Arithmetic Statistics and Iwasawa theory

Anwesh Ray

University of British Columbia

anweshray@math.ubc.ca

March 11, 2021

Joint with D. Kundu (UBC).

- Arithmetic statistics (of elliptic curves) is the study of the average behaviour of certain invariants associated to elliptic curves. The elliptic curves are parametrized according to height, conductor or discriminant.
- Iwasawa theory is concerned with the structure of certain Galois modules associated to elliptic curves. These Galois modules are considered over certain infinite extensions of $\mathbb{Q}$.

Elliptic curves and Galois Representations

- Let E be an elliptic curve over $\mathbb{Q}$.
- Fix a prime p, denote by $E[p^n]$ the p^n torsion subgroup of $E(\bar{\mathbb{Q}})$.
- The p-adic Tate-module $T_p(E)$ is the inverse limit

$$T_p(E) = \varprojlim_n E[p^n],$$

where the inverse limit is taken w.r.t. multiplication by p maps $\times p : E[p^{n+1}] \to E[p^n]$.

- The Tate-module $T_p(E)$ is a free $\mathbb{Z}_p$-module of rank 2, and is equipped with an action of the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.
- To the pair (E, p), the Galois action on the Tate-module is encoded by a Galois representation:

$$\rho_{E,p} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_p).$$

- Thus an elliptic curve E gives rise to infinitely many Galois representations $\rho_{E,p}$, as p ranges through all prime numbers.
- There are various arithmetic invariants associated to the Galois representation $\rho_{E,p}$, which are highly dependent on the prime p and the elliptic curve E.
- In this talk, we focus on certain invariants from Iwasawa theory.

We study two interrelated problems:

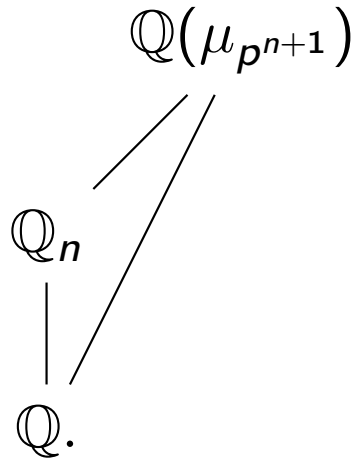
- For a fixed elliptic curve E we study invariants associated to the p-adic Galois representation $\rho_{E,p}$ as p ranges over all primes.
- For a fixed prime p, we study the average behaviour of invariants associated to $\rho_{E,p}$ as E ranges over all elliptic curves defined over $\mathbb{Q}$.

Motivation for Iwasawa theory

- Let p be a prime number.
- Iwasawa theory is concerned with the structure of certain Galois modules arising from arithmetic.
- These modules are defined over certain infinite Galois extensions of $\mathbb{Q}$.

The Cyclotomic $\mathbb{Z}_p$-extension

- Let $\mathbb{Q}_n$ be the subfield of $\mathbb{Q}(\mu_{p^{n+1}})$ such that $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n$ as depicted



- The tower of number fields $\mathbb{Q} = \mathbb{Q}_1 \subset \mathbb{Q}_2 \subset \cdots \subset \mathbb{Q}_n \subset \ldots$ is called the cyclotomic tower.
- The field $\mathbb{Q}_\infty$ is taken to be the union

$$\mathbb{Q}_\infty := \bigcup_{n \geq 1} \mathbb{Q}_n.$$

The Galois group $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ is isomorphic to $\mathbb{Z}_p$.

Early Investigations

- Iwasawa's early ivestigations led him to study the variation of p-class groups of $\mathbb{Q}_n$ as $n \to \infty$.
- For $n \geq 1$, set $\mathcal{A}_n$ to denote the p-primary part of the class group of $\mathbb{Q}_n$

$$\mathcal{A}_n := \mathrm{Cl}(\mathbb{Q}_n)[p^\infty].$$

- Iwasawa showed that there are invariants $\mu, \lambda, \nu \geq 0$ such that

$$\#\mathcal{A}_n = p^{\mu p^n + \lambda n + \nu}$$

for large values of n.

Iwasawa's approach

- There are natural maps $\mathcal{A}_{n+1} \to \mathcal{A}_n$ and the inverse limit $\mathcal{A}_\infty := \varprojlim_n \mathcal{A}_n$ is a module over $\Gamma := \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$.
- Iwasawa introduced the completed algebra $\Lambda := \varprojlim_n \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})] \simeq \mathbb{Z}_p[[x]]$.
- He showed that $\mathcal{A}_\infty$ is a finitely generated torsion $\mathbb{Z}_p[[x]]$-module and his theorem is a consequence of the structure theory of such modules.

Iwasawa theory of Elliptic Curves

- Greenberg and Mazur initiated the Iwasawa theory of elliptic curves over $\mathbb{Q}$.
- Throughout, we let E be an elliptic curve over $\mathbb{Q}$ with good ordinary reduction at p.
- They studied the variation of Selmer groups as one goes up the tower.

Some notation

- For any abelian group M, set $M[p^n] := \ker(M \xrightarrow{p^n} M)$ and $M[p^\infty] := \bigcup_{n \geq 1} M[p^n]$.
- The group $E[p^\infty]$ is isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^2$ equipped with an action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

Selmer groups

- For each number field extension F of $\mathbb{Q}$, the Selmer group $\mathrm{Sel}_{p^\infty}(E/F)$ consists of Galois cohomology classes

$$f \in H^1(\bar{F}/F, E[p^\infty])$$

satisfying suitable local conditions.

- It fits into a short exact sequence

$$0 \to E(F) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_{p^\infty}(E/F) \to Ш(E/F)[p^\infty] \to 0.$$

Selmer groups

- The Selmer group over $\mathbb{Q}_\infty$ is taken to be the direct limit

$$\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty) := \varinjlim_n \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_n).$$

- The Pontryagin dual $\mathfrak{M}_\infty := \mathrm{Hom}_{\mathrm{cnts}}(\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$ is a finitely generated and torsion $\Lambda \simeq \mathbb{Z}_p[[x]]$ module.

Iwasawa Invariants

- By the structure theory of $\mathbb{Z}_p[[x]]$ modules, up to a pseudoisomorphism, $\mathfrak{M}_\infty$ decomposes into cyclic-modules:

$$\left(\bigoplus_j \mathbb{Z}_p[[x]]/(p^{\mu_j}) \right) \oplus \left(\bigoplus_j \mathbb{Z}_p[[x]]/(f_j(x)) \right).$$

- The μ and λ invariants are as follows

$$\mu_{E,p} := \sum_j \mu_j \text{ and } \lambda_{E,p} := \sum_j \deg f_j(x).$$

- The characteristic series is defined as follows:

$$f_{E,p}(x) := p^\mu \prod_j f_j(x).$$

- It is conjectured that when $E[p]$ is irreducible as a Galois module, then, $\mu_{E,p} = 0$.
- Therefore, if E is a fixed elliptic curve, it is expected that $\mu_{E,p} = 0$ for all but a small finite set of primes p.
- Let r_E be the rank of the Mordell Weil group $E(\mathbb{Q})$. The λ-invariant satisfies the inequality $\lambda_{E,p} \geq r_E$.
- We would like to model the average behaviour of the Iwasawa invariants μ and λ in two cases:
  1. when E is fixed and p-varies,
  2. when p is fixed and E varies.

- Consider the following result of R. Greenberg:

Theorem (R. Greenberg)

Let E be an elliptic curve with $r_E = 0$. Then the following equivalent conditions are satisfied for 100% of the ordinary primes p:

- $\mu_{E,p} = 0$ *and* $\lambda_{E,p} = 0$,
- $\mathrm{Sel}(E/\mathbb{Q}_\infty) = 0$.

- The result may be generalized various ways, for instance:

Theorem

Let E be an elliptic curve with $r_E = 0$. Then the following equivalent conditions are satisfied for all but finitely many primes p at which E has supersingular reduction:

- $\mu^{\pm}_{E,p} = 0$ *and* $\lambda^{\pm}_{E,p} = 0$,
- $\text{Sel}^{\pm}(E/\mathbb{Q}_\infty) = 0$.

- Here, $\text{Sel}^{\pm}(E/\mathbb{Q}_\infty)$ are Kobayashi's signed Selmer groups and $\mu^{\pm}_{E,p}, \lambda^{\pm}_{E,p}$ the signed Iwasawa invariants.

- Let E be an elliptic curve and p a prime number. The cohomology groups $H^i(\Gamma, \mathrm{Sel}(E/\mathbb{Q}_\infty)) = 0$ for $i \geq 2$.
- Duality for Γ tells us that

$$\begin{aligned} & H^1(\Gamma, \mathrm{Sel}(E/\mathbb{Q}_\infty)) \\ \simeq & H_1(\Gamma, \mathrm{Sel}(E/\mathbb{Q}_\infty)) \\ = & \mathrm{Sel}(E/\mathbb{Q}_\infty)_\Gamma. \end{aligned}$$

- There is a natural map

$$\Phi : \mathrm{Sel}(E/\mathbb{Q}_\infty)^\Gamma \to \mathrm{Sel}(E/\mathbb{Q}_\infty)_\Gamma.$$

- The (generalized) Euler characteristic

$$\chi(\Gamma, E[p^\infty]) := \frac{\#\ker \Phi}{\#\operatorname{cok} \Phi}.$$

- Let

$$f_{E,p}(x) = a_r x^r + a_{r+1} x^{r+1} + \dots$$

be the characteristic series, whith $a_r \neq 0$.

- The order of vanishing $r = r_E$ and

$$a_r \sim \chi(\Gamma, E[p^\infty]).$$

Theorem

The truncated Euler characteristic $\chi(\Gamma, E[p^\infty])$ is an integer and the following conditions are equivalent:

- $\chi(\Gamma, E[p^\infty]) = 1$,
- $\mu_{E,p} = 0$ *and* $\lambda_{E,p} = r_E$, *where* $r_E = \mathrm{rank}\, E(\mathbb{Q})$.

p-adic BSD

- Perrin-Riou and Schneider proved the following p-adic analogue of the BSD formula:

$$\chi(\Gamma, E[p^\infty]) = \frac{R_{E,p} \times Ш_{E,p} \times \tau_{E,p} \times \alpha_{E,p}}{\#(E(\mathbb{Q})[p^\infty])^2}.$$

Consider the quantities:

- $R_{E,p}$ is the order of the p-primary part of the p-adic regulator of $E/\mathbb{Q}$,
- $Ш_{E,p}$ the order of the p-primary part of the Tate Shafarevich group is E,
- $\tau_{E,p}$ the order of the p-primary part of the Tamagawa product $\prod_\ell c_\ell(E)$,
- $\alpha_{E,p} := \#\tilde{E}(\mathbb{F}_p)[p^\infty]$.

Assume that p is an ordinary prime. Have the following implications:

$$R_{E,p} = 1, Ш_{E,p} = 1, \tau_{E,p} = 1, \alpha_{E,p} = 1$$
$$\Rightarrow \chi(\Gamma, E[p^\infty]) = 1$$
$$\Leftrightarrow \mu_{E,p} = 0 \text{ and } \lambda_{E,p} = r_E$$
$$\Leftrightarrow \text{Sel}(E/\mathbb{Q}_\infty)^\vee \text{ is a finitely generated} \mathbb{Z}_p\text{-module of rank } r_E.$$

Elliptic curve E fixed and the prime p varies

- Fix E and let p vary. We expect that for 100% of the primes,
$$\mu_{E,p} = 0 \text{ and } \lambda_{E,p} = r_E.$$
- It is easy to see that $Ш_{E,p} = 1$ and $\tau_{E,p} = 1$ for all but finitely many primes p.
- Primes p for which $\alpha_{E,p}$ is divisible by p are called *anomalous* primes. It is expected that 0% of primes are anomalous.
- The p-adic regulator $R_{E,p}$ is more mysterious, computational evidence points to $R_{E,p} = 1$ for 0% of primes.

- There are analogues in the case when E has supersingular reduction at p.
- We are led to make the following conjecture:

Conjecture

Let $E_{/\mathbb{Q}}$ be an elliptic curve of rank r_E. For 100% of the primes p at which E has good ordinary reduction (resp. supersingular), $\mu = 0$ and $\lambda = r_E$ (resp. $\mu^+ = \mu^- = 0$ and $\lambda^+ = \lambda^- = r_E$).

Fixed prime p and E varies

- Fix a prime p.
- Recall that any elliptic curve E over $\mathbb{Q}$ admits a unique Weierstrass equation

$$E : y^2 = x^3 + Ax + B$$

where A, B are integers and $\gcd(A^3, B^2)$ is not divisible by any twelfth power.

- It is expected that 50% of elliptic curves have rank 0 and the other 50% have rank 1.

- The height of E is defined as follows:

$$H(E) := \max\left(|A|^3, B^2\right).$$

- Let $\mathcal{E}(X)$ of elliptic curves of height $< X$.

- Let $\mathcal{A}_p(X) \subset \mathcal{E}(X)$ be the subset of elliptic curves with rank 0 and good ordinary reduction at p.
- Let $\mathcal{A}_p^0(X) \subseteq \mathcal{A}_p(X)$ be the subset of elliptic curves for which the Selmer group $\text{Sel}(E/\mathbb{Q}_\infty) = 0$, and let $\mathcal{A}_p'(X) := \mathcal{A}_p(X) \backslash \mathcal{A}_p^0(X)$.
- We analyze the proportion of elliptic curves $E_{/\mathbb{Q}}$ for which the quantities $Ш_{E,p}$, $\tau_{E,p}$, $\alpha_{E,p}$ are units.

- Ideally, we would like upper bounds for the proportion $\limsup_{X\to\infty} \frac{\mathcal{A}'_p(X)}{\mathcal{A}_p(X)}$. We obtain upper bounds for $\limsup_{X\to\infty} \frac{\mathcal{A}'_p(X)}{\mathcal{E}(X)}$.

Theorem

Let $p \geq 5$ be a fixed prime. We have that:

$$\limsup_{X\to\infty} \frac{\mathcal{A}'_p(X)}{\mathcal{E}(X)} \leq \mathfrak{d}_p + \sum_{\ell\neq p} \frac{(\ell-1)^2}{\ell^{p+2}} + \zeta(10)\cdot\frac{d(p)}{p^2}.$$

- Here, $\mathfrak{d}_p$ is the proportion of elliptic curves for which $Ш_{E,p}$ is a unit.
- Let $d(p)$ be the number of pairs $\kappa = (a, b) \in \mathbb{F}_p \times \mathbb{F}_p$ such that
  1. $\Delta(\kappa) \neq 0$.
  2. $E_\kappa : y^2 = x^3 + ax + b$ has a point over $\mathbb{F}_p$ of order p.

  For the primes p in the range $5 \leq p < 500$, computations on sage show that $d(p) \leq 1$ and $d(p) = 1$ for $p \in \{5, 7, 61\}$. The number $d(p)$ is closely related to the Kronecker class number of $1 - 4p$.

Thank you!