p-adic asymptotic distribution of CM points

Sebastián Herrero
(joint with Ricardo Menares and Juan Rivera-Letelier)

Geometry, Arithmetic and Differential Equations of Periods

Notation

Given an algebraically closed field K, define

$$\mathrm{Ell}(K) = \{\text{elliptic curve over } K\}/\mathrm{isomorphism}.$$

The j-invariant gives a bijection

$$j : \mathrm{Ell}(K) \to K.$$

In this talk $K = \overline{\mathbb{Q}}, \mathbb{C}, \mathbb{C}_p$ or $\overline{\mathbb{F}}_p$ (p prime).

Remark: We can endow $\mathrm{Ell}(K)$ with the topology of K.

CM points

A **CM point** in $\mathrm{Ell}(\overline{\mathbb{Q}})$ is a point representing an elliptic curve E with complex multiplication, i.e. with

$$\mathrm{End}(E) = \mathbb{Z}\left[\frac{D+\sqrt{D}}{2}\right]$$

for some integer $D < 0$. We call D the **discriminant** of the CM point and define

$$\Lambda_D = \{\text{CM point of discriminant } D\}.$$

Theorem (CM Theory)

Λ_D is finite of cardinality $h(D)$ (class number).

For simplicity let us assume D **fundamental**, i.e. $\mathbb{Z}\left[\frac{D+\sqrt{D}}{2}\right] = \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$.

Size of $\#\Lambda_D = h(D)$

Theorem (Heilbronn, 1934)

$h(D) \to \infty$ *when* $D \to -\infty$.

Hans Heilbronn
(1908-1975)

Theorem (Siegel, 1935)

$\log(h(D)) \sim \log(\sqrt{|D|})$ *when* $D \to -\infty$.

Carl Ludwig Siegel
(1896-1981)

Main question

Question:

How are CM points distributed on $\mathrm{Ell}(\overline{\mathbb{Q}})$ when $D \to -\infty$?

Remark: We can consider

$$\mathrm{Ell}(\overline{\mathbb{Q}}) \hookrightarrow \mathrm{Ell}(\mathbb{C})$$

or

$$\mathrm{Ell}(\overline{\mathbb{Q}}) \hookrightarrow \mathrm{Ell}(\mathbb{C}_p)$$

for p prime.

Asymptotic distribution of points

Given:

- a topological space X,
- a sequence $(A_n)_{n\in\mathbb{N}}$ of non-empty finite subsets of X,
- a Borel probability measure μ on X,

we write

$$\frac{1}{\#A_n}\sum_{x\in A_n}\delta_x \to \mu \quad \text{weakly,}$$

if for every f in $C_0(X)$ we have

$$\frac{1}{\#A_n}\sum_{x\in A_n} f(x) \to \int f\, d\mu.$$

In this case, the asymptotic distribution of $(A_n)_{n\in\mathbb{N}}$ is *ruled* by μ.

A baby example

- $S^1 = \{z \in \mathbb{C} : |z| = 1\}$
- $A_n = \{e^{2\pi i k/n} : k = 0, 1, \ldots, n-1\}$
- μ_{S^1} = Haar measure on S^1

In this case

$$\frac{1}{n} \sum_{x \in A_n} \delta_x \to \mu_{S^1} \quad \text{weakly.}$$

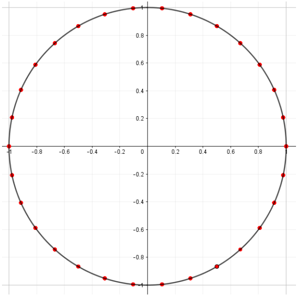


Figure: A_{30}

Another example

- $S^1 = \{z \in \mathbb{C} : |z| = 1\}$
- $B_n = \{e^{2\pi ik/n} : k = 0, 1, \ldots, n-1, \text{g.c.d.}(k, n) = 1\}$
- μ_{S^1} = Haar measure on S^1

In this case (again)

$$\frac{1}{\phi(n)} \sum_{x \in B_n} \delta_x \to \mu_{S^1} \quad \text{weakly.}$$

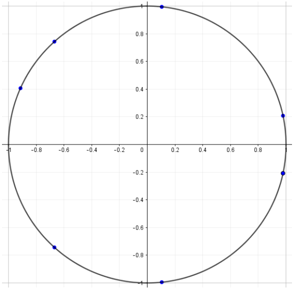


Figure: B_{30}

Distribution of CM points over $\mathbb{C}$

Consider $\mathrm{Ell}(\overline{\mathbb{Q}}) \hookrightarrow \mathrm{Ell}(\mathbb{C})$.

Theorem (Uniformization theory of elliptic curves over $\mathbb{C}$)

1. *If E is an elliptic curve over $\mathbb{C}$, then there is a w in*

$$\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$$

such that $E(\mathbb{C}) \simeq \mathbb{C}/(\mathbb{Z} + w\mathbb{Z})$, and conversely.

2. $\mathbb{C}/(\mathbb{Z} + w\mathbb{Z}) \simeq \mathbb{C}/(\mathbb{Z} + w'\mathbb{Z}) \Leftrightarrow w' = \frac{aw+b}{cw+d}$ *for some* $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ *in* $\mathrm{SL}_2(\mathbb{Z})$.

Hence $\mathrm{Ell}(\mathbb{C}) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$.

In $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ we have the hyperbolic measure $\dfrac{3}{\pi}\dfrac{dxdy}{y^2}$.

Distribution of CM points over $\mathbb{C}$

Recall $\mathrm{Ell}(\overline{\mathbb{Q}}) \hookrightarrow \mathrm{Ell}(\mathbb{C}) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$.

Theorem (Linnik, 1968)

$$\frac{1}{h(D)} \sum_{E \in \Lambda_D} \delta_E \to \frac{3}{\pi} \frac{dxdy}{y^2} \quad \textit{weakly},$$

provided $D \to -\infty$ *and* $\left(\frac{D}{p}\right) = 1$, *for some fixed odd prime* p.

Yuri Linnik (1915-1972)

Theorem (Duke, 1988)

$$\frac{1}{h(D)} \sum_{E \in \Lambda_D} \delta_E \to \frac{3}{\pi} \frac{dxdy}{y^2} \quad \textit{weakly},$$

provided $D \to -\infty$.

William Duke

Distribution of CM points over $\mathbb{C}_p$

Consider $\mathrm{Ell}(\overline{\mathbb{Q}}) \hookrightarrow \mathrm{Ell}(\mathbb{C}_p)$.

Given E in Λ_D let $\widetilde{E}$ in $\mathrm{Ell}(\overline{\mathbb{F}}_p)$ denote its **reduction**.
We have two cases:

(i) **Ordinary** reduction:

$$\mathrm{rk}_{\mathbb{Z}}(\mathrm{End}(\widetilde{E})) = 2 \Leftrightarrow \left(\frac{D}{p}\right) = 1 \Leftrightarrow \mathbb{Q}_p(\sqrt{D}) = \mathbb{Q}_p.$$

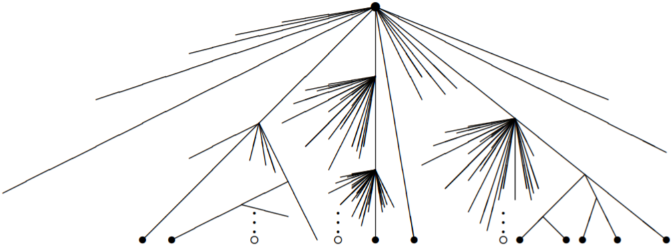
(ii) **Supersingular** reduction:

$$\mathrm{rk}_{\mathbb{Z}}(\mathrm{End}(\widetilde{E})) = 4 \Leftrightarrow \left(\frac{D}{p}\right) \neq 1 \Leftrightarrow [\mathbb{Q}_p(\sqrt{D}) : \mathbb{Q}_p] = 2.$$

The ordinary reduction case

We have $j : \mathrm{Ell}(\mathbb{C}_p) \simeq \mathbb{C}_p$ and $\mathbb{C}_p \hookrightarrow \mathbb{A}^1_{\mathrm{Berk}}$.

$\mathbb{A}^1_{\mathrm{Berk}}$ is a locally compact and arc-connected topological space (Berkovich topology) with $\mathbb{C}_p$ as a dense subspace.



$\mathbb{A}^1_{\mathrm{Berk}}$ is also an $\mathbb{R}$-tree, hence partially ordered, and there is a unique point ζ in $\mathbb{A}^1_{\mathrm{Berk}}$ such that

$$\zeta = \max \overline{\{z \in \mathbb{C}_p : |z|_p \leq 1\}}.$$

The ordinary reduction case

Theorem (H–Menares–Rivera-Letelier, 2020)

$$\frac{1}{h(D)} \sum_{E \in \Lambda_D} \delta_E \to \delta_\zeta \quad \textit{weakly},$$

provided $D \to -\infty$ *with* $\left(\frac{D}{p}\right) = 1$.

The supersingular reduction case

In this case $\mathbb{Q}_p(\sqrt{D})$ is a quadratic extension of $\mathbb{Q}_p$.

Facts: There are 3 (resp. 7) quadratic extensions of $\mathbb{Q}_p$ if $p \geq 3$ (resp. $p = 2$). Every quadratic extension $\mathcal{K}$ of $\mathbb{Q}_p$ has a p-adic discriminant

$$\mathfrak{D}_{\mathcal{K}} \in \mathbb{Z}_p/(\mathbb{Z}_p^\times)^2.$$

Example: When $p = 3$

$\mathcal{K}$	$\mathfrak{D}_{\mathcal{K}}$
$\mathbb{Q}_3(\sqrt{2})$	$2(\mathbb{Z}_3^\times)^2$
$\mathbb{Q}_3(\sqrt{3})$	$3(\mathbb{Z}_3^\times)^2$
$\mathbb{Q}_3(\sqrt{6})$	$6(\mathbb{Z}_3^\times)^2.$

We have

$$\mathbb{Q}_p(\sqrt{D}) = \mathcal{K} \Leftrightarrow D \in \mathfrak{D}_{\mathcal{K}}.$$

Hence p-adic discriminants give a partition of the set of discriminants $D < 0$ with $\left(\frac{D}{p}\right) \neq 1$.

Formal CM points

Given an elliptic curve E defined by a Weierstrass equation with coefficients in $\mathcal{O}_{\mathbb{C}_p}$, denote by $\widehat{E}$ its *formal group*.

$$\widehat{E} = \widehat{E}(X, Y) = \sum_{i,j\geq 0} c_{i,j} X^i Y^j \in \mathcal{O}_{\mathbb{C}_p}[[X, Y]].$$

We define

$$\mathrm{End}_{\mathrm{FG}}(\widehat{E}) := \{\phi \in \mathcal{O}_{\mathbb{C}_p}[[X]] : \widehat{E}(\phi(X), \phi(Y)) = \phi(\widehat{E}(X, Y))\}.$$

A **formal CM point** is a point E in $\mathrm{Ell}(\mathbb{C}_p)$ with $\mathrm{rk}_{\mathbb{Z}_p}(\mathrm{End}_{\mathrm{FG}}(\widehat{E})) = 2$. Given the p-adic discriminant $\mathfrak{D}$ of a quad. extension $\mathcal{K}$ of $\mathbb{Q}_p$ define

$$\Lambda_{\mathfrak{D}} = \{E \in \mathrm{Ell}(\mathbb{C}_p) \text{ with } \mathrm{End}_{\mathrm{FG}}(\widehat{E}) \simeq \mathcal{O}_{\mathcal{K}}\} \subset \mathrm{Ell}(\mathbb{C}_p).$$

We have

$$\Lambda_D \subset \Lambda_{\mathfrak{D}} \Leftrightarrow D \in \mathfrak{D}.$$

The supersingular reduction case

Theorem (H–Menares–Rivera-Letelier, 2021)

For a p-adic discriminant $\mathfrak{D}$ *the set* $\Lambda_{\mathfrak{D}}$ *is compact and there exists a (unique) Borel probability measure* $\nu_{\mathfrak{D}}$ *with support* $\Lambda_{\mathfrak{D}}$ *such that*

$$\frac{1}{h(D)} \sum_{E \in \Lambda_D} \delta_E \to \nu_{\mathfrak{D}} \quad \textit{weakly},$$

provided $D \to -\infty$ *with* $D \in \mathfrak{D}$.

There are 3 (resp. 7) limit measures in this case if $p \geq 3$ (resp. $p = 2$).

Example: the unramified case

Assume $D < 0$ with $\left(\frac{D}{p}\right) = -1$. Then $\mathbb{Q}_p(\sqrt{D})$ is the unique quadratic unramified extension $\mathbb{Q}_{p^2}$ of $\mathbb{Q}_p$. Let $\mathfrak{D}^{unr}$ be its p-adic discriminant.

Example: When $p = 3$

$\mathcal{K}$	$\mathfrak{D}_{\mathcal{K}}$
$\mathbb{Q}_{3^2} = \mathbb{Q}_3(\sqrt{2})$	$\mathfrak{D}^{unr} = 2(\mathbb{Z}_3^\times)^2$
$\mathbb{Q}_3(\sqrt{3})$	$3(\mathbb{Z}_3^\times)^2$
$\mathbb{Q}_3(\sqrt{6})$	$6(\mathbb{Z}_3^\times)^2.$

Example: the unramified case

- Choose e in $\mathrm{Ell}(\overline{\mathbb{F}}_p)$ supersingular ($\sim 1 + \lfloor \frac{p}{12} \rfloor$ possibilities).
- $\mathbf{Y}_e =$ Deformation space of e (we have $\mathbf{Y}_e \simeq \mathfrak{m}_{\mathbb{C}_p}$).
- $\mathbf{X}_e =$ Deformation space of $\widehat{e}$ (we have $\mathbf{X}_e \simeq \mathfrak{m}_{\mathbb{C}_p}$).
- In $\mathbf{X}_e$ the point 0 corresponds to a formal group $\mathcal{F}$ with $\mathrm{End}_{\mathrm{FG}}(\mathcal{F}) = \mathcal{O}_{\mathbb{Q}_{p^2}}$.
- $\mathrm{Aut}(e)$ is finite subgroup of $\mathrm{Aut}_{\mathrm{FG}}(\widehat{e})$.
- $\mathrm{Aut}_{\mathrm{FG}}(\widehat{e})$ is a compact group acting on $\mathbf{X}_e$.
- $\mathbf{X}_e \to \mathrm{Aut}(e)\backslash\mathbf{X}_e \simeq \mathbf{Y}_e$.
- $\Lambda_{\mathfrak{D}^{unr}} \cap \mathbf{Y}_e$ is the image of $\mathrm{Aut}_{\mathrm{FG}}(\widehat{e}) \cdot 0$ under $\mathbf{X}_e \to \mathbf{Y}_e$.
- $\nu_{\mathfrak{D}^{unr}}|_{\mathbf{Y}_e}$ is the push-forward of the Haar measure on $\mathrm{Aut}_{\mathrm{FG}}(\widehat{e})$.

A comparison

On the one hand (non-Archimedean asymptotic distribution):
• $\mathrm{Aut}_{\mathrm{FG}}(\widehat{e}) = \mathbf{R}_e^\times$ where $\mathbf{R}_e$ is the maximal order of the unique division quaternion algebra over $\mathbb{Q}_p$.
• $\mathbf{R}_e^1 =$ Subgroup of elements g in $\mathbf{R}_e^\times$ with $\mathrm{nr}(g) = 1$.
• $\Lambda_{\mathfrak{D}^{unr}} \cap \mathbf{Y}_e$ is also the image of $\mathbf{R}_e^1 \cdot 0$ under $\mathbf{X}_e \to \mathbf{Y}_e$.
• $\nu_{\mathfrak{D}^{unr}}|_{\mathbf{Y}_e}$ is also the push-forward of the Haar measure on $\mathbf{R}_e^1$.

On the other hand (Archimedean asymptotic distribution):
• $M_2(\mathbb{R})$ is a quaternion algebra over $\mathbb{R}$.
• $\mathrm{SL}_2(\mathbb{R})$ is the subgroup of $M_2(\mathbb{R})^\times$ of elements g with $\mathrm{nr}(g) = \det(g) = 1$.
• $\mathrm{Ell}(\mathbb{C})$ is the image of $\mathrm{SL}_2(\mathbb{R}) \cdot i = \mathbb{H}$ under $\mathbb{H} \to \mathrm{Ell}(\mathbb{C})$.
• The hyperbolic measure is the push-forward of the Haar measure on $\mathrm{SL}_2(\mathbb{R})$.

Thank you for your attention!