Arithmetic Statistics and Iwasawa theory

Anwesh Ray

University of British Columbia

anweshray@math.ubc.ca

August 17, 2021

Joint with Debanjana Kundu (PIMS/UBC).

- Arithmetic statistics (of elliptic curves) is the study of the average behaviour of certain invariants associated to elliptic curves.
- It is conjectured that half of elliptic curves have rank 0 and the other half have rank 1.
- In particular, 0 percent of all elliptic curves are expected to have rank ≥ 2.

- Some results in this direction are due to Bhargava and Shankar, who study the average size of Selmer groups.
- As a result of analyzing the average size of the 5-Selmer group, they are able to show that
  1. the average rank of elliptic curves is less than .885 (conjectured to be 0.5).
  2. Less than 20% of elliptic curves have rank ≥ 2 (conjectured to be 0%).
  3. At least 20% of elliptic curves have rank 0 (conjectured to be 50%).

- Iwasawa theory is concerned with the structure of certain Galois modules associated to elliptic curves.
- These Galois modules arise from Selmer groups, and the study of their structure is the primary motivation of the subject.
- Unlike the Selmer groups that Bhargava-Shankar work with, the Selmer groups in Iwasawa theory are defined over certain infinite towers of number fields.

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 $\times p : E[p^{n+1}] \rightarrow E[p^n]$.

- 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 $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.
- To the pair (E, p), the Galois action on the Tate-module is encoded by a Galois representation:

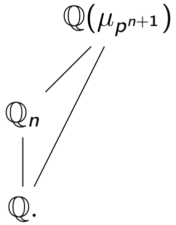
$$\rho_{E,p} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathbb{Z}_p).$$

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 over $\mathbb{Q}$.

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

- Let p be a fixed prime number.
- For $n \in \mathbb{Z}_{\geq 1}$, let $\mathbb{Q}_n$ be the subfield of $\mathbb{Q}(\mu_{p^{n+1}})$ such that $\operatorname{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n$ as depicted



- Set $\mathbb{Q}_0 := \mathbb{Q}$.

- Given a number field K, let K_n be the composite $K \cdot \mathbb{Q}_n$.
- The tower of number fields $K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n \subseteq \ldots$ is called the cyclotomic tower.
- The field K_{cyc} is taken to be the union

$$K_{\text{cyc}} := \bigcup_{n \geq 1} K_n.$$

The Galois group $\text{Gal}(K_{\text{cyc}}/K)$ is isomorphic to $\mathbb{Z}_p$.

Early Investigations

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

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

- Iwasawa showed that there are invariants μ, λ, ν such that

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

for large values of n.

Iwasawa's approach

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

Vanishing of the μ-invariant

Theorem (Fererro-Washington)

Let K be an abelian extension of $\mathbb{Q}$, the Iwasawa μ-invariant $\mu_{K,p}$ vanishes.

- The same is expected for arbitrary number field extensions $K/\mathbb{Q}$.

Iwasawa theory of Elliptic Curves

- 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.
- For a fixed elliptic curve E and prime p, Mazur studied the growth of rank $E(\mathbb{Q}_n)$ as $n \to \infty$.

Selmer groups

- The p-primary torsion group $E[p^\infty] \subset E(\bar{\mathbb{Q}})$ admits an action of the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.
- For each number field extension F of $\mathbb{Q}$, the Selmer group $\mathrm{Sel}_{p^\infty}(E/F)$ consists of Galois cohomology classes

$$f \in H^1(\mathrm{Gal}\left(\bar{\mathbb{Q}}/F\right), E[p^\infty])$$

satisfying suitable local conditions.

- It fits into a short exact sequence

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

Selmer groups

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

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

- The Pontryagin dual $\mathfrak{M}_{\text{cyc}} := \text{Hom}_{\text{cnts}}(\text{Sel}_{p^\infty}(E/\mathbb{Q}_{\text{cyc}}), \mathbb{Q}_p/\mathbb{Z}_p)$ 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, $\mathfrak{M}_{\text{cyc}}$ 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

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

Greenberg's Conjecture

Conjecture (Greenberg)

Suppose that $E[p]$ is irreducible as a Galois module, then, $\mu_{E,p} = 0$.

- For a fixed elliptic curve $E_{/\mathbb{Q}}$ without complex multiplication, it follows from Serre's Open image theorem that $E[p]$ is irreducible as a Galois module for all but finitely many primes.
- Mazur showed that if E is semistable, then $E[p]$ is irreducible for $p > 11$.
- For a fixed prime p, Duke showed that $E[p]$ is irreducible as a Galois module for 100% of elliptic curves $E_{/\mathbb{Q}}$.

- The λ-invariant satisfies the inequality $\lambda_{E,p} \geq \operatorname{rank} E(\mathbb{Q})$.
- 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 $\operatorname{rank} E(\mathbb{Q}) = 0$. Then the following equivalent conditions are satisfied for 100% of the ordinary primes p:

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

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

Theorem (D.Kundu, AR)

Let E be an elliptic curve with $\text{rank}\, E(\mathbb{Q}) = 0$. 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* $\lambda^{\pm}_{E,p} = 0$,
- $\text{Sel}^{\pm}(E/\mathbb{Q}_{\text{cyc}}) = 0$.

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

- Recall that $\Gamma = \text{Gal}(\mathbb{Q}_{\text{cyc}}/\mathbb{Q})$, the Selmer group $\text{Sel}_{p^\infty}(E/\mathbb{Q}_{\text{cyc}})$ admits an action of Γ.
- There is a natural map

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

- The (generalized) Euler characteristic

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

Relationship with Iwasawa Invariants

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* $\lambda_{E,p} = \operatorname{rank} E(\mathbb{Q})$.

p-adic Birch and Swinnerton-Dyer Conjecture

- Let E be an elliptic curve over $\mathbb{Q}$ and assume that $\text{Ш}(E/\mathbb{Q})[p^\infty]$ is finite.

Theorem (Perrin-Riou, Schneider)

The Euler characteristic $\chi(\Gamma, E[p^\infty])$ is equal to the following formula, up to a p-adic unit

$$\frac{\mathcal{R}_p(E/\mathbb{Q})}{p^{\operatorname{rank} E(\mathbb{Q})}} \times \frac{\#\text{Ш}(E/\mathbb{Q})[p^\infty] \times \prod_\ell c_\ell(E) \times \left(\#\widetilde{E}(\mathbb{F}_p)\right)^2}{\left(\#E(\mathbb{Q})[p^\infty]\right)^2}.$$

Short-hand notation

Theorem (Perrin-Riou, Schneider)

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

- $R_{E,p}$ 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 $\prod_\ell c_\ell(E)$,
- $\alpha_{E,p} := \left(\#\tilde{E}(\mathbb{F}_p)[p^\infty]\right)^2$.

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

$$\begin{aligned} & R_{E,p} = 1, Ш_{E,p} = 1, \tau_{E,p} = 1, \alpha_{E,p} = 1 \\ \Rightarrow & \chi(\Gamma, E[p^\infty]) = 1 \\ \Leftrightarrow & \mu_{E,p} = 0 \text{ and } \lambda_{E,p} = \text{rank } E(\mathbb{Q}). \end{aligned}$$

Elliptic curve E fixed and the prime p varies

- Fix E and let p vary. We expect that for 100% of the primes,
$$\mu_{E,p} = 0 \text{ and } \lambda_{E,p} = \operatorname{rank} E(\mathbb{Q}).$$
- This is the case provided $R_{E,p} = 1$ for 100% of primes p. Computational evidence shows that this is to be expected.

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

Conjecture

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

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.

- 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 $< X$.

- Fix a prime $p \geq 5$.
- Let $\mathcal{E}_p(X) \subset \mathcal{E}(X)$ be the subset of elliptic curves with
  1. rank $E(\mathbb{Q}) = 0$,
  2. good ordinary reduction at p,
  3. Either $\mu_{E,p} > 0$, or $\lambda_{E,p} > 0$ (or both).

Theorem (D. Kundu, AR)

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

$$\limsup_{X \to \infty} \frac{\mathcal{E}_p(X)}{\mathcal{E}(X)} < f_0(p) + (\zeta(p) - 1) + \zeta(10) \cdot \frac{d(p)}{p^2}.$$

- Here, $f_0(p)$ is the proportion of elliptic curves E of rank 0 for which $p \mid \#Ш(E/\mathbb{Q})$.
- Delaunay has shown that according to Cohen-Lenstra heuristics, one should expect

$$f_0(p) = 1 - \prod_{j=1}^{\infty}\left(1 - \frac{1}{p^{2j-1}}\right) = \frac{1}{p} + \frac{1}{p^3} - \frac{1}{p^4} + \frac{1}{p^5} - \frac{1}{p^6} \dots .$$

- These numbers decrease rapidly as p increases, for instance, $f_0(2) \approx 0.58$, $f_0(3) \approx 0.36$ and $f_0(5) \approx 0.21$.

- Here, $d(p)$ 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.
- The number $d(p)$ is closely related to the Kronecker class number of $1 - 4p$. Computations show that the values $d(p)/p^2$ tend to decrease as p increases, however, there is much oscillation in the data.

Values of $d(p)/p^2$ for $7 \leq p < 150$

p	$d(p)/p^2$	p	$d(p)/p^2$
7	0.0816326530612245	71	0.0208292005554453
11	0.0413223140495868	73	0.0270219553387127
13	0.0710059171597633	79	0.0374939913475405
17	0.0276816608996540	83	0.0178545507330527
19	0.0581717451523546	89	0.0222194167403106
23	0.0415879017013233	97	0.0255074928260176
29	0.0332936979785969	101	0.00980296049406921
31	0.0312174817898023	103	0.0288434348194929
37	0.0306793279766253	107	0.00925845051969604
41	0.0118976799524093	109	0.0181802878545577
43	0.0567874526771228	113	0.0263137285613595
47	0.0208239022181983	127	0.0169260338520677
53	0.0277678889284443	131	0.0189382903094225
59	0.0166618787704683	137	0.0108689860940913
61	0.0349368449341575	139	0.0142849748977796
67	0.0147026063711294	149	0.0133327327597856

Elliptic curves with large λ-invariant

- The λ-invariant $\lambda_{E,p}$ gives an upper bound for rank $E(\mathbb{Q}_n)$ as $n \to \infty$.
- On the other hand, the rank boundedness Conjecture asks if there exist elliptic curves $E_{/\mathbb{Q}}$ with arbitrarily large Mordell-Weil rank.
- Given any prime p, Greenberg showed that there exist elliptic curves $E_{/\mathbb{Q}}$ for which $\mu_{E,p} + \lambda_{E,p}$ is arbitrarily large.

Lower Bounds

Theorem (D. Kundu, AR)

Let $p \geq 5$ be a prime and $N \in \mathbb{Z}_{\geq 1}$. There is an explicit lower bound $\mathfrak{d}_{p,N} > 0$ for the density of elliptic curves $E_{/\mathbb{Q}}$ for which

$$\mu_{E,p} + \lambda_{E,p} \geq N.$$

- The quantity $\mathfrak{d}_{p,N}$ is given by some explicit infinite sums, which gets smaller as either N or p increases.
- We do assume the finiteness of $\text{Ш}(E/\mathbb{Q})[p^\infty]$ in our arguments.
- On assuming Greenberg's conjecture, the inequality $\mu_{E,p} + \lambda_{E,p} \geq N$ may be replaced with $\lambda_{E,p} \geq N$.

Recent Work

- The results have been extended to anticyclotomic $\mathbb{Z}_p$-extensions, joint with J.Hatley and D.Kundu. Here, results are proved when the imaginary quadratic field is allowed to vary.
- In joint work with L.Beneish and D.Kundu, we use techniques in Iwasawa theory to study arithmetic statistics for rank jumps and growth of Selmer groups of elliptic curves in $\mathbb{Z}/p\mathbb{Z}$-extensions.

Thank you!