Rational points on modular curves via maps to elliptic curves with rank zero

Jacob Mayle and Jeremy Rouse

ANTS XVII, Groningen
July 7, 2026

Code available at `github.com/rouseja/ModCrvToEC`

Galois representations attached to elliptic curves

- Let K be a number field and E/K an elliptic curve.

Galois representations attached to elliptic curves

- Let K be a number field and E/K an elliptic curve.
- Define $E[n] := \{P \in E(\overline{K}) : nP = 0\} \simeq (\mathbb{Z}/n\mathbb{Z})^2$.

Galois representations attached to elliptic curves

- Let K be a number field and E/K an elliptic curve.
- Define $E[n] := \{P \in E(\overline{K}) : nP = 0\} \simeq (\mathbb{Z}/n\mathbb{Z})^2$.
- Given $\sigma \in G_K := \mathrm{Gal}(\overline{K}/K)$, σ acts as an automorphism on $E[n]$.

Galois representations attached to elliptic curves

- Let K be a number field and E/K an elliptic curve.
- Define $E[n] := \{P \in E(\overline{K}) : nP = 0\} \simeq (\mathbb{Z}/n\mathbb{Z})^2$.
- Given $\sigma \in G_K := \mathrm{Gal}(\overline{K}/K)$, σ acts as an automorphism on $E[n]$.
- This gives a homomorphism $\rho_{E,n} \colon G_K \to \mathrm{Aut}(E[n]) \simeq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.

Example (1/2)

- Let $K = \mathbb{Q}$, $E : y^2 = x^3 - 88x - 363$ and $n = 4$.

Example (1/2)

• Let $K = \mathbb{Q}$, $E : y^2 = x^3 - 88x - 363$ and $n = 4$. A $\mathbb{Z}/4\mathbb{Z}$ basis for $E[4]$ is $\{P, Q\}$, where

$$P = (11 + 5\sqrt{11}, \frac{5}{2}(1 - i)(11 + 3\sqrt{11})\sqrt[4]{-11})$$

and

$$Q = \left(\frac{-11 + 11i + 3\sqrt{11} - \sqrt{-11}}{2}, \frac{(1 + 3i)(-11 + \sqrt{11})\sqrt[4]{-11}}{2} \right).$$

Example (1/2)

- Let $K = \mathbb{Q}$, $E : y^2 = x^3 - 88x - 363$ and $n = 4$. A $\mathbb{Z}/4\mathbb{Z}$ basis for $E[4]$ is $\{P, Q\}$, where

$$P = (11 + 5\sqrt{11}, \frac{5}{2}(1 - i)(11 + 3\sqrt{11})\sqrt[4]{-11})$$

and

$$Q = \left(\frac{-11 + 11i + 3\sqrt{11} - \sqrt{-11}}{2}, \frac{(1 + 3i)(-11 + \sqrt{11})\sqrt[4]{-11}}{2} \right).$$

- We have $\mathbb{Q}(E[4]) = \mathbb{Q}(i, \sqrt[4]{-11})$.

Example (1/2)

- Let $K = \mathbb{Q}$, $E : y^2 = x^3 - 88x - 363$ and $n = 4$. A $\mathbb{Z}/4\mathbb{Z}$ basis for $E[4]$ is $\{P, Q\}$, where

$$P = (11 + 5\sqrt{11}, \frac{5}{2}(1 - i)(11 + 3\sqrt{11})\sqrt[4]{-11})$$

and

$$Q = \left(\frac{-11 + 11i + 3\sqrt{11} - \sqrt{-11}}{2}, \frac{(1 + 3i)(-11 + \sqrt{11})\sqrt[4]{-11}}{2} \right).$$

- We have $\mathbb{Q}(E[4]) = \mathbb{Q}(i, \sqrt[4]{-11})$.

- $\mathrm{Gal}(\mathbb{Q}(E[4])/\mathbb{Q}) = \langle \sigma, \tau \rangle$ where

$$\sigma(i) = i \text{ and } \sigma(\sqrt[4]{-11}) = i\sqrt[4]{-11}$$
$$\tau(i) = -i \text{ and } \tau(\sqrt[4]{-11}) = \sqrt[4]{-11}.$$

Example (2/2)

- We have $\sigma(P) = 3P + 2Q$ and $\sigma(Q) = P + Q$, and so

$$\rho_{E,4}(\sigma) = \begin{bmatrix} 3 & 1 \\ 2 & 1 \end{bmatrix}.$$

Example (2/2)

- We have $\sigma(P) = 3P + 2Q$ and $\sigma(Q) = P + Q$, and so

$$\rho_{E,4}(\sigma) = \begin{bmatrix} 3 & 1 \\ 2 & 1 \end{bmatrix}.$$

- We have $\tau(P) = 3P + 2Q$ and $\tau(Q) = 2P + Q$, and so

$$\rho_{E,4}(\tau) = \begin{bmatrix} 3 & 2 \\ 2 & 1 \end{bmatrix}.$$

Example (2/2)

- We have $\sigma(P) = 3P + 2Q$ and $\sigma(Q) = P + Q$, and so

$$\rho_{E,4}(\sigma) = \begin{bmatrix} 3 & 1 \\ 2 & 1 \end{bmatrix}.$$

- We have $\tau(P) = 3P + 2Q$ and $\tau(Q) = 2P + Q$, and so

$$\rho_{E,4}(\tau) = \begin{bmatrix} 3 & 2 \\ 2 & 1 \end{bmatrix}.$$

- Thus, $\operatorname{im} \rho_{E,4} = \left\langle \begin{bmatrix} 3 & 1 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 3 & 2 \\ 2 & 1 \end{bmatrix} \right\rangle \leq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$.

Why study Galois representations?

• Galois representations naturally arise in the study of class numbers of imaginary quadratic fields, Fermat's Last Theorem, and the inverse Galois problem.

Why study Galois representations?

• Galois representations naturally arise in the study of class numbers of imaginary quadratic fields, Fermat's Last Theorem, and the inverse Galois problem.

• If E/K is an elliptic curve, one can consider the single representation

$$\rho_E \colon G_K \to \varprojlim \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) := \mathrm{GL}_2(\hat{\mathbb{Z}}).$$

Mazur's Program B

B. Given a number field K and a subgroup H of $GL_2\widehat{\mathbb{Z}} = \prod_p GL_2\mathbb{Z}_p$ classify all elliptic curves $E_{/K}$ whose associated Galois representation on torsion points maps $\mathrm{Gal}(\overline{K}/K)$ into $H \subset GL_2\widehat{\mathbb{Z}}$.

The j-invariant

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

The j-invariant

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

- If E_1/K and E_2/K are isomorphic elliptic curves, $j(E_1) = j(E_2)$. Conversely, if $j(E_1) = j(E_2)$, then E_1 and E_2 are isomorphic over some finite extension of K.

The j-invariant

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

- If E_1/K and E_2/K are isomorphic elliptic curves, $j(E_1) = j(E_2)$. Conversely, if $j(E_1) = j(E_2)$, then E_1 and E_2 are isomorphic over some finite extension of K.

- We say that E has complex multiplication (CM) if $\mathrm{End}_{\overline{K}}(E)$ is an order in an imaginary quadratic field.

Modular curves

• If H is an open subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$, there is a curve X_H together with a map $\pi_H \colon X_H \to \mathbb{P}^1$ with the property that if E/K is an elliptic curve,

$$\mathrm{im}\ \rho_E \subseteq \text{ a conjugate of } H \iff j(E) \in \pi_H(X_H(K))$$

provided $j(E) \notin \{0, 1728\}$.

Modular curves

• If H is an open subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$, there is a curve X_H together with a map $\pi_H \colon X_H \to \mathbb{P}^1$ with the property that if E/K is an elliptic curve,

$$\mathrm{im}\ \rho_E \subseteq \text{ a conjugate of } H \iff j(E) \in \pi_H(X_H(K))$$

provided $j(E) \notin \{0, 1728\}$.

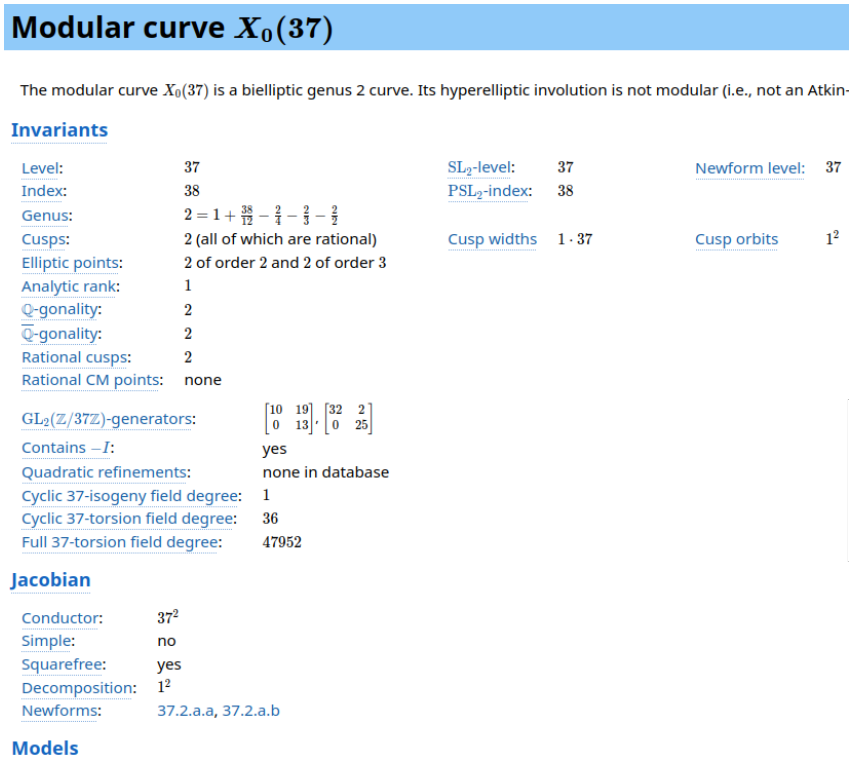
• If $\det : H \to \hat{\mathbb{Z}}^\times$ is surjective, then X_H is a nice curve defined over $\mathbb{Q}$.

LMFDB modular curves database

• There is a database of modular curves available in the beta version of the LMFDB.

LMFDB modular curves database

- There is a database of modular curves available in the beta version of the LMFDB.



Modular curve $X_0(37)$

The modular curve $X_0(37)$ is a bielliptic genus 2 curve. Its hyperelliptic involution is not modular (i.e., not an Atkin-

Invariants

Level:	37	SL_2-level:	37	Newform level:	37
Index:	38	PSL_2-index:	38		
Genus:	$2 = 1 + \frac{38}{12} - \frac{2}{4} - \frac{2}{3} - \frac{2}{2}$				
Cusps:	2 (all of which are rational)	Cusp widths	$1 \cdot 37$	Cusp orbits	1^2
Elliptic points:	2 of order 2 and 2 of order 3				
Analytic rank:	1				
$\mathbb{Q}$-gonality:	2				
$\overline{\mathbb{Q}}$-gonality:	2				
Rational cusps:	2				
Rational CM points:	none				

$\mathrm{GL}_2(\mathbb{Z}/37\mathbb{Z})$-generators:	$\begin{bmatrix}10 & 19\\ 0 & 13\end{bmatrix}, \begin{bmatrix}32 & 2\\ 0 & 25\end{bmatrix}$
Contains $-I$:	yes
Quadratic refinements:	none in database
Cyclic 37-isogeny field degree:	1
Cyclic 37-torsion field degree:	36
Full 37-torsion field degree:	47952

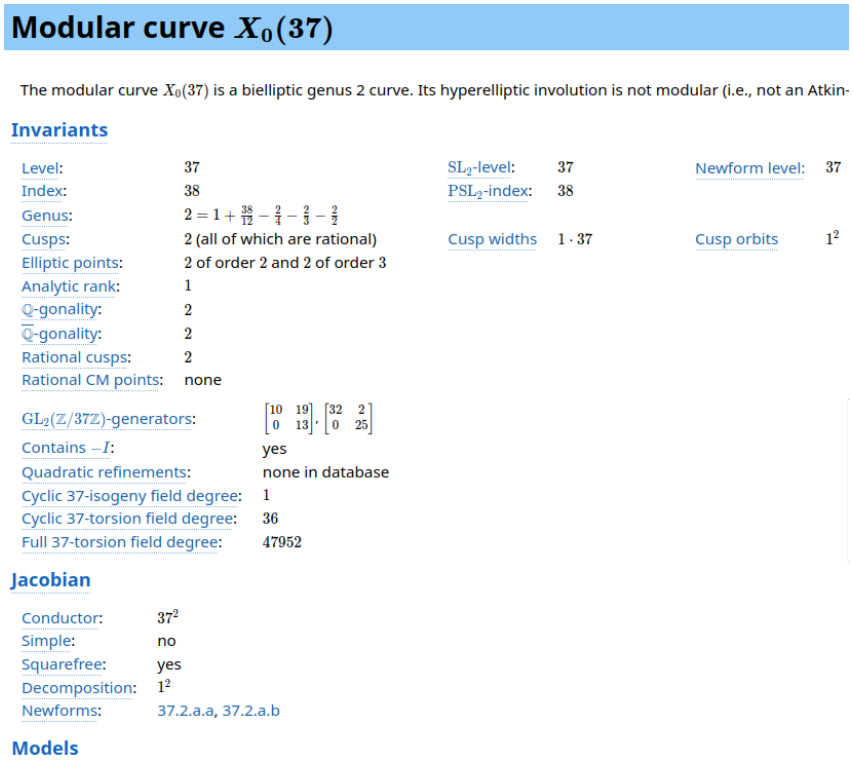
Jacobian

Conductor:	37^2
Simple:	no
Squarefree:	yes
Decomposition:	1^2
Newforms:	37.2.a.a, 37.2.a.b

Models

LMFDB modular curves database

• There is a database of modular curves available in the beta version of the LMFDB.



Modular curve $X_0(37)$

The modular curve $X_0(37)$ is a bielliptic genus 2 curve. Its hyperelliptic involution is not modular (i.e., not an Atkin-

Invariants

Level:	37	SL_2-level:	37	Newform level:	37
Index:	38	PSL_2-index:	38		
Genus:	$2 = 1 + \frac{38}{12} - \frac{2}{4} - \frac{2}{3} - \frac{2}{2}$				
Cusps:	2 (all of which are rational)	Cusp widths	$1 \cdot 37$	Cusp orbits	1^2
Elliptic points:	2 of order 2 and 2 of order 3				
Analytic rank:	1				
$\mathbb{Q}$-gonality:	2				
$\overline{\mathbb{Q}}$-gonality:	2				
Rational cusps:	2				
Rational CM points:	none				

$GL_2(\mathbb{Z}/37\mathbb{Z})$-generators:	$\begin{bmatrix}10 & 19\\ 0 & 13\end{bmatrix}, \begin{bmatrix}32 & 2\\ 0 & 25\end{bmatrix}$
Contains $-I$:	yes
Quadratic refinements:	none in database
Cyclic 37-isogeny field degree:	1
Cyclic 37-torsion field degree:	36
Full 37-torsion field degree:	47952

Jacobian

Conductor:	37^2
Simple:	no
Squarefree:	yes
Decomposition:	1^2
Newforms:	37.2.a.a, 37.2.a.b

Models

• The database includes data about labels, subgroups, rational points, equations for X_H, the map $\pi_H \colon X_H \to \mathbb{P}^1$, and the decomposition of the Jacobian $J(X_H)$.

Main question

• Suppose that H has level ≤ 70, contains $-I$ and X_H admits a map to a rank zero elliptic curve $E/\mathbb{Q}$.

Main question

- Suppose that H has level ≤ 70, contains $-I$ and X_H admits a map to a rank zero elliptic curve $E/\mathbb{Q}$.

- If we can find $\phi : X_H \to E$, then

$$X_H(\mathbb{Q}) = \bigcup_{T \in E(\mathbb{Q})} \phi^{-1}(T).$$

Main question

• Suppose that H has level ≤ 70, contains $-I$ and X_H admits a map to a rank zero elliptic curve $E/\mathbb{Q}$.

• If we can find $\phi : X_H \to E$, then

$$X_H(\mathbb{Q}) = \bigcup_{T \in E(\mathbb{Q})} \phi^{-1}(T).$$

• So if we can determine ϕ explicitly, we can use it to determine $X_H(\mathbb{Q})$.

Main result

• There are 804450 open subgroups $H \leq \mathrm{GL}_2(\hat{\mathbb{Z}})$ with level ≤ 70 that contain $-I$. For 797591 of these, there is a map $X_H \to E$ for some elliptic curve $E/\mathbb{Q}$ with rank zero.

Main result

• There are 804450 open subgroups $H \leq \mathrm{GL}_2(\hat{\mathbb{Z}})$ with level ≤ 70 that contain $-I$. For 797591 of these, there is a map $X_H \to E$ for some elliptic curve $E/\mathbb{Q}$ with rank zero.

Theorem (Mayle-R, 2026)

We determine $\pi_H(X_H(\mathbb{Q}))$ for all but 10 of the 797591. The ten cases we are unable to handle all have genus > 60.

Minimal modular curves

- If $H \leq G$ are open subgroups of $\mathrm{GL}_2(\hat{\mathbb{Z}})$, there is a natural map $X_H \to X_G$ and as a consequence, $J(X_G)$ is an isogeny factor of $J(X_H)$.

Minimal modular curves

• If $H \leq G$ are open subgroups of $\mathrm{GL}_2(\hat{\mathbb{Z}})$, there is a natural map $X_H \to X_G$ and as a consequence, $J(X_G)$ is an isogeny factor of $J(X_H)$.

• Thus, if X_G admits a map to a rank zero elliptic curve $E/\mathbb{Q}$, so does X_H. We say X_G is minimal it maps to a rank zero elliptic curve, but there is no supergroup $\tilde{G}$ so that $X_{\tilde{G}}$ does.

Minimal modular curves

• If $H \leq G$ are open subgroups of $\mathrm{GL}_2(\hat{\mathbb{Z}})$, there is a natural map $X_H \to X_G$ and as a consequence, $J(X_G)$ is an isogeny factor of $J(X_H)$.

• Thus, if X_G admits a map to a rank zero elliptic curve $E/\mathbb{Q}$, so does X_H. We say X_G is minimal it maps to a rank zero elliptic curve, but there is no supergroup $\tilde{G}$ so that $X_{\tilde{G}}$ does.

• There are only 1034 minimal modular curves of level ≤ 70. Some can be ruled out based on prime power level images of Galois, or results of Lemos.

Minimal modular curves

• If $H \leq G$ are open subgroups of $\mathrm{GL}_2(\hat{\mathbb{Z}})$, there is a natural map $X_H \to X_G$ and as a consequence, $J(X_G)$ is an isogeny factor of $J(X_H)$.

• Thus, if X_G admits a map to a rank zero elliptic curve $E/\mathbb{Q}$, so does X_H. We say X_G is minimal it maps to a rank zero elliptic curve, but there is no supergroup $\tilde{G}$ so that $X_{\tilde{G}}$ does.

• There are only 1034 minimal modular curves of level ≤ 70. Some can be ruled out based on prime power level images of Galois, or results of Lemos.

• We are able to handle X_H with genus as large as 54. In some cases the degree of $X_H \to E$ is as large as 126.

Overview (1/2)

- John Cremona's database of elliptic curves is created by finding maps from $X_0(N)$ to elliptic curves with conductor N.

Overview (1/2)

- John Cremona's database of elliptic curves is created by finding maps from $X_0(N)$ to elliptic curves with conductor N.

- We assume that $Q \in X_H(\mathbb{Q})$. We identify a weight 2 cusp form f for $H \cap \mathrm{SL}_2(\mathbb{Z})$ using Hecke operators.

Overview (1/2)

- John Cremona's database of elliptic curves is created by finding maps from $X_0(N)$ to elliptic curves with conductor N.

- We assume that $Q \in X_H(\mathbb{Q})$. We identify a weight 2 cusp form f for $H \cap \mathrm{SL}_2(\mathbb{Z})$ using Hecke operators.

- We compute the period lattice

$$\Lambda = \left\{ \int_z^{g(z)} f(s)\, ds : g \in H \cap \mathrm{SL}_2(\mathbb{Z}) \right\}.$$

Overview (2/2)

- Let α be the natural identification

$$\alpha : X_H(\mathbb{C}) \to \mathbb{H}^*/(H \cap \mathrm{SL}_2(\mathbb{Z})).$$

Overview (2/2)

- Let α be the natural identification

$$\alpha : X_H(\mathbb{C}) \to \mathbb{H}^*/(H \cap \mathrm{SL}_2(\mathbb{Z})).$$

- The map $X_H(\mathbb{C}) \to E(\mathbb{C})$ is the composition

$$X_H(\mathbb{C}) \to \mathbb{H}^*/(H \cap \mathrm{SL}_2(\mathbb{Z})) \to \mathbb{C}/\Lambda \to E(\mathbb{C}),$$

where the map from $\mathbb{H}^*/(H \cap \mathrm{SL}_2(\mathbb{Z})) \to \mathbb{C}/\Lambda$ is given by

$$P \mapsto \int_{\alpha(Q)}^{\alpha(P)} f(s)\, ds.$$

Steps in the main algorithm (1/2)

1. Use David Zywina's code to compute a model for X_H as the proj of a graded ring R of modular forms.

Steps in the main algorithm (1/2)

1. Use David Zywina's code to compute a model for X_H as the proj of a graded ring R of modular forms.
2. Test local solvability and find a rational base point.

Steps in the main algorithm (1/2)

1. Use David Zywina's code to compute a model for X_H as the proj of a graded ring R of modular forms.
2. Test local solvability and find a rational base point.
3. (*) Use Hecke operators to identify a weight 2 cusp form f corresponding to each isogeny class of rank zero $E/\mathbb{Q}$.

Steps in the main algorithm (1/2)

1. Use David Zywina's code to compute a model for X_H as the proj of a graded ring R of modular forms.
2. Test local solvability and find a rational base point.
3. (*) Use Hecke operators to identify a weight 2 cusp form f corresponding to each isogeny class of rank zero $E/\mathbb{Q}$.
4. Compute 20 periods for each f.

Steps in the main algorithm (1/2)

1. Use David Zywina's code to compute a model for X_H as the proj of a graded ring R of modular forms.
2. Test local solvability and find a rational base point.
3. (*) Use Hecke operators to identify a weight 2 cusp form f corresponding to each isogeny class of rank zero $E/\mathbb{Q}$.
4. Compute 20 periods for each f.
5. (*) Guess the period lattice for each f.

Steps in the main algorithm (1/2)

1. Use David Zywina's code to compute a model for X_H as the proj of a graded ring R of modular forms.
2. Test local solvability and find a rational base point.
3. (*) Use Hecke operators to identify a weight 2 cusp form f corresponding to each isogeny class of rank zero $E/\mathbb{Q}$.
4. Compute 20 periods for each f.
5. (*) Guess the period lattice for each f.
6. (*) For each f, identify the optimal elliptic curve in the isogeny class and compute the Manin constant c.

Steps in the main algorithm (1/2)

1. Use David Zywina's code to compute a model for X_H as the proj of a graded ring R of modular forms.
2. Test local solvability and find a rational base point.
3. (*) Use Hecke operators to identify a weight 2 cusp form f corresponding to each isogeny class of rank zero $E/\mathbb{Q}$.
4. Compute 20 periods for each f.
5. (*) Guess the period lattice for each f.
6. (*) For each f, identify the optimal elliptic curve in the isogeny class and compute the Manin constant c.
7. Compute degrees of the maps to the elliptic curves, and pick the elliptic curve E' and modular form f for which the degree is minimal.

Steps in the main algorithm (2/2)

8. (*) Compute the Fourier expansion of $P \mapsto \int_\infty^P cf\, ds$ at all cusps.

Steps in the main algorithm (2/2)

8. (*) Compute the Fourier expansion of $P \mapsto \int_\infty^P cf\, ds$ at all cusps.
9. Compute Fourier expansions of the functions $x, y : X_H \to E'$ coming from the map that sends ∞ to $(0 : 1 : 0)$.

Steps in the main algorithm (2/2)

8. (*) Compute the Fourier expansion of $P \mapsto \int_\infty^P cf\, ds$ at all cusps.
9. Compute Fourier expansions of the functions $x, y : X_H \to E'$ coming from the map that sends ∞ to $(0 : 1 : 0)$.
10. (*) Express x and y in terms of elements of $R \otimes \mathbb{Q}(\zeta_N)$ and compute $x(Q)$ and $y(Q)$. Translate to obtain $x', y' : X_H \to E'$.

Steps in the main algorithm (2/2)

8. (*) Compute the Fourier expansion of $P \mapsto \int_\infty^P cf\, ds$ at all cusps.
9. Compute Fourier expansions of the functions $x, y : X_H \to E'$ coming from the map that sends ∞ to $(0 : 1 : 0)$.
10. (*) Express x and y in terms of elements of $R \otimes \mathbb{Q}(\zeta_N)$ and compute $x(Q)$ and $y(Q)$. Translate to obtain $x', y' : X_H \to E'$.
11. (*) Express x' and y' in terms of elements of R.

Steps in the main algorithm (2/2)

8. (*) Compute the Fourier expansion of $P \mapsto \int_\infty^P cf\, ds$ at all cusps.
9. Compute Fourier expansions of the functions $x, y : X_H \to E'$ coming from the map that sends ∞ to $(0 : 1 : 0)$.
10. (*) Express x and y in terms of elements of $R \otimes \mathbb{Q}(\zeta_N)$ and compute $x(Q)$ and $y(Q)$. Translate to obtain $x', y' : X_H \to E'$.
11. (*) Express x' and y' in terms of elements of R.
12. Check that the obtained map $\phi : X_H \to E'$ works.

Steps in the main algorithm (2/2)

8. (*) Compute the Fourier expansion of $P \mapsto \int_\infty^P cf\, ds$ at all cusps.
9. Compute Fourier expansions of the functions $x, y : X_H \to E'$ coming from the map that sends ∞ to $(0 : 1 : 0)$.
10. (*) Express x and y in terms of elements of $R \otimes \mathbb{Q}(\zeta_N)$ and compute $x(Q)$ and $y(Q)$. Translate to obtain $x', y' : X_H \to E'$.
11. (*) Express x' and y' in terms of elements of R.
12. Check that the obtained map $\phi : X_H \to E'$ works.
13. Determine $X_G(\mathbb{Q}) = \bigcup_{T \in E'(\mathbb{Q})} \phi^{-1}(T)$.

Steps in the main algorithm (2/2)

8. (*) Compute the Fourier expansion of $P \mapsto \int_\infty^P cf\, ds$ at all cusps.
9. Compute Fourier expansions of the functions $x, y : X_H \to E'$ coming from the map that sends ∞ to $(0 : 1 : 0)$.
10. (*) Express x and y in terms of elements of $R \otimes \mathbb{Q}(\zeta_N)$ and compute $x(Q)$ and $y(Q)$. Translate to obtain $x', y' : X_H \to E'$.
11. (*) Express x' and y' in terms of elements of R.
12. Check that the obtained map $\phi : X_H \to E'$ works.
13. Determine $X_G(\mathbb{Q}) = \bigcup_{T \in E'(\mathbb{Q})} \phi^{-1}(T)$.
14. Compute $j(P)$ for $P \in X_H(\mathbb{Q})$.

Step 13: How to compute $\phi^{-1}(T)$?

- Given $\phi : X_H \to E'$ and $T \in E'(\mathbb{Q})$, let Z be the preimage scheme of T. How do we determine $Z(\mathbb{Q})$?

Step 13: How to compute $\phi^{-1}(T)$?

• Given $\phi : X_H \to E'$ and $T \in E'(\mathbb{Q})$, let Z be the preimage scheme of T. How do we determine $Z(\mathbb{Q})$?

• If Z has no $\mathbb{F}_p$-rational singular points, then Hensel lifting gives a bijection $Z(\mathbb{F}_p) \to Z(\mathbb{Q}_p)$.

Step 13: How to compute $\phi^{-1}(T)$?

• Given $\phi : X_H \to E'$ and $T \in E'(\mathbb{Q})$, let Z be the preimage scheme of T. How do we determine $Z(\mathbb{Q})$?

• If Z has no $\mathbb{F}_p$-rational singular points, then Hensel lifting gives a bijection $Z(\mathbb{F}_p) \to Z(\mathbb{Q}_p)$.

• See if lifts of points in $Z(\mathbb{F}_p)$ yield points of low height in $Z(\mathbb{Q})$. This gives a lower bound on $|Z(\mathbb{Q})|$.

Step 13: How to compute $\phi^{-1}(T)$?

• Given $\phi : X_H \to E'$ and $T \in E'(\mathbb{Q})$, let Z be the preimage scheme of T. How do we determine $Z(\mathbb{Q})$?

• If Z has no $\mathbb{F}_p$-rational singular points, then Hensel lifting gives a bijection $Z(\mathbb{F}_p) \to Z(\mathbb{Q}_p)$.

• See if lifts of points in $Z(\mathbb{F}_p)$ yield points of low height in $Z(\mathbb{Q})$. This gives a lower bound on $|Z(\mathbb{Q})|$.

• For good primes $\ell > p$,

$$|Z(\mathbb{Q})| \leq |Z(\mathbb{Q}_\ell)| = |Z(\mathbb{F}_\ell)|.$$

Search for ℓ where the upper bound matches our lower bound.

Results

- We run our algorithm in 613 cases and the total runtime was about 79 CPU hours. There were 28 failures.

Results

• We run our algorithm in 613 cases and the total runtime was about 79 CPU hours. There were 28 failures.

• In 23 cases, the failure was a result of insufficient power series precision and rerunning with more precision led to success.

Results

• We run our algorithm in 613 cases and the total runtime was about 79 CPU hours. There were 28 failures.

• In 23 cases, the failure was a result of insufficient power series precision and rerunning with more precision led to success.

• In 3 cases, no rational base point is found and the computation fails.

Results

• We run our algorithm in 613 cases and the total runtime was about 79 CPU hours. There were 28 failures.

• In 23 cases, the failure was a result of insufficient power series precision and rerunning with more precision led to success.

• In 3 cases, no rational base point is found and the computation fails.

• In one genus 11 case, the periods computed did not generate the period lattice. In one genus 50 case, the computation in Step 13 failed.

Bonus: a map to an elliptic curve over $\mathbb{Q}(\sqrt{-3})$

- Let X_H be the modular curve parametrizing elliptic curves whose mod 3 image of Galois is contained in the normalizer of the non-split Cartan and mod 7 image of Galois is contained in the normalizer of the split Cartan.

Bonus: a map to an elliptic curve over $\mathbb{Q}(\sqrt{-3})$

• Let X_H be the modular curve parametrizing elliptic curves whose mod 3 image of Galois is contained in the normalizer of the non-split Cartan and mod 7 image of Galois is contained in the normalizer of the split Cartan.

• We have $J(X_H) \sim E \times A$, where E is a rank one elliptic curve, and A is a rank zero abelian surface that factors as the square of an elliptic curve E' over $\mathbb{Q}(\sqrt{-3})$.

Bonus: a map to an elliptic curve over $\mathbb{Q}(\sqrt{-3})$

• Let X_H be the modular curve parametrizing elliptic curves whose mod 3 image of Galois is contained in the normalizer of the non-split Cartan and mod 7 image of Galois is contained in the normalizer of the split Cartan.

• We have $J(X_H) \sim E \times A$, where E is a rank one elliptic curve, and A is a rank zero abelian surface that factors as the square of an elliptic curve E' over $\mathbb{Q}(\sqrt{-3})$.

• We find a degree 6 map $\phi : X_H \to E'$ defined over $\mathbb{Q}(\sqrt{-3})$ and use this to determine $X_H(\mathbb{Q}(\sqrt{-3}))$.

Summary

- More than 99% of modular curves X_H of level ≤ 70 admit a map to rank zero elliptic curve E.

Summary

• More than 99% of modular curves X_H of level ≤ 70 admit a map to rank zero elliptic curve E.

• We compute these maps and use this to determine $j(X_H(\mathbb{Q}))$ for all but 10 such modular curves.

Thank you!