3-adic images of Galois for elliptic curves over $\mathbb{Q}$

Jeremy Rouse

WAKE FOREST UNIVERSITY

CTNT 2020 Conference
University of Connecticut
June 14, 2020

Acknowledgements

- The work I'm going to speak about is joint with Andrew Sutherland and David Zureick-Brown.

Definitions

- Let $E/\mathbb{Q}$ be an elliptic curve and $E[N] = \{P \in E(\mathbb{C}) : NP = 0\}$.

Definitions

- Let $E/\mathbb{Q}$ be an elliptic curve and $E[N] = \{P \in E(\mathbb{C}) : NP = 0\}$.
- Suppose now that $K/\mathbb{Q}$ is a Galois extension, and $E[N] \subseteq E(K)$.

Definitions

- Let $E/\mathbb{Q}$ be an elliptic curve and $E[N] = \{P \in E(\mathbb{C}) : NP = 0\}$.
- Suppose now that $K/\mathbb{Q}$ is a Galois extension, and $E[N] \subseteq E(K)$.
- For each $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, $\sigma|_{E[N]}$ is an automorphism of $E[N]$.

Definitions

- Let $E/\mathbb{Q}$ be an elliptic curve and $E[N] = \{P \in E(\mathbb{C}) : NP = 0\}$.
- Suppose now that $K/\mathbb{Q}$ is a Galois extension, and $E[N] \subseteq E(K)$.
- For each $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, $\sigma|_{E[N]}$ is an automorphism of $E[N]$.
- Since $\mathrm{Aut}(E[N]) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, this gives a map

$$\rho_{E,N} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

given by $\rho_{E,N}(\sigma) = \sigma|_{E[N]}$.

Galois representations

- The properties of these Galois representations play a key role in many problems:

Galois representations

• The properties of these Galois representations play a key role in many problems:

- Proving the modularity of elliptic curves.

Galois representations

• The properties of these Galois representations play a key role in many problems:

- Proving the modularity of elliptic curves.
- The “modular method” for solving Diophantine equations.

Galois representations

- The properties of these Galois representations play a key role in many problems:
    - Proving the modularity of elliptic curves.
    - The "modular method" for solving Diophantine equations.
    - The inverse Galois problem for $\mathrm{PSL}_2(\mathbb{F}_p)$.

Properties of Galois representations

- If $\rho_{E,N} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, then

Properties of Galois representations

- If $\rho_{E,N} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, then

(i) $\det \circ \rho_{E,N} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to (\mathbb{Z}/N\mathbb{Z})^\times$ is surjective, and

Properties of Galois representations

- If $\rho_{E,N} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, then

(i) $\det \circ \rho_{E,N} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to (\mathbb{Z}/N\mathbb{Z})^\times$ is surjective, and

(ii) there is a matrix M in the image of $\rho_{E,N}$ that is conjugate in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ to either $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ or $\begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}$.

Mazur's "Program B"

- Given a number field K and a subgroup $H \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, classify all elliptic curves E/K for which $\mathrm{im}\, \rho_{E,N} \subseteq H$.

Subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$

- If p is a prime number, and $\rho_{E,p}$ is not surjective, then $\mathrm{im}\ \rho_{E,p}$ is contained in a maximal subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. The options are:

Subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$

• If p is a prime number, and $\rho_{E,p}$ is not surjective, then $\mathrm{im}\ \rho_{E,p}$ is contained in a maximal subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. The options are:

(i) Borel subgroups, those of the shape $\left\{ \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \right\}$,

Subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$

• If p is a prime number, and $\rho_{E,p}$ is not surjective, then $\mathrm{im}\ \rho_{E,p}$ is contained in a maximal subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. The options are:

(i) Borel subgroups, those of the shape $\left\{ \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \right\}$,

(ii) Normalizers of Cartan subgroups. Cartan subgroups are subgroups isomorphic to $\mathbb{F}_p^\times \times \mathbb{F}_p^\times$ (split) or $\mathbb{F}_{p^2}^\times$ (non-split).

Subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$

• If p is a prime number, and $\rho_{E,p}$ is not surjective, then $\mathrm{im}\ \rho_{E,p}$ is contained in a maximal subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. The options are:

(i) Borel subgroups, those of the shape $\left\{ \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \right\}$,

(ii) Normalizers of Cartan subgroups. Cartan subgroups are subgroups isomorphic to $\mathbb{F}_p^\times \times \mathbb{F}_p^\times$ (split) or $\mathbb{F}_{p^2}^\times$ (non-split).

(iii) Exceptional subgroups (groups whose image in $\mathrm{GL}_2(\mathbb{F}_p)$ mod scalars is isomorphic to A_4, S_4 or A_5).

Results

Theorem (Serre, 1972)

If $p \geq 17$ is prime, the image of $\rho_{E,p}$ cannot be contained in an exceptional subgroup.

Results

Theorem (Serre, 1972)

If $p \geq 17$ is prime, the image of $\rho_{E,p}$ cannot be contained in an exceptional subgroup.

Theorem (Mazur, 1978)

If E is a non-CM elliptic curve over $\mathbb{Q}$, the largest prime p for which $\rho_{E,p}$ lands in a Borel subgroup is 37.

Results

Theorem (Serre, 1972)

If $p \geq 17$ is prime, the image of $\rho_{E,p}$ cannot be contained in an exceptional subgroup.

Theorem (Mazur, 1978)

If E is a non-CM elliptic curve over $\mathbb{Q}$, the largest prime p for which $\rho_{E,p}$ lands in a Borel subgroup is 37.

Theorem (Bilu-Parent-Rebolledo, 2011, 2013)

If $p \geq 17$ and E is non-CM, the image cannot be contained in the normalizer of a split Cartan subgroup.

Serre's uniformity conjecture

Conjecture

If $E/\mathbb{Q}$ is a non-CM elliptic curve and $p > 37$, then $\rho_{E,p}$ is surjective.

p-adic representations

- Fix a prime p and an elliptic curve E. For each $n \geq 1$, we have a representation $\rho_{E,p^n} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$.

p-adic representations

- Fix a prime p and an elliptic curve E. For each $n \geq 1$, we have a representation $\rho_{E,p^n} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$.

- These representations are compatible, and can be packaged as a single $\rho_{E,p^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_p)$.

p-adic representations

- Fix a prime p and an elliptic curve E. For each $n \geq 1$, we have a representation $\rho_{E,p^n} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$.

- These representations are compatible, and can be packaged as a single $\rho_{E,p^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_p)$.

- Here $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ is the ring of p-adic integers.

Goal

- Fix a (small) prime p, and determine all possibilities for $\mathrm{im}\ \rho_{E,p^\infty}$ for elliptic curves $E/\mathbb{Q}$.

Goal

- Fix a (small) prime p, and determine all possibilities for $\operatorname{im}\, \rho_{E,p^\infty}$ for elliptic curves $E/\mathbb{Q}$.

Theorem (R, Zureick-Brown, 2015)

If $E/\mathbb{Q}$ is a non-CM elliptic curve, there are 1208 possibilities for the image of $\rho_{E,2^\infty}$ in $\mathrm{GL}_2(\mathbb{Z}_2)$ (up to conjugacy). The index can be at most 96 and the image always contains all $M \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{32}$.

Goal

- Fix a (small) prime p, and determine all possibilities for $\mathrm{im}\ \rho_{E,p^\infty}$ for elliptic curves $E/\mathbb{Q}$.

Theorem (R, Zureick-Brown, 2015)

If $E/\mathbb{Q}$ is a non-CM elliptic curve, there are 1208 possibilities for the image of $\rho_{E,2^\infty}$ in $\mathrm{GL}_2(\mathbb{Z}_2)$ (up to conjugacy). The index can be at most 96 and the image always contains all $M \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{32}$.

- Álvaro Lozano-Robledo has handled the CM case (for all primes p and not just over $\mathbb{Q}$).

$p = 3$

Theorem (R, Sutherland, Zureick-Brown)

If $E/\mathbb{Q}$ is a non-CM elliptic curve, then

$p = 3$

Theorem (R, Sutherland, Zureick-Brown)

If $E/\mathbb{Q}$ is a non-CM elliptic curve, then

- $\mathrm{im}\ \rho_{E,3^\infty}$ *is one of* 47 *subgroups of* $\mathrm{GL}_2(\mathbb{Z}_3)$ *of level at most* 27 *and index at most* 72*, or*

$p = 3$

Theorem (R, Sutherland, Zureick-Brown)

If $E/\mathbb{Q}$ is a non-CM elliptic curve, then

- $\mathrm{im}\ \rho_{E,3^\infty}$ *is one of* 47 *subgroups of* $\mathrm{GL}_2(\mathbb{Z}_3)$ *of level at most* 27 *and index at most* 72*, or*
- *the image of* $\rho_{E,3^\infty}$ *is contained in the normalizer of the non-split Cartan modulo* 27*.*

$p = 3$

Theorem (R, Sutherland, Zureick-Brown)

If $E/\mathbb{Q}$ is a non-CM elliptic curve, then

- $\mathrm{im}\ \rho_{E,3^\infty}$ *is one of* 47 *subgroups of* $\mathrm{GL}_2(\mathbb{Z}_3)$ *of level at most* 27 *and index at most* 72*, or*
- *the image of* $\rho_{E,3^\infty}$ *is contained in the normalizer of the non-split Cartan modulo* 27*.*

• The index of the image is either 1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 27, 36, 72, or a multiple of 243.

Applications

- Torsion growth of elliptic curves $E/\mathbb{Q}$ over number fields of degree $d \leq 23$ (by González-Jiménez and Najman).

Applications

- Torsion growth of elliptic curves $E/\mathbb{Q}$ over number fields of degree $d \leq 23$ (by González-Jiménez and Najman).

- Classification of non-CM isolated points of odd degree with rational j-invariant on $X_1(n)$ (joint work with Bourdon, Gill, and Watson).

Applications

- Torsion growth of elliptic curves $E/\mathbb{Q}$ over number fields of degree $d \leq 23$ (by González-Jiménez and Najman).

- Classification of non-CM isolated points of odd degree with rational j-invariant on $X_1(n)$ (joint work with Bourdon, Gill, and Watson).

- ℓ-adic Kummer theory for elliptic curves over $\mathbb{Q}$ (work in progress with Cerchia, Lombardo, and Tronto).

The j-invariant

- If $E : y^2 = x^3 + Ax + B$, define $j(E) = \frac{6912A^3}{4A^3+27B^2}$.

The j-invariant

- If $E : y^2 = x^3 + Ax + B$, define $j(E) = \frac{6912A^3}{4A^3+27B^2}$.
- If E and E' are isomorphic, then $j(E) = j(E')$.

The j-invariant

- If $E : y^2 = x^3 + Ax + B$, define $j(E) = \frac{6912A^3}{4A^3+27B^2}$.

- If E and E' are isomorphic, then $j(E) = j(E')$.

- If E and E' are elliptic curves over K and $j(E) = j(E')$, then E and E' are isomorphic over some extension of K.

Background about modular curves

- Suppose that H is subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that contains $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$. Then there is a modular curve Y_H.

Background about modular curves

- Suppose that H is subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that contains $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$. Then there is a modular curve Y_H.

- If K is a number field, the elements of $Y_H(K)$ are in bijection with pairs $(E, [\iota]_H)$ where $[\iota]_H$ is an H-orbit of isomorphisms $\iota : E[N] \to (\mathbb{Z}/N\mathbb{Z})^2$.

Background about modular curves

- Suppose that H is subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that contains $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$. Then there is a modular curve Y_H.

- If K is a number field, the elements of $Y_H(K)$ are in bijection with pairs $(E, [\iota]_H)$ where $[\iota]_H$ is an H-orbit of isomorphisms $\iota : E[N] \to (\mathbb{Z}/N\mathbb{Z})^2$.

- The curve X_H is a projective curve obtained by adding finitely many "cusps" to Y_H.

Properties of modular curves

- The curve X_H is geometrically connected if $\det : H \to (\mathbb{Z}/N\mathbb{Z})^\times$ is surjective.

Properties of modular curves

- The curve X_H is geometrically connected if $\det : H \to (\mathbb{Z}/N\mathbb{Z})^\times$ is surjective.

- If E is an elliptic curve over a number field K with $j(E) \neq 0, 1728$, then there is a point $(E, [\iota]_H) \in X_H(K)$ if and only if $\mathrm{im}\ \rho_{E,N}$ is conjugate to a subgroup of H.

Properties of modular curves

- The curve X_H is geometrically connected if $\det : H \to (\mathbb{Z}/N\mathbb{Z})^\times$ is surjective.

- If E is an elliptic curve over a number field K with $j(E) \neq 0, 1728$, then there is a point $(E, [\iota]_H) \in X_H(K)$ if and only if $\mathrm{im}\ \rho_{E,N}$ is conjugate to a subgroup of H.

- If $H_1 \subseteq H_2$ are two subgroups of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, then there is a natural morphism $X_{H_1} \to X_{H_2}$.

Properties of modular curves

- The curve X_H is geometrically connected if $\det : H \to (\mathbb{Z}/N\mathbb{Z})^\times$ is surjective.

- If E is an elliptic curve over a number field K with $j(E) \neq 0, 1728$, then there is a point $(E, [\iota]_H) \in X_H(K)$ if and only if $\mathrm{im}\ \rho_{E,N}$ is conjugate to a subgroup of H.

- If $H_1 \subseteq H_2$ are two subgroups of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, then there is a natural morphism $X_{H_1} \to X_{H_2}$.

- We will often use the map $j : X_H \to X_{\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})} \cong \mathbb{P}^1$ taking a point $(E, [\iota]_H)$ to $j(E)$.

Example 1

- The modular curve $X_0(N)$ parametrizes elliptic curves with a cyclic N-isogeny. If $N = 2$, this is the same as having a rational point of order 2.

Example 1

- The modular curve $X_0(N)$ parametrizes elliptic curves with a cyclic N-isogeny. If $N = 2$, this is the same as having a rational point of order 2.

- The map $j : X_0(2) \to \mathbb{P}^1$ is given by $j = \frac{t^3}{t+16}$. The points $t = \infty$ and $t = -16$ are cusps.

Example 1

- The modular curve $X_0(N)$ parametrizes elliptic curves with a cyclic N-isogeny. If $N = 2$, this is the same as having a rational point of order 2.

- The map $j : X_0(2) \to \mathbb{P}^1$ is given by $j = \frac{t^3}{t+16}$. The points $t = \infty$ and $t = -16$ are cusps.

- An elliptic curve $E/\mathbb{Q}$ with $j(E) \neq 0, 1728$ has a rational point of order 2 if and only if $j(E) = \frac{t^3}{t+16}$ for some $t \in \mathbb{Q}$ with $t \neq -16$.

Example 2

- The modular curve $X_0(11)$ is the elliptic curve

$$y^2 + y = x^3 - x^2 - 10x - 20.$$

Example 2

- The modular curve $X_0(11)$ is the elliptic curve

$$y^2 + y = x^3 - x^2 - 10x - 20.$$

- This curve has precisely 5 rational points. The point at infinity and $(16 : 60 : 1)$ are cusps.

Example 2

- The modular curve $X_0(11)$ is the elliptic curve

$$y^2 + y = x^3 - x^2 - 10x - 20.$$

- This curve has precisely 5 rational points. The point at infinity and $(16 : 60 : 1)$ are cusps.

- The point $(5 : -6 : 1)$ maps to $j = -32768$, $(5 : 5 : 1)$ maps to $j = -24729001$ and $(16 : -61 : 1)$ maps to $j = -121$.

Examples 3 and 4

- The curve $X_0(27)$ is isomorphic to $x^3 + y^3 = z^3$.

Examples 3 and 4

- The curve $X_0(27)$ is isomorphic to $x^3 + y^3 = z^3$.
- The curve $X_0(64)$ is isomorphic to $x^4 + y^4 = z^4$.

Examples 3 and 4

- The curve $X_0(27)$ is isomorphic to $x^3 + y^3 = z^3$.

- The curve $X_0(64)$ is isomorphic to $x^4 + y^4 = z^4$.

- Aigner proved in 1934 that $x^4 + y^4 = z^4$ only has one non-trivial point in a quadratic field: $(1 + \sqrt{-7})^4 + (1 - \sqrt{-7})^4 = 2^4$.

Examples 3 and 4

- The curve $X_0(27)$ is isomorphic to $x^3 + y^3 = z^3$.

- The curve $X_0(64)$ is isomorphic to $x^4 + y^4 = z^4$.

- Aigner proved in 1934 that $x^4 + y^4 = z^4$ only has one non-trivial point in a quadratic field: $(1 + \sqrt{-7})^4 + (1 - \sqrt{-7})^4 = 2^4$.

- This point corresponds to an elliptic curve with CM by $\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$ that has an endomorphism of degree 2.

Faltings's theorem

Theorem (Faltings, 1983)

If $X/\mathbb{Q}$ is a curve with genus $g \geq 2$, then there are only finitely many rational points on X.

Faltings's theorem

Theorem (Faltings, 1983)

If $X/\mathbb{Q}$ is a curve with genus $g \geq 2$, then there are only finitely many rational points on X.

- For $H \subseteq \mathrm{GL}_2(\mathbb{Z}_3)$, the genus of X_H tends to infinity with the index of H in $\mathrm{GL}_2(\mathbb{Z}_3)$.

Outline

- As a consequence, if the index of H in $\mathrm{GL}_2(\mathbb{Z}_3)$ is high enough, then $X_H(\mathbb{Q})$ will be finite.

Outline

• As a consequence, if the index of H in $\mathrm{GL}_2(\mathbb{Z}_3)$ is high enough, then $X_H(\mathbb{Q})$ will be finite.

1. We enumerate subgroups of H of $\mathrm{GL}_2(\mathbb{Z}_3)$.

Outline

• As a consequence, if the index of H in $\mathrm{GL}_2(\mathbb{Z}_3)$ is high enough, then $X_H(\mathbb{Q})$ will be finite.

1. We enumerate subgroups of H of $\mathrm{GL}_2(\mathbb{Z}_3)$.
2. We compute models for the modular curves X_H.

Outline

• As a consequence, if the index of H in $\mathrm{GL}_2(\mathbb{Z}_3)$ is high enough, then $X_H(\mathbb{Q})$ will be finite.

1. We enumerate subgroups of H of $\mathrm{GL}_2(\mathbb{Z}_3)$.
2. We compute models for the modular curves X_H.
3. We (try to) provably find all the rational points on the curves X_H.

Step 1 - Subgroups

- We start by finding all subgroups H of $\mathrm{GL}_2(\mathbb{Z}_3)$ with the following properties:

Step 1 - Subgroups

- We start by finding all subgroups H of $\mathrm{GL}_2(\mathbb{Z}_3)$ with the following properties:
  - $\det : H \to \mathbb{Z}_3^\times$ is surjective,

Step 1 - Subgroups

• We start by finding all subgroups H of $\mathrm{GL}_2(\mathbb{Z}_3)$ with the following properties:

- $\det : H \to \mathbb{Z}_3^\times$ is surjective,
- H contains an element conjugate to $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

Step 1 - Subgroups

- We start by finding all subgroups H of $\mathrm{GL}_2(\mathbb{Z}_3)$ with the following properties:
  - $\det : H \to \mathbb{Z}_3^\times$ is surjective,
  - H contains an element conjugate to $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
  - H contains $-I$,

Step 1 - Subgroups

• We start by finding all subgroups H of $\mathrm{GL}_2(\mathbb{Z}_3)$ with the following properties:

- $\det : H \to \mathbb{Z}_3^\times$ is surjective,
- H contains an element conjugate to $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
- H contains $-I$,
- There is no subgroup K with $H \subseteq K$ so that X_K has genus ≥ 2.

Step 1 - Subgroups

• We start by finding all subgroups H of $\mathrm{GL}_2(\mathbb{Z}_3)$ with the following properties:

- det : $H \to \mathbb{Z}_3^\times$ is surjective,
- H contains an element conjugate to $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
- H contains $-I$,
- There is no subgroup K with $H \subseteq K$ so that X_K has genus ≥ 2.

• There are 80 conjugacy classes of such subgroups and the index can be as large as 729.

Step 2 - Computing equations for X_H

- We start with $X_1 = X_0(1)$. The map $j : X_0(1) \to \mathbb{P}^1$ is an isomorphism.

Step 2 - Computing equations for X_H

• We start with $X_1 = X_0(1)$. The map $j : X_0(1) \to \mathbb{P}^1$ is an isomorphism.

• In most cases, if H is one of the subgroups in our list, we construct X_H as a cover of $X_{\tilde{H}}$ for a subgroup $H \subseteq \tilde{H}$ so $[\tilde{H} : H]$ is minimal.

Step 2 - The function field

- The function field $\mathbb{Q}(X(N))/\mathbb{Q}(j)$ is a Galois extension with Galois group $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$.

Step 2 - The function field

• The function field $\mathbb{Q}(X(N))/\mathbb{Q}(j)$ is a Galois extension with Galois group $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$.

• The elements of this function field can be identified with modular functions: functions $f : \{z \in \mathbb{C} : \Im z > 0\} \to \mathbb{C}$ that satisfy

$$f\left(\frac{az+b}{cz+d}\right) = f(z) \text{ for all } z \text{ with } \Im z > 0 \text{ and } \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma(N).$$

Step 2 - Generators

- We wish to construct an element $h \in \mathbb{Q}(X(N))/\mathbb{Q}(j)$ that is fixed by H.

Step 2 - Generators

- We wish to construct an element $h \in \mathbb{Q}(X(N))/\mathbb{Q}(j)$ that is fixed by H.

- If $\vec{a} = (c, d) \in (\mathbb{Z}/N\mathbb{Z})^2$ is a vector, and $\gcd(c, d, N) = 1$, then

$$g_{\vec{a}}(z) = \frac{9}{\pi^2} \wp_z \left(\frac{cz + d}{N} \right)$$

is a weight 2 modular form for $\Gamma(N)$ and ratios of these give modular functions.

Step 2 - The model

- We take linear combinations and products of the $g_{\vec{a}}(z)$ to obtain a modular form f for the subgroup H.

Step 2 - The model

- We take linear combinations and products of the $g_{\vec{a}}(z)$ to obtain a modular form f for the subgroup H.

- We also keep track of the images $f|M$ where M runs over coset representatives of H in $\mathrm{GL}_2(\mathbb{Z}_3)$.

Step 2 - The model

- We take linear combinations and products of the $g_{\vec{a}}(z)$ to obtain a modular form f for the subgroup H.

- We also keep track of the images $f|M$ where M runs over coset representatives of H in $\mathrm{GL}_2(\mathbb{Z}_3)$.

- We divide by some standard modular form to get a modular function h, and we compute the minimal polynomial of h over $\mathbb{Q}(X_{\tilde{H}})$ to get a model of X_H.

Step 2 - Higher genus cases

• In higher genus cases, we use a variety of "modular forms tricks" to construct Fourier expansions of weight 2 cusp forms in $S_2(\Gamma(N), \mathbb{Q}(\zeta_N))$ that are fixed by the action of H.

Step 2 - Higher genus cases

• In higher genus cases, we use a variety of "modular forms tricks" to construct Fourier expansions of weight 2 cusp forms in $S_2(\Gamma(N), \mathbb{Q}(\zeta_N))$ that are fixed by the action of H.

• Eran Assaf and David Zywina have recently done some work about using modular symbols to compute bases for these spaces.

Step 2 - Higher genus cases

- In higher genus cases, we use a variety of "modular forms tricks" to construct Fourier expansions of weight 2 cusp forms in $S_2(\Gamma(N), \mathbb{Q}(\zeta_N))$ that are fixed by the action of H.

- Eran Assaf and David Zywina have recently done some work about using modular symbols to compute bases for these spaces.

- These correspond to holomorphic differentials on X_H and from these, one can compute the canonical model of X_H.

Step 2 - Data

- If we find a curve $X_{\tilde{H}}$ that has genus 1 and only finitely many rational points, we don't need to consider any curves X_H that cover it.

Step 2 - Data

- If we find a curve $X_{\tilde{H}}$ that has genus 1 and only finitely many rational points, we don't need to consider any curves X_H that cover it.

- In the end, we find

Step 2 - Data

- If we find a curve $X_{\tilde{H}}$ that has genus 1 and only finitely many rational points, we don't need to consider any curves X_H that cover it.

- In the end, we find
  - 22 genus zero curves isomorphic to $\mathbb{P}^1$,

Step 2 - Data

- If we find a curve $X_{\tilde{H}}$ that has genus 1 and only finitely many rational points, we don't need to consider any curves X_H that cover it.

- In the end, we find
  - 22 genus zero curves isomorphic to $\mathbb{P}^1$,
  - 5 genus 1 curves (all with finitely many points),

Step 2 - Data

- If we find a curve $X_{\tilde{H}}$ that has genus 1 and only finitely many rational points, we don't need to consider any curves X_H that cover it.

- In the end, we find
  - 22 genus zero curves isomorphic to $\mathbb{P}^1$,
  - 5 genus 1 curves (all with finitely many points),
  - 4 genus two curves,

Step 2 - Data

- If we find a curve $X_{\tilde{H}}$ that has genus 1 and only finitely many rational points, we don't need to consider any curves X_H that cover it.

- In the end, we find
  - 22 genus zero curves isomorphic to $\mathbb{P}^1$,
  - 5 genus 1 curves (all with finitely many points),
  - 4 genus two curves,
  - 3 genus three curves,

Step 2 - Data

- If we find a curve $X_{\tilde{H}}$ that has genus 1 and only finitely many rational points, we don't need to consider any curves X_H that cover it.

- In the end, we find
  - 22 genus zero curves isomorphic to $\mathbb{P}^1$,
  - 5 genus 1 curves (all with finitely many points),
  - 4 genus two curves,
  - 3 genus three curves,
  - 4 genus four curves,

Step 2 - Data

- If we find a curve $X_{\tilde{H}}$ that has genus 1 and only finitely many rational points, we don't need to consider any curves X_H that cover it.

- In the end, we find
  - 22 genus zero curves isomorphic to $\mathbb{P}^1$,
  - 5 genus 1 curves (all with finitely many points),
  - 4 genus two curves,
  - 3 genus three curves,
  - 4 genus four curves,
  - 1 genus six curve,

Step 2 - Data

- If we find a curve $X_{\tilde{H}}$ that has genus 1 and only finitely many rational points, we don't need to consider any curves X_H that cover it.

- In the end, we find
  - 22 genus zero curves isomorphic to $\mathbb{P}^1$,
  - 5 genus 1 curves (all with finitely many points),
  - 4 genus two curves,
  - 3 genus three curves,
  - 4 genus four curves,
  - 1 genus six curve,
  - 1 genus 12 curve,

Step 2 - Data

- If we find a curve $X_{\tilde{H}}$ that has genus 1 and only finitely many rational points, we don't need to consider any curves X_H that cover it.

- In the end, we find
  - 22 genus zero curves isomorphic to $\mathbb{P}^1$,
  - 5 genus 1 curves (all with finitely many points),
  - 4 genus two curves,
  - 3 genus three curves,
  - 4 genus four curves,
  - 1 genus six curve,
  - 1 genus 12 curve,
  - and 1 genus 43 curve.

Step 3 - Finding the rational points

- One method we use to provably find all the rational points on these curves is the theory of étale descent.

Step 3 - Finding the rational points

- One method we use to provably find all the rational points on these curves is the theory of étale descent.

- Given a curve C of genus g, we search for an étale triple cover $\phi : X \to C$. (Here X will have genus $3g - 2$.)

Step 3 - Finding the rational points

- One method we use to provably find all the rational points on these curves is the theory of étale descent.

- Given a curve C of genus g, we search for an étale triple cover $\phi : X \to C$. (Here X will have genus $3g-2$.)

- There will be a finite collection of twists $\phi_d : X_d \to C$ so that

$$\bigcup_d \phi_d(X_d(\mathbb{Q})) = C(\mathbb{Q}).$$

Step 3 - Example (1/3)

- The genus 6 curve is a Picard curve with model

$$y^3 = \frac{x(x^3 - 6x^2 + 3x + 1)}{x^3 + 3x^2 - 6x + 1}.$$

Step 3 - Example (1/3)

- The genus 6 curve is a Picard curve with model

$$y^3 = \frac{x(x^3 - 6x^2 + 3x + 1)}{x^3 + 3x^2 - 6x + 1}.$$

- We get a family of étale covers by taking $d \in \{1, 3, 9\}$ and letting X_d be the curve defined by

$$\begin{aligned} dy_1^3 &= x(x^3 - 6x^2 + 3x + 1) \\ dy_2^3 &= x^3 + 3x^2 - 6x + 1. \end{aligned}$$

Step 3 - Example (1/3)

- The genus 6 curve is a Picard curve with model

$$y^3 = \frac{x(x^3 - 6x^2 + 3x + 1)}{x^3 + 3x^2 - 6x + 1}.$$

- We get a family of étale covers by taking $d \in \{1, 3, 9\}$ and letting X_d be the curve defined by

$$\begin{aligned} dy_1^3 &= x(x^3 - 6x^2 + 3x + 1) \\ dy_2^3 &= x^3 + 3x^2 - 6x + 1. \end{aligned}$$

- For $d = 3$, the second equation has no 3-adic points.

Step 3 - Example (1/3)

- The genus 6 curve is a Picard curve with model

$$y^3 = \frac{x(x^3 - 6x^2 + 3x + 1)}{x^3 + 3x^2 - 6x + 1}.$$

- We get a family of étale covers by taking $d \in \{1, 3, 9\}$ and letting X_d be the curve defined by

$$\begin{aligned} dy_1^3 &= x(x^3 - 6x^2 + 3x + 1) \\ dy_2^3 &= x^3 + 3x^2 - 6x + 1. \end{aligned}$$

- For $d = 3$, the second equation has no 3-adic points.

- For $d = 9$, the first equation defines a genus 3 curve whose Jacobian has rank zero. This allows us to find the points on X_9.

Step 3 - Example (2/3)

- The $d = 1$ case remains. We can construct étale covers of $y_1^3 = x(x^3 - 6x^2 + 3x + 1)$ of the form

$$\begin{aligned} ey_2^3 &= x \\ e^2 y_2^3 &= x^3 - 6x^2 + 3x + 1. \end{aligned}$$

Step 3 - Example (2/3)

- The $d = 1$ case remains. We can construct étale covers of $y_1^3 = x(x^3 - 6x^2 + 3x + 1)$ of the form

$$\begin{aligned} ey_2^3 &= x \\ e^2 y_2^3 &= x^3 - 6x^2 + 3x + 1. \end{aligned}$$

- If $e = 1$, the second equation defines a rank zero elliptic curve, while if $e = 3$ the second equation has no 3-adic points.

Step 3 - Example (2/3)

• The $d = 1$ case remains. We can construct étale covers of $y_1^3 = x(x^3 - 6x^2 + 3x + 1)$ of the form

$$\begin{aligned} ey_2^3 &= x \\ e^2y_2^3 &= x^3 - 6x^2 + 3x + 1. \end{aligned}$$

• If $e = 1$, the second equation defines a rank zero elliptic curve, while if $e = 3$ the second equation has no 3-adic points.

• So $e = 9$. This means that $x^3 - 6x^2 + 3x + 1$ is 3 times a cube $x^3 + 3x^2 - 6x + 1$ is a cube. So we have a rational point on $y^3 = 9(x^3 - 6x^2 + 3x + 1)(x^3 + 3x^2 - 6x + 1)$.

Step 3 - Example (3/3)

- This curve $Y : y^3 = 9(x^3 - 6x^2 + 3x + 1)(x^3 + 3x^2 - 6x + 1)$ has genus 4 and its automorphism group is isomorphic to S_3.

Step 3 - Example (3/3)

- This curve $Y : y^3 = 9(x^3 - 6x^2 + 3x + 1)(x^3 + 3x^2 - 6x + 1)$ has genus 4 and its automorphism group is isomorphic to S_3.

- The quotient by the subgroup of order 3 is $Z : y^2 = x^6 - 2x^3 - 3$. This genus 2 curve has Jacobian of rank zero and only three rational points.

Step 3 - Example (3/3)

- This curve $Y : y^3 = 9(x^3 - 6x^2 + 3x + 1)(x^3 + 3x^2 - 6x + 1)$ has genus 4 and its automorphism group is isomorphic to S_3.

- The quotient by the subgroup of order 3 is $Z : y^2 = x^6 - 2x^3 - 3$. This genus 2 curve has Jacobian of rank zero and only three rational points.

- Pulling these back to the original curve allows us to find all of its rational points.

Hard case 1 - The genus 43 curve

- In 2006, Elkies computed a modular curve X_H parametrizing elliptic curves where $\rho_{E,3}$ was surjective but $\rho_{E,9}$ was not. This curve X_H is a degree 27 cover of the j-line and is isomorphic to $\mathbb{P}^1$.

Hard case 1 - The genus 43 curve

- In 2006, Elkies computed a modular curve X_H parametrizing elliptic curves where $\rho_{E,3}$ was surjective but $\rho_{E,9}$ was not. This curve X_H is a degree 27 cover of the j-line and is isomorphic to $\mathbb{P}^1$.

- There is a maximal subgroup $M \subseteq H$ of index 27. If x is a rational point on X_M, then the elliptic curve corresponding to x must have $\rho_{E,3}$ surjective, and $\mathbb{Q}(E[27]) = \mathbb{Q}(E[3], \zeta_{27})$.

Hard case 1 - The genus 43 curve

- In 2006, Elkies computed a modular curve X_H parametrizing elliptic curves where $\rho_{E,3}$ was surjective but $\rho_{E,9}$ was not. This curve X_H is a degree 27 cover of the j-line and is isomorphic to $\mathbb{P}^1$.

- There is a maximal subgroup $M \subseteq H$ of index 27. If x is a rational point on X_M, then the elliptic curve corresponding to x must have $\rho_{E,3}$ surjective, and $\mathbb{Q}(E[27]) = \mathbb{Q}(E[3], \zeta_{27})$.

- This is really weird, and suggests that the modular curve X_M might not have local points.

Hard case 1 - The model

- We compute the canonical model of this curve in $\mathbb{P}^{42}$. It's the vanishing set of 820 quadratic polynomials in 43 variables.

Hard case 1 - The model

- We compute the canonical model of this curve in $\mathbb{P}^{42}$. It's the vanishing set of 820 quadratic polynomials in 43 variables.

- The reduction mod 3 of this model has 19 points.

Hard case 1 - The model

- We compute the canonical model of this curve in $\mathbb{P}^{42}$. It's the vanishing set of 820 quadratic polynomials in 43 variables.

- The reduction mod 3 of this model has 19 points.

- If $P = (x_1 : x_2 : \cdots : x_{43})$ is a point on X_M modulo 3, then for every lift $(\tilde{x}_1, \tilde{x}_2, \tilde{x}_3, \tilde{x}_4) \in (\mathbb{Z}/9\mathbb{Z})^4$ of $(x_1, \ldots, x_4)$, we create an ideal in the polynomial ring in 43 variables over $\mathbb{Z}$ generated by the quadratic polynomials evaluated at $\tilde{x}_1, \ldots, \tilde{x}_4$, and 9.

Hard case 1 - No local points

- We check to see if 3 is contained in that ideal. If it is, then there is no point on $X_M(\mathbb{Z}/9\mathbb{Z})$ whose first four coordinates are $\tilde{x}_1, \ldots, \tilde{x}_4$.

Hard case 1 - No local points

- We check to see if 3 is contained in that ideal. If it is, then there is no point on $X_M(\mathbb{Z}/9\mathbb{Z})$ whose first four coordinates are $\tilde{x}_1, \ldots, \tilde{x}_4$.

- In this way, we show that $X_M(\mathbb{Z}/9\mathbb{Z})$ is empty.

Hard case 2 - $X_{\mathrm{ns}}^{+}(27)$

• The curve $X_{\mathrm{ns}}^{+}(27)$ is the modular curve corresponding to the normalizer of the non-split Cartan modulo 27. It has genus 12, at least 8 rational points, and the analytic rank of its Jacobian is 12.

Hard case 2 - $X_{\text{ns}}^{+}(27)$

- The curve $X_{\text{ns}}^{+}(27)$ is the modular curve corresponding to the normalizer of the non-split Cartan modulo 27. It has genus 12, at least 8 rational points, and the analytic rank of its Jacobian is 12.

- Provably finding all the rational points on it would give an independent solution of the class number 1 problem.

Hard case 2 - $X_{\mathrm{ns}}^{+}(27)$

- The curve $X_{\mathrm{ns}}^{+}(27)$ is the modular curve corresponding to the normalizer of the non-split Cartan modulo 27. It has genus 12, at least 8 rational points, and the analytic rank of its Jacobian is 12.

- Provably finding all the rational points on it would give an independent solution of the class number 1 problem.

- There is a map from $X_{\mathrm{ns}}^{+}(27)$ to a modular curve X_K of genus 3, but it's not defined over $\mathbb{Q}$.

Hard case 2 - Genus 3 curve

- Let $\zeta = e^{2\pi i/3}$ and $L = \mathbb{Q}(\zeta)$. This curve is

$$X_K : a^4 + (\zeta - 1)a^3b + (3\zeta + 2)a^3c - 3a^2c^2 + (2\zeta + 2)ab^3 - 3\zeta ab^2c + 3\zeta abc^2 - 2\zeta ac^3 - \zeta b^3c + 3\zeta b^2c^2 + (-\zeta + 1)bc^3 + (\zeta + 1)c^4 = 0.$$

Hard case 2 - Genus 3 curve

- Let $\zeta = e^{2\pi i/3}$ and $L = \mathbb{Q}(\zeta)$. This curve is

$$X_K : a^4 + (\zeta - 1)a^3 b + (3\zeta + 2)a^3 c - 3a^2 c^2 + (2\zeta + 2)ab^3 - 3\zeta ab^2 c + 3\zeta abc^2 - 2\zeta ac^3 - \zeta b^3 c + 3\zeta b^2 c^2 + (-\zeta + 1)bc^3 + (\zeta + 1)c^4 = 0.$$

- The Jacobian of X_K has rank 6 over L and $X_K(L)$ has size at least 13. One of these points is non-CM.

Hard case 2 - Genus 3 curve

- Let $\zeta = e^{2\pi i/3}$ and $L = \mathbb{Q}(\zeta)$. This curve is

$$X_K : a^4 + (\zeta - 1)a^3b + (3\zeta + 2)a^3c - 3a^2c^2 + (2\zeta + 2)ab^3 - 3\zeta ab^2c$$
$$+ 3\zeta abc^2 - 2\zeta ac^3 - \zeta b^3c + 3\zeta b^2c^2 + (-\zeta + 1)bc^3 + (\zeta + 1)c^4 = 0.$$

- The Jacobian of X_K has rank 6 over L and $X_K(L)$ has size at least 13. One of these points is non-CM.

- By looking at differences of L-rational points, we are able to find a point of order 3 in $\mathrm{Jac}(X_K)(L)$.

Hard case 2 - étale descent

- Using this, we can construct a family of étale triple covers $\{Y_d\}$ of X_K. Here $d = 3^a \zeta^b$ for $0 \leq a, b \leq 2$.

Hard case 2 - étale descent

• Using this, we can construct a family of étale triple covers $\{Y_d\}$ of X_K. Here $d = 3^a\zeta^b$ for $0 \leq a, b \leq 2$.

• Counting points on these étale triple covers strongly suggests that these genus 7 curves map to elliptic curves. In 8 of the 9 cases, the elliptic curve they map to has rank 0 or 1.

Hard case 2 - étale descent

• Using this, we can construct a family of étale triple covers $\{Y_d\}$ of X_K. Here $d = 3^a \zeta^b$ for $0 \leq a, b \leq 2$.

• Counting points on these étale triple covers strongly suggests that these genus 7 curves map to elliptic curves. In 8 of the 9 cases, the elliptic curve they map to has rank 0 or 1.

• In the final case (which gets a lot of the L-points on X_K), the elliptic curve is $E : y^2 = x^3 - 48$, and $E(L)$ has rank 2.

Hard case 2 - Map to an elliptic curve

- By computing with this genus 7 curve over $\mathbb{F}_7$, we are able to find the map to the elliptic curve.

Hard case 2 - Map to an elliptic curve

- By computing with this genus 7 curve over $\mathbb{F}_7$, we are able to find the map to the elliptic curve.

- We write down the scheme Z that parametrizes maps from $Y \to E$, write down the mod 7 point on this scheme and use Hensel's lemma.

Hard case 2 - Map to an elliptic curve

- By computing with this genus 7 curve over $\mathbb{F}_7$, we are able to find the map to the elliptic curve.

- We write down the scheme Z that parametrizes maps from $Y \to E$, write down the mod 7 point on this scheme and use Hensel's lemma.

- We are able to "guess" a point in $Z(L)$ and in this way construct the map $\phi : Y \to E$.

Hard case 2 - One more étale cover

- Since E has CM, there is a 3-isogeny $\psi : E \to E$. Using this, we can compute the fiber product

$$\begin{tikzcd} Y \times_E E \arrow[r] \arrow[d] & E \arrow[d, "\psi"] \\ Y \arrow[r, "\phi"] & E \end{tikzcd}$$

Hard case 2 - One more étale cover

- Since E has CM, there is a 3-isogeny $\psi : E \to E$. Using this, we can compute the fiber product

$$\begin{tikzcd} Y \times_E E \arrow[r] \arrow[d] & E \arrow[d, "\psi"] \\ Y \arrow[r, "\phi"] & E \end{tikzcd}$$

- This is an étale triple cover of Y, which has genus 19. Our last hope was that this étale triple cover might map to an elliptic curve with rank ≤ 1.

Hard case 2 - One more étale cover

- Since E has CM, there is a 3-isogeny $\psi : E \to E$. Using this, we can compute the fiber product

$$\begin{tikzcd} Y \times_E E \arrow[r] \arrow[d] & E \arrow[d, "\psi"] \\ Y \arrow[r, "\phi"] & E \end{tikzcd}$$

- This is an étale triple cover of Y, which has genus 19. Our last hope was that this étale triple cover might map to an elliptic curve with rank ≤ 1.

- It doesn't. We computed the numerator of the zeta function of $Y \times_E E$ over $\mathbb{F}_4$, and the "new part" is irreducible.

Summary

- We (almost) classify the image of the 3-adic Galois representation $\rho_{E,3^\infty}$ for non-CM elliptic curves $E/\mathbb{Q}$.

Summary

• We (almost) classify the image of the 3-adic Galois representation $\rho_{E,3^\infty}$ for non-CM elliptic curves $E/\mathbb{Q}$.

• We write down the possible images $H \subseteq \mathrm{GL}_2(\mathbb{Z}_3)$ and compute equations for the modular curves X_H.

Summary

- We (almost) classify the image of the 3-adic Galois representation $\rho_{E,3^\infty}$ for non-CM elliptic curves $E/\mathbb{Q}$.

- We write down the possible images $H \subseteq \mathrm{GL}_2(\mathbb{Z}_3)$ and compute equations for the modular curves X_H.

- We find the rational points on all of these modular curves, except $X_{\mathrm{ns}}^{+}(27)$.