LECTURE NOTES FOR CRM WORKSHOP ON "COUNTING ARITHMETIC OBJECTS (RANKS OF ELLIPTIC CURVES)" NOVEMBER 10-14, 2014

STANLEY YAO XIAO
stanley.xiao@uwaterloo.ca
Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario, Canada N2L 3G1

AND

JUSTIN SCARFY
scarfy@ugrad.math.ubc.ca
Department of Mathematics
The University of British Columbia
Room 121, 1984 Mathematics Road
Vancouver, British Columbia, Canada V6T 1Z2

ABSTRACT. This compilation contains all the lecture notes taken at the conference "Counting arithmetic objects (Ranks of elliptic curves)" held at the CRM between November 10 and 14, 2014. We would like to thank the organizers for putting together this wonderful conference with such diverse areas, for the speakers presenting their newest results, and for the CRM for its hospitality. The lecture notes were mostly typed up live by the first of us, and later corrected and polished by the second of us.

CONTENTS

1. ARITHMETIC INVARIANTS OF ELLIPTIC CURVES ON AVERAGE (1/2)

BY MANJUL BHARGAVA

Recall: Any elliptic curve E over $\mathbb{Q}$ can be expressed uniquely in the form

$$E_{A,B} : y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}, \text{and if } p^4 \mid A \text{ then } p^6 \nmid B \text{ for all primes } p.$$

Define the (naive) height

$$H(E_{A,B}) := \max\{4|A|^3, 27B^2\}.$$

Note: the discriminant Δ of the elliptic curve $E_{A,B}$ is given by

$$\Delta = -4A^3 - 27B^2.$$

Consider the number of curves $E_{A,B}$ of height at most X. This count is equal to

$$\#\{E_{A,B} : H(E_{A,B}) < X\} = cX^{5/6} + o(X^{5/6}).$$

If we order all $E_{A,B}/\mathbb{Q}$ by height, we ask:

Q1: the average rank of $E_{A,B}$?
- Conjecture 1: the average rank of $E_{A,B}$ ordered by height is equal to $1/2$ (Goldfeld, Katz-Sarnak).

Q2: the average size of the n-Selmer group of $E_{A,B}$?
- Conjecture 2: the average size of the n-Selmer group is equal to $\sigma(n)$ (NEW).

Q3: the average size of the root number of $E_{A,B}$?
- Conjecture 3: the average should be zero (equidistribution of root number).

Q4: the proportion of $E_{A,B}$ satisfying BSD?
- Conjecture 4: it should be 100%. In fact, BSD says all elliptic curves satisfy BSD.

Theorem 1.1. *Conjectures 2 and 3 imply Conjecture 1 and the parity conjecture.*

Proof. Exercise. □

Theorem 1.2. *Conjecture 2 implies Conjecture 4.*

The proof of Theorem 1.2 will be given in the Lectures 1 and 4.

Remark 1.3. *Essentially nothing known previously on Q1 to Q4 beyond trivial bounds. There were many conditional results under GRH, BSD, and other heuristics.*

We begin with some latest progress made on Q2:

Theorem 1.4. *(with Arul Shankar)*

$$\mathrm{Avg}(\mathrm{Sel}_n(E_{A,B})) = \sigma(n) \quad \textit{for } n = 1, 2, 3, 4, 5.$$

Proof. (Outline)

(a) For each n, find a representation V of an algebraic group G, defined over $\mathbb{Z}$, such that:
  (i) the ring of invariants of $G(\mathbb{C})$ on $V(\mathbb{C})$ is freely generated by two elements, which we call A, B.
  (ii) there is an injective map

(∗) $$\mathrm{Sel}_n(E_{A,B}) \hookrightarrow [G(\mathbb{Z})\backslash V(\mathbb{Z})]_{A,B}$$

For each n, we require a pair (G, V).

- For $n = 2$, we have $(G, V) = (\mathrm{PGL}_2, \mathrm{Sym}^4(2))$ ($\mathrm{Sym}^4(2)$ are binary quartic forms). This was due to Birch and Swinnerton-Dyer .
- For $n = 3$, we have $(G, V) = (\mathrm{PGL}_3, \mathrm{Sym}^3(3))$ (ternary cubic forms) due to Cassels, Cremona-Fisher-Stoll , Aronholdt .
- For $n = 4$, we have $(G, V) = ((\mathrm{GL}_2 \times \mathrm{GL}_4)/\sim, 2 \otimes \mathrm{Sym}^2 4)$ ($2 \otimes \mathrm{Sym}^2 4$) refer to two quadrics in $\mathbb{P}^3$). This was due to Clebesch , Cremona-Fisher-Stoll .
- For $n = 5$, we have $(G, V) = ((\mathrm{GL}_5 \times \mathrm{GL}_5)/\sim, 5 \otimes \Lambda^2 5)$ (5×5 skew-symmetric matrices in linear forms in five variables). This was due to Cayley , Sylvester , Buchsbawn-Eisenbud .

Note: An n-Selmer element of $E_{A,B}$ can be viewed as a map $C \to \mathbb{P}^{n-1}$ such that $\mathrm{Jac}(C) = E_{A,B}$ and C is a genus one curve that has local points everywhere.

- When $n = 2, 3, 4$, it is easy to understand geometrically from this point of view.
- When $n = 5$, it is a genus one curve in $\mathbb{P}^4$, with five quadrics contain it. One cannot take arbitrary quadrics, as they typically intersect trivially. Thus one needs to take special consideration.

Remark 1.5. *If we knew a similar way to understand the map $C \to \mathbb{P}^{n-1}$ for $n > 5$ (C is a genus one curve) then could likely understand n-Selmer for $n > 5$ (algebraic geometry problems).*

(b) Count $G(\mathbb{Z})$-orbits on $V(\mathbb{Z})$ having bounded A and B (geometry of numbers).
(c) Elements in image of $(*)$ are defined by infinitely many congruence conditions. Sieve to these elements using variant of Ekedahl sieve.
(d) Divide by $cX^{5/6}$ gives $\sigma(n)$.

□

Note: $\mathrm{Avg}(\mathrm{Sel}_5(E_{A,B})) = 6 \Rightarrow$ 5-Selmer rank of $E_{A,B}$ is 0 or 1 most of the time.
Open problems:

(0) Does p-Selmer rank zero imply analytic rank zero? We know that p-Selmer rank zero implies rank zero (due to Kolyvagin) and also that analytic rank zero imply rank zero.
(1) Does p-Selmer rank 1 implies analytic rank 1, and analytic rank 1 implies rank 1 (Gross-Zagier-Kolyvagin). But does p-Selmer rank imply rank 1?
(S) Special case: does $\mathrm{Sel}_2(E) = \mathbb{Z}/2\mathbb{Z}$ (rational 2-torsion free) imply rank 1? It is unknown!

2. IWASAWA THEORY AND RANKS OF ELLIPTIC CURVES AND SELMER GROUPS (1/2) BY ERIC URBAN

Let E be an elliptic curve over $\mathbb{Q}$. We consider the cases when p a is prime of good reduction, ordinary good reduction, or multiplicative reduction.

$$\mathrm{Sel}_p(\mathbb{Q}, E) \subset H^1(\mathbb{Q}, E_{p^\infty}(\overline{\mathbb{Q}})).$$

We have the exact sequence

$$0 \to E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_p(\mathbb{Q}, E) \to Ш_p(\mathbb{Q}, E) \to 0.$$

(C0) If E has rank 0, then the corank p-$\mathrm{Sel} = 0$ implies $L(E, 1) \neq 0$. The converse implication is due to Gross-Zagier-Kolyvagin . (and Kato has a different method)

(C1) If E has rank 1: then the corank p-$\mathrm{Sel} = 1$ implies $L(E, s) = 1$ for $s = 1$, due to Gross-Zagier-Kolyvagin.

(0) For rank 0, use p ordinary prime and it follows from the Iwasawa Main Conjecture for E (by Skinner-Urban). For p multiplicative reduction case, due to Skinner. For p supersingular, follows from Bloch-Kato conjecture for E (Skinner-Urban).

(1) For rank 1, p ordinary done by Wei Zhang good ordinary real. Venerucci dealt with the multiplicative reduction case. In these two approaches the Iwasawa Main Conjecture for E is used.

2.1. **Iwasawa theory, Iwasawa-Greenberg conjectures.**

Let $\mathcal{O}/\mathbb{Z}_p$ be a finite extension, k its residue field, R be a local noetherian complete $\mathcal{O}$-algebra with residue field k.
We have a Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_N(R)$ such that:

(1) There exists $\Sigma \subset \mathrm{Spec}(R)(\overline{\mathbb{Q}}_p)$ (Zariski dense) such that for every $x \in \Sigma$, $\rho_x = G_{\mathbb{Q}} \xrightarrow{\mathrm{ev}_x} \mathrm{GL}_N(R) \to \mathrm{GL}_N(\overline{\mathbb{Q}}_p)$. ρ_x is motivic, p-ordinay,

$$\rho_k|_{I_p} \sim \begin{pmatrix} \varepsilon^{m_N(x)} & \cdots & * \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \varepsilon^{m_1(x)} \end{pmatrix}.$$

For $\mathrm{Fil}^i(V_x)$ or $\mathrm{Fil}^i \,/\, \mathrm{Fil}^{i+1}$, the action given by $\varepsilon_{\mathrm{cyc}}^i$.

(2) For all $x \in \Sigma$, ρ_x is critical in the sense of Deligne, i.e.

$$\frac{L(\rho_x, 0)}{\Omega_\infty(\rho_x)\Omega_p(\rho_x)} \in \overline{\mathbb{Z}}_p.$$

With the assumption: $\overline{\rho}^{G_{\mathbb{Q}}} = 0$, we formulate the following conjectures:

Conjecture 2.1.

(1) There exists $\mathcal{L}_\rho \in R$ such that for all $x \in \Sigma$, $\mathcal{L}_\rho(x) = \dfrac{L(\rho_x, 0)}{\Omega_\infty(\rho_x)\Omega_p(\rho_x)}$ (up to p-adic units).

(2) If $\mathcal{L}_\rho \neq 0$ then a certain Selmer group is co-torsion over R. First, one defines $\mathrm{Sel}(\mathbb{Q}, \rho_x) \subset H^1(\mathbb{Q}, \rho_x \otimes L/\mathcal{O})$, $ev_x(R) \subset \mathcal{O} \subset \overline{\mathbb{Z}}_p$, $L = \mathrm{Frac}(\mathcal{O})$. An element in $\mathrm{Sel}(\mathbb{Q}, \rho_x)$ characterizes an isomorphism class of extensions

$$0 \to \rho_x \otimes \overline{\omega}^{-m}\mathcal{O}/\mathcal{O} \to W \to \omega^{-n}\mathcal{O}/\mathcal{O} \to 0$$

such that for all $\ell \neq p$, the restriction of I_ℓ is split plus ordinary reduction at p. W is free of rank $N+1$ over $\mathcal{O}/\omega^n\mathcal{O}$. W is ordinary if

$$\rho_W|_{I_p} \sim \begin{pmatrix} \varepsilon^{m_N(x)} & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & * \\ \vdots & \ddots & \vdots & \cdots & \cdots & \cdots & \cdots & \vdots \\ 0 & \cdots & \varepsilon^{m_{s+1}(x)} & \cdots & \cdots & \cdots & \cdots & \vdots \\ 0 & \cdots & 0 & 1 & & & & \\ 0 & \cdots & 0 & 0 & \varepsilon^{m_s(x)} & \cdots & \cdots & \vdots \\ 0 & \cdots & 0 & 0 & \ddots & \cdots & \cdots & \vdots \\ 0 & \cdots & 0 & \vdots & 0 & \ddots & \cdots & * \\ 0 & \cdots & 0 & 0 & 0 & \cdots & \cdots & \varepsilon^{m_1(x)} \end{pmatrix},$$

where $m_N(x) \geq \cdots \geq m_{s+1}(x) > 0 \geq m_s(x) \geq \cdots \geq m_1(x)$.

Let $F^t_{\rho_x} \subset \rho_x$ the subspace generated by $N-s$ first vectors of the basics, which implies

$$0 \to \rho_x/F^t_{\rho_x} \otimes \omega^{-n}\mathcal{O}/\mathcal{O} \to W/F^T_{\rho_x} \to \omega^{-n}\mathcal{O}/\mathcal{O} \to 0,$$

which then implies

$$[w]|_{I_p} \in \ker(H^1(\mathbb{Q}, \rho_x \otimes L/\mathcal{O}) \to H^1(I_p, \rho_x/\rho^t\rho_x \otimes L/\mathcal{O})).$$

2.2. **Extra condition on ρ.**

There exists $F^+\rho \subset V_\rho = R^N$ such that for all $x \in \Sigma$, $(F^+\rho)_x = F^+(\rho_x)$.

Remark 2.2.

(1) $F^+\rho$ depends on Σ and for a given ρ there exist possibly several sets Σ giving rise to different elements $F^t\rho$.
(2) Different Σ's give rise to different p-adic L-functions.

Selmer groups Sel_p, S a finite set of primes, $p \notin S$. (Upper star below denotes the pontryagin dual)

$$\mathrm{Sel}^S(\mathbb{Q}, p) = \ker(H^1(\mathbb{Q}, \rho \otimes R^*) \to \bigoplus_{\substack{l \notin S \\ \rho \neq 0}} H^1(I_l, \rho \otimes R^*) \oplus H^1(I_p, \rho/F^+\rho \otimes R^*)).$$

Conjecture 2.3. *(Iwasawa-Greenberg): If $\mathcal{L}_\rho \neq 0$, then $X_{F^+\rho}(\mathbb{Q}, \rho) = \left(\mathrm{Sel}^{\emptyset}_{F^t\rho}(\mathbb{Q}, \rho)\right)^*$ is torsion over R and $\mathrm{Fil}\, H_R(X_{F^+\rho}(\mathbb{Q}, \rho)) = \mathcal{L}_\rho$.*

Example 2.4. *Take $\rho_0 : G_\mathbb{Q} \to \mathrm{GL}_N(\mathcal{O})$ attached to a motive, ordinary at p and critical. $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$, $\mathbb{Q}_\infty/\mathbb{Q}$ $\mathbb{Z}_p$-cyclotomic extension. $\rho_0 \otimes \mathcal{O}[[\Gamma]]$*

For all ψ finite order, $x_\psi : \mathcal{O}[[\Gamma]] \mapsto \overline{\mathbb{Z}}_p$, $\sigma \mapsto \psi(\sigma)$, $\rho_x = \rho_0 \otimes \psi$ implies p-adic L-function interpolating $\dfrac{L(\rho_0 \otimes \psi, 0)}{\text{periods}}$.

Special case: take $\rho_0 : G_\mathbb{Q} \to \mathrm{GL}(T_p(E))$, E ordinary at p.

$$L(\rho_0 \otimes \psi, 0) = L(E, \psi, 1)$$

implies it is known that there exists p-adic L-function interpolating those values. Where the Main Conjecture implies that $\mathrm{Fil}^{\bullet} H(\mathrm{Sel}(\mathbb{Q}, \rho_{T_p(E)} \otimes [\cdot]))^* \sim (L_p(E, \cdot))$.

Example 2.5. *Rankin-Selberg conditions. Let f be an elliptic modular form of level N and weight k, and g an elliptic modular form of level N and weight l, both ordinary at p.*

Their Galois representations ρ_f is of Hodge-Tate weight $(k-1, 0)$, $\rho_f|_{I_p} \sim \begin{pmatrix} 1 & * \\ 0 & \varepsilon^{-k} \end{pmatrix}$, and ρ_g is of Hodge-Tate weight $(l-1, 0)$.

Define two Hida families F, G where $F \in \mathbb{I}[[q]]$, $\mathbb{I}/\mathcal{O}[[w_1]]$ $G \in \mathbb{J}[[q]]$, $\mathbb{J}/\mathcal{O}[[w_2]]$ and two big representations

$$\rho_F : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{I}),$$
$$\rho_G : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{J}).$$

$R = \mathbb{I} \otimes_{\mathcal{O}} \mathbb{J} \otimes \mathcal{O}[[\Gamma]]$, *where* $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ *and such* $\rho_{R\text{-}S} = \rho_F \otimes \rho_G \otimes [\cdot] \subset \mathrm{GL}_4(R)$. *Critical points inside* $\mathrm{Spec}(R)(\overline{\mathbb{Q}}_p)$ *are given by* $(f, g, \varepsilon^n\psi) = x$.

(I) When $k > l$, $\rho_f \otimes \rho_g \otimes \varepsilon^n\psi$ critical if $k - 1 \geq m \geq l$.

(II) $k < l$, $\rho_f \otimes \rho_g \otimes \varepsilon^n\psi$ critical if $l - 1 \geq m \geq k$.

Then

(I) $F^+\rho_x = F^+\rho_f \otimes \rho_g$

$$\rho_x|_{I_p} \sim \begin{pmatrix} \varepsilon^n & & & \\ 0 & \varepsilon^{1-l+n} & & \\ 0 & 0 & \varepsilon^{1-k+n} & \\ 0 & 0 & 0 & \varepsilon^{2-k-l+n} \end{pmatrix}$$

$F^+\rho = F^+\rho_F \otimes \rho_G$

(II) $F^+\rho_x = F^+\rho_g \otimes \rho_f$ $F^+\rho = F^+\rho_G \otimes \rho_F$.

3. IWASAWA THEORY AND RANKS OF ELLIPTIC CURVES AND SELMER GROUPS (2/2) BY ERIC URBAN

Recall we had two Hida families F, G with Galois deformation

$$\rho = \rho_F \otimes \rho_G \otimes \mathcal{O}[[\Gamma]]$$

and we had two types:

(I) $\Sigma = \{(f, g, \varepsilon_{\text{cyc}}^n \psi), k-1 \geq n \geq l\}$, $F_\rho^+ = F_{\rho_F}^+ \otimes \rho_G \otimes \Lambda$.
(II) $\Sigma = \{(f, g, \varepsilon_{\text{cyc}}^n \psi), l-1 \geq n \geq k\}$, $F_\rho^+ = \rho_F \otimes F^+\rho_G \otimes \Lambda$.

Hida defined

$$L^{\text{I}}(x) = \frac{L(f \times g, m)}{\Omega_p(g)}$$

$$L^{\text{II}}(x) = \frac{L(f, g, m)}{\langle g, g \rangle \Omega_p(g)}.$$

Special case: When $g \in G$ is an CM form, K an imaginary quadratic field, p splits in K. Let $g \to \chi$ be a Hecke character of K of Hodge-Tate type $(l-1, 0)$, then

$$K \subset \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_p \to \chi_{\mathfrak{p}} : G_K \to \overline{\mathbb{Q}}_p^x.$$

$I_p = I_{\mathfrak{p}}$, $\chi_{\mathfrak{p}}|I_{\mathfrak{p}}$ = Frobinous character $\times \varepsilon_{\text{cyc}}^{1-l}$, $\chi_{\mathfrak{p}}^c|I_{\mathfrak{p}}$ is trivial.

$\rho_g = \text{Ind}_{G_K}^{G_{\mathbb{Q}}} \chi_{\mathfrak{p}}$,

$$\rho_g|I_{\mathfrak{p}} = \begin{pmatrix} 1 & \cdots & * \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \varepsilon^{1-\ell} \times \text{roots} \end{pmatrix}$$

then G is family of CM-forms, and thus we have two p-adic L-functions:

(I) For $\sum(f, \chi, \varepsilon^n \psi)$, when $k-1 \geq n \geq l$ we have L^{I}.
(II) For $\sum(f, \chi, \varepsilon^n \psi)$, when $l-1 \geq n \geq k$ we have L^{II}.

3.1. **Selmer conditions.**

I) $F^+\rho = F^+\rho_F \otimes \text{Ind}_{G_K}^{G_{\mathbb{Q}}} \chi_\rho$, $\text{Sel}(\mathbb{Q}, \rho_x) \subset H^1(\mathbb{Q}, \rho_F \otimes \text{Ind}_{G_K}^{G_{\mathbb{Q}}} \chi_{\mathfrak{p}}) = H^1(K, \rho_F \otimes \chi_{\mathfrak{p}})$.

$$\text{Sel}(\mathbb{Q}, l_x) = \{\ker(H^1(k, \rho_F \otimes \chi_{\mathfrak{p}}) \to H^1(K, l_F/F^+\rho_F \otimes \chi_{\mathfrak{p}}).$$

$\Gamma_K = \text{Gal}(K_\infty/K)$, maximal $\mathbb{Z}_p$ extension of K, isomorphic to $\Gamma_+ \times \Gamma_-$.

I) $\text{Sel}(\mathbb{Q}, \rho_F \otimes \rho_G \otimes \Lambda) = \text{Sel}^I(K_\infty, \rho_F)$, usual Selmer condition for F.

II) $F^+\rho_x = \rho_F \otimes F^+\rho_g = \rho_F \otimes \mathcal{O}$, $\rho_x/F^+\rho_x = \rho_F \otimes \varepsilon^{1-l}$,

$$\rho_g|_{I_{\mathfrak{p}}} = \begin{pmatrix} 1 & 0 \\ 0 & \varepsilon^{1-l} \end{pmatrix}$$

implies

$$\text{Sel}^{\text{II}}(\rho_x) = \ker(H^1(K, \rho_F \otimes \chi_{\mathfrak{p}}) \to H^1(K_{\mathfrak{p}}, \rho_g \otimes \chi_{\mathfrak{p}})$$

Theorem 3.1. *(Skinner, Urban) Iwasawa-Greenberg conjecture is true for* $\text{Sel}^I(K^\infty, \rho_F)$.

Theorem 3.2. *(X. Wan) Iwasawa-Greenberg conjecture is true for* $\mathrm{Sel}^{II}(K^\infty, \rho_F)$.

The main idea in the proofs of these theorems is to study Eisenstein congruences.

Remark 3.3. *f eigenfunction inside the Hida family F. The Iwasawa Main Conjecture implies* $\mathrm{Sel}^I(K_\infty, f) \to L^I(K_\infty, f)$. *Kato has a theorem implies that* $\mathrm{Sel}(\mathbb{Q}_\infty, f) \to L_p(f, s)$.

$$L_p(f,s) \times L_p(f \otimes \left(\tfrac{\cdot}{K/\mathbb{Q}}\right), s) \to \mathrm{Sel}(F) \oplus \mathrm{Sel}(F \otimes \left(\tfrac{\cdot}{K/\mathbb{Q}}\right)).$$

(I) One looks at Eisenstein series for $U(2,2)$, $E(\pi, \chi)$, its Galois representation is going to be of the form $\sigma_\pi \oplus \chi_{\mathfrak{p}} \oplus \chi_{\mathfrak{p}}^{-c} \det(\sigma_\pi)$.

Remark 3.4. $H^1(K, \rho \otimes \chi^{-1})$

$$0 \to \rho \otimes \mathcal{O}/\omega^n \to W \to \mathcal{O}/\overline{\omega}^n(\chi) \to 0.$$

Ribet's idea: Find a Galois representation r such that

(1) r is irreducible, $r : G_K \to \mathrm{GL}_{n+1}(\mathcal{O})$ and
(2) $\overline{r} = (r \pmod{\overline{\omega}}) = \overline{\rho} \oplus \overline{\chi}$. Then construct a lattice $\mathcal{L}$ in r which is non-split.

$$0 \to \rho \otimes \mathcal{O}/\overline{\omega}^n \to \mathcal{L}/\omega^n\mathcal{L} \to \mathcal{O}/\omega^n(\chi) \to 0.$$

If moreover we know that r is ordinary, then $r_{\mathcal{L}} \pmod{\overline{\omega}^n}$ is ordinary as well. (r, V) $\mathrm{Fil}^i V/\mathrm{Fil}^{i+1}$ action of I_p is given by ε_{cyc}^i.

Look for cusp forms $E(\pi, \chi) \pmod{\overline{\omega}^n}$. Then

$$\mathrm{tr}(\rho_\sigma) \equiv \mathrm{tr}(\rho_H) + \chi + \chi^{-c} \det(\rho_\pi) \pmod{\overline{\omega}^n}.$$

the important point of the construction of the Eisenstein series is given by $E(\pi, \chi) \pmod{\frac{L(\pi \otimes \chi^{-1}, 0)}{\text{period}}}$ looks like a cusp form.

Consequences:

(I) $L(E,1) = 0$ implies $\mathrm{Sel}(\mathbb{Q}, E)$ is of rank at least 1. Selmer rank equal zero implies $L(E,1) \neq 0$.
(II) $L^{\text{II}}(E/K, 1) = 0 \Rightarrow \mathrm{Sel}^{\text{II}}(k, E)$ is of corank at least 1.

$$\ker(H^1(K, V_pE/T_pE) \to H^1(K_{\mathfrak{p}}, V_pE/T_pE)),$$

$$H^1_{\mathfrak{p}}(K, V_pE) := \ker(H^1(K, V_pE) \to H^1(K_{\mathfrak{p}}, V_pE))$$

$$H^1_F(K, V_pE) := \ker(H^1(K, V_pE) \to H^1_F(K_{\mathfrak{p}}, V_pE)) \oplus H^1_f(K_{\mathfrak{p}^c}, V_pE)$$

Lemma 3.5. *(Skinner) if $H^1_f(K, V_p(E)) \to H^1_f(K_p, V_p(E))$ and the rank of $H^1_f(K, V_p(E)) = 1$, then*

$$H^1_{\mathfrak{p}}(K, V_p(E)) = 0.$$

Theorem 3.6. *(Skinner) Assume $H^1_f(K, V_p(E)) \to H^1_f(K_p, V_p(E))$ and rank $H^1_f(K, V_p(E)) = 1$, then the analytic rank is* 1.

4. ARITHMETIC INVARIANTS OF ELLIPTIC CURVES ON AVERAGE (2/2)
BY MANJUL BHARGAVA

Recall from Lecture 1:

$$\mathrm{Sel}_n(E_{A,B}) \hookrightarrow [G(\mathbb{Z})\backslash V(\mathbb{Z})]_{A,B}\,.$$

How to count elements in the right hand side such that $H(A,B) = \max\{4|A|^3, 27B^2\} < X$ when proving Theorem 1.4

(ii) Construct fundamental domains for $G(\mathbb{Z})$ on $V(\mathbb{R})$.
  (i) Construct a fundamental domain L for $G(\mathbb{R})$ on $[V(\mathbb{R})]_{H=1}$ such that L is bounded in $V(\mathbb{R})$.
  (ii) Construct a fundamental domain $\mathcal{F}$ for $G(\mathbb{Z})$ on $G(\mathbb{R})$ that is contained in a 'Siegel set'. That is, $\mathcal{F} = N'A'K$ (the Iwasawa decomposition) where N' is a bounded set of lower triangular matrices, A' is a set of diagonal matrices, and K is a compact subgroup.

  Example: If $G = \mathrm{SL}_2$, then

$$\begin{aligned} N'(t) &= \left\{ \begin{pmatrix} 1 & 0 \\ n(t) & 1 \end{pmatrix} : |n(t)| \le 1/2 \right\}, \\ A'(t) &= \left\{ \begin{pmatrix} t^{-1} & 0 \\ 0 & t \end{pmatrix} : t \ge 3^{1/4}/2^{1/2} \right\} \\ K(t) &= \mathrm{SO}_2\,. \end{aligned}$$

Then for any $g \in G(\mathbb{R})$, $\lambda\mathcal{F}gL$ is a fundamental domain for $G(\mathbb{Z})$ on $[V(\mathbb{R})]_{H=1}$.

Proof. By symbolic manipulation.

$$[G(\mathbb{Z})\backslash G(\mathbb{R})] \times [G(\mathbb{R})\backslash V(\mathbb{R})] = G(\mathbb{Z})\backslash V(\mathbb{R}).$$

□

(iii) How to count points in $\Lambda\mathcal{F}gL$ of bounded height? (Here $\Lambda = \{\lambda : \lambda > 0\}$.)

4.1. **Averaging method.**

Choose $g \in G_0$ where G_0 is compact in $G(\mathbb{R})$. Let $N(V;X) = \#$ of generic (corresponding to n-Selmer elements of order n) $G(\mathbb{Z})$-orbits on $V(\mathbb{Z})$ of height less than X:

- for binary quartic forms "generic" means no rational root,
- for ternary cubic forms "generic" means no rational flex.

We write

$$N(V;X) = \frac{\int_{g\in G_0} \#\{v \in \Lambda\mathcal{F}gL \cap V(\mathbb{Z})^{\mathrm{gen}} : H(v) < X\} dg}{\int_{g\in G_0} dg}.$$

By switching order of integration, we have

$$N(V;X) = \frac{\int_{g\in \mathcal{F}\Lambda} \#\{v \in gG_0L \cap V(\mathbb{Z})^{\mathrm{gen}} : H(v) < X\} dg}{\int_{g\in G_0} dg}.$$

Partition $\mathcal{F}$ into "cusp part" and "main body" based on A'. Most lattice points in the cusp are not generic. On the contrary, most points in the main body are generic. After making this observation rigorous, we see that

$$\frac{\int_{g\in\mathcal{F}\Lambda} \#\{v \in gG_0L \cap V(\mathbb{Z})^{\text{gen}} : H(v) < X\}dg}{\int_{g\in G_0} dg} = \text{Vol}(\{\Lambda\mathcal{F}gL : H < X\}) + o(X^{5/6}).$$

Remark 4.1. *Order 2 elements in* 2-Sel *are non-generic.*

Remark 4.2. *"If your analytic approach is not working, there must be an algebraic reason and you should look for it and then take it out by hand." - Manjul Bhargava, Nov. 2014.*

Lemma 4.3. *Suppose that* f *is continuous on* V*. Then*

$$\int_{v\in V} f(v)dv = |J| \int_{g\in G}\int_{w\in L}\int_{\lambda>0} f(gw\lambda)dAdBdgd^\times\lambda.$$

$$\text{Avg}(\#\text{ of } n\text{-Selmer elements of order } n) =$$

$$\int_{\substack{A,B\\ H(A,B)<X}} \text{Vol}(G(\mathbb{Z})\backslash G(\mathbb{R}))\frac{\frac{\#E_{A,B}}{nE_{A,B}(\mathbb{R})}}{\#E_{A,B}(\mathbb{R})[n]}dAdB$$
$$\times \prod_p |J|_p \int_{A,B} \text{Vol}(G(\mathbb{Z}_p)) \cdot \frac{\#E_{A,B}(\mathbb{Q}_p)/nE_{A,B}(\mathbb{Q}_p)}{E_{A,B}(\mathbb{Q}_p)[n]}dAdB.$$

Many things cancel, so the final answer is

$$\text{Vol}(G(\mathbb{Z})\backslash G(\mathbb{R})) \cdot \prod_p \text{Vol}(G(\mathbb{Z}_p)) = \tau(G) = n \qquad \text{(Poonen: the adelic volume).}$$

Thus,

$$\text{Avg}(\#\,\text{Sel}_n(E_{A,B})) = \sigma(n).$$

Corollary 4.4. $\text{Avg}\,\text{Rank}(E_{A,B}) \leq 1.05.$

Proof. $\text{Avg}(20r - 15) \leq \text{Avg}(5^r) \leq 6$, so $\text{Avg}(r) \leq 21/20 = 1.05$. Equality happens if and only if 95% have rank 1 and 5% have rank 2. □

Theorem 4.5. *(Arul's lecture) There exists a family of congruences of* 55% *of all* $E_{A,B}$ *where root number is equidistributed.*

If we add Dokchitser's theorem, then we have lots of curves have even 5-Selmer rank and also lots of curves have odd 5-Selmer rank. This improves the upper bound to 0.885 *(it comes from* $0.55 \times 0.75 + 0.45 \times 1.05$*).*

Theorem 4.6. *(with C. Skinner and W. Zhang)*

We have the following statistics for elliptic curves $E_{A,B}$ *ordered by height.*

- *At least* 16.5% *of* $E_{A,B}$ *have rank and analytic rank* 0*,*
- *at least* 20.6% *of* $E_{A,B}$ *have rank and analytic rank* 1*, and most significantly*
- $\star$ *at least* 66.48% *of* $E_{A,B}$ *satisfy BSD.*

5. Asymptotics and averages for families of elliptic curves with marked points by Wei Ho

In Lecture 4, Bhargava discussed a family of elliptic curves given by an equation of the form

$$y^2 = x^3 + Ax + B = x^3 + a_4x + a_6, \quad \text{where } a_4, a_6 \in \mathbb{Z}, \text{ and } \Delta \neq 0.$$

Further, We require a minimality condition, so that there is no prime p for which both $p^4|a_4$ and $p^6|a_6$. We denote this family by $\mathcal{F}_0$. Recall the naive height $H(A, B) := \max\{4|A|^3, 27B^2\}$ and the theorem of Bhargava-Shankar:

Theorem 5.1. *(Bhargava-Shankar)*
The average size of Sel_n *for elliptic curves in* $\mathcal{F}_0$ *is* $\sigma(n)$ *for* $n = 2, 3, 4, 5$ *when ordered by height.*

We have other families. Namely:

- $\mathcal{F}_1 : y^2 + a_3y = x^3 + a_2x^2 + a_4x$, with one marked point.
- $\mathcal{F}_2 : y^2 + a_2xy + a_6y = (x - a_4)(x - a_4')(x - a_4'')$, $a_4 + a_4' + a_4'' = 0$, with two marked points.
- $\mathcal{F}_0(2) : y^2 = x^3 + a_2x^2 + a_4x$, with a 2-torsion point (over $\mathbb{Q}$)
- $\mathcal{F}_0(3) : y^2 + a_1xy + a_3y = x^3$, with a 3-torsion point (over $\mathbb{Q}$).
- $\mathcal{F}_1^{\mathbb{Q}(\sqrt{d})}$, $\mathcal{F}_{1\in\mathbb{Q}(\sqrt{d})}$, $p + \overline{p} \neq 0$.

5.1. Selmer results.

For each pair $(\mathcal{F}, p)$, we can compute $\mathrm{Avg}\,\mathrm{Sel}_p$ over that family. We have the following results

- $\mathrm{Avg}\,\mathrm{Sel}_2(\mathcal{F}_0) = 3, \mathrm{Avg}\,\mathrm{Sel}_3(\mathcal{F}_0) = 4, \mathrm{Avg}\,\mathrm{Sel}_4(\mathcal{F}_0) = 7, \mathrm{Avg}\,\mathrm{Sel}_5(\mathcal{F}_0) = 6.$
- $(\mathcal{F}_1, 2, 6), (\mathcal{F}_1, 3, 12).$
- $(\mathcal{F}_2, 2, 12)$
- $(\mathcal{F}_0(2), 3, 4).$
- $\mathrm{Avg}\,\mathrm{Sel}_2(\mathcal{F}_0(3)) = 3,$
- $\mathrm{Avg}\,\mathrm{Sel}_3(\mathcal{F}_1^{\mathbb{Q}(\sqrt{d})}) = 4.$

Remark 5.2.

- *Matches heuristics.*
- *Points are independent.*

Proof.

(1) Given G an algebraic group, V a representation of G, we want a correspondence between

$$V(\mathbb{Q})/G(\mathbb{Q}), \text{ a coarse moduli space}, \leftrightarrow \{\in \mathcal{F}, C \text{ an } E\text{-torsor}, L \text{ degree } n \text{ line bundle on } C.$$

Remark 5.3.

- $V//G \cong$ *moduli space for whatever family (affine space for these families).*
- $V//G'$ *corresponds to a weighted projective space.*
- *Stabilizers correspond to automorphism groups.*

(2) Find integral representatives (for locally soluble orbits). Take orbit in $V(\mathbb{Q})/G(\mathbb{Q})$ with integer invariants. We want an element of $V(\mathbb{Z})$ with those invariants.

Remark 5.4. *Can get stuck here.*

(3) Find fundamental domains. This is typically easy.

(4) "generic" or "irreducible" elements. Typically the non-generic points lie in the cusp.

(5) Count generic or irreducible orbits using geometry of numbers.

(6) Apply a sieve (more complicated, especially with $p = 2$). □

5.2. **Corollaries and non-corollaries.**

Example 5.5. *In $\mathcal{F}_1$, there is a positive proportion of elliptic curves with rank 1 or 2.*

Why not just rank 1? Because we cannot easily find a sub-family with equidistributed root number. If we somehow have a positive portion of rank 1's, we would like to know whether we have a positive portion of curves with rank equalling analytic rank. This cannot be done for rank 2, as the current techniques seem to get stuck at rank 1.

Example 5.6. *In $\mathcal{F}_0(3)$m p-adic methods are bad for $p = 2$.*

Example 5.7. *In $\mathcal{F}_0(2)$, there is a positive proportion having rank 0 or 1.*

Theorem 5.8. *(Skinner-Urban) Let $E/\mathbb{Q}$ be an elliptic curve with good reduction. Then subject to some p-adic conditions, we have*

$$\mathrm{Sel}_p(E) = 0 \Rightarrow \textit{rank} = \textit{analytic rank} = 0.$$

Theorem 5.9. *(Skinner-Wan, Bertolini-Darmon-Prasanna) $E/\mathbb{Q}$ good (ordinary) reduction, and subject to some p-adic conditions, we have*

$$\mathrm{Sel}_p(E) \cong \mathbb{Z}/p\mathbb{Z} \Rightarrow \textit{rank} = \textit{analytic rank} = 1.$$

In $\mathcal{F}_0(2)$, one can prove that a proportion of at least $5/8$ of curves have Sel_3 rank equalling 0 or 1. Note that we get good reduction $4/9$'s of the time ($\Delta = 16a_4^2(-4a_4 + a_2^2)$) and equidistribution ($\mathrm{Sel}_p(E) \to E(\mathbb{Q}_p)/pE(\mathbb{Q}_p)$, we obtain that at least 13.89% of $\mathcal{F}_0(2)$ satisfy conditions of Theorems 5.8 and 5.9.

6. Experiments with Arakelov class groups and ranks of elliptic curves by John Voight

The basic theme of this Lecture is: how do archimedean considerations come into into play into heuristics for class groups and ranks of elliptic curves?

6.1. **Basic Cohen-Lenstra heuristics.**

Recall the Cohen-Lenstra heuristics predict the probability that the class group $\mathrm{Cl}(D)$ of an imaginary quadratic field of (fundamental) discriminant $D < 0$ has a given p-Sylow subgroup for p odd. To each abelian p-group G, we assign the weight

$$w(G) := \frac{1}{\#\operatorname{Aut}(G)}.$$

This weight is natural comes from many sources:

- if G is an abelian group of order n and X is a set with $\#X = n$, then the number of group structures on X is isomorphic to G is $n!/\#\operatorname{Aut}(G) = n!w(G)$.
- with $w(G) = 1/\#\operatorname{Aut}(G)$, summing over abelian p-groups (Hall) , we obtain

$$\sum_G w(G) = \prod_{n=1}^{\infty}(1-p^{-n})^{-1} = \eta(p),$$

and Cohen-Lenstra then predicted that

$$\lim_{X\to\infty} \frac{\#\{0 < -D < X : \mathrm{Cl}(D)[p^\infty] \cong G\}}{\#\{0 < -D < X\}} = w(G)\frac{1}{\eta(p)}.$$

Hence, for example, $\mathrm{Cl}(D)[3^\infty] \cong \mathbb{Z}/9\mathbb{Z}$ occurs eight times more frequently than $\mathrm{Cl}(D)[3^\infty] \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. As a consequence, the average size of $\mathrm{Cl}(D)[p]$ is 2 for all p; equivalently, on average $\mathrm{Cl}(D)$ has 1 element of order (exactly) p.

6.2. **Cohen-Lenstra computations.**

To test these heuristics, we sampled $10,000$ fundamental discriminants D with $0 < -D < 10^{10}$ at random, , and found that the average number of elements of order p is:

$$\mathrm{Avg}(3) = 0.97, \quad \mathrm{Avg}(5) = 1.03, \quad \mathrm{Avg}(7) = 1.02, \quad \mathrm{Avg}(11) = 0.97.$$

It is harder to confirm that $\mathrm{Cl}(D)[3^\infty] \cong \mathbb{Z}/9\mathbb{Z}$ occurs eight times more frequently than $\mathrm{Cl}(D)[3^\infty] \cong (\mathbb{Z}/3\mathbb{Z})^2$: in a sample of $100,000$ discriminants, we find the ratio

$$\frac{281}{27} \sim 10.$$

6.3. **Cohen-Lenstra for real quadratic fields.**

The situation for real quadratic fields is slightly more complicated. Intuitively, the class group of a real quadratic field is smaller than that of an imaginary quadratic field due to the presence of the fundamental unit, and this unit gives an extra relation: so we should "modulo out by a random element": Specifically, first pick a random finite abelian p-group G with weight $w(G)$, and then modulo out by a random element. (If G is cyclic, one often gets a trivial group).

Remark 6.1. *This prediction seems to give the right answer. It is made plausible by thinking about the function field analogue, specifically hyper elliptic curves: a "real" hyper elliptic curve ($y^2 = f(x)$ with $f(x)$ of odd degree) has a unique point at infinity, so the class group of the affine coordinate ring is the quotient of the Jacobian by a "random" point. Or, think in terms of lattices and Arakelov class groups.*

6.4. **Cohen-Lenstra heuristics via lattices.**

Another natural way to produce the Cohen-Lenstra weighting is by considering random lattices. If G is a finite abelian group, then the number of lattices $L \subset \mathbb{Z}^n$ such that $\mathbb{Z}^n/L \cong G$ is asymptotic to $(\#G)^n/\#\operatorname{Aut}(G)$ as $n \to \infty$.

This observation extends quite a bit.

Friedman-Washington showed that if $M \in M_n(\mathbb{Z})$ is a random matrix with i.i.d. entries chosen according to Haar measure, then the cockerel distribution of M converges to the Cohen-Lenstra measure as $n \to \infty$.

More generally, one can show that if $M \in M_n(\mathbb{Z}/N\mathbb{Z})$ is a random matrix with iid entries, then the cockerel distribution of M converges to the Cohen-Lenstra measure for all finite $\mathbb{Z}/N\mathbb{Z}$ modules G.

6.5. **Class groups as cockerels.**

It is plausible to model the class group of a number field K by such cockerels for the following reason.

The class group $\operatorname{Cl}(K)$ is the quotient of the group of fractional ideals modulo principal ideals.

Let S be a factor base consisting of all prime ideals $\mathfrak{p}$ satisfying $N\mathfrak{p} \leq B$ for some smoothness bound B. Every $\alpha \in \mathbb{Z}_K$ whose norm factors into primes in S gives a relation. If L is the lattice spanned by the set of relations, and B is big enough ($B \geq 6 \log^2 |d_K|$ suffices on the GRH), then

$$\operatorname{Cl}(K) \cong \mathbb{Z}^{\#S}/L.$$

6.6. **Archimedean normalization for Cohen-Lenstra.**

If we model $\operatorname{Cl}(D)$ for $D < 0$ as the cockerel of a random matrix $M \in M_n(\mathbb{Z})$ with iid entries in $[-X, X]$, then we expect that

$$\#\operatorname{Cl}(D) = \det M \sim n! X^n$$

(In this Lecture, we do not make the $\sim$ rigorous). But by the Brauer-Siegel theorem, we have

$$\#\operatorname{Cl}(D) \sim \sqrt{|D|}.$$

(This estimate is pretty good on average.) Therefore

$$n! X^n \sim \sqrt{|D|}.$$

As $X, n \to \infty$, this model the usual Cohen-Lenstra heuristics for the distribution of the p-Sylow subgroups.

6.7. **Arakelov class groups.**

Returning to the real quadratic case, we now keep track of units as well.

Let K be a number field. The Arakelov divisor group of K is

$$\mathrm{Div}(K) = \bigoplus_{\mathfrak{p}<\infty} \mathbb{Z} \oplus \bigoplus_{\sigma|\infty} \mathbb{R}.$$

This gives a group analogous to the case where K is the function field of a curve X over $\mathbb{F}_q$.

A principal Arakelov divisor is a divisor of the form

$$(f) = \sum_{\mathfrak{p}} \mathrm{ord}_{\mathfrak{p}}(f)[\mathfrak{p}] + \sum_{\sigma}(-\log|\sigma(f)|)[\sigma] \in P(K)$$

for $f \in K^\times$. We define the degree map

$$\deg : \mathrm{Div}(K) \to \mathbb{R}$$

$$\deg(\mathfrak{p}) = \log N\mathfrak{p}$$

$$\deg[\sigma] = 1 \text{ or } 2 \text{ according if } \sigma \text{ is real or complex.}$$

The product formula implies that $\deg(f) = 0$ for $(f) \in P(K)$.

Let $\mathrm{Div}^0(K) = \ker \deg$ and $\mathrm{Pic}^0(K) = \mathrm{Div}^0(K)/P(K)$. Then we have an exact sequence

$$0 \to T^0(K) \to \mathrm{Pic}^0(K) \to \mathrm{Cl}(K) \to 0$$

where T^0 is the compact topological group

$$T^0 \cong \left(\prod_{\sigma} \mathbb{R}\right)^0 / \log|\mathbb{Z}_K^\times|.$$

Now suppose $K = \mathbb{Q}(\sqrt{D})$ is real quadratic. Then $\log|\mathbb{Z}_K^\times|) = (\log|\epsilon|)\mathbb{Z}$ with $\epsilon \in \mathbb{Z}_K^\times$, so

$$T^0(K) \cong \mathbb{R}/(\log|\epsilon|)\mathbb{Z}$$

is a circle group, and we have

$$0 \to \mathbb{R}/(\log|\epsilon|)\mathbb{Z} \to \mathrm{Pic}^0(K) \to \mathrm{Cl}(K) \to 0$$

The size of $\mathrm{Pic}^0(K)$ is

$$\left|\mathrm{Pic}^0(K)\right| = \#\,\mathrm{Cl}(K)\log|\epsilon| = hR = L(1,\chi)\frac{\sqrt{D}}{2}.$$

Typically, we expect $L(1,\chi) = O(D^\epsilon)$ for all $\epsilon > 0$, so

$$\left|\mathrm{Pic}^0(K)\right| \sim \sqrt{D}/2.$$

6.8. **Cohen-Lenstra heuristics, redux.**

By analogy with the imaginary quadratic case, we model the Arakelov class group of a real quadratic field $K = \sqrt{D}$ as a random homomorphism

$$\mathbb{Z}^n \to (\mathbb{Z}^{n-1} \times \mathbb{R}^2)^0 \cong \mathbb{Z}^{n-1} \times \mathbb{R},$$

represented by a matrix M whose entries lie in $[-X, X](\cap\mathbb{Z})$ and subject to the normalization

$$(\det M \sim) n! X^n \sim \sqrt{D}.$$

The map $\mathrm{Pic}^0(K) \to \mathrm{Cl}(K)$ is modelled by forgetting the last column of M (having real entries); in this way, we recover the Cohen-Lenstra model of "modelling out by an random element".

We expect to get the same answer if we instead model with a matrix with all integer entries.

6.9. **Arakelov class groups: computations.** We consider random maps $\mathbb{Z}^n = \mathbb{Z}^4 \to \mathbb{Z}^3 \times \mathbb{R}$ represented by matrices M whose entries lie in $[-X, X] = [-13, 13]$. In $100,000$ trials, we find that the average determinant of such a matrix is about $12,000$, so $\sqrt{D}/2 \in [0, 24,000]$. Therefore, this should model the Arakelov class group for discriminants $D \sim 48,000^2$. We consider $10,000$ random such discriminants.

The average number of elements of order 3 in $\mathrm{Cl}(D)$ is $1/3$ (Davenport-Heilbronn). The model gives 1.32, and the actual count is 1.30.

The average regulator: our model gives 7700, the actual count is 8500.

For instead $n = 8$ and $X = 3$, we have $\det \sim 160,000$ and regulator: Model gives $95,000$ and the actual count is $94,000$.

6.10. **Unit signatures.**

But wait! Returning to a general number field K, we an only recover $f \in K^\times$ from its divisor (f) up to a root of unity. (Joint work with Dummit).

Suppose that K is totally real. We define the signature map by

$$\mathrm{sgn} : K^\times \to \{\pm 1\}^n \cong (\mathbb{Z}/2\mathbb{Z})^n$$

$$f \mapsto (\mathrm{sgn}(\sigma(f))_{\sigma|\infty}.$$

We define the narrow Arakelov class group $\mathrm{Pic}^{+0}(K)$ in the obvious way; we obtain

$$0 \to T^0(K) \to \mathrm{Pic}^{+0}(K) \to \mathrm{Cl}^+(K) \to 0$$

where $\mathrm{Cl}^+(K)$ is the narrow class group of K so that

$$0 \to \mathbb{Z}^\times_{K,+}/\mathbb{Z}^{\times 2}_K \to \mathrm{Cl}^+(K) \to \mathrm{Cl}(K) \to 0.$$

6.11. **Signature rank.**

We define the signature rank $\operatorname{sigrk}(\mathbb{Z}_K^\times)$ of K to be the rank of the signature map restricted to $\mathbb{Z}_K^\times$.

We have $\operatorname{sigrk}(\mathbb{Z}_K^\times) \geq 1$ since $-1 \in \mathbb{Z}_K^\times$, and $\operatorname{sigrk}(\mathbb{Z}_K^\times) = 1$ if and only if K possesses a fundamental system of units that are totally positive.

So we are led to ask: what is the distribution of signature ranks over totally real fields of a fixed degree d?

6.12. **Armitage-Frohlich (AF).**

Before modelling the narrow Arakelov class group, there is one important restriction: by the theorem of Armitage-Frohlich , we have

$$\left\lceil \frac{[K:\mathbb{Q}]}{2} \right\rceil - \operatorname{rk}_2 \operatorname{Cl}(K)[2] \leq \operatorname{sigrk}(\mathbb{Z}_K^\times).$$

This theorem arises from the existence of the canonical Kummer (norm residue) pairing; in the function field case, it is the Tate pairing.

The pairing is canonical, so we do not model it separately; instead, it implies an extra compatibility and we just require that condition (AF) is satisfied fro each narrow Arakelov class group.

6.13. **Heuristics for signature ranks.**

Therefore, we model the narrow Arakelov class group of a totally real field of degree $d > 2$ as a random map

$$\mathbb{Z}^n \to \mathbb{Z}^{n-(d-1)} \times \mathbb{R}^{d-1} \times (\mathbb{Z}/2\mathbb{Z})^d$$

represented by a matrix M whose first n rows belong to $[-X, X](\cap\mathbb{Z})$ satisfying the following conditions:

(N) The vector $(\mathbf{0}, \mathbf{0}, \mathbf{1})$ is in the image of M.
(AF) Let $M_\mathbb{Z}$ be the matrix keeping only the $\mathbb{Z}$-columns, so cocker $M_\mathbb{Z}$ models $\operatorname{Cl}(K)$. Let $\mathfrak{s}(\ker M_\mathbb{Z}) \leq (\mathbb{Z}/2\mathbb{Z})^d$ be the signed components (modelling the image of $\operatorname{sgn}(\mathbb{Z}_K^\times)$). Then

$$\lceil d/2 \rceil - \operatorname{rank}_2 \operatorname{coker} M_\mathbb{Z} \leq \operatorname{rank}_2 \mathfrak{s}(\ker M_\mathbb{Z}).$$

6.14. **Computations.**

To test this conjecture, we consider totally real cubic fields K (computed by Michael Novick). To simplify, we consider a conditional probability, and we restrict to fields with odd class number $\#\operatorname{Cl}(K)$: vanilla Cohen-Lenstra predicts that this should happen for a large constant proportion of fields. for the 65 million cubic fields with discriminant $d_K \leq 10^9$, approximately 83% had odd class number.

The Armitage-Frohlich (AF) condition then implies that $\operatorname{sigrk}(\mathbb{Z}_K^\times) \neq 1$ (there cannot be a totally positive system of fundamental units) and we can ask about the distribution of signature ranks 2, 3.

Our heuristic implies that rank 2 should occur with probability 3/5 and rank 3 should occur with

probability 2/5. Of the 54 million cubic fields, we find percentages 58.6% and 41.4%. Also see the work of Bhargava.

6.15. **Ranks of elliptic curves: basic heuristic.**

The archimedean normalization of Cohen-Lenstra heuristics is a warm-up for our (PPVW) heuristics for elliptic curves.

See Bjorn Poonen's Lecture 20 for a heuristic for the rank of a random elliptic curve

$$E : y^2 = x^3 + Ax + B \text{ over } \mathbb{Q} \text{ of height } H = \max(4|A|^3, 27B^2).$$

In brief: we take n of moderate size with random parity; we choose X such that $n!X^n \sim H^{1/2}$ and we compute the rank of the kernel of a random $n \times n$ alternating $M \in M_n(\mathbb{Z})$ with entries in $[-X, X]$.

In the end, we predict that for each $r \geq 1$, the probability that E of height H has rank $\geq r$ is approximately $1/H^{(r-1)/24}$.

The setup above says how we should model the class group and regulator together. Arguing by analogy, this gives a second way to arrive at our calibration, modelling the Shafarevich-Tate group and the elliptic regulator together.

6.16. **A few computations.**

Bektemirov-Mazur-Stein-Watkins discuss the tension between data and conjecture for ranks of elliptic curves in some detail.

We consider instead some statistical sampling as follows. we take elliptic curves of height $H \in [X, X + X/100]$ and compute their analytic ranks.

$\approx X$	rank 0	rank 1	rank ≥ 2	rank ≥ 3
10^8	32%	48%	18%	2%
10^{10}	33%	48%	17%	2%
10^{12}	33%	48%	16%	2%

For what it's worth, $1/2 \cdot 10^{-10/24} = 19\%$ and $1/2 \cdot 10^{-20/24} = 7\%$.

The evidence is weak, but at least the percentage of rank at least 2 appears to be going down. Further computations are in progress, using a conditional method to bound analytic ranks by Bober (going back to work of Mestre and Fermigier).

6.17. **Final words.**

In this Lecture, we have tried to convince you that it is a reasonable philosophy for arithmetic objects to be modelled by kernels and cockerels of integer matrices whose size is normalized by archimedean (L-function) considerations.

For more on heuristics for elliptic curves, see Lecture 20!

7. Counting simple knots via arithmetic invariant theory
by Alison Miller

Recall: 1-knots are embeddings of the circle $\mathbb{S}^1$ in $\mathbb{S}^3$ which are equivalent up to some topological equivalence, whose precise form is not of relevance. We formulate the definition of an n-knot as follows:

Definition 7.1. *An n-knot $K \subset \mathbb{S}^{n+2}$ is an embedded submanifold, with K homeomorphic to $\mathbb{S}^n$. Similarly, this is up to topological equivalence.*

Knot theory studies:

- when are two knots equivalent
- what invariants can be used to tell knots apart?

Given an n-knot $K \subset \mathbb{S}^{n+2}$, one obtains the knot complement $\mathbb{S}^{n+2} \setminus K$. It turns out in most situations the knot complement contains all (or most) of the information about the knot. General n-knots are too complicated, as to understand them is equivalent to understanding finitely generated groups. It will therefore be prudent to study the family of simple knots.

7.1. Simple $(2q-1)$-knots.

Definition 7.2. *A $(2q-1)$-knot K is simple if*

$$\pi_i(\mathbb{S}^{2q+1} \setminus K) = \pi_i(\mathbb{S}^1)$$

for $i \leq q$, where π_i is the ith homotopy group, with π_1 being the fundamental group.

7.2. Arithmetic invariants.

Fox and Smythe constructed a knot invariant that is an ideal class . This comes from the Alexander module for classical knots. In the case of 3-knot K, the knot complement can be covered by an abelian cover C_∞ leading to the covering group $\mathbb{Z}$. The orientation of the knot gives us a canonical generator for the group, which we denote by t. The Alexander module of K is then defined by $H_1(C_\infty, \mathbb{Z})$. The infinite cyclic group $\langle t \rangle$ acts on Alex_K and so Alex_K is a $\mathbb{Z}[t, t^{-1}]$ module. Alex_K has the following properties:

- Alex_K is annihilated by the Alexander polynomial $\Delta(t) \neq 0$.
- $\Delta(1) = 1, \Delta(t^{-1}) = t^{-2\deg\Delta}\Delta(t)$. If $\deg\Delta = 2$ then $\Delta = mt^2 + (1-2m)t + m$ for some positive integer m.
- Alex_K is a module over the quotient ring

$$\mathcal{O}_\Delta = \mathbb{Z}[t, t^{-1}]/\Delta(t).$$

- $\mathcal{O}_\Delta \otimes_{\mathbb{Z}} \mathbb{Q}$ is a finite dimensional $\mathbb{Q}$-algebra.
- If $\Delta = mt^2 + (1-2m)t + m$, then $\mathcal{O}_\Delta = \mathbb{Z}[t, t^{-1}]/(mt^2 + (1-2m)t + m)$.
- Alex_K has the property that when Δ is square-free, Alex_K is isomorphic as an $\mathcal{O}_\Delta$-module to an ideal of $\mathcal{O}_\Delta$. This gives rise to an arithmetic invariant.
- Alex_K satisfies "Blanchfiled duality" and comes with a natural hermitian pairing over $\mathbb{Z}[t, t^{-1}]$.

7.3. **Motivating questions.**

- Does this arithmetic invariant fit into the context of arithmetic invariant theory?
- If so, can we count them?

7.4. **Alexander module of a simple $(2q-1)$-knot.**

Consider a simple $(2q-1)$-knot K, with an infinite cover C_∞ for the knot complement $S^{2q+1} \setminus K$ generated by t. Then have (in terms of the homology groups)

$$H_q(C_\infty, \mathbb{Z}) = \mathrm{Alex}_K,$$

this is a $\mathbb{Z}[t, t^{-1}]$-module annihilated by some polynomial $\Delta(t)$, and call $\Delta(t)$ the Alexander polynomial of K.

Theorem 7.3. *(Bayer-Michel, Levine) There are only finitely many simple $(2q-1)$-knots with a given Alexander polynomial, provided that the polynomial is square-free.*

Theorem 7.4. *(Kearton, Trotter) For $q > 1$ odd, simple knots are entirely classified by the Alexander modules along with the Blanchfield duality pairing on the Alexander modules.*

Theorem 7.5. *(Kearton, Levine, Trotter) Algebraic condition for which modules and pairing are realizable.*

The three theorems above enable us to "count" simple knots of square-free Alexander polynomials of a fixed degree with bounded height.

7.5. **Seifert hypersurfaces for knots.**

Definition 7.6. *A Seifert hypersurface for a 1-knot is a surface embedded in $\mathbb{S}^3$ with $\partial V = K$. This generalizes to simple n-knots.*

Theorem 7.7. *Any simple n-knot can be written as ∂V where V is a Seifert hypersurface which is a $2q$-dimensional manifold with boundary and V is $(q-1)$-connected.*

This theorem is basically saying that "all topology of V comes from $H_q(V)$, the homology groups" and thus Seifert hypersurfaces are classified by

$$\mathrm{rk}(H_q(V, \mathbb{Z})) = 2g,$$

where g is the genus along with a non-symmetric $\mathbb{Z}$-valued pairing on $H_q(V, \mathbb{Z})$. The skew symmetric part is the intersection pairing which is a perfect pairing.

Simple Seifert hypersurfaces are in one-to-one correspondence with GL_n-equivalence class of matrices P such that $\det(P - P^T) = 1$ (i.e. $(M, P) \mapsto MPM^T$). We can always change basis such that

$$P - P^T = J = \begin{pmatrix} 0 & -I_g \\ I_g & 0 \end{pmatrix}.$$

This gives us the Sp_{2g}-equivalence classes of matrices P with $P - P^T = J$, and another change of variables gives $P \mapsto P + P^T = Q$, which leads to the Sp_{2g}-equivalence classes of matrices $Q \in \mathrm{Sym}^2(2g)$ such that $Q \equiv J \pmod 2$.
The underlying representation is

$$\mathrm{Sym}^2(2g) \to \text{ adjoint representations of } \mathrm{Sp}_{2g},$$

with free ring of invariants generated by coefficients of

$$\det(J^{-1}P - tI_{2g}) = \det(tJ - P).$$

The latter polynomial is equal to the Alexander polynomial after a change of variables.
Simple Seifert hyper surfaces $\to \mathrm{Sp}_{2g}$-orbits on $\mathrm{Sym}^2(2g)$ (+ parity) $\to C$ self balanced ideal classes of $R_f = \mathbb{Z}[y]/f(y) \to$ characteristic polynomial $= f$.

Simple $(2q-1)$-knots (square-free Δ) $\to$ Alexander module + pairing $\to$ CSB ideal classes of $\mathcal{O}_\Delta$ (finite-to-one) Alexander polynomials $\Delta(f)$ which leads to characteristic polynomial $= f$.

When $\Delta(t) = mt^2 + (1-2m)t + m$ we have $\mathrm{Sp}_2 = \mathrm{SL}_2$ (hypersurfaces) orbits on binary squarefree's of discriminant dividing $4m$. Knots correspond to binary quartic forms of discriminant $1 - 4m$ over $\mathbb{Z}[1/m]$.

8. Arithmetic statistics over global fields
by Jerry Xiaoheng Wang

Let K denote a global field, which is either a number field or a function field of characteristic zero over a smooth projective variety. Let M_∞ denote the set of infinite places, or a finite non-empty set of closed points on C in the function field case. $\mathcal{O}$ denote its ring of integers and $K_\infty := \prod_{v\in M_\infty} K_v$.

Remark 8.1. *Philosophy: $\mathbb{Q}$ should correspond to K, $\mathbb{Q}_p$ should correspond to $K_\mathfrak{p}$, and $\mathbb{Z}_p$ should correspond to $\mathcal{O}_\mathfrak{p}$, but $\mathbb{Z}$ does NOT correspond to $\mathcal{O}$ in most cases.*

The first example is $\mathrm{Sel}_2(E)$.

Step 0 Height of E/K

$E : y^2 = x^3 + Ax + B, A, B \in K$. $(A, B) \in \mathbb{P}(4, 6)(K) = \mathbb{G}_m(K)\backslash\mathbb{A}^2(K)$. For $(A, B) \in S(K)$, let $I = \{\alpha \in K | \alpha(A, B) \in S(\mathcal{O})\}$.

$H(A, B) = NI \prod_{v\in M_\infty} \max(|A|_v^{1/4}, |B|_v^{1/6})$ when $|M_\infty| > 1$, the set $S(K_\infty)_{<X}$ is not bounded. What is $\mathrm{Avg}\,\mathrm{Sel}_n(E)$?

Step 1 Orbit parametrization

$\mathrm{Sel}_2(E/K)$ correspond to locally soluble orbits for the action of $G(K)$ on $V(K)$.

Step 2 Locally soluble orbits $\to$ integral orbits (not true, but close).

Lemma 8.2. *If $v \in V(K_\mathfrak{p})^{sol}$ has invariants in $\mathcal{O}_\mathfrak{p}$, then there exists $g_p \in G(K_\mathfrak{p})$ such that $g_p v \in V(\mathcal{O}_\mathfrak{p})$.*

Suppose $v \in V(K)^{loc\ sol}$ with invariants in $\mathcal{O}$. Then there exists $g_\mathfrak{p} \in G(K_\mathfrak{p}$ such that $g_\mathfrak{p} v \in V(\mathcal{O}_\mathfrak{p})$.

$$(g_\mathfrak{p}) \in G(\mathbb{A}_f) = \bigcup_{\beta\in \mathrm{Cl}(G)} \left(\prod_{\mathfrak{p}\notin M_\infty} G(\mathcal{O}_\mathfrak{p})\right) \beta G(K),$$

where $\mathrm{Cl}(G)$ is the class group of G which is finite. $(g_\mathfrak{p})_\mathfrak{p} = (g'_\mathfrak{p}) \cdot \beta \cdot h \Rightarrow \beta h v \in V(_\mathfrak{p})$ for all $\mathfrak{p} \notin M_\infty$. $hv \in V_\beta = V(K) \cap \beta^{-1}\left(\prod_{\mathfrak{p}\notin M_\infty} V(\mathcal{O}_\mathfrak{p})\right)$, with $V(\mathcal{O}) = V_{\beta=1}$.
$G_\beta = G(K) \cap \beta^{-1}\left(\prod_{\mathfrak{p}\notin M_\infty} G(\mathcal{O}_\mathfrak{p})\right)\beta$.

Proposition 8.3. *Suppose $v \in V(K)^{loc\ sol}$ has invariants in $\mathcal{O}$, then there exist $\beta \in \mathrm{Cl}(G)$ such that*

$$G(K)v \cap V_\beta \neq$$

For any subgroup $G_0 \leq G(K)$ and any subset $V_0 \subset V(K)$, any real number X, let

$$N(V_0, G_0, X) =$$

$$\#\left\{\textit{irreducible } G_0\textit{-orbit in } V_0 \textit{ of height } < X \textit{ where an orbit } G_0 v \textit{ is weighted by } \frac{1}{\#\,\mathrm{Stab}_{G_0}(v)}\right\}.$$

If $m : V(K) \to [0,1]$ is G_0-invariant, defined by congruence conditions, then

$$N_m(V_0, G_0, X) =$$

$$\#\left\{\textit{irreducible } G_0\textit{-orbit in } V_0 \textit{ of height } < X \textit{ where an orbit } G_0 v \textit{ is weighted by } \frac{m(v)}{\#\operatorname{Stab}_{G_0}(v)}\right\}.$$

Theorem 8.4.

$$N(V(K)^{\textit{loc sol}}, G(K), X) = \sum_\beta N_m(V_\beta, G_\beta, X)$$

where

$$m(v) = \chi_{V(K)^{\textit{loc sol}}}(v) \frac{1}{\#\operatorname{Stab}_{G(K)}(v)} \left(\sum_\beta \sum_{V_\beta \in G_\beta \backslash V_\beta \cap G(K)v} \frac{1}{\#\operatorname{Stab}_{G_\beta}(v_\beta)} \right)^{-1}$$

is defined by congruence conditions $\prod_{\mathfrak{p} \notin M_\infty} m_\mathfrak{p} \cdot \prod_{v \in M_\infty} m_v$.

Step 3 Count integral orbits soluble at ∞.

$L(X) = G(K_\infty) \backslash V(K_\infty)_{<X}$ scaled from $L(1)$.

$\mathcal{F}_\beta = G_\beta \backslash G(K_\infty)$.

$\mathcal{F}_\beta \cdot L(X) \to G_\beta \backslash V(K_\infty)_{<X}$ where the fibre above v has size $\dfrac{\#\operatorname{Stab}_{G(K_\infty)}(v)}{\#\operatorname{Stab}_{G_\beta}(v)}$.

We want

$$N_m(V_\beta, G_\beta, X) \sim \int_{F_\beta \cdot L(X)} \frac{m_\infty(v)}{\#\operatorname{Stab}_{G(K_\infty)}(v)} d\nu_{\infty,\beta}(v)$$

where $\nu_{\infty,\beta}$ is normalized such that $\nu_{\infty,\beta}(V_\beta \backslash V(K_\infty)) = 1$.

Problem 8.5.

(1) Davenport's lemma over function field. "$B \subset V(K_\infty)$ compact, $t \in K_\infty$, $\#tB \cap V_\beta = V_{\infty,\beta}(tB)$ as $|t| = \prod_{v \in M_\infty} |t_v|_v \to \infty$."

This is proved via Poisson summation.

(2) $\mathcal{F}_\beta$ is generally not compact, and so we need to do cusp analysis. Without loss of generality we set $V_\beta = V(0), G_\beta = G(0)$, G semi-simple.

(i) Reduction theory, $G(0) \backslash G(K_\infty) \subset N(K_\infty) A(K_\infty) K'$ (Springer).

A maximal split torus in P, N unipotent radical of P, K' compact subgroup of $G(K_\infty)$, and Δ is a basis of positive roots.

For $G = \mathrm{PGL}_2$, we have $A = \left\{ \begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} \right\}$, $N = \left\{ \begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix} \right\}$ and $\Delta = \{\alpha\}$, $\alpha \begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} = t^2$.

(ii) Cut off the cusp. Restrict V to A where $V = \bigoplus_{\chi \in U_0} \chi$. For example

$$\mathrm{Sym}^4(2) = \chi_{x^4} \oplus \chi_{x^3y} \oplus \chi_{x^2y^2} \oplus \chi_{xy^3} \oplus \chi_{y^4}$$

For $v \in V$, $\chi \in U_0$, $v(\chi)$ is a χ-isotypic composition.

For $U \subset U_0$, say $v \in V(K)$ is U-irreducible if there exists $g \in G(K)$ such that

$$gv(\chi) = 0, \forall \chi \in U$$

Let $U_1, \cdots, U_m \subset U_0$ such that if v is U_i-reducible for some i, then v is reducible.

Cusp: $V(K_\infty)^{cusp} \subset V(K_\infty)$ consists of $v \in V(K_\infty)$ such that $|v(\chi)| < c_1$ for some $\chi \in U_0$ where c_1 is chosen so that if $v \in V(\mathcal{O})$, $|v(\chi)| < c_1$ implies that $v(\chi) = 0$.

There is a combinatorial condition on the characters of a that implies: the number of irreducible points in cusp is small, the volume of the cusp is small,

(iii) The number of reducible points in the main body is small. Usually proved by p-adic analysis.

Step 4 Impose soluble conditions at $\mathfrak{p} \notin M_\infty$ via $m_\mathfrak{p} \to$ upper bound.
Step 5 Uniformity estimate which gives a lower bound. This is done for $\mathrm{Sel}_n(E)$ for $n = 2, 3, 4, 5$.
Step 6 Local volume computation.

Theorem 8.6. *(Bhargava-Shankar-Wang) When elliptic curves over K are ordered by height,*

$$\mathrm{Avg}\, \mathrm{Sel}_n(E) = \sigma(n)$$

for $n = 2, 3, 4, 5$.

9. Singular exponential sums associated to prehomogeneous vector spaces over finite fields

BY FRANK THORNE

Joint work with T. Taniguchi .

Example 9.1. *Let V be the space of binary cubic forms, and take $\mu_p : V(\mathbb{F}_p) \to \mathbb{Z}$ to be the number of roots in $\mathbb{P}^1(\mathbb{F}_p)$, whose values lie in $\{0, 1, 2, 3, p+1\}$, and let $[\cdot, \cdot] : \mathrm{SL}_2$ be an invariant bilinear form identifying V with its dual. Define*

$$[g \circ x, g \circ y] := [x, y] := x_1 y_4 - \frac{1}{3} x_2 y_3 + \frac{1}{3} x_3 y_2 - x_4 y_1.$$

$x := x(u, v) = x_1 u^3 + x_2 u^2 v + x_3 u v^2 + x_4 v^3$, $p \neq 3$.

$$\widehat{\mu}_p(x) := \frac{1}{p^4} \sum_{y \in V(\mathbb{F}_p)} \mu_p(y) \exp\left(\frac{2\pi i}{p}[x, y]\right).$$

Proposition 9.2.

$$\widehat{\mu}_p(x) = \begin{cases} 1 + p^{-1} & \text{if } x = 0 \\ p^{-1} & \text{if } x \text{ has a triple root} \\ 0 & \text{otherwise.} \end{cases}$$

The idea is to count, for example, $\mathrm{GL}_2(\chi)$ orbits of (irreducible) binary cubic forms with discriminant in $\pm(1, X)$. Call this count $N^{\pm}(X)$.

Let Φ_p describe some $\mathrm{GL}_2(\chi)$-invariant condition "at p".

(1) $v \in V_\chi$ is singular as a binary cubic form $\mathbb{F}_p$.
(2) v has a triple root as a binary cubic form over $\mathbb{F}_p$.
(3) (a) v is a multiple of p and (b) There is a $\mathrm{GL}_2(\chi)$-transformation of v such that $p^2 | v_1, p | v_2$.

Write $N^{\pm}(X, \Phi_p)$ or $N^{\pm}(X, p)$ for number of orbits satisfying condition described by Φ_p. If q is square-free, we can write $N^{\pm}(X, \Phi_q)$ or $N^{\pm}(X, q)$ for the number of orbits satisfying condition for all $p | q$.

9.1. **Sieve axiom.**

We have

$$N^{\pm}(X, q) = Cw(q) + O(X^{\alpha} q^{\beta})$$

where C is a constant, w is a multiplicative function, $\alpha < 1$ and β are constants. This is often the starting part for analytic number theory problems.

Example 9.3. *Counting fields of degree ≤ 5.*

Example 9.4. *(Belabas-Fouvry) Almost prime discriminants of cubic fields. They did it without using any power-saving error terms in Davenport-Heilbronn, for example.*

Example 9.5. *(Yang, Cho-Kim) Low lying zeroes of Artin L-functions.*

Example 9.6. *(Martin-Pollack) Average prime not to split completely*

Example 9.7. *(Lemke-Oliver-Thorne) Erdős-Kac for number field discs.*

Compute the Fourier transform of Φ_p: characteristic function of those binary cubic forms over $\mathbb{F}_p$ with a triple root.

$$\begin{aligned} p^4\Phi_p(y) &= \frac{1}{p^2-p}\sum_{g\in \mathrm{SL}_2(\mathbb{F}_p)}\sum_{m\in\mathcal{F}_p^\times}\exp\left(\frac{2\pi i}{p}\left[g\circ(m,0,0,0),y\right]\right) \\ &= \frac{1}{p^2-p}\sum_g\sum_m\exp\left(\frac{2\pi i}{p}\left[(m,0,0,0),gy\right]\right) \\ &= \frac{1}{p^2-p}\sum_g\begin{cases} p-1 & \text{if } [1:0] \text{ is a root of } g\circ y \\ -1 & \text{otherwise}\end{cases}. \end{aligned}$$

9.2. **What has been done so far.**

Space	Group	Dimension
$2\otimes 2$	$\mathrm{GL}(2)\times\mathrm{GL}(3)$	4
$3\otimes 3$	$\mathrm{GL}(2)\times\mathrm{GL}(3)$	9
$\mathrm{Sym}^2(2)$	$\mathrm{GL}(1)\times\mathrm{GL}(2)$	3
$\mathrm{Sym}^3(2)$	$\mathrm{GL}(1)\times\mathrm{GL}(2)$	4
$\mathrm{Sym}^2(3)$	$\mathrm{GL}(1)\times\mathrm{GL}(3)$	6
$\mathrm{Sym}^2(2)\otimes 2$	$\mathrm{GL}(2)\times\mathrm{GL}(2)$	6
$\mathrm{Sym}^2(3)\otimes 2$	$\mathrm{GL}(2)\times\mathrm{GL}(3)$	2
$\mathrm{Sym}^4(2)$	$\mathrm{GL}(1)\times\mathrm{GL}(2)$	5

10. Euler systems and Jochnowitz congruences
by Massimo Bertolini

Theme: anti-cyclotomic Iwasawa theory. See Lecture 12 by Wei Zhang and Lecture 13 by Rodelfo Venerucci. (See applications to converse of Gross-Zagier-Kolyvagin)

Let E be an elliptic curve of conductor N, $f \in S_2(N)$ the associated form: $A = A_f$. p an ordinary prime of E. K_∞/K the anti-cyclotomic $\mathbb{Z}_p$-extension associated to $K = \mathbb{Q}(\sqrt{-D})$.

We make the simplifying assumptions: Let N be square-free, $(D, N_p) = 1$, $p \nmid N$ (if $p \mid N$, things are ok: use work of Skinner-Zhang ; see Verevucci's Lecture 13)

$$N = N^+N^-, \qquad N^+ := \prod_{\substack{q|N \\ q \text{ split in } K}} q, \qquad N^- := \prod_{\substack{q|N \\ q \text{ inert}}} q.$$

Definite case: $\#\{q|N^-\}$ is odd. This implies that $\operatorname{sgn} L(f/K, \chi, s) = +1$ for all $\chi : G_\infty = \mathrm{Gal}(K_\infty/K) \to \overline{\mathbb{Q}}^\times$. Thus, we can define $L_p(f) = \mathfrak{L}_p(f) \cdot \mathcal{L}(f)^2 = (\text{unit}) \cdot \mathfrak{L}_p(f)^2 \in \Lambda = \mathbb{Z}_p[[G_\infty]]$ by interpolating $L(f/K, \chi, 1)$, which are described in theorems.

$\widehat{R}^\times \backslash \widehat{B}^x / B^\times$, where B is the definite quaternion algebra of discriminant $N^-\infty$, R Eisenstein of level N^+ ($\widehat{\iota} = (\cdot) \otimes \widehat{\mathbb{Z}}$).

Theorem 10.1. *(Definite Main Conjecture) (Bertolini-Darmon , Skinner-Urban , Bertolini-Verevucci) For almost all good ordinary primes p,*

$$\Lambda \cdot L_p(f) = \operatorname{char}_\Lambda \mathrm{Sel}_{p^\infty}(A/K_\infty)^\vee$$

Remark 10.2. *We know that $L_p(f) \neq 0$ by Cornut-Vatsal .*

Indefinite case: $\#\{q|N^-\}$ is even. This implies that $L(f/K, \chi, 1) = 0$. BSD implies that $\mathrm{Sel}_{p^\infty}(A/K_\infty)$ should not be a Λ-cotorsion.

Heegner points on $(\widehat{R}^\times \backslash \widehat{B}^\times \times \langle^\pm / B^\times$, B is an indefinite quaternion algebra of discriminant N^{-1} gives a class $K(1) \in \widehat{H}^1_\phi(K_\infty, T_f) = \mathrm{Tap}(A)$, where if S is a finite set of primes, $\widehat{H}^1_S(K_\infty, T_f) = \varprojlim_{\text{cores}} H^1_S(K_m, T_f)$, $K \subset K_m \subset K_\infty$. The latter corresponds to the situation where the Selmer group with the conditions at $\rho \in S$ relaxed.

Definition 10.3. *(Indefinite Main Conjecture) (X. Wan if p is split , Bertolini-Verevucci in general) For almost all good ordinary primes p,*

$$L_p(f)\Lambda = \operatorname{char}_\Lambda \left(\mathrm{Sel}_{p^\infty}(A/K_\infty)^\vee_{\mathrm{tors}}\right)$$

Remark 10.4. *Work of B. Howard.*

We describe the ingredients contained in the proof of the Indefinite Main Conjecture:

(i) Explicit reciprocity laws (Bertolini-Darmon , Skinner-Zhang)
(ii) Prove the full definite MC, adapting the induction of Bertolini-Darmon using Skinner-Verevucci over $\mathbb{Q}$.

(iii) Reduce the indefinite Main Conjecture to the definite Main Conjecture.

(i) Assume that f is in the definite case.

Definition 10.5. *$\ell \nmid Np$ is n-admissible ($n \geq 1$) with respect to (f, K, p) if:*
(a) ℓ is inert in K,
(b) $p|(\ell+1) - \epsilon a_\ell(f)$, and $p^n \nmid \ell^2 - 1$ (here $\epsilon = \pm 1$ is a choice of sign).

If ℓ is n-admissible, then there exists $f_\ell \in s_2(N\ell)$ arising on $B_\ell =$ indefinite quaternion algebra of discriminant $N^-\ell$ such that $f_\ell \equiv f \pmod{p^n}$. Write X_ℓ for the Shimura curve associated to B_l, with N^+-level structure. Set $T_{f,n} = T_f/p^n = T_{f_\ell}$, $\Lambda_n = \Lambda/p^n$. Heegner points on X_ℓ give a class $K_n(\ell) \in \widehat{H}_\ell(K_\infty, T_{f,n})$. Since ℓ is inert in K, that it is not split K_∞/K. This implies that

$$\widehat{H}(K_\infty, \ell, T_{f,n}) \cong H^1(K_\ell, T_{f,n}) \otimes \Lambda_n \cong \Lambda_m \oplus \Lambda_n.$$
$$\widehat{H}^1_{\text{fin}}(K_\infty, \ell, T_{f,n}) \cong \Lambda_m, \widehat{H}^1_{\text{sing}}(K_\ell, T_{f,n}) \cong \Lambda_m.$$
$$\Rightarrow \partial_\ell : \widehat{H}_\ell(K_\infty, T_{f,n}) \to H^1_{\text{sing}}(K_\infty, l, T_{f,n}) = \Lambda_m.$$

First reciprocity law: $\partial_\ell K_n(l) = \mathcal{L}_{p,n}(f) = \mathcal{L}_p(f) \pmod{p^n}$.

Let $\ell' \neq \ell$ be another n-admissible prime. $\upsilon_{\ell'} : \widehat{H}^1_\ell(K_\infty, T_{f,n}) \to \widehat{H}^1_{\text{fin}}(K_\infty, \ell', T_{f,n})$.

Second reciprocity law: $\upsilon_{\ell'} K_n(\ell) = \mathcal{L}_{p,n}(f_{\ell,\ell'})$.

(ii) The induction: $L_p(f) \cdot \Lambda = \text{char}_\Lambda \text{Sel}_{p^\infty}(A/K_\infty)^\vee$. Look at the image of this relation under $\chi : \Lambda \to \mathcal{O}$, which is a discrete valuation ring. Enough to check the definite MC for all $n \gg 0$ and for enough χ. Induction on the order of vanishing of $\chi L_{p,n}(f) \neq 0$ by Cornut-Vatsal . Can assume that $\text{Sel}_{p^\infty}(A/K_\infty) \otimes_\chi \mathcal{O} \neq (0)$ (Skinner-Urban).

(iii)

(a) Use the second reciprocity law to relate the indefinite $L_p(f)$ to $L_p(f_\ell)$.
(b) Compare $\text{Sel}_{p^n}(f)$ with $\text{Sel}_{p^n}(f_\ell)$.

11. Special values of Rankin-Selberg type p-adic L-functions by Ernest Hunter Brooks

11.1. p-adic Waldspurger formulas.

Recall in Urban's Lectures 2-3, we saw Hida's constructions of two p-adic L-functions $L^{\mathrm{I}}, L^{\mathrm{II}}$ interpolating special values of classical L-functions $L(f, g, n)$.

The Bertolini-Darmon-Prasanna formula implies that, when f comes from an elliptic curve E and g comes from a Hecke character, one has

$$L^{\mathrm{II}}(\mathbb{1}) = (\log(Q_{\mathbb{1}}))^2,$$

where $\mathbb{1}$ is the trivial character, $Q_{\mathbb{1}}$ is a Heegner point on $E(K)$.
What does this mean? Why is it relevant to counting problems? Why is it true? Under what conditions?

11.2. p-adic logarithms.

When $A/\mathbb{Q}_p$ is an abelian variety, there is a differential $\omega \in H^0(A, \Omega)$ and there is also a unique locally analytic homomorphism

$$\log_\omega : A(\mathbb{Q}_p) \to \mathbb{Q}_p,$$

such that $d \log_\omega = \omega$. Torsion points are obviously in the kernel of $\log_\omega$ for any ω.

Conversely, if a point is in the kernel of $\log_\omega$ for all ω (or all ω in a basis) then it is torsion. The pairing

$$(P, \omega) \mapsto \log_\omega(P)$$

gives an isomorphism of p-adic Lie groups from the kernel of the reduction map to $H^0(A, \Omega)^\vee$.

11.3. Logarithms on curves.

Let $C/\mathbb{Q}_p$ be a curve with a fixed base point $P \in C(\mathbb{Q}_p)$, J its Jacobian, $AJ : C \to J$ (algebraic, depends on P). We get an embedding $C \to J$ using P. We get an identification $H^0(C, \Omega_C) = H^0(J, \Omega_J)$. This gives for each $\omega \in H^0(C, \Omega_C)$ a logarithm on C. The logarithm on C depends on base point, but the induced map on Div^0 does not.

If $f : C_1 \to C_2$ os a morphism of curves, D is a degree zero divisor on C_1, and ω is a 1-form on C_2, then

$$\log_{f^*\omega}(D) = \log_\omega(f(D))$$

11.4. Elliptic curves.

Let E be an elliptic curve over $\mathbb{Q}$ with square-free conductor N, with associated weight 2 new form f. Fix an imaginary quadratic field K of discriminant prime to N and factor $N = N^+N^-$, where primes dividing N^+ are split in K and primes dividing N^- are inert. Now assume an even number of primes divide N^-.

11.5. **Rankin-Selberg L-functions.**

Define parameters α_p and β_p by

$$\mathcal{E}_p(E,s) = (1-\alpha_p p^{-s})^{-1}(1-\beta_p p^{-s})^{-1}.$$

where $\mathcal{E}_p$ is the Euler factor for the L-function of $E/\mathbb{Q}$ at p. For $\mathfrak{p}$ a prime of K not dividing the discriminant of K or N, and χ a character of $\mathrm{Cl}(K)$, set

$$\mathcal{E}_{\mathfrak{p}}^{\text{R-S}}(E,\chi,s) = (1-\chi(\mathfrak{p})\alpha_{\mathbf{N}\mathfrak{p}}(\mathbf{N}\mathfrak{p})^{-s})^{-1}(1-\chi(\mathfrak{p})\beta_{\mathbf{N}\mathfrak{p}}(\mathbf{N}\mathfrak{p})^{-s})^{-1}$$

The global Rankin-Selberg L-function is (up to finitely many Euler factors)

$$L(E,\chi,s) = \prod_{\mathfrak{p}\nmid Nd_k} \epsilon_{\mathfrak{p}}^{\text{R-S}}$$

It admits analytic continuation, and there is a completed L-function Λ which satisfies a functional equation with centre $s=1$ and sign ± 1.

11.6. **The Heegner hypothesis and the L-function.**

Heegner hypothesis: $N = N^- N^+$ as before and assume for a moment that $N^- = 1$.

Analytic consequence: forces sign in functional equation to be -1,

$$L(E,\chi,s) = -L(E,\chi,2-s)$$

implying $L(E,\chi,1) = 0$.

Geometric consequence: There is an ideal $\mathcal{N}$ of K of norm K, so a Heegner point $P = [\mathbb{C}/\mathfrak{N}^{-1} \to \mathbb{C}/\mathcal{O}_K] \in X_0(N)(h)$.

11.7. **Heegner points.**

Thinking of χ as a character of $\mathrm{Gal}(H/K)$, set

$$P_\chi = \sum_{\sigma\in\mathrm{Gal}(H/K)} \chi^{-1}(\sigma)P^\sigma \in \mathrm{Div}(X_0(N))(H)\otimes\mathbb{Q}(\chi).$$

Also set

$$Q_\chi = \phi(P_\chi)$$

where ϕ is the map coming from the modular parametrization. In particular, $Q_{\mathbb{1}} \in E(K)$.

11.8. **Heights.**

The height map $\widehat{h}$ extends to $\mathrm{Div}(E)(H)\otimes\mathbb{Q}(\chi)$ in $\mathbb{C}$. The height of a point in $E(K)$ is zero if and only if it is a torsion point.

Theorem 11.1. *One has* $L'(E,\chi,1) = \widehat{h}(Q_\chi)$.

Gross-Zagier 1987 : $N^- = 1$, Skinner-Zhang 2001 : $N^- > 1$ square-free, Yuan-S. Zhang, W. Zhang 2013 : no assumptions.

11.9. **Applications to the conjecture of Birch and Swinnerton-Dyer.**

BSD over K: Comparing Euler factors, one sees

$$L(E/K, s) = L(E, \mathbf{1}, s).$$

So if $L'(E/K, s) \neq 0$, then the Heegner point is non-torsion and consequently "analytic rank one implies algebraic rank at least one."

BSD over $\mathbb{Q}$: Gross and Zagier apply a result of Waldspurger to show one can choose K such that the above argument descends to $\mathbb{Q}$.

11.10. **Shimura curves.**

Let $B/\mathbb{Q}$ be the indefinite quaternion algebra with discriminant N^-, and fix a maximal order $\mathcal{O}_B$ in B.

There is an Eichler order of level N^+, called $\mathcal{O}_{B,N^+}$ in $\mathcal{O}_B$. Write Γ_{N^+,N^-} for its group of norm one elements.

The group Γ_{N^+,N^-} acts on the upper half plane via

$$B \otimes \mathbb{R} \to M_2(\mathbb{R}).$$

The quotient $X_{\mathbb{C}} = \mathcal{H}/\Gamma_{N^+,N^-}$ is a Shimura curve. If $N^- \neq 1$, the Shimura curve is compact. There are no cusps. There are modular forms for Γ_{N^+,N^-}, but they have no q-expansions.

11.11. **Moduli-theoretic interpretation.**

If $N^- \neq 1$, the Shimura curve is compact. There are no cusps.

To $\tau \in \mathcal{H}$ we attach the 2-dimensional complex torus

$$A_\tau = \frac{\mathbb{C}^2}{\mathcal{O}_B\binom{\tau}{1}}$$

There is an obvious embedding $\mathcal{O}_B \hookrightarrow \mathrm{End}(A_\tau)$ and, moreover, A_τ admits a principal polarization. This motivates: a false elliptic curve $\mathcal{A}$ over a base scheme S is a p.p. relative abelian surface over S together with an embedding $\mathcal{O}_B \hookrightarrow \mathrm{End}(\mathcal{A})$.

11.12. **Heegner points (again).**

Because the pair (K, N^+) satisfies the Heegner hypothesis, there is an embedding $\iota : K \hookrightarrow B$ with

$$\iota(\mathcal{O}_K) \subset \mathcal{O}_{B,N^+}.$$

Carayol shows that $X_{\mathbb{C}}$ admits a canonical model $\mathcal{X}$ over $\mathbb{Z}\left[\frac{1}{N}\right]$. Work of Shimura shows that the image P of any $\tau \in \mathcal{H}$ fixed by $\iota(K^\times)$ satisfies $P \in \mathcal{X}(H)$.

11.13. **Modularity.**

Write $X = X_{N+,N^-}$ for $\mathcal{X}_{\mathbb{Q}}$. The usual Eichler-Shimura construction gives $X_{N^+,N^-} \to E$, but this depends on a choice of a base point. For $N^- = 1$ it is usual to send the cusp at infinity to the origin.

For $\chi \neq \mathbb{1}$ it doesn't matter which base point we pick. On Shimura cures, replace $P_{\mathbb{1}}$ with $\epsilon_f P_{\mathbb{1}}$ where $\epsilon_f \in \mathbb{Q}[\mathbb{T}] \subset \mathbb{Q}(\mathrm{End}[X_{N^+,N^-}])$ is the projector $\epsilon_f H^*(X_{N^+,N^-}) = H^1(X_{N^+,N^-})[\omega_f]$. Then $\epsilon_f P_{\mathbb{1}}$ is degree zero and its image on E_f does not depend on any choices.

11.14. **Gross-Zagier without the Heegner hypothesis.**

One has a divisor P_χ on $X(H)$ as before. There is an Eichler-Shimura parametrization $\phi : X \to E$ coming from f as above; write $Q_\chi = \phi(P_\chi)$.

Theorem 11.2. *(Zhang, 2001), (Yuan-Zhang-Zhang, 2013) One has*

$$L'(f, \chi, 1) \doteq \langle Q_\chi, Q_\chi \rangle.$$

11.15. **First step toward p-adic L-functions.**

By analogy with the definition of the Kubota-Leopoldt p-adic L-function, one wants to define a p-adic L-function by interpolation of special values of $L(f, \chi, n)$.

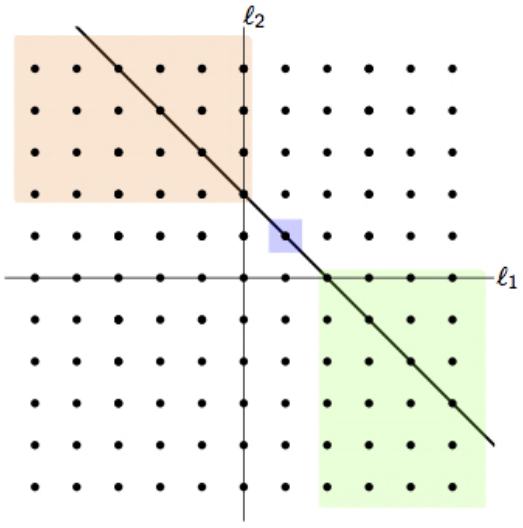
Normalization: if we let χ vary over a family of Hecke characters, we may assume $n = 0$. A Hecke character is a character of $\mathbb{A}^K/K^\times$. The restriction of such a character to $\mathbb{C}^\times$ is called its "infinity type". It is of the form

$$z \mapsto z^{-l_1}\overline{z}^{-l_2}$$

and we call the pair (l_1, l_2) the infinity type of the character.

11.16. **Hecke characters of K, (2/2).**

The central line $l_1 + l_2 = 2$ corresponds to Hecke characters such that is the centre of the functional equation for $L(f, \chi)$.



In the blue region consisting of characters of type $(1,1)$, the sign of the functional equation is negative. In the green region, the sign of the functional equation is positive. Thus, the classical L-function does not vanish at the center, even under the Heegner hypothesis! The sign of the functional equation for characters in the orange region is positive, but the orange region will not be used today. At each unshaded lattice point, some Γ-factor in the functional equation has a pole at $s = 0$. We won't use these today.

11.17. The p-adic L-function $L^{\mathbf{I}}$.

Fix a prime $p > 2$ which splits in K, with $(p, N) = 1$.

Theorem 11.3. *(Hida, 1988) There is a p-adic L-function $L^I(E, \chi)$, where χ ranges over central critical Hecke characters. It satisfies an interpolation law of the form*

$$L^I(E, \chi) \doteq L(E, \chi^{-1}, 0)$$

for χ central critical in the blue region.

The real and p-adic periods hidden in the $\doteq$ depend on E and not on χ.

11.18. Known results on $L^{\mathbf{I}}$.

By the interpolation law, $L^{\mathrm{I}}(\mathbb{1}) = 0$. The interesting invariant is $L^{\mathrm{I}'}(\mathbb{1})$.

- Perrin-Riou (1987) : $L^{\mathrm{I}'}(\mathbb{1}) \doteq \langle Q_{\mathbb{1}}, Q_{\mathbb{1}} \rangle_P$ (under Heegner hypothesis)
- Nekovár (1995) : higher weight version

$$Q_{\mathbf{1}} \to \text{ Heegner cycle on } \mathcal{E} \to X_0(N)$$

- Disegni (2013) : drops Heegner hypothesis from Perrin-Riou/Nekovár.
- Shnidman (2014) : allows twists by infinite-order Hecke characters.

11.19. The p-adic L-function $L^{\mathbf{II}}$.

Theorem 11.4. *(Hida, 1988) There is a p-adic L-function $L^{II}(E, \chi)$, where χ ranges over central critical Hecke characters. It satisfies an interpolation law of the form*

$$L^{II}(E, \chi) \doteq L(E, \chi^{-1}, 0)$$

for χ central critical in the green region.

Remark 11.5. *This is L^{II} from Lecture 3. The periods which occur are periods of Hecke characters (= periods of CM abelian varieties).*

11.20. Known results on $L^{\mathbf{II}}$.

No reason $L^{\mathrm{II}}(\mathbb{1})$ has to be zero. Instead, as mentioned above, one has

$$L_p(\mathbb{1}) \doteq (\log(\mathbb{Q}_{\mathbb{1}}))^2$$

11.21. **Assumptions needed for Bertolini-Darmon-Prasanna formula.**

- Bertolini-Darmon-Prasanna 2009 : Heegner hypothesis, $p \nmid N$. Also higher weights formula (generalized Heegner cycles).
- Masdeu 2011 : drops Heegner hypothesis, $(p||N^-)$ different p-adic L=function (p inert). Higher even weight.
- Castella 2011 : $p|N$, higher weight.
- Brooks 2013 : drops Heegner hypothesis, $p \nmid N$. Higher even weight (generalized Heegner cycles).
- Liu, S. Zhang, W. Zhang 2013 : no assumptions except p split! Formulas for Shimura curves over totally real fields.

11.22. **Applications to analytic rank.**

Theorem 11.6. *(Skinner, Theorem B) Suppose:*

- *(as above) p is split in K, $N = N^+N^-$ is square-free, prime to $d(K)$, satisfies the generalized Heegner hypothesis with respect to K.*
- *$p \geq 5$, E is p-ordinary, 2 splits in K.*
- *The mod p Galois representation $E[p]$ ramifies at some odd prime which is inert or ramified in K.*
- $\dim \mathrm{Sel}^I(K, V) = 1$ *and* $H^1_f(K, V) \hookrightarrow H^1_f(K_{\mathfrak{p}}, V) \oplus H^1_f(K_{\overline{\mathfrak{p}}}, V)$

Then

$$\mathrm{ord}_{s=1} L(E, K, s) = 1.$$

Proof. (sketch)

- The cohomological hypotheses imply
$$\ker(H^1(K, V) \to \bigoplus_{w \neq \mathfrak{p}} H^1(K_w, V)) = 0.$$
- X. Wan's divisibility in the main conjecture plus Galois cohomology (Skinner's lemma, Monday) implies that $L^{\mathrm{II}}(\mathbb{1}) \neq 0$.
- Bertolini-Darmon-Prasanna implies that $Q_{\mathbb{1}}$ is not torsion. Thus we may conclude rank 1 from Gross-Zagier.

□

11.23. **Sketch of BDP proof.**

Archimedean Waldspurger Formula: For χ of infinity type $(2 + j, -j)$ with $j \geq 0$, one has (with $\doteq$ denote the meaning of equal up to a p-adic unit),

$$L(f, \chi^{-1}, 0) \doteq \left| \sum_{\mathrm{Cl}(K)} \chi^{-1}(\mathfrak{a}) \mathbf{N}\mathfrak{a}^j \delta^j_{M-S} f(\mathfrak{a}^{-1}, 2\pi i dz) \right|^2$$

Here,

- $\delta_{M-S} = \frac{1}{2\pi i} \left(\frac{d}{d\tau} + \frac{k}{2i \operatorname{Im} \tau} \right)$
- $\delta^j_{M-S} f(\mathfrak{a}^{-1})$ does not make sense, but $\delta^j_{M-S} f(\mathfrak{a}^{-1}, 2\pi i dz)$ "does".

Atkin-Lehner argument: Remove absolute values (at the cost of more hidden in $\doteq$).

Algebraize: Replace $2\pi i dz$ with a differential ω_H on $E_{\mathfrak{a}}$ defined over H.

$$\frac{L(f,\chi^{-1},0)}{\Omega_{\mathbb{C}}^{2(2+j)}} \doteq \left(\sum_{\mathrm{Cl}(K)} \chi^{-1}(\mathfrak{a})\mathbf{N}\mathfrak{a}^j \delta_{M-S}^j f(\mathfrak{a}^{-1},\omega_H)\right)^2$$

Katz theorems on differential operators: both sides are algebraic. Can replace δ_{M-S} with $\theta = q\frac{d}{dq}$ (operator on p-adic modular forms).

p-adic interpolation: For p-adic interpolation of these algebraic numbers, replace f with p-depletion, $f^\flat$, and replace ω_H by a p-adic transcendental form $\widehat{\omega}$. The first drops an Euler factor at $\overline{\mathfrak{p}}$; the second produces a p-adic period Ω_p.

p-adic formula: Get a p-adic analytic function L_p (this is L^{II}) by

$$\begin{aligned}\frac{L_p(\chi)}{\Omega_p^{2(2+j)}} &:= \mathcal{E}_{\mathfrak{p}}(f,\chi^{-1},0)\frac{L(f,\chi^{-1},0)}{\Omega^{2(2+j)}} \\ &\doteq \left(\sum_{\mathrm{Cl}(K)} \chi^{-1}(\mathfrak{a})\mathbf{N}\mathfrak{a}^j \delta_{M-S}^j f^\flat(\mathfrak{a}^{-1},\widehat{\omega})\right)^2\end{aligned}$$

Letting $j \to -1$ p-adically (i.e. in weight space) and $\chi_n \to \mathbb{1}$, we get that

$$L_p(\mathbb{1}) \doteq \mathcal{E}_{\mathfrak{p}}(f,\chi^{-1},0)\left(\sum(\theta^{-1}f^\flat(\mathfrak{a},\widehat{\omega}))\right)^2$$

Relate θ^{-1} to $\log$: both coincide with the Coleman primitive. Use BDP to compute with p-adic modular forms as uniform limits (in the p-adic topology) of q-expansions of modular forms with integral Fourier coefficients. This definition does not make sense for Shimura curves, which is the major obstruction to dropping the Heegner hypothesis.

11.24. p-adic modular forms in the proof of BDP.

As above, the theory of Coleman integration gives the following formula:

$$\log_{\omega_f} = \theta^{-1}(f^\flat) = \theta^{-1}(f|_{1-UV}).$$

p-adic Hecke operators (Serre):

$$f|_U(q) = \sum a_{np}q^n,\ f|_V(q) = \sum a_n q^{pn}.$$

p-adic differential operator (Ramanujan-Atkin-Serre):

$$\theta = q\frac{d}{dq},\ \text{and } \theta^{-1}f = \lim_{i\to\infty}\theta^{p^i(p-1)-1}f.$$

11.25. **The case of Shimura curves.**

With definitions on the previous slide, the formula

$$\log_{\omega_f} = \theta^{-1}(f|_{1-UV})$$

is meaningless for f on a Shimura curve. However, Katz's geometric interpretation of p-adic modular forms in the classical case generalizes to Shimura curves (Kassaei, Ph. D thesis).

11.26. **The p-adic geometry of Shimura curves.**

Write $k = \overline{\mathbb{F}_p}$, $W = \mathrm{Witt}(k) = \widehat{\mathcal{O}_{\mathbb{Q}_p^{\mathrm{ur}}}}$, $L = \mathrm{Frac}(W)$. For the remainder of the lecture, X can be a Shimura curve or modular curve over L. There is no canonical model $\mathcal{X}$ for X/W:

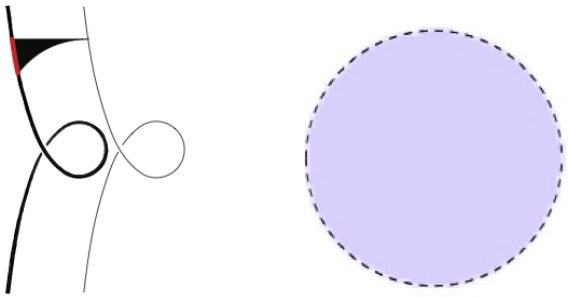
11.27. **The reduction map.**

The model $\mathcal{X}$ is proper over W and thus one has a map of sets:

$$X(L) = \mathcal{X}(W) \mapsto X(k).$$

11.28. **Residue disks.**

For a fixed $P \in X(k)$, the finer in $X(L)$ above P is called a residue disk. It has a natural structure of rigid analytic space, conformal to the open unit disk in L.



11.29. **The ordinary locus.**

The ordinary locus X^{odd} is the affinoid obtained from X by deleting the (finitely many) residue disks above points corresponding to super singular [false] elliptic curves.

11.30. **Geometric interpretation of p-adic modular forms.**

Recall that a classical modular form of weight k for $\Gamma_1(N)$ is a global section of $\underline{\omega}^{\otimes k}$ on the modular curve, where $\underline{\omega}$ is the push forward of the relative differential bundle on the universal elliptic curve. One has

$$\underline{\omega}^{\otimes 2} = \Omega_X$$

There is a similar bundle for Shimura curves (one needs to choose a projector as the obvious analogue is a rank 2 vector bundle).

Katz showed that a p-adic modular form of weight k gives rise to a section of $\underline{\omega}^{\otimes k}$ over the ordinary locus.

11.31. **Geometric interpretation of θ.**

There is a rank two vector bundle $\mathcal{V}$ on X which comes with a flat connection ∇ and an inclusion $\underline{\omega} \subset \mathcal{V}$. In the modular case, $\mathcal{V}$ is the first relative cohomolgy bundle of the universal elliptic curve (the connection has singularities at the cusps). In the Shimura curve case, the relative cohomology bundle of the universal abelian surface is too big. Get a sub-bundle from same projector as before.

By a theorem of Dwork and Katz, over the ordinary locus, the inclusion $\underline{\omega} \to \mathcal{V}$ splits:

$$\Psi : \mathcal{V} \to \underline{\omega}$$

In the modular curve case, Serre's operator θ coincides with the composition

$$\underline{\omega}^{\otimes k} \to \mathcal{V}^{\otimes k} \to_{\nabla} \mathcal{V}^{\otimes k} \otimes \Omega_X \to_{\Psi^{\otimes k}} \underline{\omega}^k \otimes \Omega \to \underline{\omega}^{k+2}.$$

We take this as the definition of θ in the Shimura curve case.

11.32. **Geometric interpretation of p-adic Hecke operators.**

Recall that Hecke operators T_l on the space of modular forms are pullbacks induced by correspondence on modular or Shimura curves. Recall that an elliptic curve with good ordinary reduction over $\mathbb{Q}_p$

has a canonical subgroup of order p - namely the unique C such that

$$E \to E/C$$

lifts the Frobenius map on the reduction. Similarly a false elliptic curve has a unique sub $\mathcal{O}_B$-module lifting the kernel of Frobenius.

Katz showed that V is induced by the correspondence

$$A \mapsto A/C.$$

Similarly, U is induced by the correspondence

$$A \mapsto \frac{1}{p} \sum_{C_i \neq C} (A/C_i).$$

Take these as definitions in Shimura curve case.

11.33. **Uniformization of ordinary residue disks.**

Start with $\mathcal{E}$ an elliptic curve over L with good ordinary reduction; call the reduction E. Pick a generator $P \in T_p(E)(k)$. Lift to $\tilde{P} \in T_p(\mathcal{E})(\overline{L})$. For $\sigma \in \mathrm{Gal}(\overline{L}/L)$ map $\sigma \mapsto (\tilde{P}^\sigma, \tilde{P}) \in \mathbb{Z}_p(1)$. This is a cocycle (!), call it $\xi_{\mathcal{E}}$.

Theorem 11.7. *(Serre-Tate) The association $\mathcal{E} \to \xi_E$ gives an embedding*

$$D = \{\textit{Lifts of } E \textit{ to } L\} \to H^1(L, T_p(1)) = L^\times.$$

The image is the set $1 + pW$ of norm one elements. So D has a natural group structure! Similarly for false elliptic curves.

11.34. **Another way to say the same thing.**

For a [false] elliptic curve $\mathcal{E}$ in the fixed residue disk D, we have a tautological sequence of p-divisible groups:

$$0 \to \widehat{\mathcal{E}}(L)[p^\infty] \to \mathcal{E}(L)[p^\infty] \to E(K)[p^\infty] \to 0$$

The left hand group depends only on E and not $\mathcal{E}$, because it's $\mathrm{Hom}(E^\vee(k)[p^\infty], \mathbb{Z}_p(1))$.

Theorem 11.8. *(Serre-Tate) The curve $\mathcal{E}$ is determined by the class of this extension, and (picking a generator of $T_p(E)$)*

$$D = \mathrm{Ext}^1(\mathbb{Q}_p/\mathbb{Z}_p, \mu_p^\infty) = 1 + pW.$$

11.35. **Serre-Tate coordinates.**

Serre-Tate theory identifies the ring of rigid functions on D with

$$W[[T]]\left[\frac{1}{p}\right]$$

where $T : D \to 1 + pW \overset{x \mapsto x-1}{\to} pW$. The bundle $\underline{\omega}$ trivializes on the disk D. Write $\widehat{\omega} \in \underline{\omega}(D)$ for a non-vanishing section obtained by choosing an isomorphism $\widehat{A} \to \widehat{\mathbb{G}_m}$ and pulling back dT/T. We can express a modular form of weight k on D by an expression of the form $F(T)\widehat{\omega}^{\otimes k}$.

11.36. **Formulas in Serre-Tate coordinates.**

Differential operator: Using computations of Brakocevic (2012) and Mori (2011), one can show

$$\theta(F(T)\widehat{\omega}^{\otimes k}) = (1+T)F'(T)\widehat{\omega}^{\otimes k+2}$$

p-adic Hecke operators: One has

$$(F(T)\widehat{\omega}^{\otimes k})|_{UV} = \frac{1}{p}\sum_{i=0}^{p-1} F(\zeta^i(1+T)-1)\widehat{\omega}^{\otimes k}$$

where $\zeta \in \overline{\mathbb{Q}}_p$ is a fixed non-trivial choice of p-th root of 1.

Making sense of the antiderivative θ^{-1} and establishing the BDP formula is then a matter of analyzing these power series operators, which is straightforward.

12. KOLYVAGIN'S CONJECTURE ON HEEGNER POINTS BY WEI ZHANG

12.1. **Theorems.** Let $E/\mathbb{Q}$ be an elliptic curve, ($f \in S_2(N), \Gamma_0(n)$-level). $E(\mathbb{Q})$ corresponds to a L-function, say $L(E/\mathbb{Q}, s)$. For $n \geq 1$, we obtain the exact sequences

$$0 \to E(\mathbb{Q} \otimes \mathbb{Z}/n\mathbb{Z} \to \mathrm{Sel}_n(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})_n \to 0$$

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

Define

$$r_p(E/\mathbb{Q}) := \mathrm{rank}_{\mathbb{Z}_p} \mathrm{Hom}(\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}), \mathbb{Q}/\mathbb{Z})$$

Note that $0 \leq r_{\text{alg}} \leq r_p$. Equality condition is is equivalent to the assertion that $Ш_{p^\infty}(E/\mathbb{Q})$ is finite.

Theorem 12.1. *(Gross-Zagier , Kolyvagin)* $\mathrm{rank}(E/\mathbb{Q}) \leq 1$ *implies that* $r_{alg}(E/\mathbb{Q}) = r_{an}$ *and* $\#Ш(E/\mathbb{Q}) < \infty$.

Theorem 12.2. *(Kato , Skinner-Urban) For* p *good ordinary (plus extra conditions), we have*

$$r_p = 0 \quad \textit{is equivalent to} \quad r_{an} = 0.$$

(and now the refined BSD),

$$\left| \frac{L(E/\mathbb{Q}, 1)}{\Omega} \right|_p = \left| \#Ш(E/\mathbb{Q}) \prod_{\ell | N} c_\ell \right|_p,$$

where c_ℓ *are the local Tamagawa number.*

What about when $r_p = 1$?

Theorem 12.3. *(W. Zhang)*
(1) For $p \geq 5$*, good ordinary, and*
(2) $\overline{\rho}_{\in p} : \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{Aut}(E_p) \cong \mathrm{GL}_2(\mathbb{F}_p)$ *surjective, ramified at least at two* $\ell || N$*, and ramified at all* $\ell || N$ *such that* $\ell \equiv \pm 1 \pmod{p}$.
Then

$$r_p = 1 \Leftrightarrow r_{an} = 1 \Leftrightarrow r_{alg} = 1 \textit{ and } \#Ш < \infty.$$

Remark 12.4.

(1) Joint work with Skinner $p || N$ *+ extra condition .*
(2) Skinner with cohomological condition .
(3) For refined BSD(p), $\mathrm{Reg}(E/\mathbb{Q}) = \dfrac{\langle y, y \rangle_{NT}}{[E(\mathbb{Q}) : \mathbb{Z}y]^2}$*, where* $\langle \cdot, \cdot \rangle_{NT}$ *is the Néron-Tate pairing.*
(4) $\mathrm{Sel}_p(E/\mathbb{Q}) = \begin{cases} 0, \\ \mathbb{Z}/p\mathbb{Z}, \end{cases}$ *implies* $r_{an} = \begin{cases} 0, \\ 1, \end{cases}$ *respectively.*

12.2. **Heegner points on Shimura curves.**

Let $K = \mathbb{Q}(\sqrt{-D})$. $N = N^+N^-$, where

$$N^+ = \prod_{\substack{\ell|N \\ \ell \text{ split}}} \ell, \quad \text{and} \quad N^- = \prod_{\substack{\ell|N \\ \ell \text{ inert}}} \ell.$$

Recall the Heegner hypothesis : N^- is square-free, and $\nu(N^-) := \#\{\ell : \ell|N^-\}$ is even. Let $K_\infty \supset K \supset \mathbb{Q}$, where K_n/K are the ray class fields, and $\mathrm{Gal}(K_n/K) = \mathrm{Pic}(\mathcal{O}_{K,n})$ under the Artin map, with $\mathcal{O}_{k,n} := \mathbb{Z} + n\mathcal{O}_K$, hence K_1 is the Hilbert class field. Let X_{N+N^-} be the Shimura curve attached to the quaternion ramified at N^- with $\Gamma_0(N^+)$-level, and $\phi : X_{N+N^-} \to E$ and continuous deformation to the "Heegner points", $P_n \in E(K_n)$, $P_1 \in E(K_1)$, $y_K = \mathrm{tr}_K^{K_1} P_1 \in E(K)$.

Then the Gross-Zagier formula is:

$$\frac{\langle y_K, y_K \rangle}{\deg(\phi)} = \frac{L'(E/K, 1)}{\frac{1}{\sqrt{|D|}} \langle f, f \rangle_{p_m}}.$$

Definition 12.5. *$\ell \nmid NpD$ are called Kolyvagin primes if ℓ is inert in K, $p|\gcd(\ell + 1, a_\ell)$ i.e., $\dim_{\mathbb{F}_p} E(\mathbb{F}_{\ell^2})/p = 2$. Define*

$$\Lambda := \{n = \prod_\ell \ell : \text{ square-free product of Kolyvagin primes}\},$$
$$\kappa := \{c(n) \in H^1(K, E_p) : n \in \Lambda\}.$$

For $M \geq 1$,

$$\kappa_M := \{c_M(n) \in H^1(K, E_{p^M}) : n \in \Lambda_M\}$$
$$\kappa_\infty := \bigcup_{M>1} \kappa_M,$$

where κ_∞ is called a "Kolyvagin system". $\mathrm{Sel}_{p^M}(E/K)$. For $n = 1$, $c_M(1)$ satisfies

$$E(K)/p^m E(K) \to H^1(K, E_{p^m})$$
$$y_K \in E(K) \mapsto C_M(1).$$

$$K_\infty := \bigcup_{M \geq 1} \kappa_M \neq 0 \text{ if } y_K \text{ is non-torsion}$$

Definition 12.6. *(Vanishing order)*

$$\mathrm{ord}\, K_\infty := \min_{c_M(n) \neq 0} \nu(n)$$

Example 12.7. $\mathrm{ord}\, \kappa_\infty = 0 \Leftrightarrow c_M(1) \neq 0 \Leftrightarrow y_K$ *is non-torsion* $\Leftrightarrow r_{an} = 1$.

12.3. **Kolyvagin conjecture.**

Conjecture 12.8. *$K_\infty \neq \{0\}$ at least $c_M(n) \neq 0$ for some $M \geq 1$, $n \in \Lambda$ ($\mathrm{ord}\, K_\infty < \infty$).*

Theorem 12.9. *(Kolyvagin) Assuming the conjecture, we have*

$$\kappa_\infty = \max\{r_p(E/K)^+, r_p(E/K)^-\} - 1.$$

- *For* $M \geq 1$,
$$\operatorname{ord} \kappa_M = \max\{\operatorname{rank} \operatorname{Sel}_{p^M}(E/K)^+, \operatorname{rank} \operatorname{Sel}_{p^M}(E/K)^-\} - 1.$$
- *For* $M = 1$,
$$\operatorname{ord} \kappa_1 = \max\{\dim_{\mathbb{F}_p} \operatorname{Sel}_p(E/K)^+, \dim_{\mathbb{F}_p} \operatorname{Sel}_p(E/K)^-\} - 1$$

Theorem 12.10. *Under earlier assumptions,* $\kappa_\infty \neq 0$. *Indeed,* $\kappa_1 \neq 0$.

Remark 12.11. *For* $\operatorname{rank} = 1$, *this is new.*

Proof. $r_p(E/K) = 1 \Leftarrow (GZK) r_{\text{an}} = 1 \Leftrightarrow \mathcal{J}_\kappa$ non torsion $\Leftrightarrow \operatorname{ord} \kappa_\infty = 0$. Further, $r_p(E/K) = 1 \Leftrightarrow \max\{r_p(E/K)^+, r_p(E/K)^-\} = 1 \Leftrightarrow \operatorname{ord} \kappa_\infty = 0$. □

Admissible BD , $m = q_1 q_2 \cdots$
$$f \bmod p = f_m \bmod p$$
$$\kappa(1) = \{c_1(n) \in H^1(K, E_p) : n \in \Lambda\}$$
$$\kappa(m) = \{c_1(n, m) \in H^1(K, E_p) : n \in \Lambda\}$$

"$\kappa(1) \equiv \kappa(m)$" known as Jochnowitz congruence or Bertolini-Darmon congruence .

13. On the p-converse of the Kolyvagin-Gross-Zagier theorem by Rodolfo Venerucci

Let $A/\mathbb{Q}$ an elliptic curve of conductor N_A, p an odd prime such that $p||N_A$ and p is of multiplicative reduction.

Theorem 13.1. *Under some technical assumptions ,*

$$\mathrm{ord}_{s=1} L(A,s) = 1 \Longleftrightarrow \mathrm{rank}_{\mathbb{Z}} A(\mathbb{Q}) = 1 \textit{ and } \#Ш(A/\mathbb{Q})_{p^\infty} < \infty$$

Credits:

- When p splits multiplicatively, Venerucci using Bertolini-Darmon and Skinner-Urban, Skinner-Zhang using Bertolini-Darmon and Skinner-Urban.
- When p even split multiplicatively: Bertolini-Darmon and Skinner-Urban ($+\varepsilon$).

From now on: $\mathrm{rank}_{\mathbb{Z}} A(\mathbb{Q}) = 1$ and $Ш(A/\mathbb{Q})_{p^\infty}$ is finite.

13.1. The p-converse for split multiplicative primes.

$A/\mathbb{Q}_p$ has split multiplicative reduction, that is, $G_{\mathbb{Q}_p} \circlearrowright A(\overline{\mathbb{Q}}_p) \cong \overline{\mathbb{Q}}_p^*/q_A\mathbb{Z}$, $q_A \in p\mathbb{Z}_p$, Tate's power of $A/\mathbb{Q}_p$. $K/\mathbb{Q}$ imaginary quadratic such that

(i) p splits in K,
(ii) $\mathrm{ord}_{s=1} L(A,\chi_K,s) = 1$ (here χ_K is the quadratic character of K).

Remark 13.2. *For K to exist we have to assume that there exists $q \neq p$ with $q||N_A$.*

$$\rho = \rho_{A,p} : G_{\mathbb{Q}} \to \mathrm{Aut}(\mathrm{T}_p(A)) \cong \mathrm{GL}_2(\mathbb{Z}_p)$$
$$\rho_\infty : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{R})$$

Pride's "central non-trivial" p-ordinary deformation of $\mathrm{Top}(A)$.

$\mathcal{R}$ is a regular, finite, flat over $\mathbb{Z}_p[[x]] \hookrightarrow \mathcal{A}(u)$, which is a $\mathbb{Q}_p$-valued locally analytic functions over a p-adic disc, and $2 \in U$. Define

$$U^d := U \cap \mathbb{Z}^{\geq 2}_{\text{even}}.$$

For every $k \in U^d$, $\rho_k : g_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{R}) \to \mathbb{Q}_p$.

$\rho_2 \cong \rho$; $\rho_k = \begin{cases} p\text{-adic Deligne representation} \\ \text{of an eigenform } f_k \in S_k(\Gamma_0(N_A),\mathbb{Z}_p) \end{cases}$ $(\kappa/2)$ as in Urban's Lectures 2-3, we can attack to these slate.

1) Mazur-Vritopound $\mathcal{L}_p(\rho_\infty/K) = \mathcal{L}_p(\rho_\infty) \cdot \mathcal{L}_p(\mathcal{L}_\chi^{\chi_k}) \in \mathcal{R}$ such that $u \in U^d$.

$$\mathcal{L}_p(\rho_\infty) = (1 - p^{n/2-1}) \cdot \mathcal{L}(f_n, n/2)^{\text{alg}} \in \overline{\mathbb{Q}}_p$$

The fact that $\rho(f_\infty, 2) = 0$ forces both $\mathcal{L}_p(\rho_\infty)$ to vanish to order at least 2.

2) "Big" Selmer group: $\mathrm{Sel}(\rho_\infty) \subset H^1(\mathbb{Q}, \rho_\infty \otimes \mathcal{R}^\vee)$ such that $X(\rho_\infty) = \mathrm{Sel}(\rho_\infty)^\vee$. Then: $X(\rho_\infty)_\kappa = X(\rho_\infty) \otimes_{\mathcal{R},ev_\kappa} \mathbb{Q}_p \sim H^1_f(\mathbb{Q}, \rho_\kappa)$, for all but finitely many $\kappa \in U^d$. Moreover,

$X(\rho_\infty)_2^* \cong \tilde{A}(\mathbb{Q}) \otimes \mathbb{Q}_p = A(\mathbb{Q}) \otimes \mathbb{Q}_p \oplus q_A \mathbb{Q}_p$.

We want to prove: $\mathrm{ord}_{s=1} L(A/K, s) = 2$ (if and only if $\mathrm{ord}_{s=1} L(A, s) = 1$). This will follow by these main steps ("Essence of Iwasawa theory").

Step A (Skinner-Urban) Write $\mathrm{char}(\rho_\infty) = \mathrm{char}_{\mathcal{R}}(X(\rho_\infty))\mathcal{R}/\mathcal{R}^*$. $\mathrm{char}(\rho_\infty/K) = \mathrm{char}(\rho_\infty) = \mathrm{char}(\rho_\infty^{\lambda_K})$.

$$\mathrm{ord}_{\kappa=2} \mathcal{L}_p(\rho_\infty.\mathbb{Q}) = (L_p^{\pm}, \cdots) \leq \mathrm{ord}_{\kappa=2} \mathrm{char}(\rho_\infty/K)$$

Remark 13.3. *The result of Skinner-Urban is over K, for p split.*

Step B (Bertolini-Darmon) $\frac{d^2}{dx^2}\mathcal{L}_p(\rho_\infty) = \log^2_{A/\mathbb{Q}_p}(\mathbb{P}_?)$, where $\mathbb{P}_? \in A^?(\mathbb{Q}) \otimes \mathbb{Q}$ is a Heegner point coming from a Shimura curve Pix of $A^?$.

By Gross-Zagier-Zhang formula, $\mathbb{P}_? \neq 0$ if and only if $\mathrm{ord}_{s=1} L(A^?, s) = 1$, so

$$\mathrm{ord}_{s=1} L(A/K, s) = 2 \text{ if and only if } \mathrm{ord}_{\kappa=2}(\rho_\infty/K) = 2.$$

Step C Prove that $\mathrm{ord}_{\kappa=2} \mathrm{char}(\rho_\infty^?) = 2$ (≥ 2 is easy). Use algebraic BSD formula

$$\frac{d^2}{d\kappa^2} \mathrm{char}(\rho_\infty^?)_{\kappa=2} = \det(\langle \cdot, \cdot \rangle^{\mathrm{Nek}}_{\rho_\infty, 2})$$

where $\langle \cdot, \cdot \rangle^{\mathrm{Nek}}_{\rho_\infty,2}$; $\tilde{A}^?(\mathbb{Q}) \times \tilde{A}^?(\mathbb{Q}) \to \mathbb{Q}_p$, is alternating and "arithmetically" defined by Néron's Poitou-Tate for Selmer complexes.

We prove that for all $p \in A(\mathbb{Q})$, $\langle p, q_A \rangle = \log_{A/\mathbb{Q}_p}(P)$. This implies

$$\frac{d^2}{dn^2} \mathrm{char}(\rho_\infty^?) = \log^2_{A/\mathbb{Q}_p}(\overline{P}),$$

$\overline{P}\mathbb{Z} = A^?(\mathbb{Q})/\mathrm{tors}$. Then,

$$2 \leq \mathrm{ord}_{\kappa=2} \mathcal{L}_p(\rho_0/\kappa) \leq \mathrm{ord}_{\kappa=2} \mathrm{char}(\rho_\infty/K) = h,$$

so BD follows.

13.2. **Non-split case.**

Let $K/\mathbb{Q}$ be imaginary quadratic, p inert in K. E/K_p has split multiplicative reduction.
(i) $L(A, \chi_K, 1) \neq 0 \Rightarrow Ш(A/K)_{p^\infty} < \infty$
(ii) $\mathrm{rank}_{\mathbb{Z}} A(K) = 1$.

Remark 13.4. *We are in the definite case.*

$$\rho_\infty : G_K \to \mathrm{GL}_2(\Lambda), \Lambda = \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]] \circlearrowleft \mathcal{A}(\mathbb{Z}_p)$$
$$\mathcal{L}_p(\rho_\infty/K) = L_p(f_A); \mathrm{char}(K_\infty/K) = \mathrm{char}_\Lambda \mathrm{Sel}_{p^\infty}(A/K_\infty)^\vee$$

Remark 13.5. *Since A/K_p has split multiplicative reduction we have* $\mathrm{ord}_{s=1} \mathcal{L} - p(\rho_\infty/K) \geq 2$, $\mathrm{ord}_{s=1} \mathrm{char}(\rho_\infty/K) \geq 2$.

We want to prove that $\mathrm{ord}_{s=1} L(A/K, s) = 1$ We thus have:

Step A (Bertolini's Lecture 10)

Step B (Bertolini-Darmon)

$$\frac{d^2}{ds^2}\mathcal{L}_p(\rho_\infty/K) = \log^2_{A/\mathbb{Q}_p}(\mathbb{P}_K - a_p(A)\overline{\mathbb{P}}_K).$$

with the assumption $a_p(A) = 1$, where $\mathbb{P}_K$ is "the" Heegner point coming from $X_{N_A^+, N_A^-} \to A$. This implies

$$\mathrm{ord}_{s=1}\, L(A/K, s), \mathrm{ord}_{s=1}\, \mathcal{L}_p(\rho_\infty/K) = 2$$

Step C

$$\frac{d^2}{ds^2}\,\mathrm{char}(\rho_\infty/K) = \#Ш(A/K)_{p^\infty}, \log^2_{A/\mathbb{Q}_p}(\overline{P}).$$

14. IWASAWA MAIN CONJECTURE FOR RANKIN-SELBERG p-ADIC L-FUNCTIONS BY XIN WAN

14.1. **Iwasawa-Greenberg main conjecture.**

Suppose T is a p-adic Galois representation for $G_{\mathbb{Q}}$ and $\dim T = d$. Let $d^{\pm}$ be the dimension of the eigenspace over $\mathbb{C}$ corresponding to ± 1, respectively. Suppose T is geometric, so that

$$V \otimes \mathbb{C}_p \cong \bigoplus_i \mathbb{C}_p(i)^{h_i},$$

where $\mathbb{C}_p$ is the algebraic closure of $\mathbb{Q}_p$, and $\mathbb{C}_p(i)$ refers to a Tate twist with i. Further, assume $\sum_{i\geq 1} h_i = d^+$.

14.2. **Panchishkin condition.**

V contains a $\mathbb{Q}_p$-subspace W_p which is invariant under G_p such that

$$W \otimes \mathbb{C}_p \cong \bigoplus_{i\geq 1} \mathbb{C}_p(i)^{h_i}.$$

If W_p exists, denote it by F^+V. Define $F^+(T \otimes \mathbb{Q}_p/\mathbb{Z}_p)$, the image of F^+V.

Greenberg defined

$$H^1_f(G_p, T \otimes \mathbb{Q}_p/\mathbb{Z}_p) := \ker \left\{ H^1(G_p, T \otimes \mathbb{Q}_p/\mathbb{Q}_p) \to H^1(I_p, \frac{T \otimes \mathbb{Q}_p/\mathbb{Z}_p}{F^+(T \otimes \mathbb{Q}_p/\mathbb{Z}_p)} \right\}$$

$$H^1_f(G_{\mathbb{Q}}, T \otimes \mathbb{Q}_p/\mathbb{Z}_p) := \ker \left\{ H^1(G_{\mathbb{Q}}, T \otimes \mathbb{Q}_p/\mathbb{Z}_p) \to \prod_{l\neq p} H^1(I_l, T \otimes \mathbb{Q}_p/\mathbb{Z}_p) \times \frac{H^1(G_p, T \otimes \mathbb{Q}_p/\mathbb{Z}_p)}{H^1_f(G_{\mathbb{Q}}, T \otimes \mathbb{Q}_p/\mathbb{Z}_p)} \right\}$$

Example 14.1. *Let $K/\mathbb{Q}$ a quadratic imaginary field extension and suppose that p splits as $v_0\overline{v_0}$. Let g_ξ be a CM form for a Hecke character ξ of K. Let f be a cuspidal eigenform.*

Case 1: If weight $g_\xi <$ weight f, *then the Panchishkin condition is true if and only if ordering at p*

$$f = \sum_{n=1}^{\infty} a_n q^n,\ p \nmid a_p$$

Case 2: if weight $g_\xi >$ weight f, *then the Panchishkin condition is always true.*

14.3. **Iwasawa theory.**

Let $K/\mathbb{Q}$ be a quadratic imaginary extension of $\mathbb{Q}$, K_∞/K the unique $\mathbb{Z}_p^2$-extension unramified outside. $\Lambda = \mathbb{Z}_p[[\Gamma]]$, $\Gamma = \mathrm{Gal}(K_\infty/K)$.

Definition 14.2.

$$\mathrm{Sel}_{K_\infty}(T \otimes \mathbb{Q}_p/\mathbb{Z}_p) := \varinjlim_{K\subset K'\subset K_\infty} \mathrm{Sel}_{K'}(T \otimes \mathbb{Q}_p/\mathbb{Z}_p)$$
$$X_{K_\infty}(T) := (\mathrm{Sel}_{K_\infty}(T \otimes \mathbb{Q}_p/\mathbb{Z}_p))^*$$

finite Λ-modules.

14.4. **Analytic side.**

Conjecturally: p-adic L-functions $\mathcal{L}_{p,K_\infty}(T) \in \Lambda$ parametrizes the "algebraic" part of special L-values of $L(T \otimes \chi, 0)$ for χ finite order characters of Γ.

Conjecture 14.3. *Iwasawa-Greenberg main conjecture:* $X_{K_\infty}(T)$ *is a* Λ*-torsion and* $\mathrm{char}_\Lambda(X_{K_\infty}(T)) = (\mathcal{L}_{p,K_\infty}(T))$ *as ideals of* Λ. $\mathrm{char}_A(M) = \{x \in A | \operatorname{ord}_P x \geq \log_{A_P}(M_P)\}$ *for any height on prime* P *of* A.

Theorem 14.4. *(X. Wan) Let* f *be a weight 2, trivial character cuspidal eigenform. Suppose* 2 *splits in* K*,* $p \geq 5$*, conductor* N *of* f *is square-free and divisible by at least one prime non-split in* K*. Suppose* $k > 6$*,* $k \equiv 0 \pmod{p-1}$*. If the* p*-adic avatar of* $\xi|\cdot|^{k/2}(\omega^{-1} \cdot N_m)$ *factors through* Γ_K*, then*

$$\mathcal{L}_{f,K_\infty}(\rho_f \otimes \rho_{g_\xi}) \supset \mathrm{char}_{\Lambda \otimes_{\mathbb{Z}_p} \mathbb{Q}_p}(X_{f,K_\infty}(\rho_f \otimes \rho_{g_\xi}).$$

Families of Klingen Eisenstein series on $U(3,1)$ are congruent modulo $\mathcal{L}_{p,K_\infty}$ to a cusp form on $U(3,1)$. Further, it is a reducible Galois representation and thus congruent to "more irreducible" representations. The congruence can be established via a lattice construction to elements in Selmer group.

How to construct family of Klingen Eisenstein series?

$$U(3,1), \begin{pmatrix} & & 1 \\ & \zeta & \\ -1 & & \end{pmatrix}, \quad \zeta \in M_2, \quad \Gamma\zeta \text{ is diagonal.}$$

P is upper triangular, Klingen parabolic. Using the doubling method , $U(3,1) \times U(0,2) \hookrightarrow U(3,3)$. Siegel Eisenstein series in $U(3,3)$ (induced from Siegel parabolic $Q = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \subset U(3,3)$. τ is a Hecke character of $K^\times$. Then

$$E_{\text{Kling}}(\tau, f, g_1) = \int_{U(0,2)Q \backslash U(0,2)(A)} E_{\text{Sieg}}(\tau, (g_1, g_2)) \overline{\tau}(\det g_2) f(g_2) dg_2$$

Hard part: make choices of primes above p.

- it is more about doing things p-adic analytically
- pulls back to (semi)-ordering Klingen Eisenstein series
- the Fourier-Jacobi coefficients (not too difficult to calculate)

Turns out that Siegel-Weil sections whose Fourier coefficients for

$$S = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & j \end{pmatrix}$$

is non-zero if and only if S has $\mathbb{Z}_p$ entries and $b \in \mathbb{Z}_p^\times$, $\det \begin{pmatrix} b & c \\ e & f \end{pmatrix} \in \mathbb{Z}_p^\times$.

In this case Fourier coefficients (local) of S to be $\xi_1(b)\xi_2\left(\begin{array}{c}\frac{\det\begin{pmatrix}b & c\\ e & f\end{pmatrix}}{\det b}\\ \\ \end{array}\right)$, ξ_1, ξ_2 depend on τ.

Choice motivated by differential operators.

14.5. **Study the Fourier-Jacobi coefficients.**

Need: Fourier-Jacobi coefficients are co-prime to p-adic L-function.

$$U(3,1), N = \begin{pmatrix}1 & * & * & *\\ & 1 & * & *\\ & & 1 & *\\ & & & 1\end{pmatrix},\ U = \begin{pmatrix}1 & & & \\ & * & * & \\ & * & * & \\ & & & 1\end{pmatrix}, \beta \in Q_+, F \text{ any form}$$

$$FJ_\beta(F) = \int F\left(\left(\begin{pmatrix}1 & & & t\\ & 1 & & \\ & & 1 & \\ & & & 1\end{pmatrix} g\right) e(-\beta t)dt\right.$$

considered as a function on NU.

We have algebraic definitions for Fourier-Jacobi coefficients involving global sections of line bundles $\mathcal{L}(\beta)$ on 2-dimensional CM abelian variety (theta function CM). Can construct another θ, on NU ($U(1) \leftrightarrow u(2)$).

$$L_{\theta_1} : M(NU(\mathbb{Q})\backslash NU(\mathbb{A}) \to M(U(\mathbb{Q})\backslash U(\mathbb{A}))$$

$$L_{\theta_1}(G)(u) = \int_{N(\mathbb{Q})\backslash N(\mathbb{A})} G(nu)\theta_1(nu)du$$

(can be made algebraic).

We construct auxiliary Hida family h on $U(2)$ and study

$$\langle L_{\theta_1} FJ_\beta(F), h\rangle \in Q_l[[\Gamma_K]]$$

Idea: doubling method.

$$FJ_\beta(E_{\text{Sieg}}(g) = \int E\left(\tau, \begin{pmatrix}1 & & & t\\ & 1 & & \\ & & 1 & \\ & & & 1\end{pmatrix} g\right) e(-\beta t)dt$$

considered as function on $U(2,2)\cdot N$.

$$N \subset N' \subset U(3,3)$$

restrict to $P \times U(0,2)$.

A calculation shows

$$FJ_\beta(E_{\text{Sieg}}) = E' \cdot \Theta$$

E' is the Siegel Eisenstein series on $U(2,2)$, Θ theta function on $U(2,2)\cdot N'$, and another calculation shows

$$\Theta|_{P\times U(2,2)} = \theta_2 \boxtimes \theta_3$$

θ_2, θ_3 are theta functions on P and $U(0,2)$. Easy to see $L_{\theta_1}(\theta_2$ is a constant function on $U(2,0)$. Set

$$A = \langle L_{\theta_1}, FJ_1(E_{\text{Kling}}), h\rangle = B\int_{U(2)\times U(2)} E'(g_1,g_2)\cdot h(g_1)\cdot\theta_3(g_2)f(g_2)dg_1dg_2$$

$$= B\cdot\mathcal{L}_{X_n}\int_{U(2)} h(g_2)\theta_3(g_2)f(g_2)dg_2$$

triple product $U(2)\times U(2)\hookrightarrow U(2,2)$ take h family of CM forms. Triple product $\mathcal{L}_1\cdot\mathcal{L}_2$, Hecke on non-vanishing modulo p of special L-values.

15. LEVEL RAISING MOD 2 AND ARBITRARY 2-SELMER RANKS
BY LI CHAO

15.1. **Motivation.**

Let $E/\mathbb{Q}$ be an elliptic curve. The celebrated B-SD conjecture says that

$$\mathrm{rank}(E(\mathbb{Q})) = \mathrm{ord}_{s=1} L(E,s).$$

The B-SD conjecture actually asserts something more refined. Indeed, they conjectured that in fact we have the following formula

$$\frac{L^{(r)}(E,1)}{r!\Omega(E)R(E)} = \frac{\prod_p c_p \cdot \#Ш(E)}{(\#E(\mathbb{Q})_{\mathrm{tor}})^2}$$

B-SD(ℓ): $r = 0, \ell \geq 3$, Skinner-Urban , Kato .
(with additional conditions): $r = 1, \ell \geq 5$, W. Zhang .

Question: What about $\ell = 2$? Why care about it?

Remark 15.1. *For the B-SD formula itself, the prime 2 is the most important to examine because it appears as a factor the most often.*

$r = 1$, E corresponds to some f.

$$f \in S_2(N), f \equiv g \in S_2(Ng) \pmod{\ell}$$

where g corresponds to some elliptic curve of rank 0 (level raising). This is done via something called the Jochnowitz congruence, due to Bertolini-Darmon .

We want a pseudo-congruence of the form

$$L(f,1)\text{“} \equiv \text{”}L(g,1) \pmod{\ell}$$

which makes no sense, as both sides are transcendental numbers. To get an expression that makes sense, we choose an auxiliary imaginary quadratic field K corresponding to $y_K \in E(K)$ with

$$\ell \nmid y_K \Leftrightarrow \mathrm{Sel}_l(A/K) = 0$$

15.2. **Level raising.**

Let ℓ be a prime number and

$$\overline{\rho}_\ell = \overline{\rho}_{E,\ell} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[\ell]) = \mathrm{GL}_2(\mathbb{F}_\ell)$$

Write the corresponding modular form as

$$f = \sum_{n \geq 1} a_n q^n$$

Definition 15.2. *A prime $q \nmid N\ell$ is <u>level raising</u>* $\pmod{\ell}$ *for E if*

$$\overline{\rho}(\mathrm{Frob}_q) = \pm \begin{pmatrix} 1 & * \\ & 1 \end{pmatrix} \Leftrightarrow a_q \equiv \pm(q+1) \pmod{\ell}$$

Theorem 15.3. *(Ribet) If $\overline{\rho}$ is absolutely irreducible and q is a level raising prime, then there exists $g \in S_2(Nq)$ new at q such that $f \equiv g \pmod{\ell}$.*

Theorem 15.4. *(Diamond-Taylor) If $\overline{\rho}$ ($\ell \geq 3$) is absolutely irreducible and $q_1, \cdots, q_m$ are level raising, then there exists $g \in S_2(Nq_1 \cdots q_m)$ new at each q_i such that $f \equiv g \pmod{l}$.*

Remark 15.5. *$g = \sum_{n \geq 1} b_n q^n$, $F = \mathbb{Q}(\{b_n\})$, there exists $\lambda | \ell$ of F such that $a_p \equiv b_p \pmod{\lambda}$ for all $p \neq q_1, \cdots, q_m$.*

Example 15.6. $E = X_0(11)$, $l = 3, q = 7$. $a_7 = 2 \equiv -8 \equiv -(7+1) \pmod 3$.
See table (tex later).

Remark 15.7. *At $p||Nq_1 \cdots q_m$, $b_p \in \{\pm 1\}$.*

(i) $p||N$, $b_p = a_p$ *($b_p \equiv a_p \pmod{\ell}$)*
(ii) $p = q_i \not\equiv -1 \pmod{\ell}$, *the b_p is determined.*
(iii) $p = q_i \equiv -1 \pmod{\ell}$, *Ribert proved both $b_p = \pm 1$ can occur.*

For $l = 2$, can $b_p = a_p$? The answer is no. Can both signs occur? The answer is yes.

Assumptions ($\star$):

(1) E is good at 2.
(2) $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_2) = S_3$ is surjective.
(3) $N(\overline{\rho}) = N$.
(4) $\overline{\rho}|_{G_{\mathbb{Q}_2}}$ is non-trivial (i.e. 2 does not split in $\mathbb{Q}(E[2])$).

Theorem 15.8. *(C. Li) Assume ($\star$) and $q_1, \cdots, q_m$ are level raising. Further, suppose $p||Nq_1 \cdots q_m$ and let $\varepsilon_p \in \{\pm 1\}$ prescribe sign. Then there exists $g \in S_2(Nq_1 \cdots q_m)^{New}$ such that $f \equiv g \pmod 2$ and $b_p = \varepsilon_p$ for all but possibly one $p||N$.*

Example 15.9. $f = 11a, q_1 = 7, q_2 = 13$. *See table, tex later.*

Example 15.10. $f = 35a$, $q = 19$. *See table, tex later.*

Strategy:

(1) $D_\tau T$ breaks down for $\ell = 2$ because of Fontaine-Laffaille theory . This can be salvaged for E super singular at 2.
(2) E ordinary at 2. Key ingredient: P. Allen , $\mathrm{big}(R) = \mathrm{big}(T)$ for nearly ordinary 2-adic representations with dihedral image.
(3) In both cases, a level raised form with prescribed signs everywhere but possibly ramified at one auxiliary prime q_0. Quadratic twist back get rid of q_0 at the cost of not prescribing one b_p, $p||N$.

15.3. 2-Selmer ranks.

Recall our f, g corresponding to elliptic curves E, A of rank $1, 0$ respectively, such that

$$f \equiv g \pmod 2.$$

($A \circlearrowleft \mathcal{O} = \mathcal{O}_F$, $k = \mathcal{O}/\lambda$).

$$E[2] \otimes k \cong A[\lambda]$$
$$\mathrm{Sel}_2(E) \otimes k \hookrightarrow H^1(\mathbb{Q}, E[2] \otimes k) = H^1(\mathbb{Q}, A[\lambda])$$

Note that $\mathrm{Sel}_\lambda(A) \hookrightarrow H^1(\mathbb{Q}, A[\lambda])$.

Theorem 15.11. *Assume conditions $(\star)$ and E has negative discriminant. Then for all $n \geq 0$, there exist infinitely many A in the level raising family such that*

$$\dim_k \mathrm{Sel}_\Lambda(A) = n.$$

Compare with

Theorem 15.12. *(Mazur-Rubin) Assume conditions $(\star)$ and E has negative discriminant. Then for all $n \geq 0$, there exist infinitely many $E^{(d)}$ in the quadratic twist family such that*

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E) = n.$$

15.4. **Bad news.**

Theorem 15.13. *Under certain conditions,*

$$\mathrm{rank}\, \mathrm{Sel}_2(E/K) = 1 \Rightarrow \mathrm{rank}\, \mathrm{Sel}_\Lambda(A/k) = 2.$$

$E = X_0(11)$.

p	A	d_K	$\mathrm{rank}(A(K))$	$\dim(Ш(A/K)[2])$	$\dim \mathrm{Sel}_2(A/K)$
7	$77a$	-8	2	0	2
7	$77b$	-8	0	2	2
13	$143a$	-7	2	0	2
13	$143a$	-8	2	0	2
17	$187a$	-7	2	0	2
17	$187a$	-24	0	2	2
19	$209a$	-7	2	0	2
19	$209a$	-19	2	0	2
29	$319a$	-8	2	0	2
29	$319a$	-19	0	2	2

16. p-ADIC WALDSPURGER FORMULA AND HEEGNER POINTS
BY YIFENG LIU

Let p be a prime number and $\mathbb{C}_p$ the algebraic closure of $\mathbb{Q}_p$. Let $E \subset \mathbb{C}_p$ be a CM number field, and $F \subset E$ a maximal totally real subfield. $\mathfrak{p}$ will denote a place of F, $\mathfrak{P}$ a place of E, over p. $\mathbb{A}$ will denote the ring of adeles of F, $\mathbb{A}^\infty$ is the ring of finite adeles of F. $\mathbb{B}$ is a totally definite incoherent quaternion algebra. This means that $\mathbb{B}_i$ is definite for any $i < \infty$, and incoherent means $\prod_v \epsilon(\mathbb{B}_v) = -1$.

Let $\mathbb{B} \to (X_v)_v$ be projective system of Shimura curves over F. X is the projective limit of X_U, U is an open compact subset $\mathbb{B}^{\infty\times} = (\mathbb{B} \otimes \mathbb{A}^\infty)^\times$.

Definition 16.1. *A function $X(\mathbb{C}_p) \to \mathbb{C}_p$ is a p-adic Maaß function if it is a pullback from a locally analytic function on X_U for some U.*

This is joint work with Shouwu Zhang and Wei Zhang .

Example 16.2. *$f : X \to A$ where A is an abelian variety over F. $\omega \in H^0(A, \Omega^1_A)$, $\log_\omega : A(\mathbb{C}_p) \to \mathbb{C}_p$, with $f^* \log_\omega : X(\mathbb{C}_p) \to \mathbb{C}_p$.*

Denote by $\mathcal{A}_{\mathbb{C}_p}(\mathbb{B}^\times) \circlearrowleft \mathbb{B}^{\infty\times}$.

16.1. The space of all p-adic Maaß functions.

An irreducible sub-representation $\pi \subset \mathcal{A}_{\mathbb{C}_p}(\mathbb{B}^\times)$ of $\mathbb{B}^{\infty\times}$ is (cuspidal) classical if there exists a non-zero function in π that is of the form $f^* \log_\omega$.

Remark 16.3. *Assume π is classical. There exists a unique classical sub-representation $\pi^\vee \subset \mathcal{A}_{\mathbb{C}_p}(\mathbb{B}^\times)$ such that $\pi^\vee$ is isomorphic to the centrag of π. There's no canonical pairing between π and $\pi^\vee$.*

We are given an embedding

$$e : \mathbb{A}_E^\infty \hookrightarrow \mathbb{B}^\infty \text{ of } \mathbb{A}^\infty\text{-algebras},$$

so that

$$E^\times \subset \mathbb{A}_E^{\infty\times} \subset \mathbb{B}^{\infty\times}$$

$Y = X^{E^\times}$, $Y = Y^+ \sqcup Y^-$ such that $E^\times$ acts on the tangent space of any point in $Y^\pm(\mathbb{C}_p)$ via the character $\left(\frac{t}{t^c}\right)^{\pm 1}, t \in E^\times$.

Definition 16.4. *For $\phi \in \mathcal{A}_{\mathbb{C}_p}(\mathbb{B}^\times)$, $\varphi_\pm$ locally constant functions on $Y^\pm(\mathbb{C}_p)$, define*

$$\mathcal{P}_{Y^\pm}(\phi, \varphi_\pm) = \int_{Y^\pm(G_p)} \phi(t)\varphi_\pm(t)dt$$

where dt is a Haar measure on $Y^\pm(\mathbb{C}_p)$ with total weight 1, which can be expressed as a finite sum.

From now on: p splits in E, $P\mathcal{O}_E = \mathfrak{P}\mathfrak{P}^c$.

Definition 16.5. *A character*

$$\chi : E^\times \backslash \mathbb{A}_E^{\infty\times} \to \mathbb{C}_p^\times$$

is a p-adic character of weight $k \in \mathbb{Z}$ if there exists $V \subset \mathbb{A}_E^{\infty\times}$ open compact such that

$$\chi(t) = \left(\frac{t_{\mathfrak{P}}}{t_{\mathfrak{P}^c}}\right)^k$$

for all $t \in V$.

χ us π-related if

$$\epsilon(1/2, \pi_v, \chi_v) = \chi_v(-1)\eta_v(-1) \in (\mathbb{B}_v)$$

for all $p \neq v < \infty$, where

$$\eta = \otimes \eta_v : F^\times \backslash \mathbb{A} \to \{\pm 1\}$$

quadratic character associated to E/F. Let $\Xi(\pi)_k$ to be the set of all π-related p-adic characters of weight k. $\mathfrak{D}(\pi)$ to be the coordinate ring of the above curve, which is a complete $\mathbb{C}_p$-algebra.

Remark 16.6. *When $F = \mathbb{Q}$, $\mathcal{D}(\pi) \to \mathcal{O}_{\mathbb{C}_p}[[\Gamma_\infty]]\left[\frac{1}{p}\right]$, Γ_∞ the Galois group of the anti-cyclotomic $\mathbb{Z}_p$-extension of E at p.*

$L : \mathbb{C}_p \to \mathbb{C}$, χ p-adic character of weight k.

$$\begin{cases} \chi_v^{(1)} = 1, & v|\infty, v \neq \iota|_F \\ \chi_v^{(\iota)} = \left(\frac{z}{z^c}\right)^k, & v = \iota|_F, z \in E \otimes_{F,\iota} \mathbb{R} \to \mathbb{C} \\ \chi_v^{(\iota)} = \iota \circ \chi_v, & v < \infty, v \neq p \\ \chi_p^{(\iota)} = \iota(\chi_q(t))\left(\frac{t}{t^c}\right)^k), & t \in E_p^\times \end{cases}$$

$\chi^\iota = \bigotimes_v \chi_v^{(\iota)} : E^\times \backslash \mathbb{A}_E^\times \to \mathbb{C}^\times$. Denote by $\pi^+ = \pi, \pi^- = \pi^\vee$. We choose:

(1) $(\cdot,\cdot)_\pi$: $\pi^+ \times \pi^- \to \mathbb{C}_p$.
(2) $\mathbb{C} : Y^+(\mathbb{C}_p) \to Y^-(\mathbb{C}_p)$ that is $\mathbb{A}_E^{\infty\times}$-equivariant.
(3) $\psi : F_p \to \mathbb{C}_p^\times$ of level 0.

The above defines some "period ratios" $\Omega_\iota(\chi)$ for any $\iota : \mathbb{C}_p \to \mathbb{C}$, $\chi \in \Xi(\pi)_k$ with $k \geq 1$.

Theorem 16.7. *(Liu, Zhang, Zhang) There is a unique element $\mathcal{L}(\pi) \in \mathcal{D}(\pi)$ such that for $\chi \in \Xi(\pi)_k$ with $k \geq 1$ and $\iota : \mathbb{C}_p \to \mathbb{C}$ we have*

$$\iota\left(\mathcal{L}(\pi)(\chi)\right) = L(1/2, \pi^{(\iota)}, \chi^{(\iota)}) \frac{S_p(2) \cdot \Omega_\iota(\chi)}{L(1,\eta)L(1,\pi^{(\iota)},\mathrm{Ad}} \frac{\epsilon(1/2, \psi, \pi_p^{(\iota)} \otimes \chi_\beta^{(\iota)})}{L(1/2, \pi_p^{(\iota)} \otimes \chi_{\beta^c}^{(\iota)})^2}$$

$\phi_\pm \in \pi^\pm$, $\varphi_\pm \in \sigma_\chi^\pm$. $\chi \in \Xi(\pi)_0$, $\sigma_\chi^\pm \subset \Gamma(Y^\pm)$ such that $\mathbb{A}^{\infty\times}$ acts via $\chi^{\pm 1}$.

$$\mathcal{P}_{Y^\pm}(\phi_\pm, \varphi_\pm) \in \mathrm{Hom}_{\mathbb{A}_E^{\infty\times}}(\pi^\pm \otimes \sigma_\chi^\pm, \mathbb{C}_p)$$

By Sato-Trennell , the latter space has dimension 1.

There is a natural basis of $\mathrm{Hom}_{\mathbb{A}_E^{\infty\times}}(\pi^+ \otimes \sigma_\chi^+, \mathbb{C}_p) \otimes \mathrm{Hom}(\cdots)(*)$ denoted by

$$\alpha^\natural(\phi_+, \phi_-, \varphi_+, \varphi_-)\text{“} = \text{”} \int_{\mathbb{A}^{\infty\times}\backslash\mathbb{A}_E^{\infty\times}} (t\phi_+, \phi_-)_\pi (t\varphi_+, \varphi_-) dt$$

with $\alpha^\natural \neq 0$ as a functional.

Theorem 16.8. *(p-adic Waldspurger)*

$$P_{Y^+}(\phi_+, \varphi_+) = \mathcal{L}(\pi)(\chi) \frac{L(1/2, \pi_p \otimes \chi_{\beta^c})^2}{(1/2, \psi, \pi_p \otimes \chi_{\beta^c})} \alpha^\natural(\phi_+, \phi_-, \varphi_+, \varphi_-)$$

where

$$P_{Y^+}(\phi_+, \varphi_+) = \int_{Y^+(\mathbb{C}_p)} (f^* \log_\omega) \varphi_+(t) dt = \log_\omega(H_E)$$

H_E is a Heegner cycle on A.

17. COLLOQUIUM - RECENT ADVANCES IN THE ARITHMETIC OF ELLIPTIC CURVES BY KARTIK PRASANNA

17.1. **Prelude.**

Classical identities:

$$\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\cdots=\frac{\pi^2}{6}$$
$$\frac{1}{1^4}+\frac{1}{2^4}+\frac{1}{3^4}+\cdots=\frac{\pi^4}{90}$$

In general,

$$\frac{1}{1^{2n}}+\frac{1}{2^{2n}}+\frac{1}{3^{2n}}+\cdots=\left|\frac{-1}{2}(2\pi i)^{2n}\frac{B_{2n}}{(2n)!}\right|$$

where the rational numbers B_n are the Bernoulli numbers, which are the coefficients corresponding to

$$\frac{z}{e^z-1}=\sum_{n=0}^{\infty}\frac{B_n\cdot z^n}{n!}.$$

Remark 17.1. *$2\pi i$ comes from geometry, and B_{2n} comes from arithmetic.*

17.2. **Products over primes.**

We first consider an absolute value defined over $\mathbb{Q}$. A function $|\cdot|:\mathbb{Q}\to\mathbb{R}^{\geq 0}$ is called an absolute value if

- $|x|=0$ if and only if $x=0$
- $|x+y|\leq|x|+|y|$
- $|xy|=|x|\cdot|y|$.

The usual absolute value on $\mathbb{R}$ gives an immediate example. However, other, not-so-obvious examples exist. Namely, for any prime number p there is an absolute value $|\cdot|_p$ which is given by

$$|\alpha|_p=\frac{1}{\text{power of } p \text{ dividing } \alpha}$$

Example 17.2. $p=5$, $|10|_5=1/5$, $|1/5|_5=5$.

A most remarkable fact, proved by Ostrowski, is that up to equivalence these are exactly all absolute values on $\mathbb{Q}$.

Theorem 17.3. *Take $\alpha\in\mathbb{Q},\alpha\neq 0$, we have*

$$\prod_{p\leq\infty}|\alpha|_p=1.$$

Example 17.4. *Take $\alpha=17/21$. If $p\neq 3,7,17$, then $|\alpha|_p=1$. On the other hand, $|\alpha|_3=3,|\alpha|_7=7,|\alpha|_17=1/17$. Further, $|\alpha|=\alpha=17/21$.*

A more interesting example is given by, for example, the Riemann zeta function. Indeed, we have

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}=\prod_p\left(1+p^{-s}+p^{-2s}+\cdots\right)=\prod_p\frac{1}{1-p^{-s}}.$$

Riemann proved the remarkable fact that ζ can in fact be extended analytically to a meromorphic function on the complex plane, with a simple pole at $s = 1$.

Recall our earlier example that the sum of the inverse of squares is equal to $\pi^2/6$. This can be expressed in terms of the ζ function

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \zeta(2) = \prod_p \frac{1}{1 - p^{-2}}.$$

What about the prime at infinity? How did we account for it in the product formula above? Riemann actually proved a functional equation for the zeta function, which is given as follows. First define

$$\Lambda(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s).$$

Then Λ satisfies the functional equation

$$\Lambda(s) = \Lambda(1 - s)$$

which is valid for all $s \in \mathbb{C}$. One can view the factor

$$\pi^{-s/2}\Gamma(s/2)$$

as the factor corresponding to the prime ∞.

The functional equation implies, by the known locations of the poles of the gamma function Γ, that ζ has simple zeroes at $s = -2, -4, -6, \cdots$.

The ζ function is the simplest example of a class of functions called L-functions. These are functions which have the following properties

(i) Defined as a product over primes
(ii) Analytic continuation
(iii) Attached to geometry
(iv) Contain arithmetic information

Geometry: Think about $\mathbb{A}^1 \setminus \{0\}$.

$$\int_\gamma \frac{dz}{z} = 2\pi i$$

We think about things with two loops. One such object is a torus, which we can think of as $\mathbb{C}/\Lambda$ where Λ is a lattice. A torus is an object with genus 1; which we can naturally associate to an elliptic curve, which is given by an equation of the form

$$y^2 = x^3 + Ax + B.$$

We assume that $A, B \in \mathbb{Z}$, since we want the corresponding L-function to have arithmetic properties. Recall that

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}.$$

Note that the denominator is linear in p^{-s}. This is because the underlying geometry contains only one loop. In the case of a torus (which naturally has two loops on its surface) we would expect

something that is quadratic in p^{-s} in the denominator, say

$$L(E,s) = \prod_p \frac{1}{(1-\alpha_p p^{-s})(1-\beta_p p^{-s})}$$

where $\alpha_p \beta_p = p$. Further, the quantity $(1-\alpha_p)(1-\beta_p) = \#E/\mathbb{F}_p$ which is the elliptic curve E over the finite field $\mathbb{F}_p$.

What about the prime at ∞, and the factor corresponding to it? In this case, we have the factor

$$(2\pi)^{-s}\Gamma(s)L(E,s)$$

If we define

$$\Lambda(E,s) = (2\pi)^{-s}\Gamma(s)L(E,s),$$

then we have the functional equation

$$\Lambda(E,s) = \pm\Lambda(E,2-s).$$

We now have the following remarkable theorem, which is essentially a consequence of the ingredients that went into proving Fermat's Last Theorem.

Theorem 17.5. *$\Lambda(E,s)$ admits analytic continuation (Wiles /Taylor-Wiles).*

17.3. **What is the Birch and Swinnerton-Dyer (BSD) Conjecture.**
If $E/\mathbb{Q}$ is an elliptic curve, we can interpret $E(\mathbb{Q})$ as follows:

$$E(\mathbb{Q}) = \{(x,y) : x,y \in \mathbb{Q}, y^2 = x^3 + Ax + B\}.$$

There is a remarkable fact that $E(\mathbb{Q})$ forms a finitely generated abelian group. In fact, there is a finite abelian group G and a non-negative integer r such that

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus G.$$

This integer r is called the rank of E.

Now, recall that we can associate to E the L-function $L(E,s)$ which has a zero at $s=1$. The Birch-Swinnerton-Dyer conjecture then asserts

Conjecture 17.6.

$$r = \mathrm{ord}_{s=1} L(E,s)$$

This conjecture is an example of a "local-global" principle, which is a fundamental phenomenon in the theory of numbers.

Remark 17.7. *The left-hand-side of the above equation is called the algebraic rank while the right hand side is called the analytic rank.*

17.4. **Recent progress.**

Theorem 17.8. *(Gross-Zagier/Kolyvagin) If* $r_{an}(E) = 0$ *or* 1*, then* $r_{alg}(E) = r_{an}(E)$.

Not much was known about the converse until recently. The situation change with a recent theorem of C. Skinner and W. Zhang.

Theorem 17.9. *(C. Skinner/W. Zhang) If* $r_{alg}(E) = 0$ *or* 1*, then* $r_{an}(E) = r_{alg}(E)$*, under some additional hypotheses.*

Hypothesis: (W. Zhang) we need that $|\operatorname{Sel}_p(E)| = 1$ or p.

Theorem 17.10. *(M. Bhargava-A. Shankar) For* $p = 2, 3, 5$, $\operatorname{Avg} \operatorname{Sel}_p(E) = p + 1$.

This implies that the previous two theorems apply frequently, in fact with at least 66% of curves.

17.5. **Epilogue.** Remember that $\mathbb{Q}$ can be embedded into $\mathbb{R}$, via the completion with respect to the usual absolute value. It can also be embedded into fields $\mathbb{Q}_p$ via completion by the p-adic absolute value $|\cdot|_p$. The field $\mathbb{Q}_p$ contains a ring which naturally corresponds to the integers, which we denote by $\mathbb{Z}_p$.

If $m \equiv 0 \pmod{p-1}$ with $n \not\equiv 0 \pmod{p-1}$, then

$$\frac{B_m}{m} \equiv \frac{B_n}{n} \pmod{p}.$$

For a power series $f(T) \in \mathbb{Z}_p[[T]]$, we have

$$f(1+p)^k - 1) = \zeta(1-k) = \cdots$$

$$Q(C_p^2) \to Q(C_p) \to Q$$

C is the inverse limit of $C_p, C_{p^2}, \cdots$, and we have

$$C = \frac{\mathbb{Z}_p[[T]]}{(g(T))}$$

Conjecture 17.11. *(Iwasawa Main Conjecture)* $f(T) = g(T)$.

This was proved by Mazur and Wiles in the 1980's. There are two types of L-functions, L^{I} and L^{II}, both with their versions of Iwasawa main conjecture. The L^{I} case was settled by Skinner-Urban and Kato while the L^{II} case was done by Xin Wan .

We have three types of objects, corresponding respectively to geometry, arithmetic, and analysis. For example, given an elliptic curve E, we can associate an L-function $L(E, s)$, which is an analytic object. We can also associate to it a Selmer group, which is an arithmetic object. We believe the underlying principle is controlled by something called motivic cohomology . Unfortunately, we do not know much about it!

18. Parity of ranks of elliptic curves
by Vladimir Dokchitser

Let $E/K : y^2 = x^3 + Ax + B$ be an elliptic curve, where K is a number field.

Conjecture 18.1. *(Parity conjecture - "explicit form")*

$$\operatorname{rank} E/K \equiv \sum_{v|\infty \Lambda_E} \lambda_v \pmod 2$$

where $\lambda_v \in \{0, 1\}$. *Further,*

- $\lambda_v = 0$ *if* E/K_v *is a good reduction*
- $\lambda_v = 1$ *if* $v|\infty$ *or if* E/K_v *has split multiplicative reduction*
- $\lambda_v = 0$ *if* E/K_v *non-split multiplicative reduction*
- $\lambda_v \equiv \dfrac{\$\mathbb{F}_v - 1}{2}$ *if* $v \nmid 2$, E/K_v *odd potentially multiplicative reduction*
- $\lambda_v = \left|\frac{\delta_E \cdot \#\mathbb{F}_v}{12}\right|$ *if* $v \nmid 2, 3$, E/K_v *odd potentially good reduction (here* δ_E *is the value minimal discriminant of* E*).*
- *there exist formulae for* $v|2, 3$.

18.1. (Conjectural) consequences.

(1) If E is semistable, then

$$\operatorname{rank} E/K \equiv \ (\text{mod } \#)v|\infty + \#\text{ split multiplicative primes } \pmod 2$$

(2) $E : y^2 = x^3 - x$, $d \in \mathbb{Z} \setminus \{0, 1\}$ square-free. Then

$$\operatorname{rank} E_d/\mathbb{Q} = \operatorname{rank} E/\mathbb{Q}(\sqrt{d}) - \operatorname{rank} E/\mathbb{Q} \equiv \sum_{v|2\infty} \lambda(E/\mathbb{Q}(\sqrt{d})_v) \pmod 2.$$

Here we remark that $\operatorname{rank} E/\mathbb{Q} = 0$, so we obtain the consequence

$$\operatorname{rank} E_d/\mathbb{Q} \equiv \sum_{v|2\infty} \lambda(E/\mathbb{Q}(\sqrt{d})_v) \equiv \begin{cases} 0 & d \equiv 1, 2, 3 \pmod 8 \\ 1 & d \equiv 5, 6, 7 \pmod 8 \end{cases}$$

(3) Heegner hypothesis: $E/\mathbb{Q}$, all $p|N_E$ in $\mathbb{Q}(\sqrt{-D})$ split ($D > 0$) implies $\operatorname{rank} E/\mathbb{Q}(\sqrt{-D})$ is odd.
(4) All $E/\mathbb{Q}$ have even rank over $\mathbb{Q}(i, \sqrt{17})$.
(5) $E : y^2 = x^3 + x^2 - 12x - 67/4$ (1369E1) has even rank over all extensions of $\mathbb{Q}((-32)^{1/4})$.
(6) All $E/\mathbb{Q}$ with split multiplicative reduction at 2 have odd rank over $\mathbb{Q}(\zeta_8)$.
(7) $E : y^2 + y = x^3 + x^2 + x$ has positive rank over $\mathbb{Q}(m^{1/3})$ for all m while having rank 0 over $\mathbb{Q}$.
(8) All quadratic twists of $E/\mathbb{Q}(i)$ by $d \in \mathbb{Q}(i)^\times$

$$E : y^2 + xy = x^3 - x^2 - 2x - 1 \text{(49A1)}$$

have positive rank.

18.2. Established cases of the parity conjecture.

Virtually nothing!

18.3. **Parity of analytic rank.**

Conjecturally, $L(E/K,s)$ is analytic on $\mathbb{C}$ and satisfies

$$L(E/K,s) = \pm(\Gamma\text{'s}, \exp\text{'s})L(E/K, 2-s)$$

The ± 1 is significant, and it is known as $w(E/K)$, the global root number. It has the form

$$w(E/K) = \prod_v w(E/K_v)$$

where $w(E/K_v)$ are local root numbers, each equal to ± 1.

$$\operatorname{ord}_{s=1} L(E/K,s) \equiv \begin{cases} \text{even} & \text{if } w=1 \\ \text{odd} & \text{if } w=-1 \end{cases} \equiv \sum_v \lambda_v^{\text{an}} \pmod 2$$

where $\lambda_v^{\text{an}} = \log_{-1} w(E/K_v)$.

Theorem 18.2. *(Rohrlich , Kobayashi , Dokchitser , Dokchitser, Whitehouse)*

$$\lambda_v = \lambda_v^{an}$$

(so the parity conjecture is equivalent to $\operatorname{rank} E/K =$ *"* $\operatorname{rank}_{an} E/K$*")*

18.4. **Parity of Selmer ranks.**

p is a prime and let $\operatorname{rank}_p E/K = \mathbb{Z}_p$-corank of $\operatorname{Sel}_p(E/K)^\vee$. Note that $\operatorname{rank} E/K$ is equal to $\operatorname{rank}_p E/K$ if $\#Ш$ is finite. What about $\operatorname{rank}_p E/K$ modulo 2?

Quasi-theorem (GZK): $\operatorname{rank}_p E/\mathbb{Q} = \operatorname{rank} E/\mathbb{Q} = \operatorname{rank}_{\text{an}} E/\mathbb{Q}$ for $\operatorname{rank}_{\text{an}} E/\mathbb{Q} \le 1$.

Theorem 18.3. *(Cassels , Fisher , Dokchitser-Dokchitser , Česnavičius) If E/K is such that it admits a p-isogeny then*

$$\operatorname{rank}_p E/K \equiv \sum_v \lambda_v \pmod 2$$

Proof. (assuming that $\#Ш < \infty$) Cassels' work implies that

$$\frac{\Omega_E \operatorname{Reg}_E \#Ш \prod_v c_v(E)}{\#E_{\text{tors}}^2} = \frac{\Omega_{E'} \operatorname{Reg}_{E'} \#Ш_{E'} \cdot \prod_v c_v(E')}{\#E_{\text{tors}}'^2}$$

which implies (where $\square$ denotes a square number),

$$p^{\operatorname{rank} E/K}\square = \frac{\operatorname{Reg}_E}{\operatorname{Reg}_{E'}} = \frac{\Omega_{E'}}{\Omega_E}\frac{\#Ш_{E'}}{\#Ш_E} \cdot \frac{\prod c_v(E')}{\prod c_v(E)} \cdot \frac{\#E_{\text{tors}}^2}{\#E_{\text{tors}}'^2}$$

This further implies

$$\operatorname{rank} E/K \pmod 2 \equiv \left(\operatorname{ord}_p \frac{\square}{\square}\right) + \sum \lambda_v'$$

(check $\sum \lambda_v = \sum \lambda_v'$). $\square$

Theorem 18.4. *(Kramer , Tunnell , Dokchitser-Dokchitser) If F/K is quadratic then*

$$\operatorname{rank}_2 E/F = \sum_v \lambda(E/F_v) \pmod 2 (\equiv \operatorname{rank}_{an} E/F)$$

Proof. Use isogeny $E \times E^F \to \operatorname{Res}_{F/K}(E/F)$. $\square$

Theorem 18.5. *(Dokchitser-Dokchitser , Mazur-Rubin , de La Rochefoucauld) If* $\mathrm{Gal}(F/K) \cong D_{2p^n}$ *(or* D_{p^n}*, depending on convention) with* p *odd, then*

$$\mathrm{rank}_p\, E/K + \mathrm{rank}_p\, E^M/K + \langle \chi, \mathrm{Sel}_{p^\infty}(E/F)^\vee \rangle \equiv \sum_v \mu_v$$

$$\equiv \mathrm{rank}_{an}\, E/K + \mathrm{rank}_{an}\, E^M/K + \mathrm{ord}_{s=1}\, L(E/M, \chi, s) \pmod 2$$

Proof. Uses an isogeny between some combination of Weil restriction of scalars of E from different fields. □

Theorem 18.6. *(Monsley , Nekovár, Kim , Dokchitser-Dokchitser) For* $E/\mathbb{Q}$*,*

$$\mathrm{rank}_p\, E/\mathbb{Q} \equiv \sum_v \lambda_v \equiv \mathrm{rank}_{an}\, E/\mathbb{Q} \pmod 2$$

Proof. Use previous result with F high in the p-anticyclotomic tower of M. This implies

$$\langle \chi, \mathrm{Sel}^\vee \rangle = \mathrm{ord}_{s=1}\, L(E/M, \chi, 1)$$

Choose M so that

$$\mathrm{rank}\, E^M/\mathbb{Q} = \mathrm{rank}_p\, E^M/\mathbb{Q} = \mathrm{rank}_{\text{an}}\, E^M/\mathbb{Q} \in \{0, 1\}$$

This implies that

$$\mathrm{rank}_p\, E/\mathbb{Q} \equiv \mathrm{rank}_{\text{an}}\, E/\mathbb{Q} \pmod 2$$

□

19. THE AVERAGE SIZE OF THE 5-SELMER GROUP OF ELLIPTIC CURVES BY ARUL SHANKAR

Joint work with M. Bhargava.
Let $E/\mathbb{Q}$ be an elliptic curve. We will discuss the 5-Selmer group, $\mathrm{Sel}_5(E)$. Recall we have the following exact sequence

$$0 \to E(\mathbb{Q})/5E(\mathbb{Q}) \to \mathrm{Sel}_5(E) \to Ш_E[5] \to 0,$$

where the main point is that

$$\#\,\mathrm{Sel}_5(E) \geq 5^{\mathrm{rank}(E)}.$$

We may ask, what is $\mathrm{Avg}\,\#\,\mathrm{Sel}_5(E)$ when $E/\mathbb{Q}$'s are ordered by height? (Recall that the height of $E = E_{A,B}$ is defined by

$$H(E) = H(A,B) := \max\{4|A|^3, 27B^2\},$$

cf. Section 1. Further, $A, B \in \mathbb{Z}$ and $p^4|A \Rightarrow p^6 \nmid B$ for all primes p.)

We consider the co-regular representation $V = 5 \otimes \Lambda^2(5)$. The group $\mathrm{GL}_5 \times \mathrm{GL}_5$ acts on this representation via the action

$$(g_1, g_2)(A, B, C, D, E) = (g_2 A g_2^t, g_2 B g_2^t, \cdots, g_2 E g_2^t)(g_1),$$

and we take the subgroup G of $\mathrm{GL}_5 \times \mathrm{GL}_5$ defined by

$$G := \{(g_1, g_2) : (\det g_1)(\det g_2)^2 = 1\}/\left\{ \begin{pmatrix} \lambda^2 & & \\ & \ddots & \\ & & \lambda^2 \end{pmatrix}, \begin{pmatrix} \lambda^{-1} & & \\ & \ddots & \\ & & \lambda^{-1} \end{pmatrix} \right\}$$

Remark 19.1.

$$(A, B, C, D, E) \mapsto (aX + bY + Cz + Ds + Et)$$

get $Q_1, \cdots, Q_5$, 5 4×4 Pfaffians. This defines a curve C of genus 1. V is locally soluble if $C(\mathbb{Q}_\nu) \neq \emptyset$ for all ν, while it is soluble if $C(\mathbb{Q}) \neq \emptyset$.

Theorem 19.2. *(Buchsbaumm-Eisenbud , Fisher , Bhargava-Ho)*

$$\mathrm{Sel}_5(E_{A,B}) \leftrightarrow G(\mathbb{Q})\backslash V(\mathbb{Q})^{\textit{loc sol}}_{A,B} \leftrightarrow G(\mathbb{Q})\backslash V(\mathbb{Z})^{\textit{loc sol}}_{A,B}$$

We can define an analogous height, which by abuse of notation we call H, on $V(\mathbb{R})$ by $H(v) = \max\{4|A(v)|^3, 27B(v)^2\}$.

Question: what is $\#G(\mathbb{Z})\backslash V(\mathbb{Z})^{\text{ire}}_{H<X}$. We have $v \in V(\mathbb{Q})$ is reducible if $\Delta(v) = 0$ or if V corresponds to $1 \in \mathrm{Sel}_5(E)$.

Let $\mathcal{F}$ be a fundamental domain on $G(\mathbb{Z})\backslash G(\mathbb{R})$, $\mathcal{R}$ a fundamental domain for $G(\mathbb{R})\backslash V(\mathbb{R})$, so

that $\mathcal{F} \cdot \mathcal{R}$ is a 5-fold cover of a fundamental domain $G(\mathbb{Z})\backslash V(\mathbb{R})$. Hence

$$\begin{aligned} 5 \cdot \#G(\mathbb{Z})\backslash V(\mathbb{Z})^{\text{irr}}_{H<X} &= \#\{\mathcal{F} \cdot \mathcal{R}_{H<X} \cap V(\mathbb{Z})^{\text{irr}}\} \\ &= \int_{g \in G_0} \#\{\mathcal{F} g \mathcal{R}_{H<X} \cap V(\mathbb{Z})^{\text{irr}}\} dg \\ &= \int_{g \in \mathcal{F}} \#\{g G_0 \mathcal{R}_{H<X} \cap V(\mathbb{Z})^{\text{irr}}\} dg \end{aligned}$$

Here G_0 is some open bounded set in $G(\mathbb{R})$ having volume 1. We can decompose $\mathcal{F}$ as follows

$$\mathcal{F} \subset N' A' K,$$

Here N' is bounded, K is compact, and

$$A' \to \left(\begin{pmatrix} t_1^{-4}t_2^{-3}t_3^{-2}t_4^{-1} & & & \\ & t_1t_2^{-3}t_3^{-2}t_4^{-1} & & \\ & & \ddots & \\ & & & t_1t_2^2t_3^3t_4^4 \end{pmatrix}, \begin{pmatrix} s_1^{-4}s_2^{-3}s_3^{-2}s_4^{-1} & & & \\ & s_1s_2^{-3}s_3^{-2}s_4^{-1} & & \\ & & \ddots & \\ & & & s_1s_2^2s_3^3s_4^4 \end{pmatrix} \right),$$

where $s_i, t_i \gg C$. This gives us the equality to

$$\text{Vol}(\mathcal{F} \cdot \mathcal{R}_{H<X}) + o(\text{Vol}(\mathcal{F} \cdot \mathcal{R}_{H<X})).$$

This implies that

$$\text{Avg}(\#\,\text{Sel}_5(E) - 1) = \tau(G) = 5.$$

Hence, by our earlier comment, since $\text{Avg}\,\#\,\text{Sel}_5 \leq 6$, it follows that

$$\text{Avg}(5^r) \leq 6.$$

- By noticing that $20r - 15 \leq 5^r$ for all $r \geq 1$, it follows that

  $$\text{Avg}(r) \leq \frac{21}{20} = 1.05$$

  This is achieved when 95% have rank 1 and 5% have rank 2.
- Proportion of curves that have rank 0 or 1 is at least $19/24$.

  $$x + 25(1 - x) \leq 6 \Rightarrow x \geq \frac{19}{24}.$$

Recall that

$$w_p(E) = \begin{cases} 1 & \text{if good reduction at } p \\ -1 & \text{if split multiplicative reduction at } p \\ 1 & \text{if non-split multiplicative reduction at } p \end{cases}.$$

Write $w(E) = -\prod_p w_p(E)$. Define $d(E)$ as follows

$$d(E) = w(E) \cdot w(E_{-1}),\ d(E) = \prod_p d_p(E),$$

where

$$d_p(E) = w_p(E) \cdot w_p(E_{-1}).$$

Lemma 19.3. *If $p > 3$, then $d_p(E) = -1$ if and only if E has multiplicative reduction at p and $p \equiv 3 \pmod 4$.*

$$d_{1/6}(E) = \prod_{p>3} d_p(E),\ \Delta_{6'}(E) = \frac{\Delta(E)}{2^{\Delta(E)/2}3^{\Delta(E)/3}}$$

$d_{1/6}(E) \equiv |\Delta_{6'}(E)| \pmod 4$ for curves having density at least 96.69%. Further, $d_{1/6}(E) \not\equiv |\Delta_{6'}(E)| \pmod 4$ for curves having density at least 3.25%.

Theorem 19.4. *There exists a family F of elliptic curves defined by congruence conditions on the coefficients of E*

- *F is closed under twists by -1, $d(E) = -1$ which implies that $w(E) = 1$ exactly half the time.*
- *Density of F is at least 55%.*

Theorem 19.5. *in a family where $w(E)$ is equidistributed and $\mathrm{Avg}(\#\,\mathrm{Sel}_5) = 6$, then*

$$\mathrm{Avg}(r) \leq 0.75.$$

Further, the density of curves with rank 0 is at least $3/8$.

Proof. Use Dokchister-Dokchitser on the 5-Selmer rank. For even n, use $12n + 1 \leq 5^n$ and for odd n, use $60n - 55 \leq 5^n$. Then

$$\frac{12\,\mathrm{Avg}_{\text{even}}(r_5) + 1}{2} + \frac{60\,\mathrm{Avg}_{\text{odd}}(r_5) - 55}{2} \leq 5$$

implies

$$\mathrm{Avg}(r_5) \leq 0.75.$$

□

20. HEURISTICS FOR BOUNDEDNESS OF RANKS OF ELLIPTIC CURVES BY BJORN POONEN

(joint with Jennifer Park, John Voight, Melanie Matchett Wood)

20.1. **Introduction.**

Question (Poincare 1901): Does there exist B such that for every $E/\mathbb{Q}$, we have $\mathrm{rank}(E/\mathbb{Q}) \leq B$?

History of guesses	Records
1950 Néron: probably bounded	
	1954 Néron: there exists $E/\mathbb{Q}$ of rank ≥ 1
1966 Cassels: "Implausible" to be bounded	1967
	1967 Shafarvich and Tate : unbounded over $\mathbb{F}_q(t)$
1982 Mestre : unbounded	1982 Mestre : rank ≥ 12
1986 Silverman : folklore conjecture; unbounded	
2006 Granville : bounded; with heuristic	2006 Elkies $\exists E/\mathbb{Q}$ of rank ≥ 28 $\exists E/\mathbb{Q}(t)$ of rank ≥ 18 $\exists$ infinitely many $E/\mathbb{Q}$ of rank ≥ 19
Almost everyone else: unbounded	

Associated with $E/\mathbb{Q}$ are the following arithmetic objects: $r = \mathrm{rank}\, E(\mathbb{Q})$, $\mathrm{Sel}_n E$, and Ш connected by the exact sequence

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

Conjecture 20.1. Ш *is finite.*

We shall assume this conjecture from now on.

Then there exists a non-degenerate alternating pairing $Ш \times Ш \to \mathbb{Q}/\mathbb{Z}$ so that $\#Ш$ is a square.

20.2. **Distribution of** Ш**.**

Given r, what is the distribution of $Ш[p^\infty]$ as E ranges over rank r elliptic curves? There are three conjectural answers.

(1) Delaunay (2001, 2007, 2013): For any finite abelian p-group G with an alternating pairing, what is the probability

$$\mathrm{Prob}(Ш[p^\infty] \cong G) = \frac{\#G^{1-r}}{\#\operatorname{Aut}(G,[\cdot,\cdot])} \cdot \prod_{i\geq r+1}(1-p^{1-2i}).$$

This is in analogy with Cohen-Lenstra for class groups.

(2) Poonen-Rains (2012), Bhargava-Kane-Lenstra-Poonen-Rains (preprint) : conjectural distribution for $(**)$ led to conjectural structure in the arithmetic of E, some of which was subsequently proven.

(3) Bhargava-Kane-Lenstra-Poonen-Rains (again) : For large n with $n \equiv r \pmod 2$, choose $A \in M_{n\times n}(\mathbb{Z}_p)$ subject to $A^T = -A$ with $\operatorname{rank}_{\mathbb{Z}_p}(\ker A) = r$. Take the limit of the distribution of

$$\operatorname{coker}\left(\mathbb{Z}_p^n \xrightarrow{A} \mathbb{Z}_p^n\right)_{\text{tors}}$$

as $n \to \infty$. In the Cohen-Lenstra case, this is analogous to a suggestion of Friedman-Washington.

Theorem 20.2. *(Bhargava-Kane-Lenstra-Poonen-Rains) The above three distributions coincide!*

20.3. **Model for rank.** To model $E/\mathbb{Q}$ of height H: choose large n of random parity, now choose $A \in M_{n\times n}(\mathbb{Z})$ subject to $A^T = -A$ and the entries of A are bounded by X. Here n, X depend on H. Then

- $(\operatorname{coker} A)_{\text{tors}}$ models $Ш(E)$
- $\operatorname{rank}_{\mathbb{Z}}(\ker A)$ models $\operatorname{rank} E(\mathbb{Q})$.

20.4. **Consequences of the model.**

- If n is even, $\operatorname{rank} A = n$ with probability approaching 1 as $H \to \infty$ (so that $X \to \infty$ as well). Indeed, this is saying that it should be increasingly difficult to land on the Pfaffian hypersurface.
- If n is odd, $\operatorname{rank} A = n-1$ with probability approaching 1 as $H \to \infty$.

This suggests that, at least asymptotically, that 50% of elliptic curves $E/\mathbb{Q}$ have rank 0 and 50% of elliptic curves have rank 1. Further, all elliptic curves of rank at least 2 have to land on some special hypersurface.

Theorem 20.3. *If $\rho < n$ and ρ is even, then approximately $X^{n\rho/2}$ of the roughly $X^{n(n-1)/2}$ possible A's, have rank $\leq \rho$ (as $X \to \infty$).*

Most of this work was done by Eskin and Katznelson for symmetric matrices.

This suggests that for each $r \geq 1$,

$$\begin{aligned}\mathrm{Prob}(\operatorname{rank} E \geq r) &\overset{\text{model}}{=} \mathrm{Prob}(\operatorname{rank} A \leq n-r)\\ &\overset{\text{Thm}}{\sim} \frac{X^{n(n-r)/2}}{X^{n(n-1)/2}}\\ &\sim \frac{1}{(X^{n/2})^{r-1}}\end{aligned}$$

20.5. **Calibration (Watkins).**

Consider E with even rank. Let

$$\#Ш_0 := \begin{cases} \#Ш & \text{if } \operatorname{rank} E = 0 \\ 0 & \text{otherwise.} \end{cases}$$

Part of BSD: $L(E,1) = \dfrac{\#Ш_0 \Omega \prod c_p}{\#E(\mathbb{Q})^2_{\text{tors}}}$ Hence

$$\begin{aligned} \sqrt{\#Ш_0} &\sim O(\Omega^{-1/2}) \\ &\sim O(H^{1/24}) \end{aligned}$$

$$\operatorname{Prob}(\operatorname{rank} E \geq 2) = \operatorname{Prob}(\sqrt{\#Ш_0} = 0) \sim \frac{1}{H^{1/24}}$$

Hence, we can see that

$$\frac{1}{(X^{n/2})^{r-1}} \sim \frac{1}{H^{(r-1)/24}}$$

20.6. **Conclusion.**

There are $\sim H^{5/6}$ elliptic curves of height $\leq H$. If $r - 1 > 20$, then

$$\sum_{E/\mathbb{Q}} \frac{1}{(\text{height } E)^{(r-1)/24}}$$

converges. So we expect only finitely many elliptic curves of rank $\geq r$.

Prediction: $\operatorname{rank} E \leq 21$ with finitely many exceptions.