Arithmetic statistics and Iwasawa theory

Sachin Kumar
University of Waterloo, Faculty of Mathematics

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% of all elliptic curves are expected to have rank ≥ 2. Some results in this direction are due to Bhargava and Shankar, who studied the average size of Selmer group, a subgroup of the Tate-Shafarevich group. As a result of analyzing the average size of the 5-Selmer group, they were able to prove that,

1. The average size of elliptic curves is less than 0.885 (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 the Selmer group, 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.

We will now discuss the classic representation related to elliptic curves, the 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 $E(\overline{\mathbb{Q}})$. The p-adic Tate-module $T_p(E)$ is the inverse limit, '

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

where the inverse limit is taken with respect to 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 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. To the pair (E, p), the Galois action on the Tate-module is encoded by the Galois representation,

$$\rho_{E,p} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}_p)$$

We study two interrelated problems: For a fixed elliptic curve E, we study the invariants associated to the p-adic Galois representation $\rho_{E,p}$ as p ranges over all primes, and 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. For $n \in \mathbb{Z}_{\geq 1}$, let $\mathbb{Q}_n$ be the subfield of $\mathbb{Q}(\mu_{p^{n+1}})$ such that $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n$. 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, $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq \cdots$ is called the cyclotomic tower. The field K_{cyc} is taken to be the union,

$$K_{\mathrm{cyc}} = \bigcup_{n\geq 1} K_n$$

The Galois group $\mathrm{Gal}(K_{\mathrm{cyc}}/K) \cong \mathbb{Z}_p$. Iwasawa's early investigation 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 proved 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. What did Iwasawa think? There are natural maps $\mathcal{A}_{n+1}(K) \to \mathcal{A}_n(K)$ and the inverse limit $A_textcyc(K) = \lim_{\leftarrow} \mathcal{A}_n(K)$ is a module over $\Gamma_K = \mathrm{Gal}(K_{\mathrm{cyc}}/K)$. Iwasawa introduced the completed algebra $\Lambda = \lim_{\leftarrow} \mathbb{Z}_p[\mathrm{Gal}(K_n/K)] \simeq \mathbb{Z}_p[[x]]$. He proved that $\mathcal{A}_{\mathrm{cyc}}(K)$ is a finitely generated torsion $\mathbb{Z}_p[[x]]$-module and his theorem is a consequence if the structure theory of such modules.

Vanishing of the μ-invariant

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

The same is expected fir arbitrary number field extensions $K/\mathbb{Q}$. Mazur initiated the Iwasawa theory of elliptic curves over $\mathbb{Q}$. Throughout, we let E be an elliptic curves over $\mathbb{Q}$ with good ordinary reduction at p. For a fixed elliptic curve E and prime p, Mazur studied the growth of rank $E(\mathbb{Q})$ as $n \to \infty$.

Selmer Group

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

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

satisfying suitable local conditions. It fits into a short exact sequence,

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

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

$$\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_{\mathrm{cyc}}) = \lim_{\to n} \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_n)$$

The Pontryagin dual,

$$\mathfrak{M}_{\mathrm{cyc}} = \mathrm{Hom}_{\mathrm{cnts}}(\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_{\mathrm{cyc}}), \mathbb{Q}_p/\mathbb{Z}_p)$$

is a finitely generated and torsion $\Lambda \simeq \mathbb{Z}_p[[x]]$ module. We will now discuss some Iwasawa Invariants, by the structure theory of $\mathbb{Z}_p[[x]]$ modules, up to a pseudoisomorphism, $\mathfrak{M}_{\mathrm{cyc}}$ 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,

$$\mu_{E.p} = \sum_j \mu_j$$

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 multipication, 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 proved that $E[p]$ is irreducible as a Galois module for 100% of elliptic curve $E/\mathbb{Q}$. The λ-invariant satisfies the inequality $\lambda_{E,p} \geq \text{rank} E(\mathbb{Q})$. We would like to model the average behaviour of the Iwasawa invarinats μ and λ in two cases:

- When E is fixed and p varies.
- When p is fixed and E varies.

Theorem (Greenberg). Let E be an elliptic curve and rank $E(\mathbb{Q}) = 0$. Then the following equivalent conditions are satisfied for 100% of the ordinary primes p,

- $\mu_{E,p} = 0$ and $\Lambda_{E,p} = 0$
- $\text{Sel}_{p^\infty}(E/\mathbb{Q}_{\text{cyc}}) = 0$

Theorem (D.Kundu). Let E be an elliptic curve with 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,

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

We will now discuss the 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 $\lambda_{E,p} = \text{rank } E(\mathbb{Q})$

p-adic Birch and Swinnerton-Dyer conjecture

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

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

We can simplify the above formlua,

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

$R_{E,p}$ 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, $\prod_\ell c_\ell(E)$ and $\alpha_{E,p} = (\#\overline{E}(\mathbb{F}_p)[p^\infty])^2$. Assume that p is an ordinary prime. Have the following implications:

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

Let Elliptic curve E be fixed and let p vary. We expect that for 100% of the primes,

$$\mu_{E,p} = 0 \text{ and } \lambda_{E,p} = \text{rank } E(\mathbb{Q})$$

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 respectively supersingular $\mu = 0$ and $\lambda = \text{rank}E(\mathbb{Q})$, respectively $\mu^+ = \mu^- = 0$ and $\lambda^+ = \lambda^- = \text{rank}E(\mathbb{Q})$. 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 $A, B \in \mathbb{Z}$ and $\gcd(A^3, B^2)$ is not divisible by any twelfth power. The height of E is defined as follows:

$$H(E) = \max(|A|^3, B^2)$$

Let $\mathcal{E}(X)$ of elliptic curves of height $< X$. Fix a primes $p \geq 5$. Let $\mathcal{E}_p(X) \subset \mathcal{E}(X)$ be the susbet of elliptic curves with $\text{rank}E(\mathbb{Q}) = 0$, good ordinary reduction at p, either $\mu_{E,p} > 0$, or $\lambda_{E,p} > 0$ (or both)

Theorem (D Kundu). Let $p \geq 5$ be a fixed prime. We have that:

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

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,

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

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, $\Delta(\kappa) \neq 0$ and $E_\kappa : y^2 = x^3 + ax + b$ 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 $\frac{d(p)}{p^2}$ tend to decrease as p increases, however, there is much oscillation in the data.

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.

Theorem (D Kundu). 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 $Ш(E/\mathbb{Q})[p^\infty]$ in our arguments. On assuming Greenberg's conjecture, the inequality $\mu_{E,p} + \lambda_{E,p} \geq N$ may be replaced with $\lambda_{E,p} \geq N$.

The results have been extended to anticyclotomic $\mathbb{Z}_p$-extension, 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. Baneish 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.