More about the p-adic images of Galois for elliptic curves over $\mathbb{Q}$

Davide Lombardo
Università di Pisa

joint with
Matthew Bisatt & Lorenzo Furio

Schney,
31 July 2025

Galois representations of elliptic curves

Let $E/\mathbb{Q}$ be an elliptic curve. For every prime p and $n \geq 1$ we have the mod-p^n Galois representation

$$\rho_{E,p^n} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}\, E[p^n] \cong \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z}).$$

Galois representations of elliptic curves

Let $E/\mathbb{Q}$ be an elliptic curve. For every prime p and $n \geq 1$ we have the mod-p^n Galois representation

$$\rho_{E,p^n} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}\, E[p^n] \cong \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z}).$$

These can be combined into a p-adic representation

$$\rho_{E,p^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}\, T_pE \cong \mathrm{GL}_2(\mathbb{Z}_p).$$

Mazur's program B (vertical aspect)

Mazur's program B for p-adic representations

Fix a prime p. Classify the possible images of ρ_{E,p^∞}.

Mazur's program B (vertical aspect)

Mazur's program B for p-adic representations

Fix a prime p. Classify the possible images of ρ_{E,p^∞}.

Reformulation

Let $n \geq 1$ and $H < \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ be a subgroup with $\det H = (\mathbb{Z}/p^n\mathbb{Z})^\times$. Determine all (non-CM, non-cuspidal) rational points on $X_H(\mathbb{Q})$.

Mod-p representations

Lemma (Serre)

Let $p \geq 5$. If $\rho_{E,p}$ is surjective, then so is ρ_{E,p^∞}.

Mod-p representations

Lemma (Serre)

Let $p \geq 5$. If $\rho_{E,p}$ is surjective, then so is ρ_{E,p^∞}.

Theorem (Serre, Mazur, Bilu–Parent–Rebolledo)

For $p > 37$, $\rho_{E,p}$ is either surjective or has image contained in the normaliser of a non-split Cartan: $\left\{ \begin{pmatrix} a & b\varepsilon \\ \pm b & \pm a \end{pmatrix} \mid a^2 - \varepsilon b^2 \neq 0 \right\}$, *where* $\varepsilon \in \mathbb{F}_p^\times \setminus \mathbb{F}_p^{\times 2}$.

Mod-p representations

Lemma (Serre)

Let $p \geq 5$. If $\rho_{E,p}$ is surjective, then so is ρ_{E,p^∞}.

Theorem (Serre, Mazur, Bilu–Parent–Rebolledo)

For $p > 37$, $\rho_{E,p}$ is either surjective or has image contained in the normaliser of a non-split Cartan: $\left\{ \begin{pmatrix} a & b\varepsilon \\ \pm b & \pm a \end{pmatrix} \mid a^2 - \varepsilon b^2 \neq 0 \right\}$, *where* $\varepsilon \in \mathbb{F}_p^\times \setminus \mathbb{F}_p^{\times 2}$.

Theorem (Le Fourn-Lemos 2021, Furio-L. 2023)

For $p > 5$ and $\operatorname{Im} \rho_{E,p} \subseteq C_{ns}^+(p)$, then $\operatorname{Im} \rho_{E,p}$ is ***equal to*** *the normaliser of a non-split Cartan $C_{ns}^+(p)$.*

Mod-p representations

Lemma (Serre)

Let $p \geq 5$. If $\rho_{E,p}$ is surjective, then so is ρ_{E,p^∞}.

Theorem (Serre, Mazur, Bilu–Parent–Rebolledo)

For $p > 37$, $\rho_{E,p}$ is either surjective or has image contained in the normaliser of a non-split Cartan: $\left\{ \begin{pmatrix} a & b\varepsilon \\ \pm b & \pm a \end{pmatrix} \mid a^2 - \varepsilon b^2 \neq 0 \right\}$, *where* $\varepsilon \in \mathbb{F}_p^\times \setminus \mathbb{F}_p^{\times 2}$.

Theorem (Le Fourn-Lemos 2021, Furio-L. 2023)

For $p > 5$ and $\operatorname{Im} \rho_{E,p} \subseteq C_{ns}^+(p)$, then $\operatorname{Im} \rho_{E,p}$ is ***equal to*** *the normaliser of a non-split Cartan $C_{ns}^+(p)$.*

Primes up to 37: Zywina (2015) gives an almost complete classification apart from the non-split Cartan cases.

The normaliser of a non-split Cartan mod p^n

Set

$$C_{ns}^{+}(p^n) = \left\{ \begin{pmatrix} a & b\varepsilon \\ \pm b & \pm a \end{pmatrix} \mid a^2 - \varepsilon b^2 \in (\mathbb{Z}/p^n\mathbb{Z})^\times \right\}$$

and let $X_{ns}^{+}(p^n)$ be the corresponding modular curve.

The normaliser of a non-split Cartan mod p^n

Set

$$C_{ns}^{+}(p^n) = \left\{ \begin{pmatrix} a & b\varepsilon \\ \pm b & \pm a \end{pmatrix} \mid a^2 - \varepsilon b^2 \in (\mathbb{Z}/p^n\mathbb{Z})^\times \right\}$$

and let $X_{ns}^{+}(p^n)$ be the corresponding modular curve.

The computation of $X_{ns}^{+}(p^n)(\mathbb{Q})$ seems to be very hard.

Progress on Mazur's program B: small p

Recent (and less recent) exciting progress!

- $p = 2$: Rouse–Zureick-Brown (2015)
- Sutherland–Zywina (2017): modular curves of prime power levels with infinitely many rational points
- $p = 13, 17$: Kenku (1980), Balakrishnan–Dogra–Müller–Tuitman–Vonk (2019 and 2021)
- $p \in \{3, 5, 7, 11\}$: almost complete classification by Rouse–Sutherland–Zureick-Brown (2022)
- $p = 3$: Balakrishnan–Betts–Hast–Jha–Müller (2025)

State of the art

Table 2. *Arithmetically maximal groups of ℓ-power level with $\ell \leq 17$ for which $X_H(\mathbb{Q})$ is unknown; each has rank = genus, rational CM points, no rational cusps and no known exceptional points.*

BBHJM (2025)

Label	Level	Group	Genus
~~27.243.12.1~~	~~3^3~~	~~$N_{ns}(3^3)$~~	~~12~~
25.250.14.1	5^2	$N_{ns}(5^2)$	14
49.1029.69.1	7^2	$N_{ns}(7^2)$	69
49.147.9.1	7^2	$\langle \begin{bmatrix} 16 & 6 \\ 20 & 45 \end{bmatrix}, \begin{bmatrix} 20 & 17 \\ 40 & 36 \end{bmatrix} \rangle$	9
49.196.9.1	7^2	$\langle \begin{bmatrix} 42 & 3 \\ 16 & 31 \end{bmatrix}, \begin{bmatrix} 16 & 23 \\ 8 & 47 \end{bmatrix} \rangle$	9
121.6655.511.1	11^2	$N_{ns}(11^2)$	511

From the paper by Rouse–Sutherland–Zureick-Brown

State of the art

Table 2. *Arithmetically maximal groups of ℓ-power level with $\ell \leq 17$ for which $X_H(\mathbb{Q})$ is unknown; each has rank = genus, rational CM points, no rational cusps and no known exceptional points.*

Label	Level	Group	Genus
~~27.243.12.1~~	~~3^3~~	~~$N_{ns}(3^3)$~~ BBHJM (2025)	~~12~~
25.250.14.1	5^2	$N_{ns}(5^2)$	14
49.1029.69.1	7^2	$N_{ns}(7^2)$	69
49.147.9.1	7^2	$\left\langle \begin{bmatrix} 16 & 6 \\ 20 & 45 \end{bmatrix}, \begin{bmatrix} 20 & 17 \\ 40 & 36 \end{bmatrix} \right\rangle$	9
49.196.9.1	7^2	$\left\langle \begin{bmatrix} 42 & 3 \\ 16 & 31 \end{bmatrix}, \begin{bmatrix} 16 & 23 \\ 8 & 47 \end{bmatrix} \right\rangle$	9
121.6655.511.1	11^2	$N_{ns}(11^2)$	511

From the paper by Rouse–Sutherland–Zureick-Brown

(+*15 pages* of tables of curves on which they are successful!)

Main question

What can we say about the p-adic image of Galois (especially assuming that $\rho_{E,p}$ has image $C_{ns}^{+}(p)$)?

7-adic representations

Theorem (Furio-L.)

1. *The set* $X_{ns}^{+}(49)(\mathbb{Q})$ *consists of CM points.*

7-adic representations

Theorem (Furio-L.)

1. *The set* $X_{ns}^{+}(49)(\mathbb{Q})$ *consists of CM points.*
2. *Let*

$$C: x^4 + 3x^3y - 3x^2yz - 3x^2z^2 + 6xy^3 - 6xy^2z + 3xyz^2 - 2xz^3 + 4y^4 + 2y^3z - 5yz^3 = 0.$$

If $\#C(\mathbb{Q}) = 4$*, then both* $X_{ns}^{\#}(49)(\mathbb{Q})$ *and* $X_{sp}^{\#}(49)(\mathbb{Q})$ *consist of CM points.*

7-adic representations

Theorem (Furio-L.)

1. *The set* $X_{ns}^{+}(49)(\mathbb{Q})$ *consists of CM points.*
2. *Let*

$$C : x^4 + 3x^3y - 3x^2yz - 3x^2z^2 + 6xy^3 - 6xy^2z + 3xyz^2 - 2xz^3 + 4y^4 + 2y^3z - 5yz^3 = 0.$$

If $\#C(\mathbb{Q}) = 4$*, then both* $X_{ns}^{\#}(49)(\mathbb{Q})$ *and* $X_{sp}^{\#}(49)(\mathbb{Q})$ *consist of CM points.*

Corollary

Unconditionally, the image of $\rho_{E,7^\infty}$ *is the inverse image in* $\mathrm{GL}_2(\mathbb{Z}_7)$ *of* $\rho_{E,49}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$.

p-adic representations for $p > 7$

Theorem (Bisatt-Furio-L., 2025+)

Let $p > 7$ and suppose that $\operatorname{Im} \rho_{E,p} \subseteq C_{ns}^{+}(p)$. Then there exists $n \geq 1$ such that $\operatorname{Im} \rho_{E,p^\infty}$ is the inverse image in $\mathrm{GL}_2(\mathbb{Z}_p)$ of $C_{ns}^{+}(p^n)$.

p-adic representations for $p > 7$

Theorem (Bisatt-Furio-L., 2025+)

Let $p > 7$ and suppose that $\operatorname{Im} \rho_{E,p} \subseteq C_{ns}^{+}(p)$. Then there exists $n \geq 1$ such that $\operatorname{Im} \rho_{E,p^\infty}$ is the inverse image in $\mathrm{GL}_2(\mathbb{Z}_p)$ of $C_{ns}^{+}(p^n)$.

Corollary

The index of the adelic representation attached to E is $\ll h(E)^{2+o(1)}$ as $h(E) \to \infty$.

Classification of p-adic representations: group theory

Group theory $+\varepsilon$

Let $\pi_k : \mathrm{GL}_2(\mathbb{Z}_p) \to \mathrm{GL}_2(\mathbb{Z}/p^k\mathbb{Z})$ be the canonical projections.

Theorem (Zywina, Furio)

Let $p \geq 7$ and assume $\operatorname{Im} \rho_{E,p} = C_{ns}^{+}(p)$. One of the following holds:

1. *There exists $n \geq 1$ such that $\operatorname{Im} \rho_{E,p^\infty} = \pi_n^{-1}\left(C_{ns}^{+}(p^n)\right)$;*

Group theory $+\varepsilon$

Let $\pi_k : \mathrm{GL}_2(\mathbb{Z}_p) \to \mathrm{GL}_2(\mathbb{Z}/p^k\mathbb{Z})$ be the canonical projections.

Theorem (Zywina, Furio)

Let $p \geq 7$ and assume $\operatorname{Im} \rho_{E,p} = C_{ns}^{+}(p)$. One of the following holds:

1. *There exists $n \geq 1$ such that $\operatorname{Im} \rho_{E,p^\infty} = \pi_n^{-1}\left(C_{ns}^{+}(p^n)\right)$;*
2. $\operatorname{Im} \rho_{E,p^\infty} = \pi_2^{-1}\left(G_{ns}^{\#}(p^2)\right)$, *where*

Group theory $+\varepsilon$

Let $\pi_k : \mathrm{GL}_2(\mathbb{Z}_p) \to \mathrm{GL}_2(\mathbb{Z}/p^k\mathbb{Z})$ be the canonical projections.

Theorem (Zywina, Furio)

Let $p \geq 7$ and assume $\operatorname{Im} \rho_{E,p} = C_{ns}^{+}(p)$. One of the following holds:

1. *There exists $n \geq 1$ such that $\operatorname{Im} \rho_{E,p^\infty} = \pi_n^{-1}\left(C_{ns}^{+}(p^n)\right)$;*
2. $\operatorname{Im} \rho_{E,p^\infty} = \pi_2^{-1}\left(G_{ns}^{\#}(p^2)\right)$, *where*

$$G_{ns}^{\#}(p^2) = C_{ns}^{+}(p) \rtimes V, \quad V = \mathrm{Id} + p \begin{pmatrix} a & b\varepsilon \\ -b & c \end{pmatrix}.$$

Group theory $+\varepsilon$

Sketch of proof.

Let $G := \operatorname{Im} \rho_{E,p^\infty}$. The sequence

$$1 \to \ker(G(p^2) \to G(p)) \to G(p^2) \to G(p) \to 1$$

shows that $G(p) = C_{ns}^+(p)$ acts by conjugation on $\ker(G(p^2) \to G(p))$,

Group theory $+\varepsilon$

Sketch of proof.

Let $G := \operatorname{Im} \rho_{E,p^\infty}$. The sequence

$$1 \to \ker(G(p^2) \to G(p)) \to G(p^2) \to G(p) \to 1$$

shows that $G(p) = C_{ns}^+(p)$ acts by conjugation on $\ker(G(p^2) \to G(p))$, so this kernel is a $C_{ns}^+(p)$-stable subspace of

$$\mathrm{M}_2(\mathbb{F}_p) \cong V_1 \oplus V_2 \oplus V_3,$$

Group theory $+\varepsilon$

Sketch of proof.

Let $G := \operatorname{Im} \rho_{E,p^\infty}$. The sequence

$$1 \to \ker(G(p^2) \to G(p)) \to G(p^2) \to G(p) \to 1$$

shows that $G(p) = C_{ns}^+(p)$ acts by conjugation on $\ker(G(p^2) \to G(p))$, so this kernel is a $C_{ns}^+(p)$-stable subspace of

$$\mathrm{M}_2(\mathbb{F}_p) \cong V_1 \oplus V_2 \oplus V_3,$$

$$V_1 = \mathbb{F}_p \cdot \mathrm{Id}, \qquad V_2 = \mathbb{F}_p \cdot \begin{pmatrix} 0 & \varepsilon \\ 1 & 0 \end{pmatrix}, \qquad V_3 = \mathbb{F}_p \cdot \left\langle \begin{pmatrix} 0 & \varepsilon \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle.$$

Group theory $+\varepsilon$

Sketch of proof.

Let $G := \operatorname{Im} \rho_{E,p^\infty}$. The sequence

$$1 \to \ker(G(p^2) \to G(p)) \to G(p^2) \to G(p) \to 1$$

shows that $G(p) = C_{ns}^{+}(p)$ acts by conjugation on $\ker(G(p^2) \to G(p))$, so this kernel is a $C_{ns}^{+}(p)$-stable subspace of

$$\mathrm{M}_2(\mathbb{F}_p) \cong V_1 \oplus V_2 \oplus V_3,$$

$$V_1 = \mathbb{F}_p \cdot \mathrm{Id}, \qquad V_2 = \mathbb{F}_p \cdot \begin{pmatrix} 0 & \varepsilon \\ 1 & 0 \end{pmatrix}, \qquad V_3 = \mathbb{F}_p \cdot \left\langle \begin{pmatrix} 0 & \varepsilon \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle.$$

Now $V_1 \oplus V_2$ gives $C_{ns}^{+}(p^2)$, while $V_1 \oplus V_3$ gives $G_{ns}^{\#}(p^2)$.

Group theory $+\varepsilon$

Sketch of proof.

Let $G := \operatorname{Im} \rho_{E,p^\infty}$. The sequence

$$1 \to \ker(G(p^2) \to G(p)) \to G(p^2) \to G(p) \to 1$$

shows that $G(p) = C_{ns}^+(p)$ acts by conjugation on $\ker(G(p^2) \to G(p))$, so this kernel is a $C_{ns}^+(p)$-stable subspace of

$$\mathrm{M}_2(\mathbb{F}_p) \cong V_1 \oplus V_2 \oplus V_3,$$

$$V_1 = \mathbb{F}_p \cdot \mathrm{Id}, \qquad V_2 = \mathbb{F}_p \cdot \begin{pmatrix} 0 & \varepsilon \\ 1 & 0 \end{pmatrix}, \qquad V_3 = \mathbb{F}_p \cdot \left\langle \begin{pmatrix} 0 & \varepsilon \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle.$$

Now $V_1 \oplus V_2$ gives $C_{ns}^+(p^2)$, while $V_1 \oplus V_3$ gives $G_{ns}^{\#}(p^2)$. To conclude the classification, one also needs information about the existence of sufficiently many homotheties in ρ_{E,p^∞}. □

Classification of p-adic representations: local analysis

p-adic classification

Theorem (Bisatt-Furio-L., 2025+)

Let $p > 7$ and suppose that $\operatorname{Im} \rho_{E,p} \subset C_{ns}^{+}(p)$. Then there exists $n \geq 1$ such that

$$\operatorname{Im} \rho_{E,p^\infty} = \pi_n^{-1}\left(C_{ns}^{+}(p^n)\right),$$

where

$$\pi_n : \mathrm{GL}_2(\mathbb{Z}_p) \to \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$$

is the canonical projection.

p-adic classification

Theorem (Bisatt-Furio-L., 2025+)

Let $p > 7$ and suppose that $\operatorname{Im} \rho_{E,p} \subset C_{ns}^{+}(p)$. Then there exists $n \geq 1$ such that

$$\operatorname{Im} \rho_{E,p^\infty} = \pi_n^{-1}\left(C_{ns}^{+}(p^n)\right),$$

where

$$\pi_n : \mathrm{GL}_2(\mathbb{Z}_p) \to \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$$

is the canonical projection.

1. Work locally over $\mathbb{Q}_p$

p-adic classification

Theorem (Bisatt-Furio-L., 2025+)

Let $p > 7$ and suppose that $\operatorname{Im} \rho_{E,p} \subset C_{ns}^+(p)$. Then there exists $n \geq 1$ such that

$$\operatorname{Im} \rho_{E,p^\infty} = \pi_n^{-1}\left(C_{ns}^+(p^n)\right),$$

where

$$\pi_n : \mathrm{GL}_2(\mathbb{Z}_p) \to \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$$

is the canonical projection.

1. Work locally over $\mathbb{Q}_p$
2. Write down an alternative 'p^2-division polynomial'

p-adic classification

Theorem (Bisatt-Furio-L., 2025+)

Let $p > 7$ and suppose that $\operatorname{Im} \rho_{E,p} \subset C_{ns}^{+}(p)$. *Then there exists $n \geq 1$ such that*

$$\operatorname{Im} \rho_{E,p^\infty} = \pi_n^{-1}\left(C_{ns}^{+}(p^n)\right),$$

where

$$\pi_n : \mathrm{GL}_2(\mathbb{Z}_p) \to \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$$

is the canonical projection.

1. Work locally over $\mathbb{Q}_p$
2. Write down an alternative 'p^2-division polynomial'
3. Explicitly compute the Galois group and check that it is incompatible with $G_{ns}^{\#}(p^2)$.

Reductions

Proposition

Let $E/\mathbb{Q}$ be a non-CM elliptic curve and suppose $\operatorname{Im} \rho_{E,p} \subseteq C_{ns}^{+}(p)$*. If* $p > 7$*, then* $E/\mathbb{Q}_p$ *has potentially good supersingular reduction.*

Reductions

Proposition

Let $E/\mathbb{Q}$ be a non-CM elliptic curve and suppose $\operatorname{Im}\rho_{E,p} \subseteq C_{ns}^{+}(p)$. *If* $p > 7$, *then* $E/\mathbb{Q}_p$ *has potentially good supersingular reduction.*

Proposition

The theorem holds if $E/\mathbb{Q}_p$ *acquires good reduction over an at most quadratic extension.*

Reductions

Proposition

Let $E/\mathbb{Q}$ be a non-CM elliptic curve and suppose $\operatorname{Im}\rho_{E,p} \subseteq C_{ns}^{+}(p)$. If $p > 7$, then $E/\mathbb{Q}_p$ has potentially good supersingular reduction.

Proposition

The theorem holds if $E/\mathbb{Q}_p$ acquires good reduction over an at most quadratic extension.

Focus on elliptic curves with semistability defect $e \in \{3, 4, 6\}$.

Reductions

Proposition

Let $E/\mathbb{Q}$ be a non-CM elliptic curve and suppose $\operatorname{Im}\rho_{E,p} \subseteq C_{ns}^{+}(p)$*. If $p > 7$, then $E/\mathbb{Q}_p$ has potentially good supersingular reduction.*

Proposition

The theorem holds if $E/\mathbb{Q}_p$ acquires good reduction over an at most quadratic extension.

Focus on elliptic curves with semistability defect $e \in \{3, 4, 6\}$.
Supersingularity $\Rightarrow e \mid p + 1$.

A sprinkle of p-adic Hodge theory

Theorem (Volkov)

Let $e \in \{3, 4, 6\}$, $e \mid p + 1$, $E/\mathbb{Q}_p$ with potentially good supersingular reduction and semistability defect e.

A sprinkle of p-adic Hodge theory

Theorem (Volkov)

Let $e \in \{3, 4, 6\}$, $e \mid p + 1$, $E/\mathbb{Q}_p$ with potentially good supersingular reduction and semistability defect e.
the points of $T_p(E)$ are in Galois-equivariant bijection with the solutions $(a^{(n)})_{n \in \mathbb{Z}}$ in $\mathbb{C}_p$ of

$$\begin{cases} (a^{(n+1)})^p = a^{(n)}, \quad v_p(a^{(n)}) > 0 \\ \end{cases}$$

A sprinkle of p-adic Hodge theory

Theorem (Volkov)

Let $e \in \{3,4,6\}$, $e \mid p+1$, $E/\mathbb{Q}_p$ with potentially good supersingular reduction and semistability defect e. There exists $\alpha \in \mathbb{P}^1(\mathbb{Q}_p)$ such that the points of $T_p(E)$ are in Galois-equivariant bijection with the solutions $(a^{(n)})_{n\in\mathbb{Z}}$ in $\mathbb{C}_p$ of

$$\begin{cases} (a^{(n+1)})^p = a^{(n)}, \quad v_p(a^{(n)}) > 0 \\ \sum_{n\in\mathbb{Z}} c_n(\alpha) p^n a^{(n)} = 0. \end{cases}$$

A sprinkle of p-adic Hodge theory

Theorem (Volkov)

Let $e \in \{3,4,6\}$, $e \mid p+1$, $E/\mathbb{Q}_p$ with potentially good supersingular reduction and semistability defect e. There exists $\alpha \in \mathbb{P}^1(\mathbb{Q}_p)$ such that the points of $T_p(E)$ are in Galois-equivariant bijection with the solutions $(a^{(n)})_{n\in\mathbb{Z}}$ in $\mathbb{C}_p$ of

$$\begin{cases} (a^{(n+1)})^p = a^{(n)}, \quad v_p(a^{(n)}) > 0 \\ \sum_{n\in\mathbb{Z}} c_n(\alpha) p^n a^{(n)} = 0. \end{cases}$$

Up to quadratic twist, $v(\alpha) \geq 0$.

p^2-torsion points

Theorem

Let $\pi_e^e = -p$,

$$g(x) = \frac{x^{p^4}}{p^2} - \frac{\alpha\pi_e^2 x^{p^3} + x^{p^2}}{p} + \alpha\pi_e^2 x^p + x$$

and

$$\mathcal{R} = \{x \in \overline{\mathbb{Q}_p} : g(x) = 0\}.$$

p^2-torsion points

Theorem

Let $\pi_e^e = -p$,

$$g(x) = \frac{x^{p^4}}{p^2} - \frac{\alpha\pi_e^2 x^{p^3} + x^{p^2}}{p} + \alpha\pi_e^2 x^p + x$$

and

$$\mathcal{R} = \{x \in \overline{\mathbb{Q}_p} : g(x) = 0\}.$$

There is a Galois-equivariant[a] *bijection*

$$\Phi : E[p^2] \to \mathcal{R}.$$

[a] for a subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ of index $2e$

p^2-torsion points

Let $\pi_e^e = -p$ and

$$g(x) = \frac{x^{p^4}}{p^2} - \frac{\alpha\pi_e^2 x^{p^3} + x^{p^2}}{p} + \alpha\pi_e^2 x^p + x.$$

Theorem

- *If $v(\alpha) = 0$, the Galois group of $\mathbb{Q}_p(E[p^2])/\mathbb{Q}_p(E[p])$ has cardinality p^4.*

p^2-torsion points

Let $\pi_e^e = -p$ and

$$g(x) = \frac{x^{p^4}}{p^2} - \frac{\alpha\pi_e^2 x^{p^3} + x^{p^2}}{p} + \alpha\pi_e^2 x^p + x.$$

Theorem

- *If $v(\alpha) = 0$, the Galois group of $\mathbb{Q}_p(E[p^2])/\mathbb{Q}_p(E[p])$ has cardinality p^4.*
- *If $v(\alpha) \geq 1$, the Galois group of $\mathbb{Q}_p(E[p^2])/\mathbb{Q}_p$ is contained in $C_{ns}^+(p^2)$.*

p^2-torsion points

Let $\pi_e^e = -p$ and

$$g(x) = \frac{x^{p^4}}{p^2} - \frac{\alpha\pi_e^2 x^{p^3} + x^{p^2}}{p} + \alpha\pi_e^2 x^p + x.$$

Theorem

- *If $v(\alpha) = 0$, the Galois group of $\mathbb{Q}_p(E[p^2])/\mathbb{Q}_p(E[p])$ has cardinality p^4.*
- *If $v(\alpha) \geq 1$, the Galois group of $\mathbb{Q}_p(E[p^2])/\mathbb{Q}_p$ is contained in $C_{ns}^+(p^2)$.*

In both cases, $\operatorname{Im}\rho_{E,p^2}$ is not contained in $G_{ns}^{\#}(p^2)$.

7-adic representations

Rational points on $X_{ns}^{+}(49)$

Theorem (Furio-L.)

The set $X_{ns}^{+}(49)(\mathbb{Q})$ consists of CM points.
Equivalently, there is no non-CM elliptic curve $E/\mathbb{Q}$ such that $\operatorname{Im} \rho_{E,49}$ is contained in $C_{ns}^{+}(49)$.

Arithmetic restrictions for $C_{ns}^{+}(49)$

Proposition

Let $E/\mathbb{Q}$ be an elliptic curve such that $\operatorname{Im}\rho_{E,49} \subseteq C_{ns}^{+}(49)$. Write $j(E) = \frac{a}{b}$ with $(a, b) = 1$.

Arithmetic restrictions for $C_{ns}^{+}(49)$

Proposition

Let $E/\mathbb{Q}$ be an elliptic curve such that $\operatorname{Im}\rho_{E,49} \subseteq C_{ns}^{+}(49)$*. Write* $j(E) = \frac{a}{b}$ *with* $(a, b) = 1$*.*

1. *There exists* $t \in \mathbb{P}^1(\mathbb{Q})$ *such that*

$$j(E) = \frac{64t^3(t^2+7)^3(t^2-7t+14)^3(5t^2-14t-7)^3}{(t^3-7t^2+7t+7)^7}$$

Arithmetic restrictions for $C_{ns}^{+}(49)$

Proposition

Let $E/\mathbb{Q}$ be an elliptic curve such that $\operatorname{Im}\rho_{E,49} \subseteq C_{ns}^{+}(49)$. Write $j(E) = \frac{a}{b}$ with $(a, b) = 1$.

1. *There exists $t \in \mathbb{P}^1(\mathbb{Q})$ such that*

$$j(E) = \frac{64t^3(t^2+7)^3(t^2-7t+14)^3(5t^2-14t-7)^3}{(t^3-7t^2+7t+7)^7}$$

2. *The denominator b is a perfect 49-th power.*

Arithmetic restrictions for $C_{ns}^+(49)$

Proposition

Let $E/\mathbb{Q}$ be an elliptic curve such that $\operatorname{Im}\rho_{E,49} \subseteq C_{ns}^+(49)$. Write $j(E) = \frac{a}{b}$ with $(a, b) = 1$.

1. *There exists $t \in \mathbb{P}^1(\mathbb{Q})$ such that*

$$j(E) = \frac{64t^3(t^2+7)^3(t^2-7t+14)^3(5t^2-14t-7)^3}{(t^3-7t^2+7t+7)^7}$$

2. *The denominator b is a perfect 49-th power.*

Proof.

1. $X_{ns}^+(7) \cong \mathbb{P}^1$ with coordinate t. The function in the statement is the j-map $j : X_{ns}^+(7) \to X(1) \cong \mathbb{P}^1$.

□

Arithmetic properties of j-invariants

Proposition

Let $E/\mathbb{Q}$ be an elliptic curve such that $\operatorname{Im}\rho_{E,49} \subseteq C_{ns}^{+}(49)$. Write $j(E) = \frac{a}{b}$ with $(a,b) = 1$. The denominator b is a perfect 49-th power.

Proof.

Let p be a prime factor of b.

- $p \neq 7$ because E has potentially good reduction at 7

Arithmetic properties of j-invariants

Proposition

Let $E/\mathbb{Q}$ be an elliptic curve such that $\operatorname{Im}\rho_{E,49} \subseteq C_{ns}^{+}(49)$. *Write* $j(E) = \frac{a}{b}$ *with* $(a,b)=1$. *The denominator b is a perfect 49-th power.*

Proof.

Let p be a prime factor of b.

- $p \neq 7$ because E has potentially good reduction at 7
- For $p \neq 7$, using the theory of the Tate curve, one can show that $\operatorname{Im}\rho_{E,49}$ contains $\begin{pmatrix} 1 & v_p(j) \\ 0 & 1 \end{pmatrix}$. This is incompatible with the non-split Cartan structure unless $v_p(j) \equiv 0 \pmod{49}$, that is, $v_p(b) \equiv 0 \pmod{49}$.

□

A generalised Fermat equation

$$\frac{u}{v^{49}} = j(E) = \frac{64t^3(t^2+7)^3(t^2-7t+14)^3(5t^2-14t-7)^3}{(t^3-7t^2+7t+7)^7}$$

A generalised Fermat equation

$$\frac{u}{v^{49}} = j(E) = \frac{64t^3(t^2+7)^3(t^2-7t+14)^3(5t^2-14t-7)^3}{(t^3-7t^2+7t+7)^7}$$

Write $t = x/y$ and homogenise to obtain

$$x^3 - 7x^2y + 7xy^2 + 7y^3 = k \cdot z^7$$

A generalised Fermat equation

$$\frac{u}{v^{49}} = j(E) = \frac{64t^3(t^2+7)^3(t^2-7t+14)^3(5t^2-14t-7)^3}{(t^3-7t^2+7t+7)^7}$$

Write $t = x/y$ and homogenise to obtain

$$x^3 - 7x^2y + 7xy^2 + 7y^3 = k \cdot z^7 \text{ for some } k \in \{1, 8\}$$

A generalised Fermat equation

$$\frac{u}{v^{49}} = j(E) = \frac{64t^3(t^2+7)^3(t^2-7t+14)^3(5t^2-14t-7)^3}{(t^3-7t^2+7t+7)^7}$$

Write $t = x/y$ and homogenise to obtain

$$x^3 - 7x^2y + 7xy^2 + 7y^3 = k \cdot z^7 \text{ for some } k \in \{1, 8\}$$

Elementary arithmetic considerations, **using crucially that $v_7(j(E)) = 0$,** lead to

$$a^2 + 28b^3 = 27c^7$$

A generalised Fermat equation

$$\frac{u}{v^{49}} = j(E) = \frac{64t^3(t^2+7)^3(t^2-7t+14)^3(5t^2-14t-7)^3}{(t^3-7t^2+7t+7)^7}$$

Write $t = x/y$ and homogenise to obtain

$$x^3 - 7x^2y + 7xy^2 + 7y^3 = k \cdot z^7 \text{ for some } k \in \{1, 8\}$$

Elementary arithmetic considerations, **using crucially that $v_7(j(E)) = 0$,** lead to

$$a^2 + 28b^3 = 27c^7$$

+arithmetic conditions: $(2 \cdot 3 \cdot 7 \cdot a \cdot b,\ c) = 1$.

A generalised Fermat equation

$$\frac{u}{v^{49}} = j(E) = \frac{64t^3(t^2+7)^3(t^2-7t+14)^3(5t^2-14t-7)^3}{(t^3-7t^2+7t+7)^7}$$

Write $t = x/y$ and homogenise to obtain

$$x^3 - 7x^2y + 7xy^2 + 7y^3 = k \cdot z^7 \text{ for some } k \in \{1, 8\}$$

Elementary arithmetic considerations, **using crucially that $v_7(j(E)) = 0$,** lead to

$$a^2 + 28b^3 = 27c^7$$

+arithmetic conditions: $(2 \cdot 3 \cdot 7 \cdot a \cdot b,\ c) = 1$.

Remark

$(a, b, c) = (\pm 1, -1, -1), (\pm 27, -3, -1), (\pm 2521, -61, -1)$ are solutions.

A generalised Fermat equation

$$\frac{u}{v^{49}} = j(E) = \frac{64t^3(t^2+7)^3(t^2-7t+14)^3(5t^2-14t-7)^3}{(t^3-7t^2+7t+7)^7}$$

Write $t = x/y$ and homogenise to obtain

$$x^3 - 7x^2y + 7xy^2 + 7y^3 = k \cdot z^7 \text{ for some } k \in \{1, 8\}$$

Elementary arithmetic considerations, **using crucially that $v_7(j(E)) = 0$,** lead to

$$a^2 + 28b^3 = 27c^7$$

+arithmetic conditions: $(2 \cdot 3 \cdot 7 \cdot a \cdot b,\ c) = 1$.

Remark

$(a, b, c) = (\pm 1, -1, -1), (\pm 27, -3, -1), (\pm 2521, -61, -1)$ are solutions. So are

$$(\pm 2 \cdot 181 \cdot 313 \cdot 317,\ 3593,\ 90), (\pm 2^{13} \cdot 5 \cdot 59957, -2^8 \cdot 1867, 2^4 \cdot 17)$$

Strategy (after Poonen-Schaefer-Stoll)

1. To a solution of
$$a^2 + 28b^3 = 27c^7$$
we attach
$$\tilde{E}_{(a,b,c)} : y^2 = x^3 + 3 \cdot 7 \cdot b \cdot x - 7 \cdot a$$
with $j(\tilde{E}_{(a,b,c)}) = 2^8 \cdot 7 \cdot \frac{b^3}{c^7}$.

Strategy (after Poonen-Schaefer-Stoll)

1. To a solution of
$$a^2 + 28b^3 = 27c^7$$
we attach
$$\tilde{E}_{(a,b,c)} : y^2 = x^3 + 3 \cdot 7 \cdot b \cdot x - 7 \cdot a$$
with $j(\tilde{E}_{(a,b,c)}) = 2^8 \cdot 7 \cdot \frac{b^3}{c^7}$. From $j(\tilde{E}_{(a,b,c)})$ we can reconstruct (a, b, c).

Strategy (after Poonen-Schaefer-Stoll)

1. To a solution of

$$a^2 + 28b^3 = 27c^7$$

we attach

$$\tilde{E}_{(a,b,c)} : y^2 = x^3 + 3 \cdot 7 \cdot b \cdot x - 7 \cdot a$$

with $j(\tilde{E}_{(a,b,c)}) = 2^8 \cdot 7 \cdot \frac{b^3}{c^7}$. From $j(\tilde{E}_{(a,b,c)})$ we can reconstruct (a, b, c).

2. (Technical step: twist $\tilde{E}_{(a,b,c)}$ by -3 to achieve good reduction at 3. Denote by $E_{(a,b,c)}$ the quadratic twist)

Strategy (after Poonen-Schaefer-Stoll)

1. To a solution of
$$a^2 + 28b^3 = 27c^7$$
we attach
$$\tilde{E}_{(a,b,c)} : y^2 = x^3 + 3 \cdot 7 \cdot b \cdot x - 7 \cdot a$$
with $j(\tilde{E}_{(a,b,c)}) = 2^8 \cdot 7 \cdot \frac{b^3}{c^7}$. From $j(\tilde{E}_{(a,b,c)})$ we can reconstruct (a, b, c).
2. (Technical step: twist $\tilde{E}_{(a,b,c)}$ by -3 to achieve good reduction at 3. Denote by $E_{(a,b,c)}$ the quadratic twist)
3. The 'usual' combination of level-lowering and modularity shows that there exists a newform $f \in S_2(\Gamma_0(N))$ with
$$N \in \{2^2 \cdot 7^2, 2^3 \cdot 7^2, 2^4 \cdot 7^2\}$$
such that $\rho_{f,\mathfrak{p}} \cong \rho_{E_{(a,b,c)},7}$

Strategy (after Poonen-Schaefer-Stoll)

1. To a solution of
$$a^2 + 28b^3 = 27c^7$$
we attach
$$\tilde{E}_{(a,b,c)} : y^2 = x^3 + 3 \cdot 7 \cdot b \cdot x - 7 \cdot a$$
with $j(\tilde{E}_{(a,b,c)}) = 2^8 \cdot 7 \cdot \frac{b^3}{c^7}$. From $j(\tilde{E}_{(a,b,c)})$ we can reconstruct (a, b, c).
2. (Technical step: twist $\tilde{E}_{(a,b,c)}$ by -3 to achieve good reduction at 3. Denote by $E_{(a,b,c)}$ the quadratic twist)
3. The 'usual' combination of level-lowering and modularity shows that there exists a newform $f \in S_2(\Gamma_0(N))$ with
$$N \in \{2^2 \cdot 7^2, 2^3 \cdot 7^2, 2^4 \cdot 7^2\}$$
such that $\rho_{f,\mathfrak{p}} \cong \rho_{E_{(a,b,c)},7}$ for some prime $\mathfrak{p}$ of the ring $\mathbb{Z}[a_n(f)]$ with residue field $\mathbb{F}_7$.

Strategy (after Poonen-Schaefer-Stoll)

4. To a solution of $a^2 + 28b^3 = 27c^7$ we attach $E_{(a,b,c)}$, hence an $f \in S_2(\Gamma_0(N))$ with $\rho_{E_{(a,b,c)},7} \sim \rho_{f,\mathfrak{p}}$.

Strategy (after Poonen-Schaefer-Stoll)

4. To a solution of $a^2 + 28b^3 = 27c^7$ we attach $E_{(a,b,c)}$, hence an $f \in S_2(\Gamma_0(N))$ with $\rho_{E_{(a,b,c)},7} \sim \rho_{f,\mathfrak{p}}$.
5. Get lucky

Strategy (after Poonen-Schaefer-Stoll)

4. To a solution of $a^2 + 28b^3 = 27c^7$ we attach $E_{(a,b,c)}$, hence an $f \in S_2(\Gamma_0(N))$ with $\rho_{E_{(a,b,c)},7} \sim \rho_{f,\mathfrak{p}}$.
5. Get lucky: all the relevant f but one have rational coefficients, or are congruent modulo 7 to forms with rational coefficients!

Strategy (after Poonen-Schaefer-Stoll)

4. To a solution of $a^2 + 28b^3 = 27c^7$ we attach $E_{(a,b,c)}$, hence an $f \in S_2(\Gamma_0(N))$ with $\rho_{E_{(a,b,c)},7} \sim \rho_{f,\mathfrak{p}}$.
5. Get lucky: all the relevant f but one have rational coefficients, or are congruent modulo 7 to forms with rational coefficients! They correspond to elliptic curves, *including* the bad one.

Strategy (after Poonen-Schaefer-Stoll)

4. To a solution of $a^2 + 28b^3 = 27c^7$ we attach $E_{(a,b,c)}$, hence an $f \in S_2(\Gamma_0(N))$ with $\rho_{E_{(a,b,c)},7} \sim \rho_{f,\mathfrak{p}}$.
5. Get lucky: all the relevant f but one have rational coefficients, or are congruent modulo 7 to forms with rational coefficients! They correspond to elliptic curves, *including* the bad one.
6. Rule out as many f as possible (symplectic criteria, image of inertia, global computations of torsion fields...): reduce from 25 (orbits of) newforms to 2.

Strategy (after Poonen-Schaefer-Stoll)

4. To a solution of $a^2 + 28b^3 = 27c^7$ we attach $E_{(a,b,c)}$, hence an $f \in S_2(\Gamma_0(N))$ with $\rho_{E_{(a,b,c)},7} \sim \rho_{f,\mathfrak{p}}$.
5. Get lucky: all the relevant f but one have rational coefficients, or are congruent modulo 7 to forms with rational coefficients! They correspond to elliptic curves, *including* the bad one.
6. Rule out as many f as possible (symplectic criteria, image of inertia, global computations of torsion fields...): reduce from 25 (orbits of) newforms to 2.
7. New objective: for each remaining f, compute all $E/\mathbb{Q}$ such that $E[7] \cong \rho_{f,7}$. Since f has rational coefficients, $\rho_{f,7} \cong \rho_{E_f,7}$ for an *explicit* elliptic curve E_f over $\mathbb{Q}$.

Strategy (after Poonen-Schaefer-Stoll)

8. To a solution of $a^2 + 28b^3 = 27c^7$ we attach $E_{(a,b,c)}$ with $E_{(a,b,c)}[7] \cong E_f[7]$, where f is one of two newforms.

Strategy (after Poonen-Schaefer-Stoll)

8. To a solution of $a^2 + 28b^3 = 27c^7$ we attach $E_{(a,b,c)}$ with $E_{(a,b,c)}[7] \cong E_f[7]$, where f is one of two newforms.
9. For each $E_f/\mathbb{Q}$, the elliptic curves $E/\mathbb{Q}$ with $E[7] \cong E_f[7]$ are parametrised by the rational points of **two** modular curves, $X_E(7)^{\pm}$.

Strategy (after Poonen-Schaefer-Stoll)

8. To a solution of $a^2 + 28b^3 = 27c^7$ we attach $E_{(a,b,c)}$ with $E_{(a,b,c)}[7] \cong E_f[7]$, where f is one of two newforms.
9. For each $E_f/\mathbb{Q}$, the elliptic curves $E/\mathbb{Q}$ with $E[7] \cong E_f[7]$ are parametrised by the rational points of **two** modular curves, $X_E(7)^{\pm}$. Each of them is a twist of the Klein quartic $x^3y + y^3z + z^3x = 0$.

Strategy (after Poonen-Schaefer-Stoll)

8. To a solution of $a^2 + 28b^3 = 27c^7$ we attach $E_{(a,b,c)}$ with $E_{(a,b,c)}[7] \cong E_f[7]$, where f is one of two newforms.
9. For each $E_f/\mathbb{Q}$, the elliptic curves $E/\mathbb{Q}$ with $E[7] \cong E_f[7]$ are parametrised by the rational points of **two** modular curves, $X_E(7)^{\pm}$. Each of them is a twist of the Klein quartic $x^3y + y^3z + z^3x = 0$.
10. Find the rational points!

Finding the rational points

We have $4 = 2 \times 2$ curves of interest.

Finding the rational points

We have $4 = 2 \times 2$ curves of interest. Of these, one does not have rational points because of a local obstruction at 2 (Kraus, Freitas).

Finding the rational points

We have $4 = 2 \times 2$ curves of interest. Of these, one does not have rational points because of a local obstruction at 2 (Kraus, Freitas). Let X_1, X_2, X_3 be the other ones.

Finding the rational points

We have $4 = 2 \times 2$ curves of interest. Of these, one does not have rational points because of a local obstruction at 2 (Kraus, Freitas). Let X_1, X_2, X_3 be the other ones.

1. Two-descent: the Jacobians of X_1, X_2, X_3 have ranks $1, 2, 2$ over $\mathbb{Q}$.

Finding the rational points

We have $4 = 2 \times 2$ curves of interest. Of these, one does not have rational points because of a local obstruction at 2 (Kraus, Freitas). Let X_1, X_2, X_3 be the other ones.

1. Two-descent: the Jacobians of X_1, X_2, X_3 have ranks $1, 2, 2$ over $\mathbb{Q}$.
2. Mordell-Weil sieve: for suitably chosen primes p_i, the images of $X_i(\mathbb{Q}) \to X_i(\mathbb{F}_{p_i})$ have size at most $1, 2, 2$.

Finding the rational points

We have $4 = 2 \times 2$ curves of interest. Of these, one does not have rational points because of a local obstruction at 2 (Kraus, Freitas). Let X_1, X_2, X_3 be the other ones.

1. Two-descent: the Jacobians of X_1, X_2, X_3 have ranks $1, 2, 2$ over $\mathbb{Q}$.
2. Mordell-Weil sieve: for suitably chosen primes p_i, the images of $X_i(\mathbb{Q}) \to X_i(\mathbb{F}_{p_i})$ have size at most $1, 2, 2$.
3. Chabauty-Coleman: each p-adic residue disc around the points in $X_i(\mathbb{F}_{p_i})$ contains at most 1 rational point.
4. Since we know a rational point in each disc, we are done.

Finding the rational points

We have $4 = 2 \times 2$ curves of interest. Of these, one does not have rational points because of a local obstruction at 2 (Kraus, Freitas). Let X_1, X_2, X_3 be the other ones.

1. Two-descent: the Jacobians of X_1, X_2, X_3 have ranks $1, 2, 2$ over $\mathbb{Q}$.
2. Mordell-Weil sieve: for suitably chosen primes p_i, the images of $X_i(\mathbb{Q}) \to X_i(\mathbb{F}_{p_i})$ have size at most $1, 2, 2$.
3. Chabauty-Coleman: each p-adic residue disc around the points in $X_i(\mathbb{F}_{p_i})$ contains at most 1 rational point.
4. Since we know a rational point in each disc, we are done.

From each rational point we reconstruct a j-invariant and a solution of the equation $a^2 + 28b^3 = -27c^7$. We get five solutions, three of which satisfy the arithmetic constraints.

Finding the rational points

We have $4 = 2 \times 2$ curves of interest. Of these, one does not have rational points because of a local obstruction at 2 (Kraus, Freitas). Let X_1, X_2, X_3 be the other ones.

1. Two-descent: the Jacobians of X_1, X_2, X_3 have ranks $1, 2, 2$ over $\mathbb{Q}$.
2. Mordell-Weil sieve: for suitably chosen primes p_i, the images of $X_i(\mathbb{Q}) \to X_i(\mathbb{F}_{p_i})$ have size at most $1, 2, 2$.
3. Chabauty-Coleman: each p-adic residue disc around the points in $X_i(\mathbb{F}_{p_i})$ contains at most 1 rational point.
4. Since we know a rational point in each disc, we are done.

From each rational point we reconstruct a j-invariant and a solution of the equation $a^2 + 28b^3 = -27c^7$. We get five solutions, three of which satisfy the arithmetic constraints. Working backwards, we compute a finite list containing the j-invariants of the rational points on $X_{ns}^+(49)$.

The other two modular curves of level 49

A very similar strategy applies. One key difference:

The other two modular curves of level 49

A very similar strategy applies. One key difference:

Using crucially that $v_7(j(E)) = 0$, *we obtain*

$$a^2 + 28b^3 = 27c^7$$

The other two modular curves of level 49

A very similar strategy applies. One key difference:

~~***Using crucially that*** $v_7(j(E)) = 0$,~~ *we obtain*

$$a^2 + 28b^3 = 27c^7 \text{ or } a^2 + 196b^3 = 27c^7.$$

The other two modular curves of level 49

A very similar strategy applies. One key difference:

~~***Using crucially that*** $v_7(j(E)) = 0$,~~ *we obtain*

$$a^2 + 28b^3 = 27c^7 \text{ or } a^2 + 196b^3 = 27c^7.$$

Unfortunately, $13^2 + 196 \cdot (-1)^3 = 27 \cdot (-1)^7$.

The other two modular curves of level 49

A very similar strategy applies. One key difference:

~~***Using crucially that*** $v_7(j(E)) = 0$,~~ *we obtain*

$$a^2 + 28b^3 = 27c^7 \text{ or } a^2 + 196b^3 = 27c^7.$$

Unfortunately, $13^2 + 196 \cdot (-1)^3 = 27 \cdot (-1)^7$. Everything else essentially goes through, but we now have one more modular form f_3, hence two more curves $X_{E_{f_3}}(7)^{\pm}$. One of them does not have points locally at 2.

The other two modular curves of level 49

A very similar strategy applies. One key difference:

~~***Using crucially that*** $v_7(j(E)) = 0$,~~ *we obtain*

$$a^2 + 28b^3 = 27c^7 \text{ or } a^2 + 196b^3 = 27c^7.$$

Unfortunately, $13^2 + 196 \cdot (-1)^3 = 27 \cdot (-1)^7$. Everything else essentially goes through, but we now have one more modular form f_3, hence two more curves $X_{E_{f_3}}(7)^{\pm}$. One of them does not have points locally at 2.

Conjecture

The set of rational points of the curve

$$C : x^4 + 3x^3y - 3x^2yz - 3x^2z^2 + 6xy^3 - 6xy^2z + 3xyz^2 - 2xz^3 + 4y^4 + 2y^3z - 5yz^3 = 0.$$

is $C(\mathbb{Q}) = \{[0:0:1], [1:1:1], [2:0:1], [-1:0:1]\}$.

Thank you for your attention!