Lightning Talks
Tuesday July 11, 2023

Presenters -

Santiago Arango (Emory University)

Hyun Jong Kim (University of Wisconsin-Madison)

Sung Min Lee (University of Illinois at Chicago)

Yongyuan Huang (University of California San Diego)

Juanita Duque Rosero (Boston University)

Garen Chiloyan

Asimina Hamakiotes (University of Connecticut)

Sachi Hashimoto (Brown University

Pietro Mercuri (Sapienza Università di Roma)

Ciaran Schembri (Dartmouth College)

Robin Visser (University of Warwick)

Tian Wang (University of Illinois at Chicago)

Frobenius distributions of abelian varieties over finite fields

Joint with Deewang Bhamidipati and Soumya Sankar

Santiago Arango-Piñeros

Emory University

LuCaNT

ICERM

July 11, 2023

The problem

- Fix a g-dimensional abelian variety A over a finite field $\mathbb{F}_q$.
- For every $r \geq 1$, Frobenius polynomial of the base extension to $\mathbb{F}_{q^r}$ is given by

$$P_r(T) = T^{2g} + a_1^{(r)} T^{2g-1} + \cdots + q^{rg} = \prod_{j=1}^{g} (T - \alpha_j^r)(T - \overline{\alpha}_j^r).$$

Question:

What is the distribution of the sequence of normalized traces of Frobenius

$$x_r := -a_1^{(r)}/q^{r/2} \in [-2g, 2g]?$$

The problem

- Fix a g-dimensional abelian variety A over a finite field $\mathbb{F}_q$.
- For every $r \geq 1$, Frobenius polynomial of the base extension to $\mathbb{F}_{q^r}$ is given by

$$P_r(T) = T^{2g} + a_1^{(r)} T^{2g-1} + \cdots + q^{rg} = \prod_{j=1}^{g} (T - \alpha_j^r)(T - \overline{\alpha}_j^r).$$

Question:

What is the distribution of the sequence of normalized traces of Frobenius

$$x_r := -a_1^{(r)}/q^{r/2} \in [-2g, 2g]?$$

The problem

- Fix a g-dimensional abelian variety A over a finite field $\mathbb{F}_q$.
- For every $r \geq 1$, Frobenius polynomial of the base extension to $\mathbb{F}_{q^r}$ is given by

$$P_r(T) = T^{2g} + a_1^{(r)} T^{2g-1} + \cdots + q^{rg} = \prod_{j=1}^{g} (T - \alpha_j^r)(T - \overline{\alpha}_j^r).$$

Question:

What is the distribution of the sequence of normalized traces of Frobenius

$$x_r := -a_1^{(r)}/q^{r/2} \in [-2g, 2g]?$$

The 35 isogeny classes of abelian surfaces over $\mathbb{F}_2$

Our results

- We identify a compact abelian Lie subgroup of $\mathrm{USp}_{2g}(\mathbb{C})$ controlling these distributions via push-forward of the Haar measure, through $U \mapsto \mathrm{tr}\, U \in [-2g, 2g]$.
- We classify the possible groups that appear for $g = \dim A \leq 3$. This is equivalent to understanding the possible multiplicative relations between the Frobenius eigenvalues $\alpha_1, \ldots, \alpha_g$ and q.
- If you are interested in learning more, please talk to me or read our paper: https://arxiv.org/abs/2306.02237!

Our results

- We identify a compact abelian Lie subgroup of $\mathrm{USp}_{2g}(\mathbb{C})$ controlling these distributions via push-forward of the Haar measure, through $U \mapsto \operatorname{tr} U \in [-2g, 2g]$.
- We classify the possible groups that appear for $g = \dim A \leq 3$. This is equivalent to understanding the possible multiplicative relations between the Frobenius eigenvalues $\alpha_1, \ldots, \alpha_g$ and q.
- If you are interested in learning more, please talk to me or read our paper: https://arxiv.org/abs/2306.02237!

Our results

- We identify a compact abelian Lie subgroup of $\mathrm{USp}_{2g}(\mathbb{C})$ controlling these distributions via push-forward of the Haar measure, through $U \mapsto \operatorname{tr} U \in [-2g, 2g]$.
- We classify the possible groups that appear for $g = \dim A \leq 3$. This is equivalent to understanding the possible multiplicative relations between the Frobenius eigenvalues $\alpha_1, \ldots, \alpha_g$ and q.
- If you are interested in learning more, please talk to me or read our paper: https://arxiv.org/abs/2306.02237!

Cohen-Lenstra Heuristics and Vanishing of Zeta Functions for Trielliptic Curves over Finite Fields

Hyun Jong Kim
University of Wisconsin-Madison

7/11/2023

Theorem (Ellenberg-Venkatesh-Westerland, 2016)

Let $\ell > 2$ *be a prime. Write*
$\mathcal{L}_{q,n} = \{L : L = \mathbb{F}_q(t)[\sqrt{f(t)}], f \text{ squarefree}, \deg f = n\}/(\text{isomorphism}).$

Theorem (Ellenberg-Venkatesh-Westerland, 2016)

Let $\ell > 2$ be a prime. Write
$\mathcal{L}_{q,n} = \{L : L = \mathbb{F}_q(t)[\sqrt{f(t)}], f \text{ squarefree}, \deg f = n\}/(\text{isomorphism})$.
There is a constant C_ℓ such that, for any finite abelian ℓ-group A,

Theorem (Ellenberg-Venkatesh-Westerland, 2016)

Let $\ell > 2$ be a prime. Write
$\mathcal{L}_{q,n} = \{L : L = \mathbb{F}_q(t)[\sqrt{f(t)}], f \textit{ squarefree}, \deg f = n\}/(\textit{isomorphism})$.
There is a constant C_ℓ such that, for any finite abelian ℓ-group A,

$$\lim_{\substack{q\to\infty \\ q\not\equiv 1 \pmod{\ell} \\ q \text{ odd}}} \lim_{\substack{n\to\infty \\ n \text{ odd}}} \frac{\#\{L \in \mathcal{L}_{q,n} : \mathrm{Cl}_L \cong A\}}{\#\mathcal{L}_{q,n}} = \frac{C_\ell}{|\operatorname{Aut}(A)|}.$$

Theorem (Ellenberg-Venkatesh-Westerland, 2016)

Let $\ell > 2$ be a prime. Write
$\mathcal{L}_{q,n} = \{L : L = \mathbb{F}_q(t)[\sqrt{f(t)}], f$ *squarefree*$, \deg f = n\}/($*isomorphism*$)$.
There is a constant C_ℓ such that, for any finite abelian ℓ-group A,

$$\lim_{\substack{q \to \infty \\ q \not\equiv 1 \pmod{\ell} \\ q \text{ odd}}} \lim_{\substack{n \to \infty \\ n \text{ odd}}} \frac{\#\{L \in \mathcal{L}_{q,n} : \mathrm{Cl}_L \cong A\}}{\#\mathcal{L}_{q,n}} = \frac{C_\ell}{|\operatorname{Aut}(A)|}.$$

Theorem (Ellenberg-Li-Shusterman, 2019)

Fix p to be a prime, and $s = \frac{1}{2} + it$.

Theorem (Ellenberg-Venkatesh-Westerland, 2016)

Let $\ell > 2$ be a prime. Write
$\mathcal{L}_{q,n} = \{L : L = \mathbb{F}_q(t)[\sqrt{f(t)}], f \text{ squarefree}, \deg f = n\}/(\text{isomorphism})$.
There is a constant C_ℓ such that, for any finite abelian ℓ-group A,

$$\lim_{\substack{q \to \infty \\ q \not\equiv 1 \pmod{\ell} \\ q \text{ odd}}} \lim_{\substack{n \to \infty \\ n \text{ odd}}} \frac{\#\{L \in \mathcal{L}_{q,n} : \mathrm{Cl}_L \cong A\}}{\#\mathcal{L}_{q,n}} = \frac{C_\ell}{|\mathrm{Aut}(A)|}.$$

Theorem (Ellenberg-Li-Shusterman, 2019)

Fix p to be a prime, and $s = \frac{1}{2} + it$. Let $\mathcal{H}_g(\mathbb{F}_q)$ be the family of genus g hyperelliptic curves over $\mathbb{F}_q$. Write Z_C for the zeta function of a curve C.

$$\lim_{k \to \infty} \lim_{g \to \infty} \frac{|\{C \in \mathcal{H}_g(\mathbb{F}_{p^k}) : Z_C(s) = 0\}|}{|\mathcal{H}_g(\mathbb{F}_{p^k})|} = 0.$$

Theorem (Ellenberg-Venkatesh-Westerland, 2016)

Let $\ell > 2$ be a prime. Write
$\mathcal{L}_{q,n} = \{L : L = \mathbb{F}_q(t)[\sqrt{f(t)}], f \text{ squarefree}, \deg f = n\}/(\text{isomorphism})$.
There is a constant C_ℓ such that, for any finite abelian ℓ-group A,

$$\lim_{\substack{q \to \infty \\ q \not\equiv 1 \pmod{\ell} \\ q \text{ odd}}} \lim_{\substack{n \to \infty \\ n \text{ odd}}} \frac{\#\{L \in \mathcal{L}_{q,n} : \mathrm{Cl}_L \cong A\}}{\#\mathcal{L}_{q,n}} = \frac{C_\ell}{|\operatorname{Aut}(A)|}.$$

Theorem (Ellenberg-Li-Shusterman, 2019)

Fix p to be a prime, and $s = \frac{1}{2} + it$. Let $\mathcal{H}_g(\mathbb{F}_q)$ be the family of genus g hyperelliptic curves over $\mathbb{F}_q$. Write Z_C for the zeta function of a curve C.

$$\lim_{k \to \infty} \lim_{g \to \infty} \frac{|\{C \in \mathcal{H}_g(\mathbb{F}_{p^k}) : Z_C(s) = 0\}|}{|\mathcal{H}_g(\mathbb{F}_{p^k})|} = 0.$$

Goal: generalize to $\mathbb{Z}/d\mathbb{Z}$-covers of $\mathbb{P}^1$

Tentative Theorem/Goal (K.)

Let $d \geq 2$. Let $\ell \nmid d$ be a prime. Write
$\mathcal{L}_{q,n} = \{L : L = \mathbb{F}_q(t)[\sqrt[d]{f(t)}], f$ *squarefree*, $\deg f = n\}/$(*isomorphism*).
There is a constant C_ℓ such that, for any $\mathbb{Z}_\ell[\zeta_d]$-module A of finite cardinality with "mild conditions",

$$\lim_{\substack{q\to\infty \\ q\not\equiv 1 \pmod{\ell} \\ q\equiv 1 \pmod{d}}} \lim_{\substack{n\to\infty \\ (d,n)=1 \text{ or } d|n}} \frac{\#\{L \in \mathcal{L}_{q,n} : \mathrm{Cl}_L \cong_{\mathbb{Z}_\ell[\zeta_d]} A\}}{\#\mathcal{L}_{q,n}} = \frac{C_\ell}{|\operatorname{Aut}_{\mathbb{Z}_\ell[\zeta_d]}(A)|}.$$

Tentative Theorem/Goal (K.)

Fix p to be a prime, and $s = \frac{1}{2} + it$.n Let $\mathcal{D}_g(\mathbb{F}_q)$ be the family of genus g tame $\mathbb{Z}/d\mathbb{Z}$-covers of $\mathbb{P}^1$ over $\mathbb{F}_q$.

$$\lim_{k\to\infty} \lim_{\substack{g\to\infty \\ \mathcal{D}_g \text{ nonempty}}} \frac{|\{C \in \mathcal{D}_g(\mathbb{F}_{p^k}) : Z_C(s) = 0\}|}{|\mathcal{D}_g(\mathbb{F}_{p^k})|} = 0.$$

Differences in $d = 2$ and $d > 2$ cases

- $T_\ell \operatorname{Pic}^0(C)$ is a module over $\mathbb{Z}_\ell[\zeta_d] = \mathbb{Z}_\ell[X]/(X^{d-1} + \cdots + 1)$.

Differences in $d = 2$ and $d > 2$ cases

- $T_\ell \operatorname{Pic}^0(C)$ is a module over $\mathbb{Z}_\ell[\zeta_d] = \mathbb{Z}_\ell[X]/(X^{d-1} + \cdots + 1)$.
- Consider surjections $T_\ell \operatorname{Pic}^0(C) \to A$ that are $\mathbb{Z}_\ell[\zeta_d]$-equivariant.

Differences in $d = 2$ and $d > 2$ cases

- $T_\ell \operatorname{Pic}^0(C)$ is a module over $\mathbb{Z}_\ell[\zeta_d] = \mathbb{Z}_\ell[X]/(X^{d-1} + \cdots + 1)$.
- Consider surjections $T_\ell \operatorname{Pic}^0(C) \to A$ that are $\mathbb{Z}_\ell[\zeta_d]$-equivariant.
- The Weil pairing $\omega : T_\ell \operatorname{Pic}^0(C) \times T_\ell \operatorname{Pic}^0(C) \to \mathbb{Z}_\ell(1)$ respects the ζ_d-action.

Differences in $d = 2$ and $d > 2$ cases

- $T_\ell \operatorname{Pic}^0(C)$ is a module over $\mathbb{Z}_\ell[\zeta_d] = \mathbb{Z}_\ell[X]/(X^{d-1} + \cdots + 1)$.
- Consider surjections $T_\ell \operatorname{Pic}^0(C) \to A$ that are $\mathbb{Z}_\ell[\zeta_d]$-equivariant.
- The Weil pairing $\omega : T_\ell \operatorname{Pic}^0(C) \times T_\ell \operatorname{Pic}^0(C) \to \mathbb{Z}_\ell(1)$ respects the ζ_d-action. Consequently, ω yields a Hermitian pairing over $\mathbb{Z}_\ell[\zeta_d]$.

Differences in $d = 2$ and $d > 2$ cases

- $T_\ell \operatorname{Pic}^0(C)$ is a module over $\mathbb{Z}_\ell[\zeta_d] = \mathbb{Z}_\ell[X]/(X^{d-1} + \cdots + 1)$.
- Consider surjections $T_\ell \operatorname{Pic}^0(C) \to A$ that are $\mathbb{Z}_\ell[\zeta_d]$-equivariant.
- The Weil pairing $\omega : T_\ell \operatorname{Pic}^0(C) \times T_\ell \operatorname{Pic}^0(C) \to \mathbb{Z}_\ell(1)$ respects the ζ_d-action. Consequently, ω yields a Hermitian pairing over $\mathbb{Z}_\ell[\zeta_d]$.
- Big monodromy results: how big is the image of

Differences in $d = 2$ and $d > 2$ cases

- $T_\ell \operatorname{Pic}^0(C)$ is a module over $\mathbb{Z}_\ell[\zeta_d] = \mathbb{Z}_\ell[X]/(X^{d-1} + \cdots + 1)$.
- Consider surjections $T_\ell \operatorname{Pic}^0(C) \to A$ that are $\mathbb{Z}_\ell[\zeta_d]$-equivariant.
- The Weil pairing $\omega : T_\ell \operatorname{Pic}^0(C) \times T_\ell \operatorname{Pic}^0(C) \to \mathbb{Z}_\ell(1)$ respects the ζ_d-action. Consequently, ω yields a Hermitian pairing over $\mathbb{Z}_\ell[\zeta_d]$.
- Big monodromy results: how big is the image of

$$\pi_1(\mathcal{D}_g, \bar{s}) \to \operatorname{Aut}_{\mathbb{Z}_\ell[\zeta_d]}(T_\ell \operatorname{Pic}^0(C_{\bar{s}}))$$

Differences in $d = 2$ and $d > 2$ cases

- $T_\ell \operatorname{Pic}^0(C)$ is a module over $\mathbb{Z}_\ell[\zeta_d] = \mathbb{Z}_\ell[X]/(X^{d-1} + \cdots + 1)$.
- Consider surjections $T_\ell \operatorname{Pic}^0(C) \to A$ that are $\mathbb{Z}_\ell[\zeta_d]$-equivariant.
- The Weil pairing $\omega : T_\ell \operatorname{Pic}^0(C) \times T_\ell \operatorname{Pic}^0(C) \to \mathbb{Z}_\ell(1)$ respects the ζ_d-action. Consequently, ω yields a Hermitian pairing over $\mathbb{Z}_\ell[\zeta_d]$.
- Big monodromy results: how big is the image of

$$\pi_1(\mathcal{D}_g, \bar{s}) \to \operatorname{Aut}_{\mathbb{Z}_\ell[\zeta_d]}(T_\ell \operatorname{Pic}^0(C_{\bar{s}}))$$

  - $d = 2$ by Jiu-Kang Yu (1997)

Differences in $d = 2$ and $d > 2$ cases

- $T_\ell \operatorname{Pic}^0(C)$ is a module over $\mathbb{Z}_\ell[\zeta_d] = \mathbb{Z}_\ell[X]/(X^{d-1} + \cdots + 1)$.
- Consider surjections $T_\ell \operatorname{Pic}^0(C) \to A$ that are $\mathbb{Z}_\ell[\zeta_d]$-equivariant.
- The Weil pairing $\omega : T_\ell \operatorname{Pic}^0(C) \times T_\ell \operatorname{Pic}^0(C) \to \mathbb{Z}_\ell(1)$ respects the ζ_d-action. Consequently, ω yields a Hermitian pairing over $\mathbb{Z}_\ell[\zeta_d]$.
- Big monodromy results: how big is the image of

$$\pi_1(\mathcal{D}_g, \bar{s}) \to \operatorname{Aut}_{\mathbb{Z}_\ell[\zeta_d]}(T_\ell \operatorname{Pic}^0(C_{\bar{s}}))$$

  - $d = 2$ by Jiu-Kang Yu (1997)
  - $d = 3$ by Jeff Achter and Rachel Pries (2007)

Differences in $d = 2$ and $d > 2$ cases

- $T_\ell \operatorname{Pic}^0(C)$ is a module over $\mathbb{Z}_\ell[\zeta_d] = \mathbb{Z}_\ell[X]/(X^{d-1} + \cdots + 1)$.
- Consider surjections $T_\ell \operatorname{Pic}^0(C) \to A$ that are $\mathbb{Z}_\ell[\zeta_d]$-equivariant.
- The Weil pairing $\omega : T_\ell \operatorname{Pic}^0(C) \times T_\ell \operatorname{Pic}^0(C) \to \mathbb{Z}_\ell(1)$ respects the ζ_d-action. Consequently, ω yields a Hermitian pairing over $\mathbb{Z}_\ell[\zeta_d]$.
- Big monodromy results: how big is the image of

$$\pi_1(\mathcal{D}_g, \bar{s}) \to \operatorname{Aut}_{\mathbb{Z}_\ell[\zeta_d]}(T_\ell \operatorname{Pic}^0(C_{\bar{s}}))$$

  - $d = 2$ by Jiu-Kang Yu (1997)
  - $d = 3$ by Jeff Achter and Rachel Pries (2007)
  - $d > 3$?

On the congruence class bias of distribution of primes of cyclic reduction for elliptic curves

Sung Min Lee

University of Illinois at Chicago

LuCaNT: Lightning Talk

ICERM

July 11 2023

Say p is a prime of good reduction for $E/\mathbb{Q}$. Then,

$$\tilde{E}_p(\mathbb{F}_p) \cong \mathbb{Z}/d_p(E)\mathbb{Z} \times \mathbb{Z}/e_p(E)\mathbb{Z},$$

for some integers $d_p(E) \mid e_p(E)$. J-P. Serre studied the distribution of primes for which $d_p(E) = 1$, under GRH.

Say p is a prime of good reduction for $E/\mathbb{Q}$. Then,

$$\tilde{E}_p(\mathbb{F}_p) \cong \mathbb{Z}/d_p(E)\mathbb{Z} \times \mathbb{Z}/e_p(E)\mathbb{Z},$$

for some integers $d_p(E) \mid e_p(E)$. J-P. Serre studied the distribution of primes for which $d_p(E) = 1$, under GRH.

Let $E^{a,b} : Y^2 = X^3 + aX + b$.

Theorem (Banks-Shparlinski, 2009)

Let $x > 0$ and $\epsilon > 0$. Let $A := A(x)$ and $B := B(x)$ be integers satisfying

$$x^{\epsilon} \leq A, B \leq x^{1-\epsilon}, \quad AB \geq x^{1+\epsilon}.$$

There exists a positive constant $C > 0$ for which

$$\frac{1}{4AB} \sum_{|a| \leq A} \sum_{|b| \leq B} \#\{p \leq x : d_p(E^{a,b}) = 1\} \sim C \frac{x}{\log x}, \quad \text{as } x \to \infty.$$

Objective: to consider the case of primes lying in an arithmetic progression.

Theorem (L., 2023)

Under the same assumptions of Banks-Shparlinski, there exists $C_{n,k} > 0$ for which

$$\frac{1}{4AB} \sum_{|a| \leq A} \sum_{|b| \leq B} \#\{p \leq x : d_p(E^{a,b}) = 1, p \equiv k \pmod{n}\} \sim C_{n,k} \frac{x}{\log x}, \quad \text{as } x \to \infty.$$

Theorem (L., 2023)

Under the same assumptions of Banks-Shparlinski, there exists $C_{n,k} > 0$ for which

$$\frac{1}{4AB} \sum_{|a| \leq A} \sum_{|b| \leq B} \#\{p \leq x : d_p(E^{a,b}) = 1, p \equiv k \pmod{n}\} \sim C_{n,k} \frac{x}{\log x}, \quad \text{as } x \to \infty.$$

Given n and k coprime, define $n_k := \prod_{\substack{q|n \\ k \equiv 1 (q)}} q$, and

$$C_{n,k} := \frac{1}{\phi(n)} \prod_{\ell | n_k} \left(1 - \frac{1}{\ell(\ell^2 - 1)}\right) \prod_{\ell' \nmid n} \left(1 - \frac{1}{|\mathrm{GL}_2(\mathbb{Z}/\ell'\mathbb{Z})|}\right).$$

Note that $C_{n,k} > 0$ for any n and k coprime.

Theorem (L., 2023)

Under the same assumptions of Banks-Shparlinski, there exists $C_{n,k} > 0$ for which

$$\frac{1}{4AB} \sum_{|a| \leq A} \sum_{|b| \leq B} \#\{p \leq x : d_p(E^{a,b}) = 1, p \equiv k \pmod{n}\} \sim C_{n,k} \frac{x}{\log x}, \quad \text{as } x \to \infty.$$

Given n and k coprime, define $n_k := \prod_{\substack{q|n \\ k \equiv 1 (q)}} q$, and

$$C_{n,k} := \frac{1}{\phi(n)} \prod_{\ell | n_k} \left(1 - \frac{1}{\ell(\ell^2 - 1)}\right) \prod_{\ell' \nmid n} \left(1 - \frac{1}{|\mathrm{GL}_2(\mathbb{Z}/\ell'\mathbb{Z})|}\right).$$

Note that $C_{n,k} > 0$ for any n and k coprime.

Proposition (L., 2023)

Fix n. For any k coprime to n, we have $n_{-1} \mid n_k \mid n_1$. Thus, $C_{n,1} \leq C_{n,k} \leq C_{n,-1}$.

If n is a power of two, then $n_1 = n_{-1}$. In this case, $C_{n,1} = C_{n,k} = C_{n,-1}$ for any k.

Theorem (Akbal-Güloğlu, 2022)

Let $E/\mathbb{Q}$. Assume GRH. If E has a CM, assume that it has a CM by a full ring of integers of an imaginary quadratic field. Then, there exists $C_{E,n,k} \geq 0$

$$\pi_E(x; n, k) := \#\{p \leq x : d_p(E) = 1, p \equiv k \pmod{n}\} \sim C_{E,n,k} \frac{x}{\log x}, \quad \text{as } x \to \infty.$$

Theorem (Akbal-Güloğlu, 2022)

Let $E/\mathbb{Q}$. Assume GRH. If E has a CM, assume that it has a CM by a full ring of integers of an imaginary quadratic field. Then, there exists $C_{E,n,k} \geq 0$

$$\pi_E(x; n, k) := \#\{p \leq x : d_p(E) = 1, p \equiv k \pmod{n}\} \sim C_{E,n,k} \frac{x}{\log x}, \quad \text{as } x \to \infty.$$

They also made a following observation:

$$\begin{pmatrix} \exists \text{ a prime } \ell \text{ such that } \mathbb{Q}(E[\ell]) \subset \mathbb{Q}(\zeta_n) \\ \text{and } \sigma_k : \zeta_n \mapsto \zeta_n^k \text{ fixes } \mathbb{Q}(E[\ell]) \end{pmatrix} \implies \pi_E(x; n, k) < \infty,$$

and asked whether the converse is true.

Theorem (Akbal-Güloğlu, 2022)

Let $E/\mathbb{Q}$. Assume GRH. If E has a CM, assume that it has a CM by a full ring of integers of an imaginary quadratic field. Then, there exists $C_{E,n,k} \geq 0$

$$\pi_E(x;n,k) := \#\{p \leq x : d_p(E) = 1, p \equiv k \pmod{n}\} \sim C_{E,n,k}\frac{x}{\log x}, \quad \text{as } x \to \infty.$$

They also made a following observation:

$$\begin{pmatrix} \exists \text{ a prime } \ell \text{ such that } \mathbb{Q}(E[\ell]) \subset \mathbb{Q}(\zeta_n) \\ \text{and } \sigma_k : \zeta_n \mapsto \zeta_n^k \text{ fixes } \mathbb{Q}(E[\ell]) \end{pmatrix} \implies \pi_E(x;n,k) < \infty,$$

and asked whether the converse is true.

Example (Jones-L., 2022)

Consider an elliptic curve (LMFDB: 71610.s6)

$$E : Y^2 + XY + Y = X^3 + 32271697X - 1200056843302.$$

For any prime ℓ, $\mathbb{Q}(E[\ell]) \not\subset \mathbb{Q}(\zeta_8)$ while $\pi_E(x;8,3) = 0$ for any $x > 0$.

Model-free Coleman Integration on Modular Curves

Joint work with Kiran S. Kedlaya and Christopher Xu

Yongyuan (Steve) Huang[1]

[1]Department of Mathematics
University of California San Diego

LMFDB, Computation, and Number Theory (LuCaNT)
ICERM, Providence, RI
July 11, 2023

Background on Coleman Integrals

Motivating Question 1

Let X be a nice curve of genus $g \geq 2$. We know $X(\mathbb{Q})$ is finite [Fal83]. Given such X, how do we compute $X(\mathbb{Q})$?

Coleman's theory of p-adic line integration [Col82, Col85]

Let $X/\mathbb{Q}_p$ be a nice curve with good reduction at p. For each pair of points $P, Q \in X(\mathbb{Q}_p)$, and a regular differential $\omega \in H^0(X, \Omega^1)$, one can define a p-adic Coleman integral

$$\int_P^Q \omega \in \overline{\mathbb{Q}}_p$$

satisfying the usual properties of line integrals from calculus.

Notable property: If $P \equiv Q \mod p$, $\int_P^Q \omega$ can be computed by expanding ω into a power series in terms of a uniformizer t at P and integrating term-by-term.

Computation of Coleman Integrals

For X a hyperelliptic curve, the BBK (Balakrishnan-Bradshaw-Kedlaya) algorithm computes the Coleman integral $\int_P^Q \omega$ using Kedlaya's algorithm which gives the matrix representation of the action of Frobenius on the basis differentials for $H^1_{\mathrm{dR}}X$.
Balakrishnan-Tuitman extends BBK to work for all curves.

The BBK and BT algorithms relies on knowing the singular plane model for X. For modular curves, however, their plane models are not always known.

Motivating Question 2

Can we compute Coleman integrals on a modular curve X without knowing its plane model?

Computing Coleman Integrals on Modular Curves

Let X be a modular curve corresponding to a congruence subgroup Γ. Fix a prime p a prime of good reduction for X. Given $P, Q \in X(\mathbb{Q}_p)$, Chen, Kedlaya, and Lau give an algorithm computing the Coleman integral $\int_P^Q \omega$ for $\omega \in H^1(X, \Omega^1)$ *without* using a plane model for X.

Outline

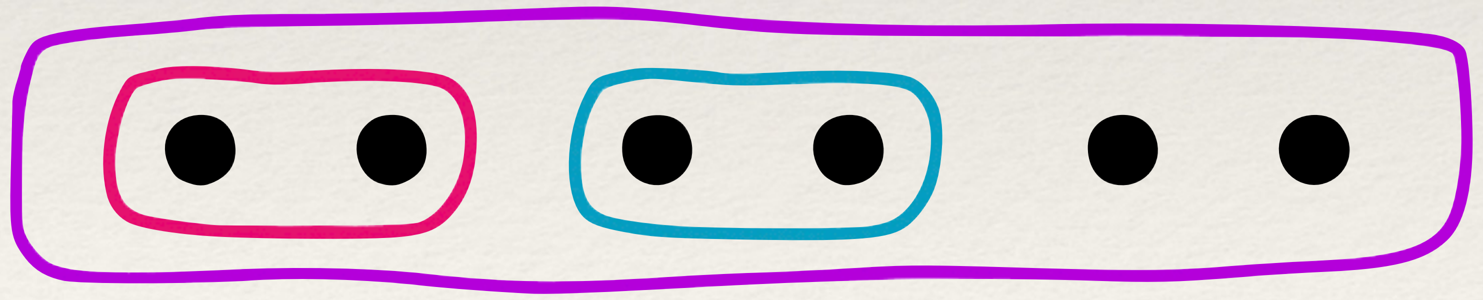
1. Using the q-expansion of the cusp form corresponding to ω, expand ω as a power series in terms of a choice of uniformizer at P.
2. The computation of $\int_P^Q \omega$ can be reduced to computing the matrix representation of the Hecke action T_p on an eigenbasis for $S_2(\Gamma)$ and $\int_P^{P_i} \omega$, where $T_p(P) = \sum_{i=0}^{p} P_i$, which are tiny integrals by the Eichler-Shimura congruence relation.

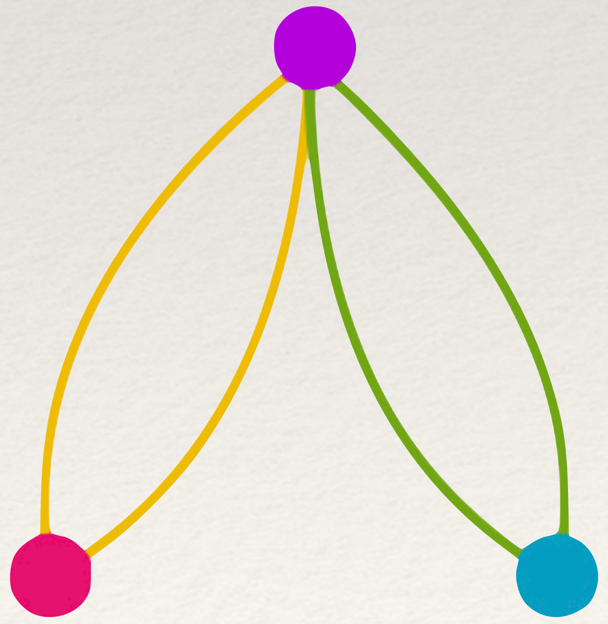
Chen, Kedlaya, and Lau employ the method of complex approximations to compute specific examples. In recent joint work with Kedlaya and Xu, we give an p-adic alternative in order to avoid having to approximate complex numbers.

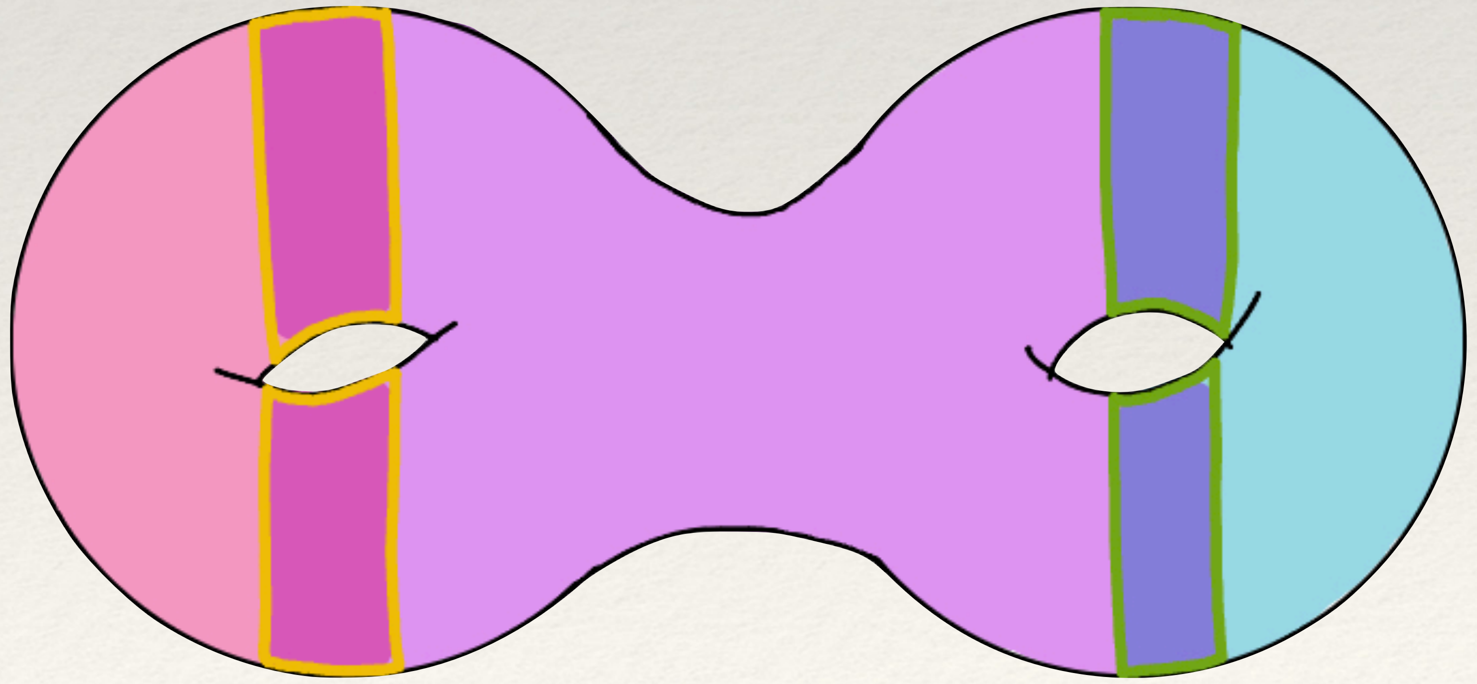
Local heights computations for quadratic Chabauty

Juanita Duque-Rosero
Boston University

Joint work with Alexander Betts, Sachi Hashimoto, and Pim Spelier.







Local heights computations: why?

- Set-up: Let C be a nice curve of genus $g \geq 2$. Then $\#C(\mathbb{Q}) < \infty$.
- **Goal:** To describe explicitly $C(\mathbb{Q})$.
- Method: **quadratic Chabauty** (explicitly presented by Balakrishnan & Dogra, '18 '21). This is a p-adic method that has been successfully used to compute $C(\mathbb{Q})$ in many new cases.
- Key input: Let p be a prime and $Z \subset C \times C$ be a trace 0 correspondence. There is an associated **p-adic** (Coleman Gross) **height function** $h_Z : C(\mathbb{Q}) \to \mathbb{Q}_p$ which can be decomposed as

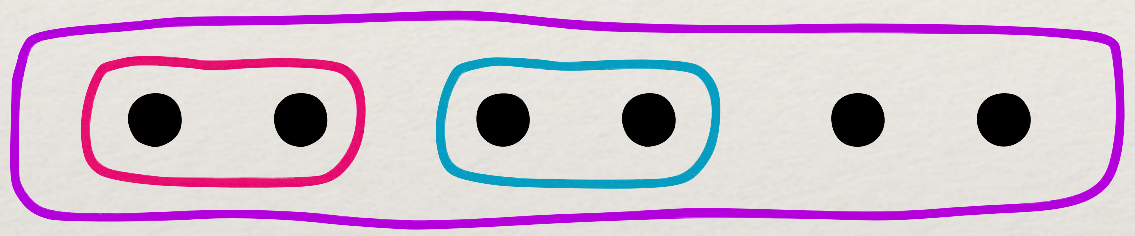
$$h_Z(Q) = \sum_{\ell} h_{Z,\ell}(Q),$$

  where $h_{Z,\ell} : C(\mathbb{Q}_\ell) \to \mathbb{Q}_p$.
- **One challenge:** Computing local heights.

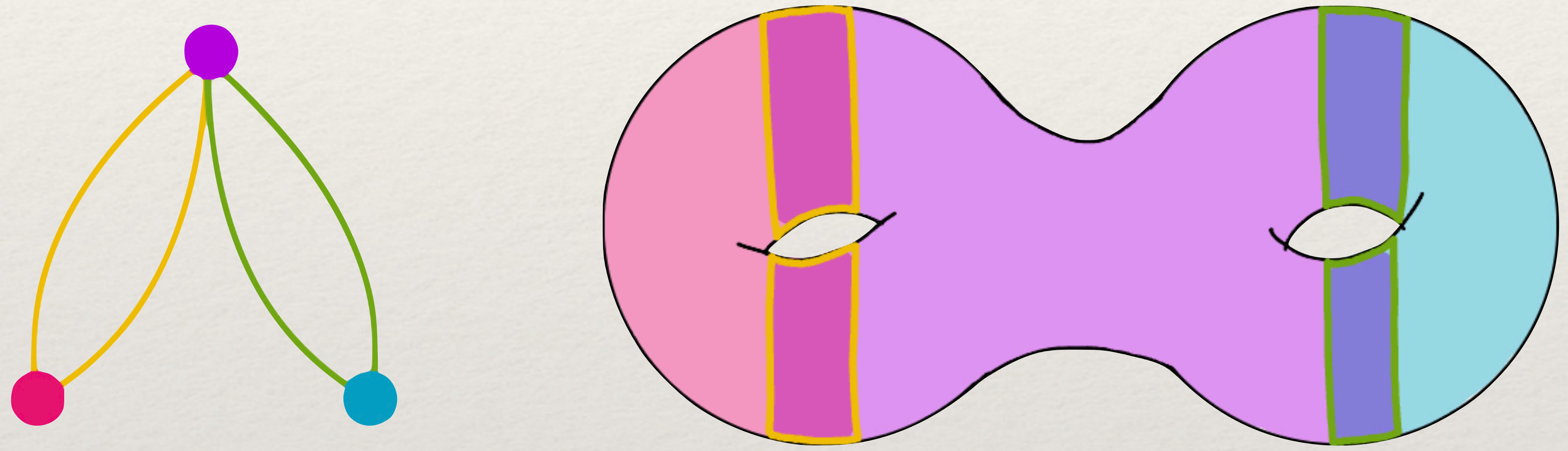
Local heights computations on hyperelliptic curves: how?

$$y^2 = x^6 + 2x^4 + 6x^3 + 5x^2 - 6x + 1$$

We pick a correspondence $Z \subset C \times C$ with action on $H^0(X, \Omega^1_X)$ given by $\begin{pmatrix} -1 & 2 \\ 2 & 1 \end{pmatrix}$.



Cluster picture

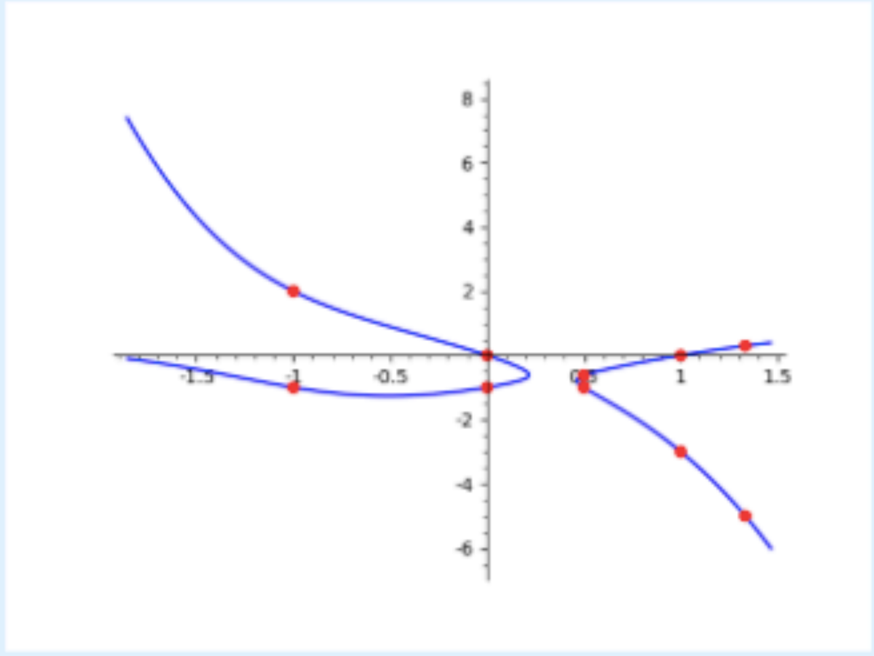


Berkovich space decomposition

$$h_{Z,3}(x,y) = \begin{cases} -\frac{1}{4}\log^p(3) & \text{if } x \equiv -1 \bmod 3, \\ +\frac{1}{4}\log^p(3) & \text{if } x \equiv +1 \bmod 3, \\ 0 & \text{otherwise.} \end{cases}$$

Properties

Label	8649.a.77841.1



Conductor	8649
Discriminant	77841
Mordell-Weil group	$\mathbb{Z} \oplus \mathbb{Z}$
Sato-Tate group	$\mathrm{SU}(2) \times \mathrm{SU}(2)$
$\mathrm{End}(J_{\overline{\mathbb{Q}}}) \otimes \mathbb{R}$	$\mathbb{R} \times \mathbb{R}$
$\mathrm{End}(J_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$	RM
$\mathrm{End}(J) \otimes \mathbb{Q}$	RM

Prime	**Cluster picture**
3	

2-adic Galois Images of Isogeny-Torsion Graphs

Garen Chiloyan

July 11, 2023

Isogeny graphs and isogeny-torsion graphs

Let $\mathcal{E}$ be an isogeny class of elliptic curves defined over the rationals. Then $\mathcal{E}$ has a corresponding isogeny graph and a corresponding isogeny-torsion graph

- Theorem

  There are 26 isomorphism types of isogeny graphs that are associated to elliptic curves defined over $\mathbb{Q}$, 16 types of (linear) L_k graphs of $k = 1$-4 vertices, 3 types of (nonlinear two-primary torsion) T_k graphs of $k = 4$, 6, or 8 vertices, 6 types of (rectangular) R_k graphs of $k = 4$ or 6 vertices, and 1 (special) S graph.

- Theorem (C., Lozano-Robledo).

  There are 52 isomorphism types of isogeny-torsion graphs that are associated to elliptic curves defined over $\mathbb{Q}$. In particular, there are 23 types of L_k graphs, 13 types of T_k graphs, 12 types of R_k graphs, and 4 types of S graphs.

  See Tables 1 – 4 in https://arxiv.org/abs/2001.05616

2-adic Galois images (1/2)

Recently, the image of the 2-adic Galois representation at all vertices of all isogeny-torsion graphs has been classified.

Isogeny Graph	p	Torsion	$\rho_{E_1,2^\infty}(G_\mathbb{Q})$	$\rho_{E_2,2^\infty}(G_\mathbb{Q})$	Example
$E_1 \overset{p}{\text{———}} E_2$	2	$([2],[2])$	$\left\langle 3\cdot\mathrm{Id}, \begin{bmatrix}1&0\\0&-1\end{bmatrix}, \begin{bmatrix}1&1\\-2&1\end{bmatrix}\right\rangle$	$\left\langle 3\cdot\mathrm{Id}, \begin{bmatrix}-1&0\\0&1\end{bmatrix}, \begin{bmatrix}1&1\\-2&1\end{bmatrix}\right\rangle$	`256.a`
			$\mathcal{N}_{-2,0}(2^\infty)$	$\mathcal{N}_{-2,0}(2^\infty)$	`2304.h`
			$\left\langle -\mathrm{Id}, 3\cdot\mathrm{Id}, \begin{bmatrix}2&1\\-1&2\end{bmatrix}, \begin{bmatrix}1&0\\0&-1\end{bmatrix}\right\rangle$	$\left\langle -\mathrm{Id}, 3\cdot\mathrm{Id}, \begin{bmatrix}2&1\\-1&2\end{bmatrix}, \begin{bmatrix}0&1\\1&0\end{bmatrix}\right\rangle$	`2304.a`
			$\left\langle 3\cdot\mathrm{Id}, \begin{bmatrix}2&-1\\1&2\end{bmatrix}, \begin{bmatrix}1&0\\0&-1\end{bmatrix}\right\rangle$	$\left\langle 3\cdot\mathrm{Id}, \begin{bmatrix}2&-1\\1&2\end{bmatrix}, \begin{bmatrix}0&1\\1&0\end{bmatrix}\right\rangle$	`256.c`
			$\left\langle 3\cdot\mathrm{Id}, \begin{bmatrix}-2&1\\-1&-2\end{bmatrix}, \begin{bmatrix}1&0\\0&-1\end{bmatrix}\right\rangle$	$\left\langle 3\cdot\mathrm{Id}, \begin{bmatrix}-2&1\\-1&-2\end{bmatrix}, \begin{bmatrix}0&1\\1&0\end{bmatrix}\right\rangle$	`256.b`
			$\mathcal{N}_{-1,0}(2^\infty)$	$\mathcal{N}_{-1,0}(2^\infty)$	`288.a`
	3	$([3],[1])$	$\mathcal{N}_{-1,1}(2^\infty)$	$\mathcal{N}_{-1,1}(2^\infty)$	`108.a`
		$([1],[1])$			`225.c`
	11	$([1],[1])$	$\mathcal{N}_{-3,1}(2^\infty)$	$\mathcal{N}_{-3,1}(2^\infty)$	`121.b`
	19		$\mathcal{N}_{-5,1}(2^\infty)$	$\mathcal{N}_{-5,1}(2^\infty)$	`361.a`
	43		$\mathcal{N}_{-11,1}(2^\infty)$	$\mathcal{N}_{-11,1}(2^\infty)$	`1849.b`
	67		$\mathcal{N}_{-17,1}(2^\infty)$	$\mathcal{N}_{-17,1}(2^\infty)$	`4489.b`
	163		$\mathcal{N}_{-41,1}(2^\infty)$	$\mathcal{N}_{-41,1}(2^\infty)$	`26569.a`

TABLE 2. Classification of $\rho_{\mathcal{G},2^\infty}(G_\mathbb{Q})$ for $\mathcal{G}$ CM of type $L_2(p)$

2-adic Galois images (2/2)

Isogeny Graph	Torsion	$\rho_{E_1,2^\infty}(G_\mathbb{Q})$	$\rho_{E_2,2^\infty}(G_\mathbb{Q})$	$\rho_{E_3,2^\infty}(G_\mathbb{Q})$	$\rho_{E_4,2^\infty}(G_\mathbb{Q})$	Example
$E_1 \overset{3}{\text{---}} E_2 \overset{3}{\text{---}} E_3 \overset{3}{\text{---}} E_4$	$([3],[3],[3],[1])$	$\mathcal{N}_{-1,1}(2^\infty)$	$\mathcal{N}_{-1,1}(2^\infty)$	$\mathcal{N}_{-1,1}(2^\infty)$	$\mathcal{N}_{-1,1}(2^\infty)$	27.a
	$([1],[1],[1],[1])$					432.e
$\begin{array}{ccc} E_1 & \overset{2}{\text{---}} & E_2 \\ 3 \vert & & \vert 3 \\ E_3 & \underset{2}{\text{---}} & E_4 \end{array}$	$([6],[6],[2],[2])$	$\left\langle \text{-Id}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 7 & 4 \\ -4 & 3 \end{bmatrix}, \begin{bmatrix} 3 & 6 \\ -6 & -3 \end{bmatrix} \right\rangle$	$\mathcal{N}_{-3,0}(2^\infty)$	$\left\langle \text{-Id}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 7 & 4 \\ -4 & 3 \end{bmatrix}, \begin{bmatrix} 3 & 6 \\ -6 & -3 \end{bmatrix} \right\rangle$	$\mathcal{N}_{-3,0}(2^\infty)$	36.a
	$([2],[2],[2],[2])$					144.a
$\begin{array}{ccc} E_1 & \overset{2}{\text{---}} & E_2 \\ 7 \vert & & \vert 7 \\ E_3 & \underset{2}{\text{---}} & E_4 \end{array}$	$([2],[2],[2],[2])$	$\mathcal{N}_{-7,0}(2^\infty)$	$\mathcal{N}_{-2,1}(2^\infty)$	$\mathcal{N}_{-7,0}(2^\infty)$	$\mathcal{N}_{-2,1}(2^\infty)$	49.a
$\begin{array}{ccc} & E_2 & \\ & 2 \vert & \\ & E_1 & \\ {}^2\swarrow & & \searrow^2 \\ E_3 & & E_4 \end{array}$	$([2,2],[4],[4],[2])$	$\left\langle 5\cdot\text{Id} \begin{bmatrix} -1 & -2 \\ 2 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right\rangle$	$\left\langle 5\cdot\text{Id} \begin{bmatrix} -1 & -2 \\ 2 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle$	$\left\langle 5\cdot\text{Id}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ 4 & -1 \end{bmatrix} \right\rangle$	$\left\langle 5\cdot\text{Id}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ 4 & -1 \end{bmatrix} \right\rangle$	32.a
	$([2,2],[2],[4],[2])$	$\left\langle 5\cdot\text{Id} \begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right\rangle$	$\left\langle 5\cdot\text{Id} \begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle$	$\left\langle 5\cdot\text{Id}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ -4 & 1 \end{bmatrix} \right\rangle$	$\left\langle 5\cdot\text{Id}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ -4 & 1 \end{bmatrix} \right\rangle$	64.a
	$([2,2],[2],[2],[2])$	$\left\langle \text{-Id}, 3\cdot\text{Id}, \begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right\rangle$	$\left\langle \text{-Id}, 3\cdot\text{Id}, \begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle$	$\mathcal{N}_{-4,0}(2^\infty)$	$\mathcal{N}_{-4,0}(2^\infty)$	288.d

TABLE 1. Classification of $\rho_{\mathcal{G},2^\infty}(G_\mathbb{Q})$ for $\mathcal{G}$ CM of type L_4, R_4, or T_4

Theorem (C.).
Let $\mathcal{G}$ be an isogeny-torsion graph associated to a $\mathbb{Q}$-isogeny class of non-CM elliptic curves defined over $\mathbb{Q}$. Then the image of the 2-adic Galois representation attached to $\mathcal{G}$ is one of 385 arrangements

See Tables 10 – 19 in https://arxiv.org/abs/2302.06094

Elliptic curves with CM and abelian division fields

Asimina Hamakiotes
joint with Álvaro Lozano-Robledo

University of Connecticut

LuCaNT, July 10-14, 2023

Background and Motivation

Let E be an elliptic curve defined over a number field F.

- Let $N \geq 2$ and $E[N] = E(\overline{F})[N]$ be the N-torsion subgroup of $E(\overline{F})$.
- $F(E[N])$ is the field of definition of the coordinates of points in $E[N]$.
- $F(E[N])/F$ is a Galois extension.

When is $F(E[N])/F$ an abelian extension?

- Halberstadt, Merel, Merel and Stein, and Rebolledo, show that if p is prime, and $F(E[p]) = \mathbb{Q}(\zeta_p)$, then $p = 2, 3, 5$ or $p > 1000$.
- When $F = \mathbb{Q}$, González-Jiménez and Lozano-Robledo prove that
    - $\mathbb{Q}(E[N]) = \mathbb{Q}(\zeta_N)$ only for $N = 2, 3, 4$, or 5;
    - if $\mathbb{Q}(E[N])/\mathbb{Q}$ is abelian, then $N = 2, 3, 4, 5, 6$, or 8;
    - for $E/\mathbb{Q}$ with CM, if $\mathbb{Q}(E[n])/\mathbb{Q}$ is abelian, then $n = 2, 3$, or 4.

Theorem (H. and Lozano-Robledo)

Let E/F have CM and $F = \mathbb{Q}(j(E))$, then $F(E[N])/F$ is only abelian for $N = 2$, 3, or 4.

Main theorem

Let K be an imaginary quadratic field, and let $\mathcal{O}_{K,f}$ be an order in K of conductor $f \geq 1$. Let Δ_K denote the discriminant of K.

Theorem (H. and Lozano-Robledo). *Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$, $f \geq 1$. Let $N \geq 2$ and let $G_{E,N} = \mathrm{Gal}(\mathbb{Q}(j_{K,f}, E[N])/\mathbb{Q}(j_{K,f}))$ be the Galois group of the Nth division field of E. Then $G_{E,N}$ is only abelian for $N = 2, 3$, and 4. Moreover:*

(a) If $N = 2$, then $G_{E,2}$ is abelian if and only if $G_{E,2} \subsetneq \mathcal{N}_{\delta,\phi}(2)$, or $G_{E,2} \cong \mathcal{N}_{\delta,\phi}(2)$, with $G_{E,2} \cong \mathbb{Z}/2\mathbb{Z}$ and either
- *$\Delta_K f^2 \equiv 0 \bmod 4$, or*
- *$\Delta_K \equiv 1 \bmod 8$ and $f \equiv 1 \bmod 2$.*

(b) If $N = 3$, then $G_{E,3}$ is abelian if and only if $G_{E,3} \subsetneq \mathcal{N}_{\delta,\phi}(3)$, and $\Delta_K = -3$, $f = 1$ (so $j_{K,f} = 0$), and $G_{E,3}$ has index 3 or 6 in $\mathcal{N}_{\delta,\phi}(3)$.

(c) If $N = 4$, then $G_{E,4}$ is abelian if and only if $G_{E,4} \subsetneq \mathcal{N}_{\delta,\phi}(4)$, and $\Delta_K = -4$, $f = 1$ (so $j_{K,f} = 1728$), and $G_{E,4}$ has index 2 or 4 in $\mathcal{N}_{\delta,\phi}(4)$.

<table>
<tr><td>N</td><td colspan="4">2</td><td colspan="2">3</td><td colspan="2">4</td></tr>
<tr><td>Δ_K</td><td>-3</td><td colspan="2">-4</td><td>$-7, -8$</td><td colspan="2">-3</td><td colspan="2">-4</td></tr>
<tr><td>f</td><td>$0 \bmod 2$</td><td colspan="2">≥ 1</td><td>$0 \bmod 2, \geq 1$</td><td colspan="2">1</td><td colspan="2">1</td></tr>
<tr><td>$[\mathcal{N}_{\delta,\phi}(N) : G_{E,N}]$</td><td>3</td><td>1</td><td>2, 4</td><td>2</td><td>3</td><td>6</td><td>2</td><td>4</td></tr>
<tr><td>$G_{E,N}$</td><td>$\mathbb{Z}/2\mathbb{Z}$</td><td>$\mathbb{Z}/2\mathbb{Z}$</td><td>$\{0\}$
$\mathbb{Z}/2\mathbb{Z}$</td><td>$\mathbb{Z}/2\mathbb{Z}$</td><td>$(\mathbb{Z}/2\mathbb{Z})^2$</td><td>$\mathbb{Z}/2\mathbb{Z}$</td><td>$(\mathbb{Z}/2\mathbb{Z})^3$</td><td>$(\mathbb{Z}/2\mathbb{Z})^2$</td></tr>
</table>

Sketch of proof

Theorem (H. and Lozano-Robledo)

Let E/F have CM and $F = \mathbb{Q}(j(E))$, then $F(E[N])/F$ is only abelian for $N = 2$, 3, or 4.

Sketch of proof:

(1) For an elliptic curve $E/\mathbb{Q}(j_{K,f})$ with CM by an arbitrary order $\mathcal{O}_{K,f}$, Lozano-Robledo explicitly describes the groups of $\mathrm{GL}(2, \mathbb{Z}_p)$ that can occur as images of ρ_{E,p^∞}, up to conjugation.

(2) We understand what subgroups of $\mathcal{N}_{\delta,\phi}(N)$ are images of $\rho_{E,N}$ and we give conditions that will help characterize when a subgroup of $\mathcal{N}_{\delta,\phi}(N)$ is abelian (e.g. the Cartan subgroup is abelian).

(3) We apply the results from above to all possible images $G_{E,N} = \mathrm{im}\,\rho_{E,N}$ from (1) and analyze under what circumstances we have that $G_{E,N}$ is abelian.

Automorphism group of Cartan modular curves

Pietro Mercuri
a joint work with V. Dose and G. Lido

Sapienza Università di Roma

LuCaNT
July 11, 2023

Notation

Let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ containing $-I$ and let X_H be the corresponding modular curve. If $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$, then X_H is a geometrically connected algebraic curve defined over $\mathbb{Q}$ and there is an isomorphism of Riemann surfaces $X_H(\mathbb{C}) \cong \Gamma_H \backslash \mathcal{H}^*$, where $\mathcal{H}^* := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\} \cup \mathbb{Q} \cup \{\infty\}$ is the extended complex upper half-plane, $\Gamma_H := \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \pmod{n} \in H\}$, is a congruence subgroup and $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathcal{H}^*$ by linear fractional transformations.

Let p be an odd prime and let $\xi \in (\mathbb{Z}/p^r\mathbb{Z})^\times$ be a nonsquare element:

$$C_{\mathrm{s}}(p^r) := \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}, a, d \in (\mathbb{Z}/p^r\mathbb{Z})^\times \right\};$$

$$C_{\mathrm{s}}^+(p^r) := C_{\mathrm{s}}(p^r) \cup \left\{ \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}, b, c \in (\mathbb{Z}/p^r\mathbb{Z})^\times \right\};$$

$$C_{\mathrm{ns}}(p^r) := \left\{ \begin{pmatrix} a & b\xi \\ b & a \end{pmatrix}, a, b \in \mathbb{Z}/p^r\mathbb{Z}, (a, b) \not\equiv (0, 0) \bmod p \right\};$$

$$C_{\mathrm{ns}}^+(p^r) := C_{\mathrm{ns}}(p^r) \cup \left\{ \begin{pmatrix} a & b\xi \\ -b & -a \end{pmatrix}, a, b \in \mathbb{Z}/p^r\mathbb{Z}, (a, b) \not\equiv (0, 0) \bmod p \right\}.$$

Modular automorphisms

Let $\mathrm{GL}_2^+(\mathbb{Q}) := \{g \in \mathrm{GL}_2(\mathbb{Q}) : \det g > 0\}$ and let

$$\pi \colon \mathrm{GL}_2^+(\mathbb{Q}) \to \mathrm{PGL}_2^+(\mathbb{Q}) := \mathrm{GL}_2^+(\mathbb{Q})/\{\text{scalar matrices}\}$$

be the natural quotient map.

Definition (Modular automorphisms)

If $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$, we call an automorphism defined over $\mathbb{C}$ of X_H *modular* if its action on $X_H(\mathbb{C}) = \Gamma_H \backslash \mathcal{H}^*$ is described by a fractional linear transformation of $\mathcal{H}^*$ associated to an element $m \in \mathrm{PGL}_2^+(\mathbb{Q})$ that normalizes $\pi(\Gamma_H)$ in $\mathrm{PGL}_2^+(\mathbb{Q})$.

Is every automorphism of X_H modular?

The answer is no when the genus is 0 or 1. It is not hard to see that in these cases there are non-modular automorphisms.

It is true, for example, for $X_0(n)$ when the genus is at least 2 and $n \neq 37, 63, 108$.

Results

Theorem (Dose, Lido, M., 2022)

1. *If $p > 3$ is a prime, then every automorphism of the modular curves $X_{C_s(p^r)}$, $X_{C_s^+(p^r)}$, $X_{C_{ns}(p^r)}$, $X_{C_{ns}^+(p^r)}$ with genus at least 2 and $p^r \neq 11$ is modular and*

$$\mathrm{Aut}(X_{C_s(p^r)}) \cong \mathrm{Aut}(X_{C_{ns}(p^r)}) \cong \mathbb{Z}/2\mathbb{Z},$$
$$\mathrm{Aut}(X_{C_s^+(p^r)}) \cong \mathrm{Aut}(X_{C_{ns}^+(p^r)}) \cong \{1\}.$$

2. *If $n \geq 10^{400}$ is odd with prime factorization $n = \prod_{i=1}^{\omega(n)} p_i^{e_i}$ and $H \cong \prod_{i=1}^{\omega(n)} H_{p_i}$ is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ such that, for each $i = 1, \ldots, \omega(n)$, either $H_{p_i} \in \{C_s(p_i^{e_i}), C_{ns}(p_i^{e_i})\}$ or $H_{p_i} \in \{C_s^+(p_i^{e_i}), C_{ns}^+(p_i^{e_i})\}$, then every automorphism of X_H is modular and we have*

$$\mathrm{Aut}(X_H) \cong N'/H',$$

where $N' < \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ is the normalizer of $H' := H \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.

THANK YOU!

Abelian surfaces with quaternionic multiplication and their rational torsion subgroups

Ciaran Schembri, Dartmouth College

July 2023, LuCaNT

Joint work with Jef Laga, Ari Shnidman and John Voight

Introduction

If A is an abelian variety over a number field F then

$$A(F) \simeq \mathbb{Z}^r \oplus A(F)_{\mathrm{tors}}$$

Question

What can $A(F)_{\mathrm{tors}}$ be?

Introduction

If A is an abelian variety over a number field F then

$$A(F) \simeq \mathbb{Z}^r \oplus A(F)_{\text{tors}}$$

Question

What can $A(F)_{\text{tors}}$ be?

Let $A/\mathbb{Q}$ be an abelian surface and suppose that for a maximal order O in a division quaternion algebra:

$$O \xhookrightarrow{\simeq} \mathrm{End}(A_{\overline{\mathbb{Q}}}).$$

Such a surface is called an *O-PQM surface* (PQM = potential quaternionic multiplication).

The associated moduli space is 1-dimensional, called a *Shimura curve*.

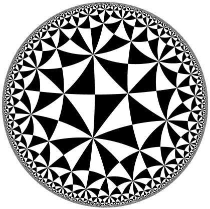


Figure: Shimura curve $X^*(6, 1)$

O-PQM surfaces

$$A[N](\overline{\mathbb{Q}}) = \{\ P \in A(\overline{\mathbb{Q}}) \mid N \cdot P = 0\ \}$$

- $A[N](\overline{\mathbb{Q}})$ is a left O-module and a right $\mathrm{Gal}_{\mathbb{Q}}$-module.
- O is a right $\mathrm{Gal}_{\mathbb{Q}}$-module via the action on the equations defining elements of $O = \mathrm{End}(A_{\overline{\mathbb{Q}}})$.
- $(a \cdot P)^{\sigma} = a^{\sigma} \cdot P^{\sigma}$.

The existence of rational torsion places restrictions on where the endomorphisms are defined.

O-PQM surfaces

$$A[N](\overline{\mathbb{Q}}) = \{ \ P \in A(\overline{\mathbb{Q}}) \mid N \cdot P = 0 \ \}$$

- $A[N](\overline{\mathbb{Q}})$ is a left O-module and a right $\mathrm{Gal}_{\mathbb{Q}}$-module.
- O is a right $\mathrm{Gal}_{\mathbb{Q}}$-module via the action on the equations defining elements of $O = \mathrm{End}(A_{\overline{\mathbb{Q}}})$.
- $(a \cdot P)^{\sigma} = a^{\sigma} \cdot P^{\sigma}$.

The existence of rational torsion places restrictions on where the endomorphisms are defined.

- A has potentially good reduction at all primes p.

A rational torsion point also places restrictions on the reduction properties of A mod p.

For example, if $A/\mathbb{Q}$ has a rational torsion point of prime order $\ell \geqslant 5$ then $\mathrm{End}(A_{\mathbb{Q}})$ is a real quadratic field, which forces A to have purely additive reduction at ℓ and good reduction everywhere else.

Main result

Theorem (Laga, S., Shnidman, Voight)

Let $A/\mathbb{Q}$ be a $\mathcal{O}$-PQM surface. Then

- *if $A[\ell](\mathbb{Q}) \neq 0$ for a prime ℓ, $\ell \in \{2, 3\}$;*
- *each of the six groups*

$$\{1\}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}, (\mathbb{Z}/2\mathbb{Z})^2, (\mathbb{Z}/3\mathbb{Z})^2$$

  occurs as $A(\mathbb{Q})_{\mathrm{tors}}$ for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of $\mathcal{O}$-PQM surfaces $A/\mathbb{Q}$;
- *all of the remaining possible groups have been ruled out except*

$$\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, (\mathbb{Z}/2\mathbb{Z})^3, (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/3,$$

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, (\mathbb{Z}/4\mathbb{Z})^2, (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^2.$$

Main result

Theorem (Laga, S., Shnidman, Voight)

Let $A/\mathbb{Q}$ be a $\mathcal{O}$-PQM surface. Then

- *if $A[\ell](\mathbb{Q}) \neq 0$ for a prime ℓ, $\ell \in \{2,3\}$;*
- *each of the six groups*

$$\{1\}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}, (\mathbb{Z}/2\mathbb{Z})^2, (\mathbb{Z}/3\mathbb{Z})^2$$

  occurs as $A(\mathbb{Q})_{\mathrm{tors}}$ for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of $\mathcal{O}$-PQM surfaces $A/\mathbb{Q}$;
- *all of the remaining possible groups have been ruled out except*

$$\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, (\mathbb{Z}/2\mathbb{Z})^3, (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/3,$$
$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, (\mathbb{Z}/4\mathbb{Z})^2, (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^2.$$

Thank you for listening!

Abelian surfaces with good reduction away from 2

LMFDB, Computation, and Number Theory (LuCaNT) workshop

Robin Visser
Mathematics Institute
University of Warwick

11 July 2023

Problem

Problem

Classify all abelian surfaces $A/\mathbb{Q}$ with good reduction away from 2.

Problem

Problem

Classify all abelian surfaces $A/\mathbb{Q}$ with good reduction away from 2.

- This seems quite hard (at least for me)!

Problem

Problem

Classify all abelian surfaces $A/\mathbb{Q}$ with good reduction away from 2.

- This seems quite hard (at least for me)!

(Hopefully easier) subproblem

Classify all isogeny classes of abelian surfaces $A/\mathbb{Q}$ with good reduction away from 2 and with full rational 2-torsion (i.e. $\mathbb{Q}(A[2]) = \mathbb{Q}$).

Faltings–Serre–Livné method

Let A/K be an abelian variety. Its L-function factors as an Euler product,

$$L(A/K, s) = \prod_{p \text{ prime}} L_p(A/K, s).$$

Faltings–Serre–Livné method

Let A/K be an abelian variety. Its L-function factors as an Euler product,

$$L(A/K,s) = \prod_{p \text{ prime}} L_p(A/K,s).$$

Theorem (Faltings–Serre–Livné)

Let A/K and B/K be two abelian varieties. If $L_p(A/K,s) = L_p(B/K,s)$ for some effectively computable finite set of primes p, then $L(A/K,s) = L(B/K,s)$.

Faltings–Serre–Livné method

Let A/K be an abelian variety. Its L-function factors as an Euler product,

$$L(A/K,s) = \prod_{p \text{ prime}} L_p(A/K,s).$$

Theorem (Faltings–Serre–Livné)

Let A/K and B/K be two abelian varieties. If $L_p(A/K,s) = L_p(B/K,s)$ for some effectively computable finite set of primes p, then $L(A/K,s) = L(B/K,s)$.

Theorem (Faltings–Serre–Livné (effective))

Let $A/\mathbb{Q}$ and $B/\mathbb{Q}$ be two abelian varieties with good reduction away from 2 and with full rational 2-torsion. Then if $L_p(A/\mathbb{Q},s) = L_p(B/\mathbb{Q},s)$ for each $p \in \{3,5,7\}$, then A and B are isogenous over $\mathbb{Q}$.

Computations

We brute force the possible Euler factors $L_p(A/\mathbb{Q}, s)$ for $p = 3, 5, 7$!

Computations

We brute force the possible Euler factors $L_p(A/\mathbb{Q}, s)$ for $p = 3, 5, 7$!

- Use that $\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$ embeds in $\mathrm{GL}_4(\mathbb{Z}/2^n\mathbb{Z})$, for each $n \geq 1$.

Computations

We brute force the possible Euler factors $L_p(A/\mathbb{Q}, s)$ for $p = 3, 5, 7$!

- Use that $\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$ embeds in $\mathrm{GL}_4(\mathbb{Z}/2^n\mathbb{Z})$, for each $n \geq 1$.
- Compute the characteristic polynomials for each matrix in the image of each embedding. This gives a finite number of possibilities for $L_p(A/\mathbb{Q}, s)$ mod 2^n.

Computations

We brute force the possible Euler factors $L_p(A/\mathbb{Q}, s)$ for $p = 3, 5, 7$!

- Use that $\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$ embeds in $\mathrm{GL}_4(\mathbb{Z}/2^n\mathbb{Z})$, for each $n \geq 1$.
- Compute the characteristic polynomials for each matrix in the image of each embedding. This gives a finite number of possibilities for $L_p(A/\mathbb{Q}, s)$ mod 2^n.

n	$\mathbb{Q}(A[2^n])$	$\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$	$\#L_3(A/\mathbb{Q}, s)$	$\#L_5(A/\mathbb{Q}, s)$	$\#L_7(A/\mathbb{Q}, s)$
0	$\mathbb{Q}$	C_1	63	129	207

Computations

We brute force the possible Euler factors $L_p(A/\mathbb{Q}, s)$ for $p = 3, 5, 7$!

- Use that $\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$ embeds in $\mathrm{GL}_4(\mathbb{Z}/2^n\mathbb{Z})$, for each $n \geq 1$.
- Compute the characteristic polynomials for each matrix in the image of each embedding. This gives a finite number of possibilities for $L_p(A/\mathbb{Q}, s)$ mod 2^n.

n	$\mathbb{Q}(A[2^n])$	$\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$	$\#L_3(A/\mathbb{Q}, s)$	$\#L_5(A/\mathbb{Q}, s)$	$\#L_7(A/\mathbb{Q}, s)$
0	$\mathbb{Q}$	C_1	63	129	207
1	$\mathbb{Q}$	C_1	17	35	53

Computations

We brute force the possible Euler factors $L_p(A/\mathbb{Q}, s)$ for $p = 3, 5, 7$!

- Use that $\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$ embeds in $\mathrm{GL}_4(\mathbb{Z}/2^n\mathbb{Z})$, for each $n \geq 1$.
- Compute the characteristic polynomials for each matrix in the image of each embedding. This gives a finite number of possibilities for $L_p(A/\mathbb{Q}, s)$ mod 2^n.

n	$\mathbb{Q}(A[2^n])$	$\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$	$\#L_3(A/\mathbb{Q}, s)$	$\#L_5(A/\mathbb{Q}, s)$	$\#L_7(A/\mathbb{Q}, s)$
0	$\mathbb{Q}$	C_1	63	129	207
1	$\mathbb{Q}$	C_1	17	35	53
2	$\mathbb{Q}(\zeta_8)$	$C_2 \times C_2$	6	12	16

Computations

We brute force the possible Euler factors $L_p(A/\mathbb{Q}, s)$ for $p = 3, 5, 7$!

- Use that $\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$ embeds in $\mathrm{GL}_4(\mathbb{Z}/2^n\mathbb{Z})$, for each $n \geq 1$.
- Compute the characteristic polynomials for each matrix in the image of each embedding. This gives a finite number of possibilities for $L_p(A/\mathbb{Q}, s)$ mod 2^n.

n	$\mathbb{Q}(A[2^n])$	$\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$	$\#L_3(A/\mathbb{Q}, s)$	$\#L_5(A/\mathbb{Q}, s)$	$\#L_7(A/\mathbb{Q}, s)$
0	$\mathbb{Q}$	C_1	63	129	207
1	$\mathbb{Q}$	C_1	17	35	53
2	$\mathbb{Q}(\zeta_8)$	$C_2 \times C_2$	6	12	16
3	$\mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$	$C_2^2 \rtimes C_4$	2	5	6

Computations

We brute force the possible Euler factors $L_p(A/\mathbb{Q}, s)$ for $p = 3, 5, 7$!

- Use that $\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$ embeds in $\mathrm{GL}_4(\mathbb{Z}/2^n\mathbb{Z})$, for each $n \geq 1$.
- Compute the characteristic polynomials for each matrix in the image of each embedding. This gives a finite number of possibilities for $L_p(A/\mathbb{Q}, s)$ mod 2^n.

n	$\mathbb{Q}(A[2^n])$	$\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$	$\#L_3(A/\mathbb{Q}, s)$	$\#L_5(A/\mathbb{Q}, s)$	$\#L_7(A/\mathbb{Q}, s)$
0	$\mathbb{Q}$	C_1	63	129	207
1	$\mathbb{Q}$	C_1	17	35	53
2	$\mathbb{Q}(\zeta_8)$	$C_2 \times C_2$	6	12	16
3	$\mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$	$C_2^2 \rtimes C_4$	2	5	6
4	?	$C_2^2 \rtimes C_8$, $D_4 \rtimes C_8$, $C_2^2.C_4 \wr C_2$	1	4	2

Computations

We brute force the possible Euler factors $L_p(A/\mathbb{Q}, s)$ for $p = 3, 5, 7$!

- Use that $\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$ embeds in $\mathrm{GL}_4(\mathbb{Z}/2^n\mathbb{Z})$, for each $n \geq 1$.
- Compute the characteristic polynomials for each matrix in the image of each embedding. This gives a finite number of possibilities for $L_p(A/\mathbb{Q}, s)$ mod 2^n.

n	$\mathbb{Q}(A[2^n])$	$\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$	$\#L_3(A/\mathbb{Q}, s)$	$\#L_5(A/\mathbb{Q}, s)$	$\#L_7(A/\mathbb{Q}, s)$
0	$\mathbb{Q}$	C_1	63	129	207
1	$\mathbb{Q}$	C_1	17	35	53
2	$\mathbb{Q}(\zeta_8)$	$C_2 \times C_2$	6	12	16
3	$\mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$	$C_2^2 \rtimes C_4$	2	5	6
4	?	$C_2^2 \rtimes C_8$, $D_4 \rtimes C_8$, $C_2^2.C_4 \wr C_2$	1	4	2
5	?	(many)	1	3	1

Results

Theorem

There are exactly 3 isogeny classes of abelian surfaces $A/\mathbb{Q}$ with good reduction away from 2 which contain surfaces with full rational 2-torsion. These are given by $E_1 \times E_1$, $E_1 \times E_2$ and $E_2 \times E_2$, where E_1, E_2 are the elliptic curves $E_1 : y^2 = x^3 - x$ and $E_2 : y^2 = x^3 - 4x$.

Results

Theorem

There are exactly 3 isogeny classes of abelian surfaces $A/\mathbb{Q}$ with good reduction away from 2 which contain surfaces with full rational 2-torsion. These are given by $E_1 \times E_1$, $E_1 \times E_2$ and $E_2 \times E_2$, where E_1, E_2 are the elliptic curves $E_1 : y^2 = x^3 - x$ and $E_2 : y^2 = x^3 - 4x$.

Doing a similar (albeit longer) computation also gives the following result:

Theorem

There are exactly 19 isogeny classes of abelian surfaces $A/\mathbb{Q}$ with good reduction away from 2 which contain surfaces such that either $A[2](\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^4$ or $A[2](\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^3$.

Effective Open Image Theorem for elliptic curves

Jacob Mayle and Tian Wang

University of Illinois at Chicago

July 11, 2023

Serre's Open Image Theorem

Let $E/\mathbb{Q}$ be an elliptic curve. For a prime ℓ, we denote by

$E[\ell]$: the group of ℓ-torsion points of E, $T_\ell(E)$: the ℓ-adic Tate module of E,
$\overline{\rho}_{E,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[\ell]) \simeq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$: mod-ℓ Galois representation of E,
$\rho_{E,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_\ell(E)) \simeq \mathrm{GL}_2(\mathbb{Z}_\ell)$: ℓ-adic Galois representation of E.

Serre's Open Image Theorem (1972)

Let $E/\mathbb{Q}$ be a non-CM elliptic curve. Then, there is a constant $c(E)$ such that

$$\ell > c(E) \quad \Longrightarrow \quad \overline{\rho}_{E,\ell} \text{ is surjective}^{1}$$

Serre's Uniformity Question

$c(E) \leq 37$ holds for all non-CM elliptic curves $E/\mathbb{Q}$.

Goal: Give an explicit bound on $c(E)$.

[1] For $\ell \geq 5$, $\overline{\rho}_{E,\ell}$ is surjective if and only if $\rho_{E,\ell}$ is surjective.

Examples

LMFDB label	conductor	nonsurjective (ℓ-adic) primes	$c(E)$
11.a1	11	$\{5\}$	5
37.a1	37	$\emptyset$	1
1225.b1	$5^2 \cdot 7^2$	$\{37\}$	37
11094.g1	$2 \cdot 3 \cdot 43^2$	$\{2, 13\}$	13
462400.ir1	$2^6 \cdot 5^2 \cdot 17^2$	$\{17\}$	17
705600.bej1	$2^6 \cdot 3^2 \cdot 5^2 \cdot 7^2$	$\{37\}$	37
299996953.a1	299996953	$\emptyset$	1

Table 1: LMFDB data for nonsurjective primes

Past results

- **Uniform Result**

Theorem

Let $E/\mathbb{Q}$ be a non-CM elliptic curve. If $\ell > 37$, then either

1. $\bar{\rho}_{E,\ell}$ is surjective or
2. the image of $\bar{\rho}_{E,\ell}$ is the normalizer of a non-split Cartan $\mathcal{C}_{ns}^{+}(\ell)$.

- **Individual Results**

•**Unconditionally** (Kraus 1995, Cojocaru 2005)

$c(E) \leq \frac{4\sqrt{6}}{3} N_E \prod_{p \mid N_E} \left(1 + \frac{1}{p}\right)^{1/2}.$

- **Under GRH** (Serre 1981)

$c(E) \ll (\log \operatorname{rad} N_E)(\log \log \operatorname{rad} 2N_E)^3$, where the implicit constant is effective.

- **Under GRH** (Larson-Vaintrob 2004)

$c(E) \ll \log N_E$, where the implicit constant is absolute but not effective.

Main Theorem

Theorem (Mayle-Wang, 2023)

Assume GRH for Dedekind zeta functions. If $E/\mathbb{Q}$ is a non-CM elliptic curve, then

$$c(E) \leq 964 \log \operatorname{rad}(2N_E) + 5760,$$

where $\operatorname{rad} n := \prod_{p|n} p$ denotes the radical of an integer n.

- **Example**

LMFDB label	conductor	nonsurjective primes up to 10915
76204800.ut1	$2^8 \cdot 3^5 \cdot 5^2 \cdot 7^2$	$\emptyset$

Conclusion: $\overline{\rho}_{E,\ell}$ is surjective for each prime ℓ.

- **Proof Strategy**

ℓ: any nonsurjective prime. There exist p and $C'(E)$ such that

$$\ell \,|\, |a_p(E)| \leq 2\sqrt{p} \leq 2\sqrt{C'(E)}.$$

Thank you very much for your attention!