Twist-parametrized points on modular curves

Filip Najman

joint work with Maarten Derickx, Sachi Hashimoto, and Ari Shnidman

ChaBONNty conference, June 30th 2026

This work was supported by the Croatian Science Foundation under the project number HRZZ IP-2022-10-5008.

Upcoming conference in Opatija

Modular curves and Applications of AI to Number Theory

September 14–18, 2026 · Opatija, Croatia

Themes

- Modular curves and Galois representations attached to elliptic curves.
- Applications of Artificial Intelligence to Number Theory.

Practical information

- No registration fee.
- Registration deadline: July 15.
- Limited space for short contributed talks.

Invited speakers:

Jennifer Balakrishnan, Abbey Bourdon, Kathrin Bringmann, Sachi Hashimoto, Daeyeol Jeon, Davide Lombardo, Álvaro Lozano-Robledo, Bartosz Naskręcki, Ken Ono, Pierre Parent, Alexey Pozdnyakov, Domagoj Vlah.

▸ Conference webpage and registration

Galois representations attached to elliptic curves

Let $E/\mathbb{Q}$ be an elliptic curve. For $n \geq 1$,

$$E[n] := \{P \in E(\overline{\mathbb{Q}}) : nP = 0\} \simeq (\mathbb{Z}/n\mathbb{Z})^2.$$

The group $\mathrm{Gal}_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $E[n]$

$$\rho_{E,n} : \mathrm{Gal}_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(E[n]) \simeq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}),$$

giving the mod n Galois representataion attached to E, which is well defined after choosing a basis of $E[n]$.

Putting all n together, we get the adelic Galois representation attached to E, coming from the action of $\mathrm{Gal}_{\mathbb{Q}}$ on $T(E) := \varprojlim_n E[n]$:

$$\rho_E : \mathrm{Gal}_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\widehat{\mathbb{Z}}).$$

Write

$$G_E := \mathrm{im}(\rho_E) \leq \mathrm{GL}_2(\widehat{\mathbb{Z}}).$$

Modular curves as detectors of Galois images

For an elliptic curve $E/\mathbb{Q}$ and an open $G \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$, if

$$G_E \leq G,$$

then E gives a rational point on the modular curve X_G:

$$E/\mathbb{Q}, \quad G_E \leq G \rightsquigarrow \quad x_E \in X_G(\mathbb{Q}).$$

Important point

Classifying non-CM adelic images G_E is a rational-points problem on modular curves.

Simplifying convention

Throughout the talk, rational points on modular curves will mean non-CM non-cuspidal points.

Images of Galois

Theorem (Serre's open image theorem)

For a non-CM $E/\mathbb{Q}$, it holds that $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E] < \infty$, so G_E is an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

It follows that for non-CM $E/\mathbb{Q}$, there exists C_E such that

$$\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \quad \text{for all primes} \quad \ell \geq C_E.$$

Serre's uniformity problem/conjecture

There is a C such that for all primes $\ell \geq C$ and $E/\mathbb{Q}$ without CM $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

Explicit Serre's uniformity conjecture (Zywina/Sutherland '16)

If E is a non-CM elliptic curve over $\mathbb{Q}$ and $\ell > 13$ is a prime, then $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ or

$$(\ell, j(E)) \in \left\{(17, -17^2 \cdot 101^3/2), (17, -17 \cdot 373^3/2^{17}), (37, -7 \cdot 11^3), (37, -7 \cdot 137^3 \cdot 2083^3)\right\}.$$

Mazur's torsion theorem

Mazur's torsion theorem

$$\{E(\mathbb{Q})_{\mathrm{tors}}\} = \{\mathbb{Z}/n\mathbb{Z},\ n = 1, \ldots, 10, 12\} \cup \{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ n = 1, \ldots, 4\}.$$

A rational point $P \in E(\mathbb{Q})$ of order N means

$$\sigma(P) = P \quad \forall \sigma \in \mathrm{Gal}_{\mathbb{Q}}\,.$$

Thus the mod-N image fixes a basis point:

$$\rho_{E,N}(\mathrm{Gal}_{\mathbb{Q}}) \leq \mathrm{Stab}(P) \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

The modular curve $X_1(N)$ classifies pairs

$$(E, P), \qquad P \text{ of order } N.$$

Mazur determined exactly which $X_1(N)$ have non-cuspidal rational points.

Mazur's Program B as a generalization

Replace "find all images fixing a a torsion point" by "find all images".

Mazur's Program B: three versions

Mazur's Program B (original version)

Given a number field K and a subgroup $H \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$, classify elliptic curves E/K such that $\rho_E(\mathrm{Gal}_K) \leq H$. Equivalently, find all the K-rational points on the modular curve X_H.

1. **Algorithmic version.** Construct an algorithm that given K and H, determines $X_H(K)$.
2. **Parameterization version.** Determine or parametrize all possible adelic images G_E over $\mathbb{Q}$ or equivalently determine or parameterize all non-CM rational points on all modular curves.
3. **Geometric explanation version.** Explain why the rational points exist. Is there a reason they exist, are they forced by cusps, CM points, maps between modular curves, or other geometric constructions?

Main result

Assuming standard conjectures about Galois representations, we prove the "best possible" parameterization version, and give an affirmative answer to (3).

Problems

For most of the remainder of the talk I will focus on parametrizing the adelic images G_E. There are infinitely many modular curves X_G, of arbitrarily high genus.

Among the modular curves with rational points, there are both infinitely many modular curves X_G such that:

$$\#X_G(\mathbb{Q}) = \infty \qquad \text{and} \qquad 0 < \#X_G(\mathbb{Q}) < \infty.$$

Need an organizing principle

Not a finite list of curves, so we need a finite way to organize the infinite data we have.

Motivating example

Let $E/\mathbb{Q}$ be an elliptic curve with a 25-isogeny:

$$x \in X_0(25)(\mathbb{Q}), \qquad x = (E, \alpha),$$

$$X_0(25) \simeq \mathbb{P}^1.$$

By assumption $G_E \leq B_0(25)$, which is an index 120 subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

X_{G_E} is again a modular curve.

Question

What should we expect the genus $g(X_{G_E})$ to be?

Motivating example

Label	Class	Class size	CM	Adelic index	Adelic genus	Weierstrass equation
11.a1	11.a	3		1200	37	$y^2 + y = x^3 - x^2 - 7820x - 263580$
99.d1	99.d	3		1200	37	$y^2 + y = x^3 - 70383x + 7187035$
121.d1	121.d	3		1200	37	$y^2 + y = x^3 - x^2 - 946260x + 354609639$
176.b1	176.b	3		1200	37	$y^2 = x^3 + x^2 - 125125x + 16994227$
275.b1	275.b	3		1200	37	$y^2 + y = x^3 + x^2 - 195508x - 33338481$
539.a1	539.a	3		1200	37	$y^2 + y = x^3 + x^2 - 383196x + 91174234$
550.e1	550.e	3		1200	37	$y^2 + xy + y = x^3 - 758201x + 254051548$
550.j1	550.j	3		1200	37	$y^2 + xy + y = x^3 + x^2 - 30328x + 2020281$
704.c1	704.c	3		1200	37	$y^2 = x^3 - x^2 - 31281x + 2139919$
704.h1	704.h	3		1200	37	$y^2 = x^3 + x^2 - 31281x - 2139919$
1089.b1	1089.b	3		1200	37	$y^2 + y = x^3 - 8516343x - 9565943918$
1342.b1	1342.b	3		1200	37	$y^2 + xy + y = x^3 + x^2 - 117257250x - 488766109679$
1584.g1	1584.g	3		1200	37	$y^2 = x^3 - 1126128x - 459970256$
1859.b1	1859.b	3		1200	37	$y^2 + y = x^3 - x^2 - 1321636x - 584371175$
1936.i1	1936.i	3		1200	37	$y^2 = x^3 + x^2 - 15140165x - 22679876749$
2475.a1	2475.a	3		1200	37	$y^2 + y = x^3 - 1759575x + 898379406$
3025.a1	3025.a	3		1200	37	$y^2 + y = x^3 + x^2 - 23656508x + 44278891894$
3179.a1	3179.a	3		1200	37	$y^2 + y = x^3 + x^2 - 2260076x - 1308527588$
3971.b1	3971.b	3		1200	37	$y^2 + y = x^3 + x^2 - 2823140x + 1824832093$
4400.i1	4400.i	3		1200	37	$y^2 = x^3 - x^2 - 3128133x + 2130534637$
4400.k1	4400.k	3		1200	37	$y^2 = x^3 - x^2 - 12131208x - 16259299088$

The genus is (at least) 37, much larger than prescribed. Also $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E] \geq 1200$.

Rational point lift to a rational points on a twist

Suppose $G \trianglelefteq H \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$, so

$$\pi : X_G \longrightarrow X_H$$

is a modular cover with

$$T = H/G.$$

If $x \in X_H(\mathbb{Q})$, then T acts on the fiber $\pi^{-1}(x)$, so Galois permutes its points via a character $\psi_x : \mathrm{Gal}_{\mathbb{Q}} \longrightarrow T$.

Twisting principle

Twisting the cover by ψ_x gives a new curve

$$X_G^{\psi_x} \longrightarrow X_H$$

for which the point x does lift to a rational point:

$$\widetilde{x} \in X_G^{\psi_x}(\mathbb{Q}), \qquad \pi(\widetilde{x}) = x.$$

Explanation: Abelian twists of modular curves are again modular curves

The map $X_1(25) \longrightarrow X_0(25)$ is abelian

$$\implies \quad x \in X_0(25)(\mathbb{Q}) \text{ lifts to a rational point } x' \in X_1(25)^{\psi}(\mathbb{Q})$$

on some abelian twist of $X_1(25)$, which has genus 12.

Key mechanism over $\mathbb{Q}$

Abelian twists of modular curves are again modular curves. This is true only over $\mathbb{Q}$, and essentially relies on the Kronecker-Weber theorem.

So for a $G \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ and a character ψ, there exists a twisted group $G^{\psi} \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ of G such that $X_G^{\psi} = X_{G^{\psi}}$.

This implies that for our curve E we have $G_E \leq G^{\psi}$, where $G^{\psi} \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ is the group corresponding to $X_1(25)^{\psi}$.

Abelian twists of modular curves are modular curves over $\mathbb{Q}$

Recall that $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E]$ is always divisible by 2, even though for density-one set of elliptic curves $E/\mathbb{Q}$, each local projection $G_E \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$ is surjective.

This can be seen in this language by the fact that there is an index 2 subgroup $Ns(2) \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$, so the corresponding modular map $X_{\mathrm{ns}}(2) \longrightarrow X(1)$ is abelian.

So any elliptic curve E lifts to a rational point on $X_{\mathrm{ns}}(2)^\psi$, for some abelian twist ψ, corresponding to a subgroup $G^\psi \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ of index 2. So $G_E \leq G^\psi$.

This is also true for the elliptic curve in our example, so it follows that E induces a rational point on the normalization of

$$X_{\mathrm{ns}}(2)^{\psi_1} \times_{X(1)} X_1(25)^{\psi_2}$$

for some abelian characters ψ_1, ψ_2. This curve is of genus 37.

Twist families

Suppose

$$G \trianglelefteq H \leq \mathrm{GL}_2(\widehat{\mathbb{Z}}), \qquad T := H/G \text{ finite abelian.}$$

Then we have an abelian modular cover $X_G \longrightarrow X_H$.

So any rational point $x \in X_H(\mathbb{Q})$, lifts to some $\tilde{x} \in X_G^{\psi_x}(\mathbb{Q})$ for some

$$\psi_x : \mathrm{Gal}_{\mathbb{Q}} \longrightarrow T.$$

Important point

So even though all the $\tilde{x}$ live on (a priori) different curves, they are all "tied together" by the bottom curve X_G.

Twist-parametrized and twist-isolated points

Definition (Twist-parameterized and twist-isolated curves)

Let $G \leq H \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ be open subgroups.

1. X_G is *twist parameterized over* X_H if $\pi : X_G \to X_H$ is abelian and $\#X_H(\mathbb{Q}) = \infty$.
2. For a group $G \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$, we say that X_G is *twist parameterized* if there exists a group $G \leq H \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ such that X_G is twist parameterized over X_H.
3. If X_G is not twist parameterized, we say that it is *twist isolated*.

Definition (Twist-parameterized and twist-isolated points)

1. If X_G is twist isolated, any point $x \in X_G(\mathbb{Q})$ is a *twist-isolated point* on X_G. If X_G is twist parameterized, any point $x \in X_G(\mathbb{Q})$ is a *twist-parameterized point* on X_G.
2. A non-CM j-invariant $j_0 \in \mathbb{Q}$ is *twist isolated* if there exists an open $G \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ such that $x \in X_G(\mathbb{Q})$ with $j(x) = j_0$, and X_G is twist isolated.
3. A non-CM j-invariant $j_0 \in \mathbb{Q}$ is *twist parameterized* if it is not twist isolated.

Zywina's agreeable closure

Agreeable groups

There is an operator $G \mapsto G^{\mathrm{ag}}$ that to an open $G \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ adjoins an overgroup $G \leq G^{\mathrm{ag}} \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ that is called the agreeable closure. A group is agreeable if $G^{\mathrm{ag}} = G$.

For each open subgroup G, the group G^{ag}, satisfies:

1. G^{ag} is agreeable.
2. G^{ag} is the smallest agreeable overgroup of G.
3. $[G^{\mathrm{ag}}, G^{\mathrm{ag}}] = [G, G]$.

Hence $X_G \longrightarrow X_{G^{\mathrm{ag}}}$ is abelian, and is universal among agreeable groups.

Theorem (Zywina)

Assuming Serre's uniformity conjecture, there are finitely many G_E^{ag}.

So, although there are infinitely many X_G with rational points, they lie in finitely many twist families.

Twist isolated points

One can easily show that any twist-isolated j-invariant has to correspond to an "exceptional" rational point

$$x \in X_{G^{\mathrm{ag}}}(\mathbb{Q}) \quad \text{s.t.} \quad 0 < |X_{G^{\mathrm{ag}}}(\mathbb{Q})| < +\infty.$$

Zywina found 77 such j-invariants.

Conjecture (Zywina)

There are no other such j-invariants except the 77 already found.

To prove this conjecture, one needs to find all the rational points on many modular curves of genus ≥ 2 (perhaps using Chabauty).

Algorithm (DHNS)

Algorithm (DHNS). Given $j \in \mathbb{Q}$, determines whether j is twist parametrized.

Using this algorithm show that $41/77$ exceptional j-invariants are TI.

Main theorem

Theorem (DHNS)

Assume Zywina's conjecture and Explicit Serre's uniformity conjecture. Then there are 160 explicit pairs

$$K_i \trianglelefteq M_i \leq \mathrm{GL}_2(\widehat{\mathbb{Z}}), \qquad 1 \leq i \leq 160,$$

such that

$$T_i := M_i/K_i$$

is finite abelian, and such that for every non-CM $E/\mathbb{Q}$ there exist

$$i \in \{1, \ldots, 160\}, \qquad x \in X_{M_i}(\mathbb{Q}), \qquad x = (E, \alpha),$$

and a character $\psi_x : \mathrm{Gal}_{\mathbb{Q}} \longrightarrow T_i$ such that

$$G_E \sim K_i^{\psi_x}.$$

Numerology

$$\boxed{160 = 138 + 22}$$

138 : bases with infinitely many rational points,
22 : finite-base families over which the twist-isolated points live.

1. The largest genus of X_{K_i} is 97.
2. The largest genus of X_{K_i} with $\#X_{M_i} = \infty$, and the second largest genus appearing is 53.
3. The largest genus of X_{M_i} is 7.

A second theorem: rational points explained by geometry

The only $X_1(N)$ that have rational points are those that have to because they have genus 0.

The only $X_0(N)$ that have rational points are those that have genus 0, CM points, or forced by cusps and automorphisms.

Mazur–Ogg philosophy

Rational points on modular curves exist for geometric reasons.

Start with special points: cusps and CM points. Then close under geometric operations:

push-forward abelian lifts collinearity fiber splicing

Theorem (DHNS)

Assume Zywina's conecture and Explicit Serre's uniformity conjecture. Every rational point on every modular curve over $\mathbb{Q}$ is explained by geometry in this formal sense.

The end

Thank you!