras**:

- $\mathcal{O}$ es un orden maximal
- d_n es un discriminante fundamental para todo n
- $p \nmid d_n$
- $p \equiv 1 \mod 4$
- $\mathrm{Aut}(e) = \{\pm 1\}$

En particular, $\left(\frac{d_n}{p}\right) = -1$ y $\mathcal{O}_{d_n} \otimes \mathbb{Z}_p \simeq \mathcal{O}$ es el orden maximal de la única extensión cuadrática no ramificada de $\mathbb{Q}_p$.

Uniformización de $\Lambda_{\mathcal{O}}$

En el caso complejo, tenemos una uniformización

$$\mathbb{H} \longrightarrow SL_2(\mathbb{Z})\backslash\mathbb{H} \simeq Y(\mathbb{C}).$$

Más aún,

$$GL_2^+(\mathbb{R}) \longrightarrow \mathbb{H}, \quad g \mapsto g \cdot i$$

transporta la medida de Haar en $GL_2^+(\mathbb{R})$ a la medida hiperbólica.
En el caso p-ádico, uniformizaremos el conjunto $\Lambda_{\mathcal{O}} \cap D_e \subseteq Y(\mathbb{C}_p)$ por un álgebra de cuaterniones.

Uniformización de $\Lambda_{\mathcal{O}}$

$B_{/\mathbb{Q}_p}$ álgebra (de división) de cuaterniones, O_B su orden maximal.
$\mathrm{End}(e) \otimes \mathbb{Z}_p \simeq O_B$.
La teoría de deformaciones del grupo formal asociado a e dota a D_e de una acción de O_B^* (aquí usamos $\mathrm{Aut}(e) = \{\pm 1\}$).
Sea $\ell \in \mathbb{Z}_p$ un discriminante de $\mathcal{O}$. Sea

$$S(\ell) = \{g \in O_B : \mathrm{tr}(g) = 0 \text{ y } \mathrm{nr}(g) = -\ell\} \subset O_B^*.$$

Proposición (Uniformización de $\Lambda_{\mathcal{O}}$ por una esfera p-ádica)

Todo $g \in S(\ell)$ tiene un único punto fijo. Tal punto fijo es un elemento de $\Lambda_{\mathcal{O}}$. Más aún, la función

$$S(\ell)/\{\pm 1\} \to \Lambda_{\mathcal{O}}, \quad g \mapsto Fix(g)$$

es una biyección continua.

La medida uniforme en $S(\ell)$

$$S(\ell) = \{g \in O_B : \mathrm{tr}(g) = 0 \text{ y } \mathrm{nr}(g) = -\ell\} \subset O_B^*$$

es un conjunto compacto, invariante bajo conjugación por B^*.
Definición: la medida uniforme μ_ℓ on $S(\ell)$ es la única medida de probabilidad en $S(\ell)$ invariante bajo esta acción.
Más concretamente: para todo $r \geq 1$, escogemos una "función de reducción"

$$red : O_B^{\text{traza } =0} \to (\mathbb{Z}/p^r\mathbb{Z})^3.$$

Entonces, la colección de conjuntos
$\Phi_r := \{red^{-1}(x) \cap S(\ell) : x \in (\mathbb{Z}/p^r\mathbb{Z})^3\}$ es un recubrimiento de $S(\ell)$. Sea m_r el número de conjuntos no vacíos en Φ_r. Entonces, para tales $C \in \Phi_r$,

$$\mu_\ell(C) = \frac{1}{m_r}.$$

Puntos CM como puntos fijos

Sea

$$V_d = \{g \in \mathrm{End}(e) : \mathrm{tr} g = 0, \mathrm{nr}(g) = -d\} \subseteq O_B^*.$$

Proposición (Puntos CM como puntos fijos)

Sea d un discriminante fundamental tal que $p \nmid d$ y $\left(\frac{d}{p}\right) = -1$. Entonces, todo $g \in V_d$ tiene un único punto fijo en D_e. Más aún,

$$\mathcal{H}_d \cap D_e = \cup_{g \in V_d} Fix(g).$$

Teorema supersingular, estrategia de demostración

Sea (d_n) una sucesión de discriminantes fundamentales con $p \nmid d_n$ y $\left(\frac{d_n}{p}\right) = -1$.

$V_{d_n} = \{g \in \mathrm{End}(e) : \mathrm{tr} g = 0, \mathrm{nr}(g) = -d_n\} \subseteq \mathrm{End}(e)^{\mathrm{tr}=0} \simeq \mathbb{Z}^3$

$O_B^{\mathrm{trace}=0} \simeq \mathbb{Z}_p^3$

Supondremos que d_n converge p-ádicamente a algún $\ell \in \mathbb{Z}_p^*$.

Escribimos $d_n = \ell \cdot a_n^2, \quad a_n \in \mathbb{Z}_p$. Se tiene

$$\frac{1}{a_n} V_{d_n} \subseteq S(\ell).$$

Así, para entender la distribución de $\mathcal{H}_{d_n} \cap D_e$, debemos entender la distribución de los "puntos enteros" $\frac{1}{a_n} V_{d_n}$ en la "esfera p-ádica" $S(\ell)$ ("problema de Linnik p-ádico").

Teorema (HMR-L)

Los conjuntos $\frac{1}{a_n} V_{d_n}$ se equidistribuyen según la medida uniforme en $S(\ell)$.

Teorema supersingular, estrategia de demostración

Teorema (HMR-L)

Los conjuntos $\frac{1}{a_n} V_{d_n}$ *se equidistribuyen según la medida uniforme en* $S(\ell)$.

Observación: usamos las cotas (Iwaniec '87, Duke '88, Blomer '04) sobre los coeficientes de Fourier de formas modulares de peso medio entero.

Conclusión:

Por la fórmula de puntos fijos,

$$\mathrm{Fix}(V_{d_n}) = \mathcal{H}_{d_n} \cap D_e.$$

Si μ_ℓ es la medida uniforme en $S(\ell)$, entonces los conjuntos $\mathcal{H}_{d_n} \cap D_e$ se equidistribuyen según la medida $\nu := \mathrm{Fix}_*(\mu_\ell)$.
ν no depende de ℓ. Solo depende de $\mathbb{Q}_p(\sqrt{\ell})$.■

Como eliminar las hipótesis simplificadoras

Para eliminar	usar
($\mathcal{O}$ es un orden maximal) (d_n es un discriminante fundamental para todo n)	teoría de Katz sobre el grupo canónico
$p \nmid d_n$	cuando $p \| \ell$, los elementos en $S(\ell)$ tienen dos puntos fijos
$p \equiv 1 \mod 4$	subdividir $\Lambda_{\mathcal{O}} = \Lambda_{\mathcal{O}}^{+} \sqcup \Lambda_{\mathcal{O}}^{-}$
$\mathrm{Aut}(e) = \{\pm 1\}$	trabajar en un cubrimiento $X_e \to D_e$ de grado $\frac{\lvert\mathrm{Aut}(e)\rvert}{2}$

¡Gracias por su atención!