ON THE POSSIBLE IMAGES OF THE MOD ℓ REPRESENTATIONS ASSOCIATED TO ELLIPTIC CURVES OVER $\mathbb{Q}$

DAVID J. ZYWINA

Abstract. Consider a non-CM elliptic curve E defined over $\mathbb{Q}$. For each prime ℓ, there is a representation $\rho_{E,\ell}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\ell)$ that describes the Galois action on the ℓ-torsion points of E. A famous theorem of Serre says that $\rho_{E,\ell}$ is surjective for all large enough ℓ. We will describe all known, and conjecturally all, pairs (E,ℓ) such that $\rho_{E,\ell}$ is not surjective. Together with another paper, this produces an algorithm that given an elliptic curve $E/\mathbb{Q}$, outputs the set of such *exceptional primes* ℓ and describes all the groups $\rho_{E,\ell}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ up to conjugacy. Much of the paper is dedicated to computing various modular curves of genus 0 with their morphisms to the j-line.

1. Possible images

Consider an elliptic curve E defined over $\mathbb{Q}$. For each prime ℓ, let $E[\ell]$ be the ℓ-torsion subgroup of $E(\overline{\mathbb{Q}})$, where $\overline{\mathbb{Q}}$ is a fixed algebraic closure of $\mathbb{Q}$. The group $E[\ell]$ is a free $\mathbb{F}_\ell$-module of rank 2 and there is a natural action of the absolute Galois group $\mathrm{Gal}_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E[\ell]$ which respects the group structure. After choosing a basis for $E[\ell]$, this action can be expressed in terms of a Galois representation

$$\rho_{E,\ell}\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\ell);$$

its image $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is uniquely determined up to conjugacy in $\mathrm{GL}_2(\mathbb{F}_\ell)$. A renowned theorem of Serre [Ser72] says that $\rho_{E,\ell}$ is surjective for all but finitely many ℓ when E is non-CM.

In this paper, we shall describe all known (and conjecturally all) proper subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$ that occur as the image of such a representation $\rho_{E,\ell}$. Applying our classification with earlier work, we will obtain an algorithm to determine the set $\mathcal{S}$ of primes ℓ for which $\rho_{E,\ell}$ is not surjective and also compute $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ for each $\ell \in \mathcal{S}$.

Before stating our classification in §§1.1–1.7, let us make some comments. We will consider each prime ℓ separately. For simplicity, assume that the j-invariant $j_E \in \mathbb{Q}$ of $E/\mathbb{Q}$ is neither 0 nor 1728. Our first step in determining $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is to compute the group

$$G := \pm\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}}),$$

i.e., the group generated by $-I$ and $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$. The benefit of studying G, up to conjugacy in $\mathrm{GL}_2(\mathbb{F}_\ell)$, is that it does not change if E is replaced by a quadratic twist. Moreover, if $E'/\mathbb{Q}$ is a quadratic twist of $E/\mathbb{Q}$, then after choosing appropriate bases, we will have $\rho_{E',\ell} = \chi \cdot \rho_{E,\ell}$ for some quadratic character $\chi\colon \mathrm{Gal}_{\mathbb{Q}} \to \{\pm 1\}$. Since $j_E \notin \{0, 1728\}$, all twists of E are quadratic twists and hence G, up to conjugacy, depends only on the value j_E. The character $\det \circ \rho_{E,\ell}\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathbb{F}_\ell^\times$ describes the Galois action on the ℓ-th roots of unity, so $\det(G) = \mathbb{F}_\ell^\times$.

For a subgroup G of $\mathrm{GL}_2(\mathbb{F}_\ell)$ with $\det(G) = \mathbb{F}_\ell^\times$ and $-I \in G$, we can associate a modular curve X_G; it is a smooth, projective and geometrically irreducible curve defined over $\mathbb{Q}$. It comes with a natural morphism

$$\pi_G\colon X_G \to \mathrm{Spec}\,\mathbb{Q}[j] \cup \{\infty\} =: \mathbb{P}^1_{\mathbb{Q}}$$

2010 *Mathematics Subject Classification.* Primary 11G05; Secondary 11F80.

such that for an elliptic curve $E/\mathbb{Q}$ with $j_E \notin \{0, 1728\}$, the group $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_\ell)$ to subgroup of G if and only if the $j_E = \pi_G(P)$ for some rational point $P \in X_G(\mathbb{Q})$.

Much of this paper is dedicated to describing those modular curves X_G of genus 0 with $X_G(\mathbb{Q}) \neq \emptyset$. Such modular curves are isomorphic to the projective line and their function field is of form $\mathbb{Q}(h)$ for some modular function h of level ℓ. Giving the morphism π_G is then equivalent to expressing the modular j-invariant in the form $J(h)$ for a unique rational function $J(t) \in \mathbb{Q}(t)$.

Once we have determined G, we know that $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ will either be the full group G or equal to an index 2 subgroup H of G for which $-I \notin H$. For each such H, it is then a matter of determining whether the quadratic character $\mathrm{Gal}_{\mathbb{Q}} \xrightarrow{\rho_{E,\ell}} G \to G/H \cong \{\pm 1\}$ is trivial or not.

We will first focus on the general case of non-CM elliptic curves over $\mathbb{Q}$. In §1.9, we will give a complete description of the groups $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ when $E/\mathbb{Q}$ has complex multiplication.

Notation. We now define some specific subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$ for an odd prime ℓ. Let $C_s(\ell)$ be the subgroup of diagonal matrices. Let $\epsilon = -1$ if $\ell \equiv 3 \pmod 4$ and otherwise let $\epsilon \geq 2$ be the smallest integer which is not a quadratic residue modulo ℓ. Let $C_{ns}(\ell)$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} a & b\epsilon \\ b & a \end{smallmatrix}\right)$ with $(a, b) \in \mathbb{F}_\ell^2 - \{(0, 0)\}$. Let $N_s(\ell)$ and $N_{ns}(\ell)$ be the normalizers of $C_s(\ell)$ and $C_{ns}(\ell)$, respectively, in $\mathrm{GL}_2(\mathbb{F}_\ell)$. We have $[N_s(\ell) : C_s(\ell)] = 2$ and the non-identity coset of $C_s(\ell)$ in $N_s(\ell)$ is represented by $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. We have $[N_{ns}(\ell) : C_{ns}(\ell)] = 2$ and the non-identity coset of $C_{ns}(\ell)$ in $N_{ns}(\ell)$ is represented by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Let $B(\ell)$ be the subgroup of upper triangular matrices in $\mathrm{GL}_2(\mathbb{F}_\ell)$.

1.1. $\underline{\ell = 2}$**.** Up to conjugacy, there are three proper subgroups of $\mathrm{GL}_2(\mathbb{F}_2)$:

$$G_1 = \{I\}, \qquad G_2 = \{I, \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\}, \qquad G_3 = \{I, \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)\}.$$

For $i = 1, 2$ and 3, the index $[\mathrm{GL}_2(\mathbb{F}_2) : G_i]$ is 6, 3 and 2, respectively. Define the rational functions

$$J_1(t) = 256\frac{(t^2 + t + 1)^3}{t^2(t + 1)^2}, \qquad J_2(t) = 256\frac{(t + 1)^3}{t}, \qquad J_3(t) = t^2 + 1728.$$

Theorem 1.1. *Let E be a non-CM elliptic curve over $\mathbb{Q}$. Then $\rho_{E,2}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_2)$ to a subgroup of G_i if and only if j_E is of the form $J_i(t)$ for some $t \in \mathbb{Q}$.*

1.2. $\underline{\ell = 3}$**.** Define the following subgroups of $\mathrm{GL}_2(\mathbb{F}_3)$:

- Let G_1 be the group $C_s(3)$.
- Let G_2 be the group $N_s(3)$.
- Let G_3 be the group $B(3)$.
- Let G_4 be the group $N_{ns}(3)$.
- Let $H_{1,1}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right)$.
- Let $H_{3,1}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$.
- Let $H_{3,2}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$.

The index in $\mathrm{GL}_2(\mathbb{F}_3)$ of the above subgroups are 12, 6, 4, 3, 24, 8 and 8, respectively. Each of the groups G_i contain $-I$. The groups $H_{i,j}$ do not contain $-I$ and we have $G_i = \pm H_{i,j}$.

Define the rational functions:

$$J_1(t) = 27\frac{(t + 1)^3(t + 3)^3(t^2 + 3)^3}{t^3(t^2 + 3t + 3)^3}, \; J_2(t) = 27\frac{(t + 1)^3(t - 3)^3}{t^3}, \; J_3(t) = 27\frac{(t + 1)(t + 9)^3}{t^3}, \; J_4(t) = t^3.$$

For $t \in \mathbb{Q} - \{0\}$, let $\mathcal{E}_{1,t}$ be the elliptic curve over $\mathbb{Q}$ defined by Weierstrass equation

$$y^2 = x^3 - 3(t + 1)(t + 3)(t^2 + 3)x - 2(t^2 - 3)(t^4 + 6t^3 + 18t^2 + 18t + 9).$$

For $t \in \mathbb{Q} - \{0, -1\}$, let $\mathcal{E}_{3,t}$ be the elliptic curve over $\mathbb{Q}$ defined by Weierstrass equation

$$y^2 = x^3 - 3(t+1)^3(t+9)x - 2(t+1)^4(t^2 - 18t - 27).$$

The j-invariant of $\mathcal{E}_{i,t}$ is $J_i(t)$.

Theorem 1.2. *Let E be a non-CM elliptic curve over $\mathbb{Q}$.*

(i) *If $\rho_{E,3}$ is not surjective, then $\rho_{E,3}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_3)$ to one of the groups G_i or $H_{i,j}$.*

(ii) *The group $\rho_{E,3}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to a subgroup of G_i if and only if j_E is of the form $J_i(t)$ for some $t \in \mathbb{Q}$.*

(iii) *Suppose that $\pm\rho_{E,3}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to G_1. Fix an element $t \in \mathbb{Q}$ such that $J_1(t) = j_E$. The group $\rho_{E,3}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to $H_{1,1}$ if and only if E is isomorphic to $\mathcal{E}_{1,t}$ or the quadratic twist of $\mathcal{E}_{1,t}$ by -3.*

(iv) *Suppose that $\pm\rho_{E,3}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to G_3. Fix an element $t \in \mathbb{Q}$ such that $J_3(t) = j_E$. The group $\rho_{E,3}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to $H_{3,1}$ if and only if E is isomorphic to $\mathcal{E}_{3,t}$. The group $\rho_{E,3}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to $H_{3,2}$ if and only if E is isomorphic to the quadratic twist of $\mathcal{E}_{3,t}$ by -3.*

Remark 1.3.

(i) Let us briefly explain how Theorem 1.2 can be used to compute $\rho_{E,3}(\mathrm{Gal}_{\mathbb{Q}})$; similar remarks will hold for the remaining primes (the case $\ell = 2$ is particularly simple since $-I = I$). If j_E is not of the form $J_i(t)$ for any $i \in \{1,2,3,4\}$ and $t \in \mathbb{Q}$, then $\rho_{E,3}(\mathrm{Gal}_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{F}_3)$. To check if j_E is of the form $J(t)$, clear denominators in $J(t) - j_E$ to obtain a polynomial in t which one can then determine whether it has rational roots or not.

So assume that $\rho_{E,3}$ is not surjective, and let i be the smallest value in $\{1,2,3,4\}$ for which $j_E = J_i(t)$ for some $t \in \mathbb{Q}$. By Theorem 1.2(i) and (ii), we deduce that $\pm\rho_{E,3}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to G_i; note that the groups G_i are ordered by decreasing index in $\mathrm{GL}_2(\mathbb{F}_3)$. After possibly conjugating $\rho_{E,3}$, we may assume that $\pm\rho_{E,3}(\mathrm{Gal}_{\mathbb{Q}}) = G_i$. If $\rho_{E,3}(\mathrm{Gal}_{\mathbb{Q}})$ does not equal G_i, then it is equal to one of the subgroups $H_{i,j}$ and parts (iii) and (iv) give necessary and sufficient conditions to check this.

(ii) Our rational functions $J_i(t)$ are certainly not unique. In particular, any function of the form $J_i((at+b)/(ct+d))$ will work with fixed $a, b, c, d \in \mathbb{Q}$ satisfying $ad - bc \neq 0$ (though in general, one needs to also consider the value of $J_i(t)$ at ∞). Given $J_i(t)$, our equations for $\mathcal{E}_{i,t}$ were produced by an algorithm that we will later describe; there are other possibly simpler choices.

1.3. $\underline{\ell = 5}$**.** Define the following subgroups of $\mathrm{GL}_2(\mathbb{F}_5)$:

- Let G_1 be the subgroup consisting of the matrices of the form $\pm\left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right)$.
- Let G_2 be the group $C_s(5)$.
- Let G_3 be the unique subgroup of $N_{ns}(5)$ of index 3; it is generated by $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 6 \\ 3 & 0 \end{smallmatrix}\right)$.
- Let G_4 be the group $N_s(5)$.
- Let G_5 be the subgroup consisting of the matrices of the form $\pm\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$.
- Let G_6 be the subgroup consisting of the matrices of the form $\pm\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$.
- Let G_7 be the group $N_{ns}(5)$.
- Let G_8 be the group $B(5)$.
- Let G_9 be the unique maximal subgroup of $\mathrm{GL}_2(\mathbb{F}_5)$ which contains $N_s(5)$; it is generated by $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$.
- Let $H_{1,1}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right)$.
- Let $H_{1,2}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix} a^2 & 0 \\ 0 & a \end{smallmatrix}\right)$.

- Let $H_{5,1}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$.
- Let $H_{5,2}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix} a & * \\ 0 & a^2 \end{smallmatrix}\right)$.
- Let $H_{6,1}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$.
- Let $H_{6,2}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix} a^2 & * \\ 0 & a \end{smallmatrix}\right)$.

The index in $\mathrm{GL}_2(\mathbb{F}_5)$ of the above subgroups are 60, 30, 30, 15, 12, 12, 10, 6, 5, 120, 120, 24, 24, 24 and 24, respectively. Each of the groups G_i contain $-I$. The groups $H_{i,j}$ do not contain $-I$ and we have $G_i = \pm H_{i,j}$.

Define the rational functions:

$$J_1(t) = \frac{(t^{20} + 228t^{15} + 494t^{10} - 228t^5 + 1)^3}{t^5(t^{10} - 11t^5 - 1)^5}$$

$$J_2(t) = \frac{(t^2 + 5t + 5)^3(t^4 + 5t^2 + 25)^3(t^4 + 5t^3 + 20t^2 + 25t + 25)^3}{t^5(t^4 + 5t^3 + 15t^2 + 25t + 25)^5}$$

$$J_3(t) = \frac{5^4t^3(t^2 + 5t + 10)^3(2t^2 + 5t + 5)^3(4t^4 + 30t^3 + 95t^2 + 150t + 100)^3}{(t^2 + 5t + 5)^5(t^4 + 5t^3 + 15t^2 + 25t + 25)^5}$$

$$J_4(t) = \frac{(t + 5)^3(t^2 - 5)^3(t^2 + 5t + 10)^3}{(t^2 + 5t + 5)^5}$$

$$J_5(t) = \frac{(t^4 + 228t^3 + 494t^2 - 228t + 1)^3}{t(t^2 - 11t - 1)^5}$$

$$J_6(t) = \frac{(t^4 - 12t^3 + 14t^2 + 12t + 1)^3}{t^5(t^2 - 11t - 1)}$$

$$J_7(t) = \frac{5^3(t + 1)(2t + 1)^3(2t^2 - 3t + 3)^3}{(t^2 + t - 1)^5}$$

$$J_8(t) = \frac{5^2(t^2 + 10t + 5)^3}{t^5}$$

$$J_9(t) = t^3(t^2 + 5t + 40)$$

For $t \in \mathbb{Q} - \{0\}$, let $\mathcal{E}_{1,t}$ be the elliptic curve over $\mathbb{Q}$ defined by the Weierstrass equation

$$y^2 = x^3 - 27(t^{20} + 228t^{15} + 494t^{10} - 228t^5 + 1)x + 54(t^{30} - 522t^{25} - 10005t^{20} - 10005t^{10} + 522t^5 + 1).$$

For $t \in \mathbb{Q} - \{0\}$, let $\mathcal{E}_{5,t}$ be the elliptic curve over $\mathbb{Q}$ defined by the Weierstrass equation

$$y^2 = x^3 - 27(t^4 + 228t^3 + 494t^2 - 228t + 1)x + 54(t^6 - 522t^5 - 10005t^4 - 10005t^2 + 522t + 1).$$

For $t \in \mathbb{Q} - \{0\}$, let $\mathcal{E}_{6,t}$ be the elliptic curve over $\mathbb{Q}$ defined by the Weierstrass equation

$$y^2 = x^3 - 27(t^4 - 12t^3 + 14t^2 + 12t + 1)x + 54(t^6 - 18t^5 + 75t^4 + 75t^2 + 18t + 1)$$

The j-invariant of $\mathcal{E}_{i,t}$ is $J_i(t)$.

Theorem 1.4. *Let E be a non-CM elliptic curve over $\mathbb{Q}$.*

(i) *If $\rho_{E,5}$ is not surjective, then $\rho_{E,5}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_5)$ to one of the groups G_i or $H_{i,j}$.*

(ii) *The group $\rho_{E,5}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to a subgroup of G_i if and only if j_E is of the form $J_i(t)$ for some $t \in \mathbb{Q}$.*

(iii) *Suppose that $\pm\rho_{E,5}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to G_i with $i \in \{1, 5, 6\}$. Fix an element $t \in \mathbb{Q}$ such that $J_i(t) = j_E$.*
The group $\rho_{E,5}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to $H_{i,1}$ if and only if E is isomorphic to $\mathcal{E}_{i,t}$.

The group $\rho_{E,5}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to $H_{i,2}$ if and only if E is isomorphic to the quadratic twist of $\mathcal{E}_{i,t}$ by 5.

1.4. $\underline{\ell = 7}$**.** Define the follow subgroups of $\mathrm{GL}_2(\mathbb{F}_7)$:

- Let G_1 be the subgroup of $N_s(7)$ consisting of elements of $C_s(7)$ with square determinant and elements of $N_s(7) - C_s(7)$ with non-square determinant; it is generated by $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 4 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.
- Let G_2 be the group $N_s(7)$.
- Let G_3 be the subgroup consisting of matrices of the form $\pm\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$.
- Let G_4 be the subgroup consisting of matrices of the form $\pm\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$.
- Let G_5 be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} a & * \\ 0 & \pm a \end{smallmatrix}\right)$.
- Let G_6 be the group $N_{ns}(7)$.
- Let G_7 be the group $B(7)$.
- Let $H_{1,1}$ be the subgroup generated by $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 4 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right)$.
- Let $H_{3,1}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$.
- Let $H_{3,2}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix} \pm 1 & * \\ 0 & a^2 \end{smallmatrix}\right)$.
- Let $H_{4,1}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$.
- Let $H_{4,2}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix} a^2 & * \\ 0 & \pm 1 \end{smallmatrix}\right)$.
- Let $H_{5,1}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix} \pm a^2 & * \\ 0 & a^2 \end{smallmatrix}\right)$.
- Let $H_{5,2}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix} a^2 & * \\ 0 & \pm a^2 \end{smallmatrix}\right)$.
- Let $H_{7,1}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix} * & * \\ 0 & a^2 \end{smallmatrix}\right)$.
- Let $H_{7,2}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix} a^2 & * \\ 0 & * \end{smallmatrix}\right)$.

The index in $\mathrm{GL}_2(\mathbb{F}_7)$ of the above subgroups are 56, 28, 24, 24, 24, 21, 8, 112, 48, 48, 48, 48, 48, 48, 16 and 16, respectively. Each of the groups G_i contain $-I$. The groups $H_{i,j}$ do not contain $-I$ and we have $G_i = \pm H_{i,j}$.

Define the rational functions

$$
\begin{aligned}
J_1(t) &= 3^3 \cdot 5 \cdot 7^5/2^7 \\
J_2(t) &= \frac{t(t+1)^3(t^2-5t+1)^3(t^2-5t+8)^3(t^4-5t^3+8t^2-7t+7)^3}{(t^3-4t^2+3t+1)^7} \\
J_3(t) &= \frac{(t^2-t+1)^3(t^6-11t^5+30t^4-15t^3-10t^2+5t+1)^3}{(t-1)^7t^7(t^3-8t^2+5t+1)} \\
J_4(t) &= \frac{(t^2-t+1)^3(t^6+229t^5+270t^4-1695t^3+1430t^2-235t+1)^3}{(t-1)t(t^3-8t^2+5t+1)^7} \\
J_5(t) &= -\frac{(t^2-3t-3)^3(t^2-t+1)^3(3t^2-9t+5)^3(5t^2-t-1)^3}{(t^3-2t^2-t+1)(t^3-t^2-2t+1)^7} \\
J_6(t) &= \frac{64t^3(t^2+7)^3(t^2-7t+14)^3(5t^2-14t-7)^3}{(t^3-7t^2+7t+7)^7} \\
J_7(t) &= \frac{(t^2+245t+2401)^3(t^2+13t+49)}{t^7}
\end{aligned}
$$

Let $\mathcal{E}_1$ be the elliptic curve over $\mathbb{Q}$ defined by the Weierstrass equation

$$y^2 = x^3 - 5^3 7^3 x - 5^4 7^2 106$$

For $t \in \mathbb{Q} - \{0, 1\}$, let $\mathcal{E}_{3,t}$ be the elliptic curve over $\mathbb{Q}$ defined by the Weierstrass equation

$$\begin{aligned} y^2 = x^3 &- 27(t^2 - t + 1)(t^6 - 11t^5 + 30t^4 - 15t^3 - 10t^2 + 5t + 1)x \\ &+54(t^{12} - 18t^{11} + 117t^{10} - 354t^9 + 570t^8 - 486t^7 \\ &\quad + 273t^6 - 222t^5 + 174t^4 - 46t^3 - 15t^2 + 6t + 1). \end{aligned}$$

For $t \in \mathbb{Q} - \{0, 1\}$, let $\mathcal{E}_{4,t}$ be the elliptic curve over $\mathbb{Q}$ defined by the Weierstrass equation

$$\begin{aligned} y^2 = x^3 &- 27(t^2 - t + 1)(t^6 + 229t^5 + 270t^4 - 1695t^3 + 1430t^2 - 235t + 1)x \\ &+54(t^{12} - 522t^{11} - 8955t^{10} + 37950t^9 - 70998t^8 + 131562t^7 \\ &\quad - 253239t^6 + 316290t^5 - 218058t^4 + 80090t^3 - 14631t^2 + 510t + 1). \end{aligned}$$

For $t \in \mathbb{Q}$, let $\mathcal{E}_{5,t}$ be the elliptic curve over $\mathbb{Q}$ defined by the Weierstrass equation

$$\begin{aligned} y^2 = x^3 &- 27 \cdot 7(t^2 - 3t - 3)(t^2 - t + 1)(3t^2 - 9t + 5)(5t^2 - t - 1)x \\ &- 54 \cdot 7^2(t^4 - 6t^3 + 17t^2 - 24t + 9)(3t^4 - 4t^3 - 5t^2 - 2t - 1)(9t^4 - 12t^3 - t^2 + 8t - 3). \end{aligned}$$

For $t \in \mathbb{Q} - \{0\}$, let $\mathcal{E}_{7,t}$ be the elliptic curve over $\mathbb{Q}$ defined by the Weierstrass equation

$$\begin{aligned} y^2 = x^3 &- 27(t^2 + 13t + 49)^3(t^2 + 245t + 2401)x \\ &+ 54(t^2 + 13t + 49)^4(t^4 - 490t^3 - 21609t^2 - 235298t - 823543). \end{aligned}$$

The j-invariant of $\mathcal{E}_{i,t}$ is $J_i(t)$.

Theorem 1.5. *Let E be a non-CM elliptic curve over $\mathbb{Q}$.*

(i) *If $\rho_{E,7}$ is not surjective, then $\rho_{E,7}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_7)$ to one of the groups G_i or $H_{i,j}$.*

(ii) *The group $\rho_{E,7}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to a subgroup of G_i if and only if j_E is of the form $J_i(t)$ for some $t \in \mathbb{Q}$.*

(iii) *The group $\rho_{E,7}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to $H_{1,1}$ if and only if $E/\mathbb{Q}$ is isomorphic to $\mathcal{E}_1$ or to the quadratic twist of $\mathcal{E}_1$ by -7.*

(iv) *Suppose that $\pm\rho_{E,7}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to G_i with $i \in \{3, 4, 5, 7\}$. Fix an element $t \in \mathbb{Q}$ such that $J_i(t) = j_E$.*
The group $\rho_{E,7}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to $H_{i,1}$ if and only if E is isomorphic to $\mathcal{E}_{i,t}$.
The group $\rho_{E,7}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to $H_{i,2}$ if and only if E is isomorphic to the quadratic twist of $\mathcal{E}_{i,t}$ by -7.

1.5. $\underline{\ell = 11}$**.**

- Let G_1 be the subgroup generated by $\pm \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 4 & 0 \\ 0 & 6 \end{smallmatrix}\right)$.
- Let G_2 be the subgroup generated by $\pm \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 5 & 0 \\ 0 & 7 \end{smallmatrix}\right)$.
- Let G_3 be the group $N_{ns}(11)$.
- Let $H_{1,1}$ be the subgroup generated by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 4 & 0 \\ 0 & 6 \end{smallmatrix}\right)$.
- Let $H_{1,2}$ be the subgroup generated by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 7 & 0 \\ 0 & 5 \end{smallmatrix}\right)$.
- Let $H_{2,1}$ be the subgroup generated by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 5 & 0 \\ 0 & 7 \end{smallmatrix}\right)$.
- Let $H_{2,2}$ be the subgroup generated by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 6 & 0 \\ 0 & 4 \end{smallmatrix}\right)$.

The index in $\mathrm{GL}_2(\mathbb{F}_{11})$ of the above subgroups are 60, 60, 55, 110, 120, 120, 120 and 120, respectively. Each of the groups G_i contain $-I$. The groups $H_{i,j}$ do not contain $-I$ and we have $G_i = \pm H_{i,j}$.

Let $\mathcal{E}$ be the elliptic curve over $\mathbb{Q}$ defined by the Weierstrass equation $y^2 + y = x^3 - x^2 - 7x + 10$ and let $\mathcal{O}$ be the point at infinity. The Mordell-Weil group $\mathcal{E}(\mathbb{Q})$ is an infinite cyclic group generated

by the point $(4,5)$. Define

$$J(x,y) := \frac{(f_1 f_2 f_3 f_4)^3}{f_5^2 f_6^{11}},$$

where

$$f_1 = x^2 + 3x - 6, \qquad f_2 = 11(x^2-5)y + (2x^4 + 23x^3 - 72x^2 - 28x + 127),$$
$$f_3 = 6y + 11x - 19, \qquad f_4 = 22(x-2)y + (5x^3 + 17x^2 - 112x + 120),$$
$$f_5 = 11y + (2x^2 + 17x - 34), \qquad f_6 = (x-4)y - (5x-9).$$

We shall view J as a morphism $\mathcal{E} \to \mathbb{A}^1_{\mathbb{Q}} \cup \{\infty\}$.

Let $\mathcal{E}_1/\mathbb{Q}$ be the elliptic curve defined by the Weierstrass equation $y^2 = x^3 - 27 \cdot 11^4 x + 54 \cdot 11^5 \cdot 43$ Let $\mathcal{E}_2/\mathbb{Q}$ be the elliptic curve defined by the Weierstrass equation $y^2 = x^3 - 27 \cdot 11^3 \cdot 131x + 54 \cdot 11^4 \cdot 4973$.

Theorem 1.6. *Let E be a non-CM elliptic curve defined over $\mathbb{Q}$.*

(i) *If $\rho_{E,11}$ is not surjective, then $\rho_{E,11}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_{11})$ to one of the groups G_i or $H_{i,j}$.*
(ii) *The group $\pm\rho_{E,11}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to G_1 in $\mathrm{GL}_2(\mathbb{F}_{11})$ if and only if $j_E = -11^2$.*
(iii) *The group $\pm\rho_{E,11}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to G_2 in $\mathrm{GL}_2(\mathbb{F}_{11})$ if and only if $j_E = -11 \cdot 131^3$.*
(iv) *The group $\rho_{E,11}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to G_3 in $\mathrm{GL}_2(\mathbb{F}_{11})$ if and only if $j_E = J(P)$ for some point $P \in \mathcal{E}(\mathbb{Q}) - \{\mathcal{O}\}$.*
(v) *For $i \in \{1,2\}$, the group $\rho_{E,11}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_{11})$ to $H_{i,1}$ if and only if E is isomorphic to $\mathcal{E}_i$.*
(vi) *For $i \in \{1,2\}$, the group $\rho_{E,11}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_{11})$ to $H_{i,2}$ if and only if E is isomorphic to the quadratic twist of $\mathcal{E}_i$ by -11.*

Remark 1.7. The modular curve $X^+_{ns}(11) = X_{G_3}$ is the only one in our classification that has genus 1 with infinitely many rational points. Halberstadt [Hal98] showed that $X^+_{ns}(11)$ is isomorphic to $\mathcal{E}$ and that the morphism to the j-line corresponds to $J(x,y)$.

In §4.5.5, we give explicit polynomials $A, B, C \in \mathbb{Q}[X]$ of degree 55 such that for a non-CM elliptic curve $E/\mathbb{Q}$, we have $j_E = J(P)$ for some $P \in \mathcal{E}(\mathbb{Q}) - \{\mathcal{O}\}$ if and only if the polynomial $A(x)j_E^2 + B(x)j_E + C(x) \in \mathbb{Q}[x]$ has a rational root. This gives a straightforward way to check the criterion of Theorem 1.6(iv).

1.6. $\underline{\ell = 13}$**.** Define the following subgroups of $\mathrm{GL}_2(\mathbb{F}_{13})$:

- Let G_1 be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} * & * \\ 0 & b^3 \end{smallmatrix}\right)$.
- Let G_2 be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} a^3 & * \\ 0 & * \end{smallmatrix}\right)$.
- Let G_3 be the subgroup consisting of matrices $\left(\begin{smallmatrix} a & * \\ 0 & b \end{smallmatrix}\right)$ for which $(a/b)^4 = 1$.
- Let G_4 be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} * & * \\ 0 & b^2 \end{smallmatrix}\right)$.
- Let G_5 be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} a^2 & * \\ 0 & * \end{smallmatrix}\right)$.
- Let G_6 be the group $B(13)$.
- Let G_7 be the subgroup generated by the matrices $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 3 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 1 \\ -1 & 1 \end{smallmatrix}\right)$; it contains the scalar matrices and its image in $\mathrm{PGL}_2(\mathbb{F}_{13})$ is isomorphic to $\mathfrak{S}_4$.
- Let $H_{4,1}$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} * & * \\ 0 & a^4 \end{smallmatrix}\right)$.
- Let $H_{4,2}$ be the subgroup generated by matrices of the form $\left(\begin{smallmatrix} b^2 & * \\ 0 & a^4 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 4 \end{smallmatrix}\right)$.
- Let $H_{5,1}$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} a^4 & * \\ 0 & * \end{smallmatrix}\right)$.
- Let $H_{5,2}$ be the subgroup generated by matrices of the form $\left(\begin{smallmatrix} a^4 & * \\ 0 & b^2 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 4 & 0 \\ 0 & 2 \end{smallmatrix}\right)$.

The index in $\mathrm{GL}_2(\mathbb{F}_{13})$ of the above subgroups are 42, 42, 42, 28, 28, 14, 91, 56, 56, 56 and 56, respectively. Each of the groups G_i contain $-I$. The groups $H_{i,j}$ do not contain $-I$ and we have $G_i = \pm H_{i,j}$.

Define the polynomials

$$\begin{aligned}
P_1(t) &= t^{12} + 231t^{11} + 269t^{10} - 3160t^9 + 6022t^8 - 9616t^7 + 21880t^6 \\
&\quad - 34102t^5 + 28297t^4 - 12455t^3 + 2876t^2 - 243t + 1 \\
P_2(t) &= t^{12} - 9t^{11} + 29t^{10} - 40t^9 + 22t^8 - 16t^7 + 40t^6 - 22t^5 - 23t^4 + 25t^3 - 4t^2 - 3t + 1 \\
P_3(t) &= (t^4 - t^3 + 2t^2 - 9t + 3)(3t^4 - 3t^3 - 7t^2 + 12t - 4)(4t^4 - 4t^3 - 5t^2 + 3t - 1) \\
P_4(t) &= t^8 + 235t^7 + 1207t^6 + 955t^5 + 3840t^4 - 955t^3 + 1207t^2 - 235t + 1 \\
P_5(t) &= t^8 - 5t^7 + 7t^6 - 5t^5 + 5t^3 + 7t^2 + 5t + 1 \\
P_6(t) &= t^4 + 7t^3 + 20t^2 + 19t + 1 \\
Q_4(t) &= t^{12} - 512t^{11} - 13079t^{10} - 32300t^9 - 104792t^8 - 111870t^7 \\
&\quad - 419368t^6 + 111870t^5 - 104792t^4 + 32300t^3 - 13079t^2 + 512t + 1, \\
Q_5(t) &= t^{12} - 8t^{11} + 25t^{10} - 44t^9 + 40t^8 + 18t^7 - 40t^6 - 18t^5 + 40t^4 + 44t^3 + 25t^2 + 8t + 1
\end{aligned}$$

and the rational functions

$$\begin{aligned}
J_1(t) &= \frac{(t^2 - t + 1)^3 P_1(t)^3}{(t-1)t(t^3 - 4t^2 + t + 1)^{13}} & J_2(t) &= \frac{(t^2 - t + 1)^3 P_2(t)^3}{(t-1)^{13}t^{13}(t^3 - 4t^2 + t + 1)} \\
J_3(t) &= -\frac{13^4(t^2 - t + 1)^3 P_3(t)^3}{(t^3 - 4t^2 + t + 1)^{13}(5t^3 - 7t^2 - 8t + 5)} & J_4(t) &= \frac{(t^4 - t^3 + 5t^2 + t + 1)P_4(t)^3}{t(t^2 - 3t - 1)^{13}} \\
J_5(t) &= \frac{(t^4 - t^3 + 5t^2 + t + 1)P_5(t)^3}{t^{13}(t^2 - 3t - 1)} & J_6(t) &= \frac{(t^2 + 5t + 13)P_6(t)^3}{t}.
\end{aligned}$$

For $t \in \mathbb{Q} - \{0\}$, let $\mathcal{E}_{4,t}$ be the elliptic curve over $\mathbb{Q}$ defined by the Weierstrass equation

$$y^2 = x^3 - 27(t^4 - t^3 + 5t^2 + t + 1)^3 P_4(t)x + 54(t^2 + 1)(t^4 - t^3 + 5t^2 + t + 1)^4 Q_4(t).$$

For $t \in \mathbb{Q} - \{0\}$, let $\mathcal{E}_{5,t}$ be the elliptic curve over $\mathbb{Q}$ defined by the Weierstrass equation

$$y^2 = x^3 - 27(t^4 - t^3 + 5t^2 + t + 1)^3 P_5(t)x + 54(t^2 + 1)(t^4 - t^3 + 5t^2 + t + 1)^4 Q_5(t).$$

Theorem 1.8. *Let E be a non-CM elliptic curve over $\mathbb{Q}$.*

(i) *If $\rho_{E,13}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to a subgroup of $B(13)$, then $\rho_{E,13}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to one of the groups G_i with $1 \le i \le 6$ or to a group $H_{i,j}$.*

(ii) *For $1 \le i \le 6$, $\rho_{E,13}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_{13})$ to a subgroup of G_i if and only if j_E is of the form $J_i(t)$ for some $t \in \mathbb{Q}$.*

(iii) *For an $i \in \{4, 5\}$, suppose that $J_i(t) = j_E$ for some $t \in \mathbb{Q}$.*
The group $\rho_{E,13}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to $H_{i,1}$ if and only if E is isomorphic to $\mathcal{E}_{i,t}$.
The group $\rho_{E,13}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to $H_{i,2}$ if and only if E is isomorphic to the quadratic twist of $\mathcal{E}_{i,t}$ by 13.

(iv) *If j_E is*

$$\frac{2^4 \cdot 5 \cdot 13^4 \cdot 17^3}{3^{13}}, \quad -\frac{2^{12} \cdot 5^3 \cdot 11 \cdot 13^4}{3^{13}} \quad \text{or} \quad \frac{2^{18} \cdot 3^3 \cdot 13^4 \cdot 127^3 \cdot 139^3 \cdot 157^3 \cdot 283^3 \cdot 929}{5^{13} \cdot 61^{13}},$$

then $\rho_{E,13}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to G_7.

Up to conjugacy, there are four maximal subgroups G of $\mathrm{GL}_2(\mathbb{F}_{13})$ that satisfy $\det(G) = \mathbb{F}_{13}^\times$; they are $G_6 = B(13)$, $N_s(13)$, $N_{ns}(13)$ and G_7. The cases concerning subgroups of $B(13)$ are completely handled in Theorem 1.8.

Baran [Bar14] has shown that the modular curves $X_s^+(13)$ and $X_{ns}^+(13)$ attached to $N_s(13)$ and $N_{ns}(13)$, respectively, are both isomorphic to the genus 3 curve C defined in $\mathbb{P}^2_{\mathbb{Q}}$ by the equation

$$(-y-z)x^3 + (2y^2+zy)x^2 + (-y^3+zy^2-2z^2y+z^3)x + (2z^2y^2-3z^3y) = 0.$$

In [Bar14], the morphism from the model of the modular curves to the j-line is given. The seven rational points $(0,0,1)$, $(0,1,0)$, $(0,3,2)$, $(1,0,-1)$, $(1,0,0)$, $(1,0,1)$, $(1,1,0)$ of C all correspond to cusps and CM points on $X_s(13)$ and $X_{ns}(13)$. Conjecturally, there are no non-CM elliptic curves E over $\mathbb{Q}$ with $\rho_{E,13}(\mathrm{Gal}_{\mathbb{Q}})$ conjugate to a subgroup of $N_s(13)$ or $N_{ns}(13)$; equivalently, C has no other rational points.

Denote by $X_{\mathfrak{S}_4}(13)$ the modular curve corresponding to G_7. Banwait and Cremona [BC14] have shown that $X_{\mathfrak{S}_4}(13)$ is isomorphic to the genus 3 curve C' defined in $\mathbb{P}^2_{\mathbb{Q}}$ by the equation

$$4x^3y - 3x^2y^2 + 3xy^3 - x^3z + 16x^2yz - 11xy^2z + 5y^3z + 3x^2z^2 + 9xyz^2 + y^2z^2 + xz^3 + 2yz^3 = 0$$

and have found the morphism from the modular curve to the j-line. The four rational points $(0,1,0)$, $(0,0,1)$, $(1,0,0)$ and $(1,3,-2)$ of C' correspond to a CM point and three non-CM points; the non-CM points give rise to the three j-invariants in Theorem 1.8(iv).

Suppose $E/\mathbb{Q}$ is an elliptic curve with one of the j-invariants from Theorem 1.8(iv). From [BC14], we find that the image of $\rho_{E,13}(\mathrm{Gal}_{\mathbb{Q}})$ in $\mathrm{PGL}_2(\mathbb{F}_{13})$ is isomorphic to $\mathfrak{S}_4$. Therefore, $\rho_{E,13}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to G_7 since G_7 has no proper subgroups H whose image in $\mathrm{PGL}_2(\mathbb{F}_{13})$ is isomorphic to $\mathfrak{S}_4$ and satisfies $\det(H) = \mathbb{F}_{13}^\times$. In particular, this proves Theorem 1.8(iv).

Conjecturally, if E is a non-CM elliptic curve over $\mathbb{Q}$, then $\rho_{E,13}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to a subgroup of G_7 if and only if j_E is one of three values from Theorem 1.8(iv); equivalently, C' has no other rational points.

Remark 1.9. The case $\ell = 13$ is the first for which we do not have a complete description. As explained above, it remains to determine all the rational points of the genus 3 curves C and C'.

1.7. $\underline{\ell \geq 17}$**.** We first describe all the known cases of non-CM elliptic curves $E/\mathbb{Q}$ for which $\rho_{E,\ell}$ is not surjective for some prime $\ell \geq 17$. Define the following groups:

- Let G_1 be the subgroup of $\mathrm{GL}_2(\mathbb{F}_{17})$ generated by $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 11 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 4 & 0 \\ 0 & -4 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.
- Let G_2 be the subgroup of $\mathrm{GL}_2(\mathbb{F}_{17})$ generated by $\left(\begin{smallmatrix} 11 & 0 \\ 0 & 2 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} -4 & 0 \\ 0 & 4 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.
- Let G_3 be the subgroup of $\mathrm{GL}_2(\mathbb{F}_{37})$ consisting of the matrices of the form $\left(\begin{smallmatrix} a^3 & * \\ 0 & * \end{smallmatrix}\right)$.
- Let G_4 be the subgroup of $\mathrm{GL}_2(\mathbb{F}_{37})$ consisting of the matrices of the form $\left(\begin{smallmatrix} * & * \\ 0 & a^3 \end{smallmatrix}\right)$.

Theorem 1.10.

(i) *If $E/\mathbb{Q}$ has j-invariant $-17 \cdot 373^3/2^{17}$ or $-17^2 \cdot 101^3/2$, then $\rho_{E,17}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_{17})$ to G_1 or G_2, respectively.*

(ii) *If $E/\mathbb{Q}$ has j-invariant $-7\cdot 11^3$ or $-7\cdot 137^3\cdot 2083^3$, then $\rho_{E,37}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_{37})$ to G_3 or G_4, respectively.*

Theorem 1.11 (Mazur, Serre, Bilu-Parent-Rebolledo)**.** *Fix a prime $\ell \geq 17$ and let E be a non-CM elliptic curve defined over $\mathbb{Q}$. If (ℓ, j_E) does not belong to the set*

$$\{(17, -17\cdot 373^3/2^{17}),\ (17, -17^2\cdot 101^3/2),\ (37, -7\cdot 11^3),\ (37, -7\cdot 137^3\cdot 2083^3)\}, \tag{1.1}$$

then either $\rho_{E,\ell}$ is surjective or $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to a subgroup of $N_{ns}(\ell)$.

Proof. The group $\mathrm{GL}_2(\mathbb{F}_\ell)$ has either three or four maximal subgroups with determinant $\mathbb{F}_\ell^\times$. They are $B(\ell)$, $N_s(\ell)$, $N_{ns}(\ell)$ and when $\ell \equiv \pm 3 \pmod 8$, we also have a maximal subgroup $H_{\mathfrak{S}_4}(\ell)$ whose image in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is isomorphic to the symmetric group $\mathfrak{S}_4$.

Take any non-CM elliptic curve E over $\mathbb{Q}$. Serre has shown that $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ cannot be conjugate to a subgroup of $H_{\mathfrak{S}_4}(\ell)$, cf. [Ser81, §8.4]. Bilu, Parent and Rebolledo have proved that $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ cannot be conjugate to a subgroup of $N_s(\ell)$, cf. [BPR11] (they make effective the bounds in earlier works of Bilu and Parent using improved isogeny bounds of Gaudron and Rémond). The $B(\ell)$ case follows from a famous theorem of Mazur, cf. [Maz78]. The modular curves $X_0(17)$ and $X_0(37)$ each have two rational points which are not cusps or CM points and they are accounted for by the curves of Theorem 1.10. □

We conjecture that Theorem 1.11 describes all the reasons that $\rho_{E,\ell}$ can fail to be surjective for a non-CM $E/\mathbb{Q}$ and a prime $\ell \geq 17$; this is a problem raised by Serre, cf. [Ser81, p.399], who asked if $\rho_{E,\ell}$ is surjective whenever $\ell > 37$.

Conjecture 1.12. *If E is a non-CM elliptic curve over $\mathbb{Q}$ and $\ell \geq 17$ is a prime such that the pair (ℓ, j_E) does not belong to the set (1.1), then $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q}) = \mathrm{GL}_2(\mathbb{F}_\ell)$.*

Even if Conjecture 1.12 is false for some $E/\mathbb{Q}$ and $\ell \geq 17$, the following proposition gives at most two possibilities for the image of $\rho_{E,\ell}$ (they can be distinguished computationally by looking at the division polynomial of E at ℓ).

Proposition 1.13. *Suppose that $\rho_{E,\ell}$ is not surjective for a non-CM elliptic curve $E/\mathbb{Q}$ and a prime $\ell \geq 17$ for which (ℓ, j_E) does not lie in the set (1.1).*

(i) *If $\ell \equiv 1 \pmod 3$, then $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_\ell)$ to $N_{ns}(\ell)$.*

(ii) *If $\ell \equiv 2 \pmod 3$, then $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_\ell)$ to $N_{ns}(\ell)$ or to the group*

$$G := \left\{a^3 : a \in C_{ns}(\ell)\right\} \cup \left\{ \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \cdot a^3 : a \in C_{ns}(\ell)\right\}.$$

1.8. **Algorithm.** Let $E/\mathbb{Q}$ be a non-CM elliptic curve (when $E/\mathbb{Q}$ has complex multiplication, the groups $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ are all described in §1.9 below). In [Zyw15], we give an algorithm to compute the set S' of primes $\ell \geq 13$ for which $\rho_{E,\ell}$ is not surjective.

Combined with the theorems from §§1.1–1.5, we are now able to compute the (finite) set S of primes ℓ for which $\rho_{E,\ell}$ is not surjective. Moreover, using the results from §§1.1–1.5, we can give the group $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$, up to conjugacy in $\mathrm{GL}_2(\mathbb{F}_\ell)$, for each $\ell \in S$.

Sutherland has a probabilistic algorithm to determine the groups $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ by consider Frobenius at many primes p, [Sut15]. His algorithm can in principle be made deterministic using effective versions of the Chebotarev density theorem. Sutherland's algorithm has the advantage that it can be used for elliptic curves over a number field $K \neq \mathbb{Q}$ (for our approach, we would have more modular curves to consider and those modular curves not isomorphic to $\mathbb{P}^1_\mathbb{Q}$ would need to be reconsidered).

The next task that needs to be completed is to consider the images of ρ_{E,ℓ^n} for small primes ℓ and $n \geq 2$. Rouse and Zureick-Brown have already done this for $\ell = 2$, cf. [RZB14]; the case $\ell = 2$ is rather accessible since all the groups that occur are solvable.

1.9. **Complex multiplication.** Up to isomorphism over $\overline{\mathbb{Q}}$, there are thirteen elliptic curves with complex multiplication that are defined over $\mathbb{Q}$. In Table 1 below, we give an elliptic curve $E_{D,f}/\mathbb{Q}$ with each of these thirteen j-invariants (this comes from [Sil94, Appendix A §3] though with some different models). The curve $E_{D,f}$ has conductor N and has complex multiplication by an order R of conductor f in the imaginary quadratic field with discriminant $-D$.

j-invariant	D	f	Elliptic curve $E_{D,f}$	N
0	3	1	$y^2 = x^3 + 16$	3^3
$2^4 3^3 5^3$		2	$y^2 = x^3 - 15x + 22$	$2^2 3^2$
$-2^{15} 3 \cdot 5^3$		3	$y^2 = x^3 - 480x + 4048$	3^3
$2^6 3^3 = 1728$	4	1	$y^2 = x^3 + x$	2^6
$2^3 3^3 11^3$		2	$y^2 = x^3 - 11x + 14$	2^5
$-3^3 5^3$	7	1	$y^2 = x^3 - 1715x + 33614$	7^2
$3^3 5^3 17^3$		2	$y^2 = x^3 - 29155x + 1915998$	7^2
$2^6 5^3$	8	1	$y^2 = x^3 - 4320x + 96768$	2^8
-2^{15}	11	1	$y^2 = x^3 - 9504x + 365904$	11^2
$-2^{15} 3^3$	19	1	$y^2 = x^3 - 608x + 5776$	19^2
$-2^{18} 3^3 5^3$	43	1	$y^2 = x^3 - 13760x + 621264$	43^2
$-2^{15} 3^3 5^3 11^3$	67	1	$y^2 = x^3 - 117920x + 15585808$	67^2
$-2^{18} 3^3 5^3 23^3 29^3$	163	1	$y^2 = x^3 - 34790720x + 78984748304$	163^2

TABLE 1. CM elliptic curves over $\mathbb{Q}$

We first describe the group $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ up to conjugacy when E is a CM elliptic curve with non-zero j-invariant and ℓ odd.

Proposition 1.14. *Let E be a CM elliptic curve defined over $\mathbb{Q}$ with $j_E \neq 0$. The ring of endomorphisms of $E_{\overline{\mathbb{Q}}}$ is an order of conductor f in the ring of integers of an imaginary quadratic field of discriminant $-D$. Take any odd prime ℓ.*

(i) *If $\left(\frac{-D}{\ell}\right) = 1$, then $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_\ell)$ to $N_s(\ell)$.*
(ii) *If $\left(\frac{-D}{\ell}\right) = -1$, then $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_\ell)$ to $N_{ns}(\ell)$.*
(iii) *Suppose that ℓ divides D and hence $D = \ell$. Define the groups*

$$G = \left\{\left(\begin{smallmatrix} a & b \\ 0 & \pm a \end{smallmatrix}\right) : a \in \mathbb{F}_\ell^\times, b \in \mathbb{F}_\ell\right\},$$

$$H_1 = \left\{\left(\begin{smallmatrix} a & b \\ 0 & \pm a \end{smallmatrix}\right) : a \in (\mathbb{F}_\ell^\times)^2, b \in \mathbb{F}_\ell\right\}, \quad \text{and} \quad H_2 = \left\{\left(\begin{smallmatrix} \pm a & b \\ 0 & a \end{smallmatrix}\right) : a \in (\mathbb{F}_\ell^\times)^2, b \in \mathbb{F}_\ell\right\}$$

If E is isomorphic to $E_{D,f}$, then $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_\ell)$ to H_1.
If E is isomorphic to the quadratic twist of $E_{D,f}$ by $-\ell$, then $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_\ell)$ to H_2.
If E is not isomorphic to $E_{D,f}$ or its quadratic twist by $-\ell$, then $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_\ell)$ to G.

The following deals with the excluded prime $\ell = 2$.

Proposition 1.15. *Let $E/\mathbb{Q}$ be a CM elliptic curve. Define the subgroup $G_2 = \{I, \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\}$ of $\mathrm{GL}_2(\mathbb{F}_2)$.*

(i) *If $j_E \in \{2^4 3^3 5^3, 2^3 3^3 11^3, -3^3 5^3, 3^3 5^3 17^3, 2^6 5^3\}$, then $\rho_{E,2}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to G_2.*
(ii) *If $j_E \in \{-2^{15} 3 \cdot 5^3, -2^{15}, -2^{15} 3^3, -2^{18} 3^3 5^3, -2^{15} 3^3 5^3 11^3, -2^{18} 3^3 5^3 23^3 29^3\}$, then $\rho_{E,2}(\mathrm{Gal}_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{F}_2)$.*

(iii) *Suppose that $j_E = 1728$. The curve can be given by a Weierstrass equation $y^2 = x^3 - dx$ for some $d \in \mathbb{Q}^\times$.*
If d is a square, then $\rho_{E,2}(\mathrm{Gal}_\mathbb{Q}) = \{I\}$.
If d is not a square, then the group $\rho_{E,2}(\mathrm{Gal}_\mathbb{Q})$ is conjugate to G_2.

(iv) *Suppose that $j_E = 0$. The curve E can be given by a Weierstrass equation $y^2 = x^3 + d$ for some $d \in \mathbb{Q}^\times$.*
If d is a cube, then $\rho_{E,2}(\mathrm{Gal}_\mathbb{Q})$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_2)$ to the group G_2.
If d is not a cube, then $\rho_{E,2}(\mathrm{Gal}_\mathbb{Q}) = \mathrm{GL}_2(\mathbb{F}_2)$.

It remains to consider the situation where ℓ is an odd prime and $E/\mathbb{Q}$ is an elliptic curve with $j_E = 0$. That such curves have cubic twists make the classification more involved.

Proposition 1.16. *Let E be an elliptic curve over $\mathbb{Q}$ with $j_E = 0$. Take any odd prime ℓ.*

(i) *If $\ell \equiv 1 \pmod 9$, then $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ is conjugate to $N_s(\ell)$ in $\mathrm{GL}_2(\mathbb{F}_\ell)$.*

(ii) *If $\ell \equiv 8 \pmod 9$, then $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ is conjugate to $N_{ns}(\ell)$ in $\mathrm{GL}_2(\mathbb{F}_\ell)$.*

(iii) *Suppose that ℓ is congruent to 4 or 7 modulo 9. Let $E'/\mathbb{Q}$ be the elliptic curve over $\mathbb{Q}$ defined by $y^2 = x^3 + 16\ell^e$, where $e \in \{1, 2\}$ satisfies $\frac{\ell-1}{3} \equiv e \pmod 3$.*
If E is not isomorphic to a quadratic twist of E', then $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ is conjugate to $N_s(\ell)$ in $\mathrm{GL}_2(\mathbb{F}_\ell)$.
If E is isomorphic to a quadratic twist of E', then $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_\ell)$ to the subgroup G of $N_s(\ell)$ consisting of the matrices of the form $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 0 & a \\ b & 0 \end{smallmatrix}\right)$ with $a/b \in (\mathbb{F}_\ell^\times)^3$.

(iv) *Suppose that ℓ is congruent to 2 or 5 modulo 9. Let $E'/\mathbb{Q}$ be the elliptic curve over $\mathbb{Q}$ defined by $y^2 = x^3 + 16\ell^e$, where $e \in \{1, 2\}$ satisfies $\frac{\ell+1}{3} \equiv -e \pmod 3$.*
If E is not isomorphic to a quadratic twist of E', then $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ is conjugate to $N_{ns}(\ell)$ in $\mathrm{GL}_2(\mathbb{F}_\ell)$.
If E is isomorphic to a quadratic twist of E', then $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_\ell)$ to the subgroup G of $N_{ns}(\ell)$ generated by the unique index 3 subgroup of $C_{ns}(\ell)$ and by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.

(v) *Suppose that $\ell = 3$. The curve E can be given by a Weierstrass equation $y^2 = x^3 + d$ for some $d \in \mathbb{Q}^\times$. Fix notation as in §1.2.*
If d or $-3d$ is a square and $-4d$ is a cube, then $\rho_{E,3}(\mathrm{Gal}_\mathbb{Q})$ is conjugate to $H_{1,1}$.
If d and $-3d$ are not squares and $-4d$ is a cube, then $\rho_{E,3}(\mathrm{Gal}_\mathbb{Q})$ is conjugate to G_1.
If d is a square and $-4d$ is not a cube, then $\rho_{E,3}(\mathrm{Gal}_\mathbb{Q})$ is conjugate to $H_{3,1}$.
If $-3d$ is a square and $-4d$ is not a cube, then $\rho_{E,3}(\mathrm{Gal}_\mathbb{Q})$ is conjugate to $H_{3,2}$.
If d and $-3d$ are not squares and $-4d$ is not a cube, then $\rho_{E,3}(\mathrm{Gal}_\mathbb{Q})$ is conjugate to G_3.

1.10. **Overview.** We now give a very brief overview of the paper. In §2, we describe applicable subgroups G of $\mathrm{GL}_2(\mathbb{F}_\ell)$; these groups have many of the properties that the groups $\pm\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ do.

In §3, we recall what we need concerning the modular curve $X_G/\mathbb{Q}$; we will identify its function field with a subfield of the field of modular function for the congruence subgroup $\Gamma(\ell)$.

In §4, we prove the parts of our main theorems that determine $\pm\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$. We describe the rational points of X_G when ℓ is small. When X_G has genus 0 and $X_G(\mathbb{Q}) \neq \emptyset$, then the function field of X_G is of the form $\mathbb{Q}(h)$ for some modular function h. Much of this section is dedicated to describing such h and determining the rational function $J(t) \in \mathbb{Q}(t)$ such that $J(h)$ is the modular j-invariant.

Assuming that $G := \pm\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ is known, with $E/\mathbb{Q}$ non-CM, we describe in §5 how to determine the (finite number of) quadratic twists of E' of E for which $\rho_{E',\ell}(\mathrm{Gal}_\mathbb{Q})$ is not conjugate to G. In §6, we prove the parts of our main theorems that determine $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ given $\pm\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$.

In §7, we prove the propositions from §1.9 concerning CM elliptic curves defined over $\mathbb{Q}$. The j-invariant 0 case requires special attention since one has to worry about cubic twists. Finally, in §8, we prove Proposition 1.13.

The equations in §1.1–1.7 and `Magma` code verifying some claims in §4 and §6 can be found at:

http://www.math.cornell.edu/~zywina/papers/PossibleImages/

Acknowledgments. Thanks to Andrew Sutherland, David Zureick-Brown and René Schoof. The computations in this paper were performed using the `Magma` computer algebra system [BCP97].

2. Applicable subgroups

Fix an integer $N \geq 2$. For an elliptic curve $E/\mathbb{Q}$, let $E[N]$ be the N-torsion subgroup of $E(\overline{\mathbb{Q}})$. After choosing a basis for $E[N]$ as a $\mathbb{Z}/N\mathbb{Z}$-module, the natural $\mathrm{Gal}_{\mathbb{Q}}$-action on $E[N]$ can be expressed in terms of a Galois representation

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

When N is a prime, these agree with the representations of §1. We now describe some restrictions on the possible images of $\rho_{E,N}$.

Definition 2.1. We say that a subgroup G of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is applicable if it satisfies the following conditions:

- $G \neq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$,
- $-I \in G$ and $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$,
- G contains an element with trace 0 and determinant -1 that fixes a point in $(\mathbb{Z}/N\mathbb{Z})^2$ of order N.

This definition is justified by the following.

Proposition 2.2. *Let E be an elliptic curve over $\mathbb{Q}$ for which $\rho_{E,N}$ is not surjective. Then $\pm\rho_{E,N}(\mathrm{Gal}_{\mathbb{Q}})$ is an applicable subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.*

Proof. The group $G := \pm\rho_{E,N}(\mathrm{Gal}_{\mathbb{Q}})$ clearly contains $-I$. The character $\det\circ\rho_{E,N}\colon \mathrm{Gal}_{\mathbb{Q}} \to (\mathbb{Z}/N\mathbb{Z})^\times$ is the surjective homomorphism describing the Galois action on the group of N-th roots of unity in $\overline{\mathbb{Q}}$, i.e., for a N-th root of unity $\zeta \in \overline{\mathbb{Q}}$, we have $\sigma(\zeta) = \zeta^{\det(\rho_{E,N}(\sigma))}$ for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$. Therefore, $\det\circ\rho_{E,N}$ is surjective and hence $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$.

Let $c \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be an automorphism corresponding to complex conjugation under some embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. Set $g := \rho_{E,N}(c)$. As a topological group, the connected component of $E(\mathbb{R})$ containing the identity is isomorphic to $\mathbb{R}/\mathbb{Z}$. Therefore, $E(\mathbb{R})$ contains a point P_1 of order N. We may assume that $\rho_{E,N}$ is chosen with respect to a basis whose first term is P_1, and hence g is upper triangular whose first diagonal term is 1. We have $\det(g) = -1$ since c acts by inversion on N-th roots of unity. Therefore, g is upper triangular with diagonal entries 1 and -1, and hence $\mathrm{tr}(g) = 0$.

Now suppose that $G = \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Define $S = \rho_{E,N}(\mathrm{Gal}_{\mathbb{Q}}) \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Since $G = \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, $\rho_{E,N}(\mathrm{Gal}_{\mathbb{Q}}) \neq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and $\det(\rho_{E,N}(\mathrm{Gal}_{\mathbb{Q}})) = (\mathbb{Z}/N\mathbb{Z})^\times$, we deduce that $S \neq \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and $\pm S = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. However, this is impossible by Lemma 2.3 below, so we must have $G \neq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. □

Lemma 2.3. *There is no proper subgroup S of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ such that $\pm S = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.*

Proof. Suppose that S is a subgroup of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ for which $\pm S = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. By [Zyw10, Lemma A.6], we deduce that there is a prime power ℓ^e dividing N such that the image $\tilde{S}$ of S in $\mathrm{SL}_2(\mathbb{Z}/\ell^e\mathbb{Z})$ is a proper subgroup satisfying $\pm\tilde{S} = \mathrm{SL}_2(\mathbb{Z}/\ell^e\mathbb{Z})$. So without loss of generality, we may assume that $N = \ell^e$.

The group S has index 2 in $\mathrm{SL}_2(\mathbb{Z}/\ell^e\mathbb{Z})$. Therefore, S is normal in $\mathrm{SL}_2(\mathbb{Z}/\ell^e\mathbb{Z})$ and the quotient is cyclic of order 2. However, the abelianization of $\mathrm{SL}_2(\mathbb{Z}/\ell^e\mathbb{Z})$ is a cyclic group of order $\gcd(\ell^e, 12)$, cf. [Zyw10, Lemma A.1]. Therefore, we must have $\ell = 2$. Since the abelianization of $\mathrm{SL}_2(\mathbb{Z}/2^e\mathbb{Z})$ is

cyclic of order 2 or 4, we find that S is the unique subgroup of $\mathrm{SL}_2(\mathbb{Z}/2^e\mathbb{Z})$ of index 2. The group S is now easy to describe; it is the group of elements in $\mathrm{SL}_2(\mathbb{Z}/2^e\mathbb{Z})$ whose image in $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ lies in the unique cyclic group of order 3. However, this implies that $\pm S \neq \mathrm{SL}_2(\mathbb{Z}/2^e\mathbb{Z})$ since $-I \equiv I \pmod 2$. This contradiction ensures that no such S exists. □

Remark 2.4. When N is a prime ℓ, which is the setting of this paper, the last condition in the definition of applicable subgroup can be simplified to say simply that G contains an element with trace 0 and determinant -1.

3. Modular curves

Fix an integer $N \geq 1$; in our later application, we will take N to be a prime ℓ. In §3.1, we recall the Galois theory of the field of modular functions of level N. In §3.2, we define modular curves in terms of their functions fields. We take an unsophisticated approach to modular curves and develop what we need from Shimura's book [Shi94]; it will be useful for reference in future work. Alternatively, one could develop modular curves as in [DR73, IV-3].

3.1. **Modular functions of level N.** The group $\mathrm{SL}_2(\mathbb{Z})$ acts on the complex upper half plane $\mathfrak{h}$ via linear fractional transformations, i.e., $\gamma_*(\tau) = (a\tau + b)/(c\tau + d)$ for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $\tau \in \mathfrak{h}$. Let $\Gamma(N)$ be the congruence subgroup consisting of matrices in $\mathrm{SL}_2(\mathbb{Z})$ that are congruent to I modulo N. The quotient $\Gamma(N)\backslash\mathfrak{H}$ is a Riemann surface and can be completed to a compact and smooth Riemann surface X_N. Let τ be a variable of the complex upper half plane.

Every meromorphic function f on X_N has a q-expansion $\sum_{n\in\mathbb{Z}} c_n q^{n/N}$; here the c_n are complex numbers which are 0 for all but finitely many negative n and $q^{1/N} := e^{2\pi i\tau/N}$. We define $\mathcal{F}_N$ to be the field of meromorphic functions on X_N whose q-expansion has coefficients in $\mathbb{Q}(\zeta_N)$, where ζ_N is the N-th root of unity $e^{2\pi i/N}$. For example, $\mathcal{F}_1 = \mathbb{Q}(j)$ where $j = j(\tau)$ is the modular j-invariant with the familiar expansion

$$j = q^{-1} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \dots.$$

For each $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, let σ_d be the automorphism of the field $\mathbb{Q}(\zeta_N)$ for which $\sigma_d(\zeta_N) = \zeta_N^d$. We extend σ_d to an automorphism of $\mathcal{F}_N$ by taking a function with q-expansion $\sum_n c_n q^{n/N}$ to $\sum_n \sigma_d(c_n) q^{n/N}$. We let $\mathrm{SL}_2(\mathbb{Z})$ act on $\mathcal{F}_N$ by taking a modular function $f \in \mathcal{F}_N$ and a matrix $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ to $f \circ \gamma^t$, i.e., the function $(f \circ \gamma^t)(\tau) = f(\gamma_*^t(\tau))$ where γ^t is the transpose of γ.

Proposition 3.1. *The extension $\mathcal{F}_N$ of $\mathbb{Q}(j)$ is Galois. There is a unique isomorphism*

$$\theta_N \colon \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\} \xrightarrow{\sim} \mathrm{Gal}(\mathcal{F}_N/\mathbb{Q}(j))$$

such that the following holds for all $f \in \mathcal{F}_N$:

(a) *For $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, we have $\theta_N(A)f = f \circ \gamma^t$, where γ is any matrix in $\mathrm{SL}_2(\mathbb{Z})$ that is congruent to A modulo N.*

(b) *For $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, we have $\theta_N(A)f = \sigma_d(f)$.*

The field $\mathbb{Q}(\zeta_N)$ is the algebraic closure of $\mathbb{Q}$ in $\mathcal{F}_N$ and corresponds to the subgroup $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$.

We will sketch Propostion 3.1 in §3.4. Throughout the paper, we will let $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ act on $\mathcal{F}_N$ via the isomorphism θ_N (with $-I$ acting trivially).

Remark 3.2. There are other choices for an isomorphism $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$; for example, one could instead replace the transpose by an inverse in (a). Our choice is explained by our application to modular curves. As a warning, there are several places in the literature where incompatible choices are made with respect to modular curves.

3.2. **Modular curves.** Let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ containing $-I$ that satisfies $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$. Denote by $\mathcal{F}_N^G$ the subfield of $\mathcal{F}_N$ fixed by the action of G from Proposition 3.1. Using Proposition 3.1 and the assumption $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$, we find that $\mathbb{Q}$ is algebraically closed in $\mathcal{F}_N^G$.

Let X_G be the smooth projective curve with function field $\mathcal{F}_N^G$; it is defined over $\mathbb{Q}$ and is geometrically irreducible. The inclusion of fields $\mathcal{F}_N^G \supseteq \mathbb{Q}(j)$ gives rise to a non-constant morphism

$$\pi_G \colon X_G \to \operatorname{Spec} \mathbb{Q}[j] \cup \{\infty\} = \mathbb{P}^1_{\mathbb{Q}}.$$

The morphism π_G is non-constant and we have

$$\deg(\pi_G) = [\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\} : G/\{\pm I\}] = [\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : G].$$

We will also denote the function field $\mathcal{F}_N^G$ of X_G by $\mathbb{Q}(X_G)$. A point in X_G is a cusp or a CM point if π_G maps it to ∞ or to the j-invariant of a CM elliptic curve, respectively.

The following property of the curve X_G is key to our application; we will give a proof in §3.5.

Proposition 3.3. *Let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that contains $-I$ and satisfies $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$. Let E be an elliptic curve defined over $\mathbb{Q}$ with $j_E \notin \{0, 1728\}$. Then $\rho_{E,N}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ to a subgroup of G if and only if j_E belongs to $\pi_G(X_G(\mathbb{Q}))$.*

The following lemma will be key to finding modular curves of genus 0 with rational points.

Lemma 3.4. *Fix a modular function $h \in \mathcal{F}_N - \mathbb{Q}(j)$ such that $J(h) = j$ for a rational function $J(t) \in \mathbb{Q}(t)$. Let G be the subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that fixes h under the action on $\mathcal{F}_N$ from Proposition 3.1.*

(i) *The subgroup G of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is applicable.*
(ii) *The modular curve X_G has function field $\mathbb{Q}(h)$. In particular, it is isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$.*
(iii) *Let $E/\mathbb{Q}$ be an elliptic curve with $j_E \notin \{0, 1728\}$. The group $\rho_{E,N}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ to a subgroup of G if and only if $j_E = J(t)$ for some $t \in \mathbb{Q} \cup \{\infty\}$.*

Proof. By the Galois correspondence coming from the isomorphism θ_N of Proposition 3.1, the field $\mathbb{Q}(h)$ equals $\mathcal{F}_N^G$ and is an extension of $\mathbb{Q}(j)$ of degree

$$[\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\} : G/\{\pm I\}] = [\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : G].$$

The field $\mathbb{Q}$ is algebraically closed in $\mathcal{F}_N^G = \mathbb{Q}(h)$, so $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$ by Proposition 3.1. Therefore, $\mathbb{Q}(h)$ is the function field of X_G and the field extension $\mathbb{Q}(h)/\mathbb{Q}(j)$ given by $j = J(h)$ corresponds to the morphism $\pi_G \colon X_G \to \mathbb{P}^1_{\mathbb{Q}}$. The modular curve X_G is thus isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$ and we have $\pi_G(X_G(\mathbb{Q})) = J(\mathbb{Q} \cup \{\infty\})$. This proves (ii). Part (iii) follows from Proposition 3.3.

Finally, we prove that G is applicable. We have $G \neq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ since the extension $\mathbb{Q}(h)/\mathbb{Q}(j)$ is non-trivial by our assumption on h. Using part (iii) and Proposition 2.2, we find that G contains an applicable subgroup. Since $G \neq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and G contains an applicable subgroup, we deduce that G is applicable. □

If X_G has genus 0 and has rational points, then there are in fact curves $E/\mathbb{Q}$ with $\pm\rho_{E,N}(\mathrm{Gal}_{\mathbb{Q}})$ conjugate to G.

Lemma 3.5. *Suppose that X_G is isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$; equivalently, the function field of X_G is of the form $\mathbb{Q}(h)$. We have $j = J(h)$ for a unique $J(t) \in \mathbb{Q}(t)$ because of the inclusion $\mathbb{Q}(h) \supseteq \mathbb{Q}(j)$. Then for "most" $u \in \mathbb{Q}$ (more precisely, outside a set of density 0 with respect to height), the groups $\pm\rho_{E,N}(\mathrm{Gal}_{\mathbb{Q}})$ and G are conjugate in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ for any elliptic curve $E/\mathbb{Q}$ with j-invariant $J(u)$.*

Proof. Let $\mathcal{G}$ be the (finite) set of applicable subgroups H of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ satisfying $H \subsetneq G$. For each $H \in \mathcal{G}$, let $\pi_{H,G}$ be the natural morphism $X_H \to X_G$; it has degree $[G : H] > 1$. To prove the lemma, it suffices to show that the set $\mathcal{S} := \cup_{H\in\mathcal{H}} \pi_{H,G}(X_H(\mathbb{Q}))$ has density 0 (with respect to the height) in $X_G(\mathbb{Q}) \cong \mathbb{P}^1(\mathbb{Q})$. This is a consequence of Hilbert irreducibility; in the language of [Ser97, §9], the set $\mathcal{S}$ is *thin* and hence has density 0. □

3.3. **The modular curve $X_0(N)$.** Let $X_0(N)/\mathbb{Q}$ be the modular curve $X_{B(N)^t}$, where $B(N)^t$ is the transpose of $B(N)$; it consists of the lower triangular matrices and is conjugate to $B(N)$ in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Let $\Gamma_0(N)$ be the group of matrices in $\mathrm{SL}_2(\mathbb{Z})$ whose image modulo N is upper triangular. A function $f \in \mathcal{F}_N$ belongs to $\mathbb{Q}(X_0(N))$ if and only if it has rational Fourier coefficients and $f \circ \gamma = f$ for all $\gamma \in \Gamma_0(N)$. Define the modular curve $X_s(N) := X_{C_s(N)}$, where $C_s(N)$ is the subgroup of diagonal matrices in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

Lemma 3.6. *The map $\mathbb{Q}(X_0(N^2)) \to \mathbb{Q}(X_s(N))$, $f(\tau) \mapsto f(\tau/N)$ is an isomorphism of fields. This isomorphism induces an isomorphism between the modular curves $X_s(N)$ and $X_0(N^2)$ which gives a bijection between their cusps.*

Proof. Let $\Gamma_s(N)$ be the group of matrices in $\mathrm{SL}_2(\mathbb{Z})$ whose image modulo N is diagonal. The function field of $X_s(N)$ then consist of the $f \in \mathcal{F}_N$ with rational Fourier coefficients for which $f \circ \gamma = f$ for all γ in $\Gamma_s(N)$.

Define $w = \left(\begin{smallmatrix} 1 & 0 \\ 0 & N \end{smallmatrix}\right)$; it acts on $\mathfrak{h}$ by linear fractional transformation, i.e., $w_*(\tau) = \tau/N$. Take any $f \in \mathcal{F}_N$ whose Fourier coefficients are rational. We have $f \circ w$ in $\mathbb{Q}(X_s(N))$ if and only if $f \circ w \circ \gamma = f \circ w$ for all $\gamma \in \Gamma_s(N)$. Since $w\Gamma_s(N)w^{-1} = \Gamma_0(N^2)$, we deduce that $f \circ w$ belongs to $\mathbb{Q}(X_s(N))$ if and only if f belongs to $\mathbb{Q}(X_0(N^2))$. It is now straightforward to show that the map of fields is well-defined and an isomorphism. The isomorphism of function fields of course induces an isomorphism of the corresponding curves. That the cusps are in correspondence is a consequence of the map $\Gamma_0(N^2)\backslash\mathfrak{h} \to \Gamma_s(N)\backslash\mathfrak{h}$, $\tau \to w_*(\tau) = \tau/N$ being an isomorphism of Riemann surfaces. □

Lemma 3.7. *Let $\eta(\tau)$ be the Dedekind eta function.*

(i) *We have $\mathbb{Q}(X_0(4)) = \mathbb{Q}(h)$, where $h(\tau) = \eta(\tau)^8/\eta(4\tau)^8$.*
(ii) *We have $\mathbb{Q}(X_0(9)) = \mathbb{Q}(h)$, where $h(\tau) = \eta(\tau)^3/\eta(9\tau)^3$.*

Proof. This is well-known; for example see [Elk01]. □

3.4. **Proof of Proposition 3.1.** For $\tau \in \mathfrak{H}$, let Λ_τ be the lattice $\mathbb{Z}\tau + \mathbb{Z}$ in $\mathbb{C}$. Set $g_2(\tau) = g_2(\Lambda_\tau)$ and $g_3(\tau) = g_3(\Lambda_\tau)$, and let $\wp(z;\tau)$ be the Weierstrass $\wp$-function relative to Λ_τ, cf. [Sil09, §VI.3] for background on elliptic functions. For each pair $a = (a_1, a_2) \in N^{-1}\mathbb{Z}^2 - \mathbb{Z}^2$, define the function

$$f_a(\tau) := \frac{g_2(\tau)g_3(\tau)}{g_2(\tau)^3 - 27g_3(\tau)^2} \cdot \wp(a_1\tau + a_2; \tau)$$

of the upper half plane. The function f_a is modular of level N. Moreover, Proposition 6.9(1) of [Shi94] says that

$$\mathcal{F}_N = \mathbb{Q}\big(j, f_a \,\big|\, a \in N^{-1}\mathbb{Z}^2 - \mathbb{Z}^2\big). \tag{3.1}$$

For $a, b \in N^{-1}\mathbb{Z}^2 - \mathbb{Z}^2$, we have $f_a = f_b$ if and only if a lies in the same coset of $\mathbb{Q}^2/\mathbb{Z}^2$ as b or $-b$, cf. equation (6.1.5) of [Shi94]. So for any $A \in M_2(\mathbb{Z})$ with determinant relatively prime to N, the function f_{aA} depends only on the image $\tilde{A}$ of A in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$. By abuse of notation, we shall denote f_{aA} by $f_{a\tilde{A}}$.

By Theorem 6.6 of [Shi94], there is a unique isomorphism

$$\theta_N \colon \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\} \xrightarrow{\sim} \mathrm{Gal}(\mathcal{F}_N/\mathbb{Q}(j))$$

such that $\theta_N(A)f_a = f_{aA^t}$ for all $A \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ and $a \in N^{-1}\mathbb{Z}^2 - \mathbb{Z}^2$; we have added the transpose so the map is a homomorphism (and not an antihomorphism).

Fix any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and let $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ be its image modulo N. For any $a \in N^{-1}\mathbb{Z}^2 - \mathbb{Z}^2$, the function $f_a \circ \gamma^t$ agrees with $f_{a\cdot\gamma^t} = \theta_N(A) f_a$ by equation (6.1.3) of [Shi94]. Using (3.1), we deduce that $\theta_N(A) f = f \circ \gamma^t$ for all $f \in \mathcal{F}_N$; this shows that (a) holds.

Now take integer d relatively prime to N and let A be the image of $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$ in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Take any $a \in N^{-1}\mathbb{Z}^2 - \mathbb{Z}^2$; we have $a = (r/N, s/N)$ with $r, s \in \mathbb{Z}$. Since $f_a = f_b$ when $a \equiv b \pmod{\mathbb{Z}^2}$, we may assume that $0 \le r < N$. We have $\theta_N(A) f_a = f_{aA^t} = f_{(r/N, ds/N)}$. By equation (6.2.1) of [Shi94], we have

$$\begin{aligned}(2\pi)^{-2}\wp(a_1\tau + a_2; \tau) = &-1/12 + 2\sum\nolimits_{n=1}^{\infty} nq^n/(1-q^n) - \zeta_N^s q^{r/N}/(1-\zeta_N^s q^{r/N})^2 \\ &- \sum\nolimits_{n=1}^{\infty} (\zeta_N^{ns} q^{nr/N} + \zeta_N^{-ns} q^{-nr/N}) \cdot nq^n/(1-q^n);\end{aligned}$$

applying σ_d to this series gives the same thing with s replaced by ds. The Fourier coefficients of the expansion of $g_2(\tau)/g_3(\tau)$ are all π^{-2} times a rational number. Therefore, $\sigma_d(f_a) = \sigma_d(f_{(r/N, s/N)})$ equals $f_{(r/N, ds/N)} = f_{aA^t}$. Using (3.1), we deduce that $\theta_N(A) f = \sigma_d(f)$ for all $f \in \mathcal{F}_N$; this shows that (b) holds.

This explains the existence of an isomorphism θ_N as in the statement of Proposition 3.1. The uniqueness if immediate since $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is generated by $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and matrices of the form $\left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right)$. Theorem 6.6 of [Shi94] implies that $\mathbb{Q}(\zeta_N)$ is the algebraic closure of $\mathbb{Q}$ in $\mathcal{F}_N$ and that $\theta_N(A)\zeta_N = \zeta_N^{\det A}$.

3.5. **Proof of Proposition 3.3.** We first construct the inverse of θ_N using elliptic curves; we shall freely use definitions from §3.4. Let E be an elliptic curve defined over an algebraically closed field k of characteristic 0. Take any non-zero N-torsion point $P \in E(k)$. If $P = (x_0, y_0)$ with respect to some Weierstrass model $y^2 = 4x^3 - c_2 x - c_3$ of E/k, define $h_E(P) := c_2 c_3/(c_2^3 - 27c_3^2) \cdot x_0$. If $j_E \notin \{0, 1728\}$, then one can show that $h_E(P)$ does not depend on the choice of model.

Let $\mathcal{E}$ be the elliptic curve over $\mathcal{F}_1 = \mathbb{Q}(j)$ defined by the Weierstrass equation

$$y^2 = 4x^3 - \frac{27j}{j-1728}x - \frac{27j}{j-1728}; \tag{3.2}$$

it has j-invariant j. Fix an algebraic closed field K that contains $\mathcal{F}_N \supseteq \mathbb{Q}(j)$ and let $\mathcal{E}[N]$ be the N-torsion subgroup of $\mathcal{E}(K)$.

Lemma 3.8. *There is a basis $\{P_1, P_2\}$ of the $\mathbb{Z}/N\mathbb{Z}$-module $\mathcal{E}[N]$ such that $h_{\mathcal{E}}(rP_1 + sP_2) = f_{(r/N, s/N)}$ for all $(r, s) \in \mathbb{Z}^2 - N\mathbb{Z}^2$.*

Proof. Let K_0 be the extension of $\mathcal{F}_N$ generated by the functions $g_2(\tau)$, $g_3(\tau)$, $\wp(\tau/N; \tau)$, $\wp'(\tau/N; \tau)$, $\wp(1/N; \tau)$ and $\wp'(1/N; \tau)$. We may assume that $K \supseteq K_0$. Let E be the elliptic curve over K_0 defined by $y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$; its j-invariant is $j = j(\tau)$. The curves E and $\mathcal{E}$ are isomorphic over K since they both have j-invariant j. Since $j \notin \{0, 1728\}$, it suffices to prove the lemma for E instead of $\mathcal{E}$.

Define the pairs

$$P_1 := (\wp(\tau/N; \tau), \wp'(\tau/N; \tau)) \quad \text{and} \quad P_2 := (\wp(1/N; \tau), \wp'(1/N; \tau)).$$

We claim that P_1 and P_2 form a basis of the $\mathbb{Z}/N\mathbb{Z}$-module of N-torsion in $E(K)$. To prove the claim it suffices to prove the analogous results after specializing the coefficients of E and the entries of P_1 and P_2 by an arbitrary $\tau_0 \in \mathfrak{h}$ (since the claim comes down to verifying certain polynomial equations whose variables are the coefficients of the model of E and the entries of the points). So fix an arbitrary $\tau_0 \in \mathfrak{h}$. Specializing the model of E at τ_0 gives an elliptic curve E_{τ_0} over $\mathbb{C}$ defined by $y^2 = 4x^3 - g_2(\tau_0)x - g_3(\tau_0)$. From Weierstrass, we know that the map

$$\mathbb{C}/\Lambda_{\tau_0} \to E_{\tau_0}(\mathbb{C}), \quad z \mapsto (\wp(z; \tau_0), \wp'(z; \tau_0)),$$

with 0 mapping to the point at infinity, gives an isomorphism of complex Lie groups. In particular, the points $P_{1,\tau_0} = (\wp(\tau_0/N;\tau_0), \wp'(\tau_0/N;\tau_0))$ and $P_{2,\tau_0} = (\wp(1/N;\tau_0), \wp'(1/N;\tau_0))$ give a basis for the N-torsion in $E_{\tau_0}(\mathbb{C})$. This is enough to prove our claim. Moreover, we have $rP_{1,\tau_0} + sP_{2,\tau_0} = (\wp(r/N\cdot\tau_0 + s/N;\tau_0), \wp'(r/N\cdot\tau_0 + s/N;\tau_0))$ for all $(r,s) \in \mathbb{Z}^2 - N\mathbb{Z}^2$. Therefore,

$$h_{E_{\tau_0}}(rP_1 + sP_2) = g_2(\tau_0)g_3(\tau_0)/(g_2(\tau_0)^3 - 27g_3(\tau_0)^2)\cdot\wp(r/N\cdot\tau_0 + s/N;\tau_0) = f_{(r/N,s/N)}(\tau_0).$$

for all $(r,s) \in \mathbb{Z}^2 - N\mathbb{Z}$. Since this holds for all $\tau_0 \in \mathfrak{h}$, we deduce that $h_E(rP_1+sP_2) = f_{(r/N,s/N)}$. □

Let $\rho_N\colon \mathrm{Gal}(K/\mathbb{Q}(j)) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be the representation describing the Galois action on $\mathcal{E}[N]$ with respect to the basis $\{P_1, P_2\}$ of Lemma 3.8. The fixed field of the kernel of $\mathrm{Gal}(K/\mathbb{Q}(j)) \xrightarrow{\rho_N} \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ is generated by the x-coordinates of the non-zero points in $\mathcal{E}[N]$. By (3.1) and Lemma 3.8, the extension $\mathcal{F}_N$ of $\mathbb{Q}(j)$ is generated by the x-coordinates of the non-zero points in $\mathcal{E}[N]$. Therefore, the representation ρ_N induces an injective homomorphism

$$\overline{\rho}_N\colon \mathrm{Gal}(\mathcal{F}_N/\mathbb{Q}(j)) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}. \tag{3.3}$$

In fact, (3.3) is an isomorphism since the groups have the same cardinality by Proposition 3.1.

Lemma 3.9. *The homomorphism $\overline{\rho}_N$ is an isomorphism. Moreover, the inverse of $\overline{\rho}_N$ is the homomorphism $\theta_N\colon \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\} \to \mathrm{Gal}(\mathcal{F}_N/\mathbb{Q}(j))$.*

Proof. Take any $\sigma \in \mathrm{Gal}(K/\mathbb{Q}(j))$ and set $\tilde{\sigma} := \sigma|_{\mathcal{F}_N}$. There are integers $a,b,c,d \in \mathbb{Z}$ such that $\sigma(P_1) = aP_1 + cP_2$ and $\sigma(P_2) = bP_1 + dP_2$, so $\rho_N(\sigma) = A$, where $A \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is the image of $\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right)$ modulo N. Therefore, $\overline{\rho}_N(\tilde{\sigma})$ is the class of A in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$. We need to show that $\theta_N(A) = \tilde{\sigma}$.

Take any pair of integers $(r,s) \in \mathbb{Z}^2 - N\mathbb{Z}^2$. We have

$$\sigma(rP_1 + sP_2) = r\sigma(P_1) + s\sigma(P_2) = (ra+sb)P_1 + (rc+sd)P_2.$$

Comparing x-coordinates and using Lemma 3.8, we find that $\tilde{\sigma}(f_{(r/N,s/N)}) = \sigma(f_{(r/N,s/N)})$ is equal to $f_{((ra+sb)/N,(rc+sd)/N)} = f_{(r/N,s/N)A^t}$ which is $\theta_N(A)f_{(r/N,s/N)}$ from §3.4. Since the extension $\mathcal{F}_N/\mathbb{Q}(j)$ is generated by the functions f_a with $a \in \mathbb{Z}^2 - N\mathbb{Z}^2$, we deduce that $\theta_N(A) = \tilde{\sigma}$. □

Define the $\mathbb{Q}$-variety

$$U := \mathbb{A}^1_{\mathbb{Q}} - \{0, 1728\} = \mathrm{Spec}\,\mathbb{Q}[j, j^{-1}, (j-1728)^{-1}];$$

note that we are now viewing j as simply a transcendental variable. The equation (3.2) defines a (relative) elliptic curve $\pi\colon \mathscr{E} \to U$. The fiber of $\mathscr{E} \to U$ over the generic fiber of U is the elliptic curve $\mathcal{E}/\mathbb{Q}(j)$.

Let $\overline{\eta}$ be the geometric generic point of U corresponding to the algebraically closed extension K of $\mathcal{F}_N$. Let $\mathscr{E}[N]$ be the N-torsion subscheme of $\mathscr{E}$. We can identify the fiber of $\mathscr{E}[N] \to U$ at $\overline{\eta}$ with the group $\mathcal{E}[N]$. Let $\pi_1(U,\overline{\eta})$ be the étale fundamental group of U. We can view $\mathscr{E}[N]$ as a rank 2 lisse sheaf of $\mathbb{Z}/N\mathbb{Z}$-modules U and it hence corresponds to a representation

$$\varrho_N\colon \pi_1(U,\overline{\eta}) \to \mathrm{Aut}(\mathcal{E}[N]) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

where the isomorphism uses the basis $\{P_1, P_2\}$ of Lemma 3.8. Taking the quotient by the group generated by $-I$, we obtain a homomorphism

$$\overline{\varrho}_N\colon \pi_1(U,\overline{\eta}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}.$$

Note that the representation $\mathrm{Gal}(K/\mathbb{Q}(j)) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ coming from $\overline{\varrho}_N$ factors through the homomorphism $\overline{\rho}_N$. So by Proposition 3.1 and Lemma 3.9, the representation $\overline{\varrho}_N$ is surjective and satisfies $\overline{\varrho}_N(\pi_1(U_{\overline{\mathbb{Q}}})) = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$.

Now take any subgroup G of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that satisfies $-I \in G$ and $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$. Using $\overline{\varrho}_N$, the group $G/\{\pm I\}$ corresponds to an étale morphism $\pi\colon Y_G \to U$. The smooth projective closure of Y_G is thus X_G and the morphism $X_G \to \mathbb{P}^1_{\mathbb{Q}}$ arising from π is simply π_G.

Take any rational point $u \in U(\mathbb{Q}) = \mathbb{Q} - \{0, 1728\}$. Viewed as a morphism $\operatorname{Spec}\mathbb{Q} \to U$, the point u induces a homomorphism $u_*\colon \mathrm{Gal}_{\mathbb{Q}} \to \pi_1(U)$; we are suppressing base points so everything is uniquely defined only up to conjugacy. Composing u_* with $\overline{\varrho}_N$ we obtain a homomorphism $\beta_u\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$. Observe that the group $\beta_u(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to a subgroup of $G/\{\pm I\}$ if and only if u lies in $\pi_1(Y_G(\mathbb{Q})) = \pi_G(X_G(\mathbb{Q})) - \{0, 1728, \infty\}$.

The fiber of $\mathscr{E} \to U$ over u is the elliptic curve $\mathscr{E}_u/\mathbb{Q}$ obtained by setting j to u in (3.2). Composing $\rho_{\mathscr{E}_u,N}\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ with the quotient map $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ gives a homomorphism that agrees with β_u up to conjugation. Since $-I \in G$, we find that $\rho_{\mathscr{E}_u,N}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ to a subgroup of G if and only if $u \in \pi_G(X_G(\mathbb{Q}))$.

Finally, let $E/\mathbb{Q}$ be any elliptic curve with j-invariant u. The curve $\mathscr{E}_u/\mathbb{Q}$ also has j-invariant u. As noted in the introduction, since E and $\mathscr{E}_u$ are elliptic curves over $\mathbb{Q}$ with common j-invariant $u \notin \{0, 1728\}$, the groups $\pm\rho_{E,N}(\mathrm{Gal}_{\mathbb{Q}})$ and $\pm\rho_{\mathscr{E}_u,N}(\mathrm{Gal}_{\mathbb{Q}})$ must be conjugate. This completes the proof of Proposition 3.3.

4. Classification up to a sign

In this section, we prove the parts of the theorems of §1 that involve the groups $\pm\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ for an elliptic curve $E/\mathbb{Q}$. In the notation of §2, the group $\pm\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is either applicable or is the full group $\mathrm{GL}_2(\mathbb{F}_\ell)$. We consider the primes ℓ separately and keep the notation of the relevant subsection of §1.

One of the main tasks is to construct modular curves of genus 0. We will do this by finding functions $h \in \mathcal{F}_\ell - \mathbb{Q}(j)$ such that $j = J(h)$ for some $J \in \mathbb{Q}(t)$. Let H be the subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ consisting of elements that fix h under the action from Proposition 3.1. By Lemma 3.4, the group H is an applicable subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$. Furthermore, X_H has function field $\mathbb{Q}(h)$ and the morphism $\pi_H\colon X_H \to \mathbb{P}^1_{\mathbb{Q}}$ is described by the inclusion $\mathbb{Q}(h) \supseteq \mathbb{Q}(j)$. So if $E/\mathbb{Q}$ is a non-CM elliptic curve, then $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to a subgroup of H if and only if j_E belongs to $\pi_H(X_H(\mathbb{Q})) = J(\mathbb{Q} \cup \{\infty\})$.

We will need to recognize H as a conjugate of one of our applicable subgroups G_i of $\mathrm{GL}_2(\mathbb{F}_\ell)$. The degree of π_H, which is the same as the degree of $J(t)$, is equal to the index $[\mathrm{GL}_2(\mathbb{F}_\ell) : H]$; this observation will immediately rule out most candidates. We will also make use of Proposition 3.3; observe that the set $\pi_H(X_H(\mathbb{Q}))$ depends only on the conjugacy class of H.

Most of this section involves basic algebraic verifications (which are straightforward to check with a computer, see the link in §1.10 for many such details); much of the work, which we will not touch on, is finding the various equations in the first place.

4.1. $\ell = 2$. Fix notation as in §1.1. Up to conjugacy, G_1, G_2 and G_3 are the proper subgroups of $\mathrm{GL}_2(\mathbb{F}_2)$.

- Define the function
$$h_1(\tau) := 16\eta(2\tau)^8/\eta(\tau/2)^8 = 16\big(q^{1/2} + 8q + 44q^{3/2} + 192q^2 + 718q^{5/2} + \cdots\big).$$
By Lemmas 3.6 and 3.7(i), we have $\mathbb{Q}(X_s(2)) = \mathbb{Q}(h_1)$. We have $C_s(2) = G_1$, so $\mathbb{Q}(X_{G_1}) = \mathbb{Q}(h_1)$. The extension $\mathbb{Q}(h_1)/\mathbb{Q}(j)$ has degree 6, so there is a unique rational function $J(t) \in \mathbb{Q}(t)$ such that $j = J(h_1)$. We have $J(t) = f_1(t)/f_2(t)$ for relatively prime $f_1, f_2 \in \mathbb{Q}[t]$ of degree at most 6. Expanding the q-expansion of $jf_2(h_1) - f(h_1) = J(h_1)f_2(h_1) - f_1(h_1) = 0$ gives many linear equations in the coefficients of f_1 and f_2. Using enough terms of the q-expansion, we can compute the coefficients of f_1 and f_2 (they are unique up to scaling f_1 and f_2 by some constant in $\mathbb{Q}^\times$). Doing this, we found that $J_1(h_1) = j$.
- Define $h_2 := h_1^2/(h_1 + 1)$. Since $J_2(t^2/(t+1)) = J_1(t)$, we have $J_2(h_2) = j$.

- Define $h_3 := F(h_1)$ where $F(t) = (-16t^3 - 24t^2 + 24t + 16)/(t^2 + t)$. Since $J_3(F(t)) = J_1(t)$, we have $J_3(h_3) = j$.

For each integer $1 \le i \le 3$, let H_i be the subgroup of $\mathrm{GL}_2(\mathbb{F}_2)$ that fixes h_i. By Lemma 3.4, H_i is an applicable subgroup of $\mathrm{GL}_2(\mathbb{F}_2)$ with index equal to the degree of $J_i(t)$. By comparing the degree of $J_i(t)$ with our list of proper subgroups, we deduce that H_i is conjugate to G_i in $\mathrm{GL}_2(\mathbb{F}_2)$.

Theorem 1.1 now follows from Lemma 3.4(iii); we can ignore $t = \infty$ since $J_i(\infty) = \infty$.

4.2. $\ell = 3$. Fix notation as in §1.2. Up to conjugacy, the groups G_i with $1 \le i \le 4$ are the applicable subgroups of $\mathrm{GL}_2(\mathbb{F}_3)$.

- Define the function $h_1 := 1/3 \cdot \eta(\tau/3)^3/\eta(3\tau)^3$. By Lemmas 3.6 and 3.7(ii), we have $\mathbb{Q}(X_s(3)) = \mathbb{Q}(h_1)$. We have $C_s(3) = G_1$, so $\mathbb{Q}(X_{G_1}) = \mathbb{Q}(h_1)$. The extension $\mathbb{Q}(h_1)/\mathbb{Q}(j)$ has degree 12, so there is a unique rational function $J(t) \in \mathbb{Q}(t)$ such that $j = J(h_1)$. We have $J(t) = f_1(t)/f_2(t)$ for relatively prime $f_1, f_2 \in \mathbb{Q}[t]$ of degree at most 12. Expanding the q-expansion of $jf_2(h_1) - f(h_1) = J(h_1)f_2(h_1) - f_1(h_1) = 0$ gives many linear equations in the coefficients of f_1 and f_2. Using enough terms of the q-expansion, we can compute the coefficients of f_1 and f_2 (they are unique up to scaling f_1 and f_2 by some constant in $\mathbb{Q}^\times$). Doing this, we found that $J_1(h_1) = j$.
- Define $h_2 = F_1(h_1)$ where $F_1(t) = (t^2 + 3t + 3)/t$. Since $J_2(F_1(t)) = J_1(t)$, we have $J_2(h_2) = j$.
- Define $h_3 = F_2(h_1)$ where $F_2(t) = t(t^2+3t+3)$. Since $J_3(F_2(t)) = J_1(t)$, we have $J_3(h_3) = j$.
- Define $h_4 = F_3(h_2)$ where $F_3(t) = 3(t + 1)(t - 3)/t$. Since $J_4(F_3(t)) = J_2(t)$, we have $J_4(h_4) = j$.

Fix an integer $1 \le i \le 4$, and let H_i be the subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ that fixes h_i. By Lemma 3.4, we find that H_i is an applicable subgroup and the morphism $\pi_{H_i} \colon X_{H_i} \to \mathbb{P}^1_{\mathbb{Q}}$ is described by the rational function $J_i(t)$. The index $[\mathrm{GL}_2(\mathbb{F}_3) : H_i]$ agrees with the degree of $J_i(t)$. By comparing the degree of $J_i(t)$ with our list of applicable subgroups, we deduce that H_i is conjugate to G_i in $\mathrm{GL}_2(\mathbb{F}_3)$.

Theorem 1.2(ii) now follows from Lemma 3.4(iii); we can ignore $t = \infty$ since $J_i(\infty) = \infty$. A computation shows that if H is a proper subgroup of G_i satisfying $\pm H = G_i$, then $i \in \{1, 3\}$ and H is one of the groups $H_{i,j}$; this proves Theorem 1.2(i).

4.3. $\ell = 5$. Fix notation as in §1.3. Up to conjugacy, the applicable subgroups of $\mathrm{GL}_2(\mathbb{F}_5)$ are the groups G_i with $1 \le i \le 9$. Recall that the Rodgers-Ramanunjan continued fraction is

$$r(\tau) := q^{1/5} \cdot \frac{1}{1+}\,\frac{q}{1+}\,\frac{q^2}{1+}\,\frac{q^3}{1+}\,\frac{q^4}{1+}\cdots.$$

The function

$$h_1(\tau) := 1/r(\tau) = q^{-1/5}(1 + q - q^3 + q^5 + q^6 - q^7 - 2q^8 + 2q^{10} + 2q^{11} + \cdots)$$

is a modular function of level 5 and satisfies $J_1(h_1) = j$; we refer to Duke [Duk05] for an excellent exposition. An expression for $h_1(\tau)$ in terms of Klein forms can be found in [CC06].

Set $w := (1 + \sqrt{5})/2 \in \mathbb{Q}(\zeta_5)$.

- Define the function $h_2 = h_1 - 1 - 1/h_1$. We have $J_2(t - 1 - 1/t) = J_1(t)$, so $J_2(h_2) = j$. (As noted in equation (7.2) of [Duk05], h_2 equals $\eta(\tau/5)/\eta(5\tau)$.)
- Define $h_3 = F_1(h_2)$ where

$$F_1(t) = \frac{(-3 + w)t - 5}{t + (3 - w)}.$$

  We have $J_3(F_1(t)) = J_2(t)$ and hence $J_3(h_3) = j$.
- Define $h_4 = h_2 + 5/h_2$. We have $J_4(t + 5/t) = J_2(t)$ and hence $J_4(h_4) = j$.

- Define $h_5 = h_1^5$. We have $J_5(t^5) = J_1(t)$ and hence $J_5(h_5) = j$.
- Define $h_6 = F_2(h_5)$ where
$$F_2(t) = \frac{-(w-1)^5 t + 1}{t + (w-1)^5}$$
We have $J_6(F_2(t)) = J_5(t)$ and hence $J_6(h_6) = j$. (In the notation of [Duk05, §8], we have $b = h_6$.)
- Define $h_7 = F_3(h_3)$ where
$$F_3(t) = -\frac{t^3 + 10t^2 + 25t + 25}{2t^3 + 10t^2 + 25t + 25}.$$
We have $J_7(F_3(t)) = J_3(t)$ and hence $J_7(h_7) = j$.
- Define $h_8 = h_5 - 11 - h_5^{-1}$. We have $J_8(t - 11 - t^{-1}) = J_5(t)$ and hence $J_8(h_8) = j$. (As noted in equation (7.7) of [Duk05], h_8 equals $(\eta(\tau)/\eta(5\tau))^6$.)
- Define $h_9 = F_4(h_4)$ where
$$F_4(t) = \frac{(t+5)(t^2-5)}{t^2 + 5t + 5}.$$
We have $J_9(F_4(t)) = J_4(t)$ and hence $J_9(h_9) = j$.

Fix an integer $1 \leq i \leq 9$. Let H_i be the subgroup of $\mathrm{GL}_2(\mathbb{F}_5)$ that fixes h_i. By Lemma 3.4, we find that H_i is an applicable subgroup and the morphism $\pi_{H_i} \colon X_{H_i} \to \mathbb{P}^1_{\mathbb{Q}}$ is described by the rational function $J_i(t)$.

Lemma 4.1. *The groups H_i and G_i are conjugate in $\mathrm{GL}_2(\mathbb{F}_5)$ for each $1 \leq i \leq 9$.*

Proof. The index $[\mathrm{GL}_2(\mathbb{F}_5) : H_i]$ agrees with the degree of $J_i(t)$. By comparing the degree of $J_i(t)$ with our list of applicable subgroups, we deduce that H_i is conjugate to G_i in $\mathrm{GL}_2(\mathbb{F}_5)$ for all $i \in \{1, 4, 7, 8, 9\}$.

The groups H_5 and H_6 are not conjugate since one can check that the image of $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$ under $J_5(t)$ and $J_6(t)$ are different. The groups H_5 and H_6 have index 12 in $\mathrm{GL}_2(\mathbb{F}_5)$ and are not conjugate, so they are conjugate to G_5 and G_6 (though we need to determine which is which). The elliptic curve given by the Weierstrass equation $y^2 + (1-t)xy - ty = x^3 - tx^2$ has j-invariant $J_6(t)$ and the point $(0, 0)$ has order 5. Therefore, H_6 is conjugate to G_6 and thus H_5 is conjugate to G_5.

The groups H_2 and H_3 are not conjugate since one can check that the image of $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$ under $J_2(t)$ and $J_3(t)$ are different. The groups H_2 and H_3 have index 30 in $\mathrm{GL}_2(\mathbb{F}_5)$ and are not conjugate, so they are conjugate to G_2 and G_3 (though we need to determine which is which). Since $h_7 = F_3(h_3)$ and $F_3(t)$ belongs to $\mathbb{Q}(t)$, we find that H_3 is a subgroup of H_7. We already know that H_7 is conjugate to $N_{ns}(5)$ and one can check that $G_2 = C_s(5)$ is not conjugate to a subgroup of $N_{ns}(5)$. Therefore, H_3 is conjugate to G_3 and thus H_2 is conjugate to G_2. □

Theorem 1.4(ii) now follows from Lemma 3.4(iii); we have $J_i(\infty) = \infty$ for $i \notin \{3, 7\}$ and we can ignore the values $J_3(\infty) = 0$ and $J_7(\infty) = 8000$ since they are the j-invariants of CM elliptic curves. A direct computation shows that if H is a proper subgroup of G_i satisfying $\pm H = G_i$, then $i \in \{1, 5, 6\}$ and H is one of the groups $H_{i,j}$; this proves Theorem 1.4(i).

4.4. **$\ell = 7$.** Fix notation as in §1.4. Up to conjugacy, the applicable subgroups of $\mathrm{GL}_2(\mathbb{F}_7)$ are the groups G_i with $1 \leq i \leq 7$ from §1.4 and the groups:

- Let G_8 be the subgroup of $\mathrm{GL}_2(\mathbb{F}_7)$ consisting of matrices of the form $\pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right)$.
- Let G_9 be the subgroup of $\mathrm{GL}_2(\mathbb{F}_7)$ consisting of matrices of the form $\left(\begin{smallmatrix} a & 0 \\ 0 & \pm a \end{smallmatrix}\right)$.
- Let G_{10} be the subgroup of $\mathrm{GL}_2(\mathbb{F}_7)$ generated by $\left(\begin{smallmatrix} 0 & -2 \\ 2 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.
- Let G_{11} be the subgroup $C_s(7)$ of $\mathrm{GL}_2(\mathbb{F}_7)$.

- Let G_{12} be the subgroup of $\mathrm{GL}_2(\mathbb{F}_7)$ generated by $\left(\begin{smallmatrix}1 & -1\\ 1 & 1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$.

For $i = 8, 9, 10, 11$ and 12, the index $[\mathrm{GL}_2(\mathbb{F}_7) : G_i]$ is 168, 168, 84, 56 and 42, respectively.

The Klein quartic is the curve $\mathcal{X}$ in $\mathbb{P}^2_{\mathbb{Q}}$ defined by the equation $x^3y + y^3z + z^3x = 0$; it is a non-singular curve of genus 3. The relevance to us is that $\mathcal{X}$ is isomorphic to the modular curve $X(7) := X_{G_8}$; we refer to Elkies [Elk99] for a lucid exposition. In §4 of [Elk99], Elkies defines a convenient basis x, y and z for the space of cusp forms of $\Gamma(7)$ which satisfy the equation of the Klein quartic and have product expansions

$$\mathsf{x},\ \mathsf{y},\ \mathsf{z} = \varepsilon q^{a/7} \prod_{n=1}^{\infty} (1-q^n)^3(1-q^7) \prod_{\substack{n>0 \\ n \equiv \pm n_0 \bmod 7}} (1-q^n)$$

where (ε, a, n_0) is $(-1, 4, 1)$, $(1, 2, 2)$ or $(1, 1, 4)$ for x, y or z, respectively. The coordinates $(\mathsf{x} : \mathsf{y} : \mathsf{z})$ then give the desired isomorphism $X(7) \to \mathcal{X}$.

Define

$$h_4 := -(\mathsf{y}^2\mathsf{z})/\mathsf{x}^3 = q^{-1} + 3 + 4q + 3q^2 - 5q^4 - 7q^5 + \ldots;$$

it is a modular function of level 7. Define $h_7 := F_1(h_4)$ where

$$F_1(t) = t + \frac{1}{1-t} + \frac{t-1}{t} - 8.$$

From equations (4.20) and (4.24) of [Elk99], with a correction in the sign of (4.23) of loc. cit., we have $J_7(h_7) = j$. Since $J_7(F_1(t)) = J_4(t)$, we have $J_4(h_4) = j$.

Define $h_3 := F_2(h_4)$ and $h_5 := F_3(h_4)$, where

$$F_2(t) = \frac{\beta t - (\beta - 1)}{t - \beta} \quad \text{and} \quad F_3(t) = \frac{t - \gamma}{\gamma t - (\gamma - 1)}$$

with $\beta = 4 + 3\zeta_7 + 3\zeta_7^{-1} + \zeta_7^2 + \zeta_7^{-2}$ and $\gamma = \zeta_7^5 + \zeta_7^4 + \zeta_7^3 + \zeta_7^2 + 1$. Since $J_3(F_2(t)) = J_4(t)$ and $J_5(F_3(t)) = J_4(t)$, we have $J_3(h_3) = j$ and $J_5(h_5) = j$.

For $i \in \{3, 4, 5, 7\}$, let H_i be the subgroup of $\mathrm{GL}_2(\mathbb{F}_7)$ that fixes h_i. We have shown that $J_i(h_i) = j$. By Lemma 3.4, we find that H_i is an applicable subgroup and that the morphism $\pi_{H_i} \colon X_{H_i} \to \mathbb{P}^1_{\mathbb{Q}}$ is described by the rational function $J_i(t)$.

Lemma 4.2. *The groups H_i and G_i are conjugate in $\mathrm{GL}_2(\mathbb{F}_7)$ for all $i \in \{3, 4, 5, 7\}$.*

Proof. The index of H_i in $\mathrm{GL}_2(\mathbb{F}_7)$ agrees with the degree of $J_i(t)$ which is 24 or 8 if $i \in \{3, 4, 5\}$ or $i = 7$, respectively. By our list of applicable subgroups, we deduce that H_7 is conjugate to G_7 in $\mathrm{GL}_2(\mathbb{F}_7)$. The groups H_3, H_4 and H_5 are not conjugate in $\mathrm{GL}_2(\mathbb{F}_7)$ (since one can show that the images of $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$ under J_3, J_4 and J_5 are pairwise distinct). By our list of applicable subgroups, the groups H_3, H_4 and H_5 are conjugate to the three subgroups G_3, G_4 and G_5; we still need to identify H_3 with G_3, etc.

The modular function $h_4 \in \mathcal{F}_7$ is a Laurent series in q and has rational coefficients. Using Proposition 3.1, this implies that H_4 contains the group of matrices of the form $\pm\left(\begin{smallmatrix}1 & 0\\ * & *\end{smallmatrix}\right)$ in $\mathrm{GL}_2(\mathbb{F}_7)$. Therefore, H_4 must be conjugate to G_4 in $\mathrm{GL}_2(\mathbb{F}_7)$. The elliptic curve given by the Weierstrass equation $y^2 + (1 + t - t^2)xy + (t^2 - t^3)y = x^3 + (t^2 - t^3)x^2$ has j-invariant $J_3(t)$ and the point $(0, 0)$ has order 7, so H_3 is conjugate to G_3. Therefore, H_5 is conjugate to G_5. □

Following Elkies ([Elk99, p.68]), we multiply the equation of the Klein curve to obtain $(\mathsf{x}^3\mathsf{y} + \mathsf{y}^3\mathsf{z} + \mathsf{z}^3\mathsf{x})(\mathsf{x}^3\mathsf{z} + \mathsf{z}^3\mathsf{y} + \mathsf{y}^3\mathsf{x}) = 0$. Noting that the left hand side is a symmetric polynomial in x, y and

z, one can show that $s_2^4 + s_3(s_1^5 - 5s_1^3 s_2 + s_1 s_2^2 + 7s_1^2 s_3) = 0$ where $s_1 = \mathsf{x}+\mathsf{y}+\mathsf{z}$, $s_2 = \mathsf{xy}+\mathsf{yz}+\mathsf{zx}$ and $s_3 = \mathsf{xyz}$. We now deviate from Elkies' treatment. Divide by $s_1^2 s_3^2$ and rearrange to obtain

$$\left(\frac{s_2^2}{s_1 s_3}\right)^2 + \left(\frac{s_1^2}{s_2}\right)^2 \cdot \frac{s_2^2}{s_1 s_3} - 5\frac{s_1^2}{s_2} \cdot \frac{s_2^2}{s_1 s_3} + \frac{s_2^2}{s_1 s_3} + 7 = 0.$$

We thus have $v^2 + (h_2^2 - 5h_2 + 1)v + 7 = 0$, where

$$h_2 := s_1^2/s_2 = q^{-1/7} + 2 + 2q^{1/7} + q^{2/7} + 2q^{3/7} + 3q^{4/7} + 4q^{5/7} + 5q^{6/7} + 7q + 8q^{8/7} + \cdots$$

and $v := s_2^2/(s_1 s_3)$ are modular functions. We claim that

$$h_7 + (h_2^3 - 4h_2^2 + 3h_2 + 1)((h_2^2 - 5h_2 + 1)v + 7) = 0. \tag{4.1}$$

This can be verified algebraically: In the left-hand side of (4.1), replace h_7 by $F_1(-y^2 z/x^3)$, h_2 by $(x+y+z)^2/(xy+yz+zx)$, and v by $(xy+yz+zx)^2/((x+y+z)xyz)$; the numerator of the resulting rational function is divisible by $xy^3 + yz^3 + zx^3$.

Completing the square in the equation $v^2 + (h_2^2 - 5h_2 + 1)v + 7 = 0$, we have

$$w^2 = h_2^4 - 10h_2^3 + 27h_2^2 - 10h_2 - 27, \tag{4.2}$$

where $w := 2v + (h_2^2 - 5h_2 + 1)$. From (4.1), we find that

$$h_7 = \tfrac{1}{2}(h_2^3 - 4h_2^2 + 3h_2 + 1)((h_2^4 - 10h_2^3 + 27h_2^2 - 10h_2 - 13) - (h_2^2 - 5h_2 + 1)w). \tag{4.3}$$

We have $j = J_7(h_7)$, so (4.2) and (4.3) imply that j can be written in the form $\alpha(h_2) + \beta(h_2)w$ for rational functions $\alpha(t)$ and $\beta(t)$. A direct computation shows that $\alpha(t) = J_2(t)$ and $\beta(t) = 0$, and hence $J_2(h_2) = j$.

Let H_2 be the subgroup of $\mathrm{GL}_2(\mathbb{F}_7)$ that fixes h_2. We have $J_2(h_2) = j$, so Lemma 3.4 implies that H_2 is an applicable subgroup and that the morphism $\pi_{H_2}\colon X_{H_2} \to \mathbb{P}^1_{\mathbb{Q}}$ is described by the rational function $J_2(t)$. The index of H_2 in $\mathrm{GL}_2(\mathbb{F}_7)$ is 28 since it agrees with the degree of $J_2(t)$. By our list of applicable subgroups, we deduce that H_2 is conjugate to G_2 in $\mathrm{GL}_2(\mathbb{F}_7)$.

Let H_{11} be the subgroup of $\mathrm{GL}_2(\mathbb{F}_7)$ that fixes h_2 and w. The group H_{11} is an index 2 subgroup of H_2 since the extension $\mathbb{Q}(h_2, w)/\mathbb{Q}(h_2)$ has degree 2. The group H_{11} contains G_8 since $\mathbb{Q}(h_2, w)$ is contained in $\mathbb{Q}(\mathsf{x}/\mathsf{z}, \mathsf{y}/\mathsf{z})$ which is the function field of $X(7)$; in particular, H_{11} is applicable. From our classification of applicable subgroups, we find that H_{11} is conjugate to G_{11}. The modular curve $X_{G_{11}}$ thus has function field $\mathbb{Q}(h_2, w)$ and is hence isomorphic to the smooth projective curve over $\mathbb{Q}$ with affine model

$$y^2 = x^4 - 10x^3 + 27x^2 - 10x - 27. \tag{4.4}$$

The only rational points for the smooth model of (4.4) are the two points at infinity (one can show that it is isomorphic to the quadratic twist by -7 of the curve $E_{7,1}$ from §1.9, and that this curve has only two rational points). Using that $J_2(\infty) = \infty$, we find that the two rational points of $X_{H_{11}}$, and hence of $X_{G_{11}}$, are cusps. Therefore, there is no non-CM elliptic curve $E/\mathbb{Q}$ for which $\rho_{E,7}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to a subgroup of G_{11}; the same holds for the group G_8 since $G_8 \subseteq G_{11}$.

Now consider the subfield $K := \mathbb{Q}(h_2, w/\sqrt{-7})$ of $\mathcal{F}_7$. Let H_1 be the subgroup of $\mathrm{GL}_2(\mathbb{F}_7)$ that fixes K. From the inclusions $K \supseteq \mathbb{Q}(h_2) \supseteq \mathbb{Q}(j)$ and (4.2), we find that K is the function field of the geometrically irreducible curve

$$-7y^2 = x^4 - 10x^3 + 27x^2 - 10x - 27 \tag{4.5}$$

defined over $\mathbb{Q}$ (with $(x, y) = (h_2, w/\sqrt{-7})$). The curve X_{H_1} is defined over $\mathbb{Q}$ since $\mathbb{Q}$ is algebraically closed in K. The only rational points of the smooth projective model of (4.5) are $(x, y) = (5/2, \pm 1/4)$ (one can show that it is isomorphic to the curve $E_{7,1}$ from §1.9, and that this curve has only two rational points). These two rational points on X_{H_1} lie over the j-invariant

$J_2(5/2) = 3^3 \cdot 5 \cdot 7^5/2^7$. This shows that for an elliptic curve $E/\mathbb{Q}$, $\rho_{E,7}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to a subgroup of H_1 in $\mathrm{GL}_2(\mathbb{F}_7)$ if and only if $j_E = 3^3 \cdot 5 \cdot 7^5/2^7$. Since X_{H_1} has a rational point that is not a cusp, the group H_1 must be applicable and not conjugate to G_{11}. The group H_1 is an index 2 subgroup of H_2 since $[\mathbb{Q}(h_2, w/\sqrt{-7}) : \mathbb{Q}(h_2)] = 2$. From our description of applicable groups, we deduce that H_1 is conjugate to G_1.

Remark 4.3. The rational points on X_{H_1} were first described by A. Sutherland in [Sut12]. An elliptic curve $E/\mathbb{Q}$ with j-invariant $3^3 \cdot 5 \cdot 7^5/2^7$ has the distinguished property of not having a 7-isogeny, yet its reduction at primes of good reduction all have a 7-isogeny.

From equation (4.35) of [Elk99], the modular curve $X_{ns}^+(7) := X_{G_6}$ has function field of the form $\mathbb{Q}(x)$ and the morphism down to the j-line is given by $J_6(x)$; note that there is a small typo in the numerator of equation (4.35) of [Elk99] though the given expression for $j - 1728$ is correct.

Lemma 4.4. *The rational points of the modular curve $X_{G_{12}}$ are all CM.*

Proof. The fiber in $X_{ns}^+(7)$ over $j = 1728$ is the (non-reduced) subscheme given by

$$(2x^4 - 14x^3 + 21x^2 + 28x + 7)(x - 3)\big((x^4 - 7x^3 + 14x^2 - 7x + 7)(x^4 - 14x^2 + 56x + 21)\big)^2 = 0;$$

this can be found by factoring $J_6(x) - 1728$. Define the modular curve $X_{ns}(7) := X_{C_{ns}(7)}$. One can show that the morphism $X_{ns}(7) \to X_{ns}^+(7)$ is ramified at precisely four points lying over $j = 1728$. Since it is defined over $\mathbb{Q}$, these four ramification points are the ones given by $2x^4 - 14x^3 + 21x^2 + 28x + 7 = 0$. Therefore, $X_{ns}(7)$ is defined by an equation

$$y^2 = c(2x^4 - 14x^3 + 21x^2 + 28x + 7)$$

for some squarefree $c \in \mathbb{Z}$.

We claim that $c = -1$. Consider an elliptic curve $E/\mathbb{Q}$ with j-invariant -2^{15}. The value $x = 1$ is the unique rational solution to $J(x) = -2^{15}$. Setting $x = 1$, we have $y^2 = 44c$. Therefore, $K = \mathbb{Q}(\sqrt{11c})$ is the unique quadratic extension of $\mathbb{Q}$ for which $\rho_{E,7}(\mathrm{Gal}_K) \subseteq C_{ns}(7)$. Since $j_E = -2^{15}$, the curve E has CM by $\mathbb{Q}(\sqrt{-11})$ and hence $\rho_{E,7}(\mathrm{Gal}_{\mathbb{Q}(\sqrt{-11})}) = C_{ns}(7)$ and $\rho_{E,7}(\mathrm{Gal}_{\mathbb{Q}}) = N_{ns}(7)$; see §7. Therefore, $K = \mathbb{Q}(\sqrt{-11})$ and hence $c = -1$ as claimed. (The above argument comes from Schoof.)

Define the subfield $L = \mathbb{Q}(x, v)$ of $\mathcal{F}_7$ where $v := y/\sqrt{-7}$; we have

$$7v^2 = 2x^4 - 14x^3 + 21x^2 + 28x + 7. \tag{4.6}$$

Let G be the subgroup of $\mathrm{GL}_2(\mathbb{F}_7)$ that fixes L; it is an index 2 subgroup of $G_6 = N_{ns}(11)$ since $L/\mathbb{Q}(x)$ has degree 2. The field $\mathbb{Q}$ is algebraically closed in L since $L/\mathbb{Q}(x)$ is a geometric extension. Therefore, $\det(G) = \mathbb{F}_7^\times$. There are only two index 2 subgroups of G_6 with full determinant; they are G_{12} and $C_{ns}(7)$. The group G is thus G_{12} since $C_{ns}(7)$ corresponds to the field $\mathbb{Q}(x, y)$.

Therefore, $X_{G_{12}}$ has function field $\mathbb{Q}(x, v)$ with x and v related by (4.6). The smooth projective curve defined by (4.6) has genus 1 and a rational point $(x, v) = (0, 1)$; it is thus an elliptic curve. A computation shows that this elliptic curve is isomorphic to the curve $E_{7,2}$ of §1.9. The curve $E_{7,2}$ has only two rational points, so $(x, v) = (0, \pm 1)$ are the only rational points of the curve defined by (4.6). The lemma follows since $J_6(0) = 0$. □

If $E/\mathbb{Q}$ is a non-CM elliptic curve, Lemma 4.4 shows that $\rho_{E,7}(\mathrm{Gal}_{\mathbb{Q}})$ is not conjugate to a subgroup of G_{12}. The same holds for G_9 and G_{10} since they are both subgroups of G_{12}.

Suppose that H is a proper subgroup of G_i satisfying $\pm H = G_i$ for a fixed $1 \le i \le 7$. If $i \ne 1$, then $i \in \{3, 4, 5, 7\}$ and H is one of the groups $H_{i,j}$. If $i = 1$, the H is either $H_{1,1}$ or another subgroup that is conjugate to $H_{1,1}$ in $\mathrm{GL}_2(\mathbb{F}_7)$. This completes the proof of Theorem 1.5(i) and

(ii); we can ignore $t = \infty$ for $2 \le i \le 7$ since $J_i(\infty)$ is either ∞ or the j-invariant of a CM elliptic curve.

4.5. $\ell = 11$. Fix notation as in §1.5. Up to conjugacy, the group $\mathrm{GL}_2(\mathbb{F}_{11})$ has four maximal applicable subgroups: $B(11)$, $N_s(11)$, $N_{ns}(11)$ and a group $H_{\mathfrak{S}_4}$ whose image in $\mathrm{PGL}_2(\mathbb{F}_{11})$ is isomorphic to $\mathfrak{S}_4$.

4.5.1. *Exceptional case.* The curve $X_{\mathfrak{S}_4}(11) := X_{H_{\mathfrak{S}_4}}$ has no rational points corresponding to a non-CM elliptic curve; it is isomorphic to an elliptic curve which has only one rational point [Lig77, Prop. 4.4.8.1] and this point corresponds to an elliptic curve with CM by $\sqrt{-3}$.

4.5.2. *Split case.* The curve $X_s^+(11) := X_{N_s(11)}$ has no rational points corresponding to a non-CM elliptic curve; see [BPR11] for a more general result. Therefore, there are no non-CM elliptic curves $E/\mathbb{Q}$ such that $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to a subgroup of $N_s(11)$.

4.5.3. *Non-split case.* The modular curve $X_{ns}^+(11) := X_{G_3} = X_{N_{ns}(11)}$ has genus 1. Halberstadt [Hal98] showed that the function field of $X_{ns}^+(11)$ is of the form $K := \mathbb{Q}(x, y)$ with $y^2 + y = x^3 - x^2 - 7x + 10$ such that the inclusion $\mathbb{Q}(j) \subseteq \mathbb{Q}(x, y)$ is given by $j = J(x, y)$. Therefore, if $E/\mathbb{Q}$ is a non-CM elliptic curve, then $\rho_{E,11}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to a subgroup of $N_{ns}(11)$ if and only if $j_E = J(P)$ for some point $P \in \mathcal{E}(\mathbb{Q})$. We only need consider $P \neq \mathcal{O}$ since, as noted in [Hal98], $J(\mathcal{O})$ is the j-invariant of a CM elliptic curve.

Let G_4 be the subgroup of G_3 consisting of $g \in G_3 = N_{ns}(11)$ such that $g \in C_{ns}(11)$ and $\det(g) \in (\mathbb{F}_{11}^\times)^2$, or $g \notin C_{ns}(11)$ and $\det(g) \notin (\mathbb{F}_{11}^\times)^2$.

Lemma 4.5. *The modular curve X_{G_4} has no rational points.*

Proof. Define the modular curve $X_{ns}(11) := X_{C_{ns}(11)}$. Proposition 1 of [DFGS14] shows that $X_{ns}(11)$ can be defined by the equations $y^2 + y = x^3 - x^2 - 7x + 10$ and $u^2 = -(4x^3 + 7x^2 - 6x + 19)$, where $K = \mathbb{Q}(x, y)$.

Define the field $L := K(v)$ with $v = u/\sqrt{-11}$. We have $L \subseteq \mathcal{F}_{11}$ since $\sqrt{-11} \in \mathbb{Q}(\zeta_{11})$. Let G be the subgroup of $\mathrm{GL}_2(\mathbb{F}_{11})$ that fixes L; it is an index 2 subgroup of G_3 since L/K has degree 2. The field $\mathbb{Q}$ is algebraically closed in L since it is algebraically closed in K and L/K is a geometric extension. Therefore, $\det(G) = \mathbb{F}_{11}^\times$. There are only two index 2 subgroups of G_3 with full determinant; they are G_4 and $C_{ns}(11)$. The group G is thus G_4 since $C_{ns}(11)$ corresponds to the field $K(u)$.

Therefore, X_{G_4} has function field $\mathbb{Q}(x, y, v)$ where $y^2 + y = x^3 - x^2 - 7x + 10$ and $v^2 = 11(4x^3 + 7x^2 - 6x + 19)$. We now homogenize our equations:

$$y^2z + yz^2 = x^3 - x^2z - 7xz^2 + 10z^3, \quad 11v^2z = (4x^3 + 7x^2z - 6xz^2 + 19z^3). \tag{4.7}$$

Combining the two equations (4.7) to remove the x^3 term, we find that $11v^2z = (4y^2z + 4yz^2 + 11x^2z + 22xz^2 - 21z^3)$. Factoring off z, we deduce that the following equations give a model of X_{G_4} in $\mathbb{P}^3_{\mathbb{Q}}$:

$$y^2z + yz^2 = x^3 - x^2z - 7xz^2 + 10z^3, \quad 11v^2 = (4y^2 + 4yz + 11x^2 + 22xz - 21z^2). \tag{4.8}$$

Suppose $(x, y, z, v) \in \mathbb{P}^3(\mathbb{Q})$ is a solution to (4.8). If $z = 0$, then we have $0 = x^3$ and $11v^2 = 4y^2$, which is impossible since 44 is not a square in $\mathbb{Q}$. So assume that $z = 1$. We can then recover the equation $v^2 = 11(4x^3 + 7x^2 - 6x + 19)$ which has no solutions $(x, v) \in \mathbb{Q}^2$; it defines an elliptic curve and a computation shows that its only rational point is the point at ∞. Therefore, $X_{G_4}(\mathbb{Q}) = \emptyset$. □

Let $E/\mathbb{Q}$ be a non-CM elliptic curve for which $\rho_{E,11}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to a subgroup of G_3. Suppose that $\rho_{E,11}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to a subgroup of G_3. The group G_3 has no index 2 subgroups H that satisfy $\pm H = G_3$. Therefore, $\rho_{E,11}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to a subgroup of a maximal applicable subgroup of G_3. Up to conjugacy, there are two maximal applicable subgroups of G_3; one is G_4 and

the other is a subgroup G_5 of index 3 in G_3. The image $\overline{G}_5$ of G_5 in $\mathrm{PGL}_2(\mathbb{F}_{11})$ has order 8 and is hence a 2-Sylow subgroup of $\mathrm{PGL}_2(\mathbb{F}_{11})$. Therefore, $\overline{G}_5$ lies in a subgroup of $\mathrm{PGL}_2(\mathbb{F}_{11})$ that is isomorphic to $\mathfrak{S}_4$ and hence G_5 is conjugate to a subgroup of $H_{\mathfrak{S}_4}$. However, we saw in §4.5.1 that $\rho_{E,11}(\mathrm{Gal}_{\mathbb{Q}})$ cannot be conjugate to a subgroup of $H_{\mathfrak{S}_4}$. This implies that $\rho_{E,11}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to a subgroup of G_4 which is impossible by Lemma 4.5. Therefore, $\rho_{E,11}(\mathrm{Gal}_{\mathbb{Q}})$ must be conjugate to G_3.

4.5.4. *Borel case.* The modular curve $X_{B(11)}$ is known to have exactly three rational points that are not cusps; they lie above the j-invariants -2^{15}, -11^2 and $-11\cdot 131^3$, cf. [BK75, p. 79]. An elliptic curve with j-invariant -2^{15} has CM, so we need only consider the other two.

Consider the elliptic curve $E/\mathbb{Q}$ defined by $y^2+xy+y=x^3+x^2-305x+7888$; it has j-invariant -11^2 and conductor 11^2. The division polynomial at 11 of E factors as the product of the irreducible polynomial $f(x)=x^5-129x^4+800x^3+81847x^2-421871x-4132831$ and an irreducible polynomial $g(x)$ of degree 55. Since 11 divides the degree of $g(x)$, we find that $\rho_{E,11}(\mathrm{Gal}_{\mathbb{Q}})$ contains an element of order 11. Therefore, there are unique characters $\chi_1,\chi_2\colon \mathrm{Gal}_{\mathbb{Q}}\to\mathbb{F}_{11}^{\times}$ such that with respect to an appropriate change of basis we have

$$\rho_{E,11}(\sigma)=\begin{pmatrix}\chi_1(\sigma) & *\\ 0 & \chi_2(\sigma)\end{pmatrix}. \tag{4.9}$$

We have $\chi_1\chi_2=\omega$ where $\omega\colon \mathrm{Gal}_{\mathbb{Q}}\to\mathbb{F}_{11}^{\times}$ is the character describing the Galois action on the 11-th roots of unity (we have $\omega(p)\equiv p \pmod{11}$ for primes $p\neq 11$). The characters χ_1 and χ_2 are unramified at primes $p\nmid 11$, so $\chi_1=\omega^a$ and $\chi_2=\omega^{11-a}$ for a unique integer $0\le a<10$. Let $w\in\overline{\mathbb{Q}}$ be a fixed root of $f(x)$. One can show that

$$P=\big(w,-(w^4-79w^3-3150w^2+12193w+1520110)/11^4\big)$$

is an 11-torsion point of $E(\overline{\mathbb{Q}})$. The field $\mathbb{Q}(w)$ is a Galois extension of $\mathbb{Q}$ and that the group generated by P is stable under the action of $\mathrm{Gal}_{\mathbb{Q}}$. We thus have $\sigma(P)=\chi_1(\sigma)\cdot P$ for all $\sigma\in\mathrm{Gal}_{\mathbb{Q}}$, and hence $\chi_1(\mathrm{Gal}_{\mathbb{Q}})$ is a group of order $[\mathbb{Q}(w):\mathbb{Q}]=5$.

We have $a_2(E)=-1$, so the roots of the polynomial $\det(xI-\rho_{E,11}(\mathrm{Frob}_2))\equiv x^2-(-1)x+2 \pmod{11}$ are $4=2^2$ and $6\equiv 2^9 \pmod{11}$. Since $\chi_1(\mathrm{Frob}_2)\equiv 2^a$ and $\chi(\mathrm{Frob}_2)\equiv 2^{11-a}$ are the roots of $\det(xI-\rho_{E,11}(\mathrm{Frob}_2))$ and 2 is a primitive root modulo 11, we have $a\in\{2,9\}$ and hence $\{\chi_1,\chi_2\}=\{\omega^2,\omega^9\}$. Since $\chi_1(\mathrm{Gal}_{\mathbb{Q}})$ has cardinality 5, we have $\chi_1=\omega^2$ and $\chi_2=\omega^9$. Since 2 is a primitive root modulo 11, the group $\rho_{E,11}(\mathrm{Gal}_{\mathbb{Q}})$ is generated by $\left(\begin{smallmatrix}2^2 & 0\\ 0 & 2^9\end{smallmatrix}\right)=\left(\begin{smallmatrix}4 & 0\\ 0 & 6\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$, i.e., it equals $H_{1,1}$. In particular, $\pm\rho_{E,11}(\mathrm{Gal}_{\mathbb{Q}})=G_1$.

Consider the elliptic curve $E/\mathbb{Q}$ defined by $y^2+xy=x^3+x^2-3632x+82757$; it has j-invariant $-11\cdot 131^3$ and conductor 11^2. The division polynomial at 11 of E factors as the product of the irreducible polynomial $f(x)=x^5-129x^4+4793x^3+9973x^2-3694800x+52660939$ and an irreducible polynomial $g(x)$ of degree 55. Since 11 divides the degree of $g(x)$, we find that $\rho_{E,11}(\mathrm{Gal}_{\mathbb{Q}})$ contains an element of order 11. Therefore, there are unique characters $\chi_1,\chi_2\colon \mathrm{Gal}_{\mathbb{Q}}\to\mathbb{F}_{11}^{\times}$ such that with respect to an appropriate change of basis we have (4.9). The characters χ_1 and χ_2 are unramified at primes $p\nmid 11$ and $\chi_1\chi_2=\omega$, so $\chi_1=\omega^a$ and $\chi_2=\omega^{11-a}$ for a unique integer $a\in\{0,1,\dots,9\}$. Let $w\in\overline{\mathbb{Q}}$ be a fixed root of $f(x)$. One can show that

$$P=\big(w,(w^4-79w^3+843w^2+45468w-722625)/11^3\big)$$

is an 11-torsion point of $E(\overline{\mathbb{Q}})$. The field $\mathbb{Q}(w)$ is a Galois extension of $\mathbb{Q}$ and that the group generated by P is stable under the action of $\mathrm{Gal}_{\mathbb{Q}}$. We thus have $\sigma(P)=\chi_1(\sigma)\cdot P$ for all $\sigma\in\mathrm{Gal}_{\mathbb{Q}}$, and hence $\chi_1(\mathrm{Gal}_{\mathbb{Q}})$ is a group of order $[\mathbb{Q}(w):\mathbb{Q}]=5$. We have $a_2(E)=1$, so the roots of the polynomial $\det(xI-\rho_{E,11}(\mathrm{Frob}_2))\equiv x^2-1\cdot x+2 \pmod{11}$ are $5\equiv 2^4$ and $7\equiv 2^7 \pmod{11}$. Since

$\chi_1(\mathrm{Frob}_2) \equiv 2^a$ and $\chi(\mathrm{Frob}_2) \equiv 2^{11-a}$ are the roots of $\det(xI - \rho_{E,11}(\mathrm{Frob}_2))$ and 2 is a primitive root modulo 11, we have $a \in \{4,7\}$ and hence $\{\chi_1,\chi_2\} = \{\omega^4,\omega^7\}$. Since $\chi_1(\mathrm{Gal}_{\mathbb{Q}})$ has cardinality 5, we have $\chi_1 = \omega^4$ and $\chi_2 = \omega^7$. Since 2 is a primitive root modulo 11, the group $\rho_{E,11}(\mathrm{Gal}_{\mathbb{Q}})$ is generated by $\left(\begin{smallmatrix} 2^4 & 0 \\ 0 & 2^7 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 5 & 0 \\ 0 & 7 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, i.e., it equals $H_{2,1}$. In particular, $\pm\rho_{E,11}(\mathrm{Gal}_{\mathbb{Q}}) = G_2$.

4.5.5. *Polynomials for $X_{ns}^+(11)$.* This subsection is dedicated to sketching Remark 1.7 and making the polynomials explicit; fix notation as in §1.5. Define the polynomials:

$$
\begin{aligned}
A(x) &= (x^5 - 9x^4 + 17x^3 + 20x^2 - 73x + 43)^{11},\\
B(x) &= -(x^2+3x-6)^3\big(108000x^{49} + 23793840x^{48} - 413223722x^{47} - 5377010368x^{46} + 230799738529x^{45}\\
&\quad - 3137869050351x^{44} + 23205911712335x^{43} - 90936268647246x^{42} + 33563647471596x^{41}\\
&\quad + 1631415220074871x^{40} - 7744726079195413x^{39} - 3218815397602111x^{38} + 23671205143721764 4x^{37}\\
&\quad - 16864286980222533 44x^{36} + 79848040020230635 54x^{35} - 30444784135263860996x^{34}\\
&\quad + 96849826504401032248x^{33} - 23206439488353967321 3x^{32} + 21017553541339535385 7x^{31}\\
&\quad + 16096958063249464848 26x^{30} - 11768533689837648360109x^{29} + 48291196122826259771817x^{28}\\
&\quad - 14394393189930637317 0309x^{27} + 31582702578156323242 0857x^{26} - 42159697972048599262 9121x^{25}\\
&\quad - 23492988588016254764 5306x^{24} + 36682414375530228019 50917x^{23} - 14221091463553801024770599x^{22}\\
&\quad + 39148264563215734730610917x^{21} - 87534472061810348609315974x^{20}\\
&\quad + 16647424021961957537 9485393x^{19} - 27504077157305483424 7036345x^{18}\\
&\quad + 39914472537722390993 7142938x^{17} - 51184096038235814459 5839458x^{16}\\
&\quad + 58165616553533421466 5717816x^{15} - 58620657809698124398 0668654x^{14}\\
&\quad + 52346565584190107937 0457175x^{13} - 41320082463280250335 4807972x^{12}\\
&\quad + 28727083277531664395 2335709x^{11} - 17504957713126908779 5781453x^{10}\\
&\quad + 92916572268973769104 815620x^9 - 42636417323385892254 033027x^8\\
&\quad + 16754292456737738144 357709x^7 - 55709110681111617263 502302x^6 + 15426488019953308741 84236x^5\\
&\quad - 34781905342492833679 3068x^4 + 61683475328903338239 178x^3 - 81170562507209372289 85x^2\\
&\quad + 70831874034094144979 9x - 30857360406231018655\big),\\
C(x) &= (4x-5)(x^2+3x-6)^6(9x^2-28x+23)^3(x^4-5x^3+74x^2-245x+223)^3\\
&\quad \cdot (4x^4-9x^3-x^2+21x-32)^3(25x^4-114x^3+167x^2-86x+20)^3.
\end{aligned}
$$

Proposition 4.6. *For $j \in \mathbb{Q}$, we have $J(P) = j$ for some point $P \in \mathcal{E}(\mathbb{Q}) - \{\mathcal{O}\}$ if and only if $A(x)j^2 + B(x)j + C(x) \in \mathbb{Q}[x]$ has a rational root.*

Proof. Take $(x,y) \in \mathcal{E} - \{\mathcal{O}\}$. Using the equation $y^2 + y = x^3 - x^2 - 7x + 10$, a direct computation shows that $J(x,y)A(x) = a(x)y + b(x)$ for unique $a, b \in \mathbb{Q}[x]$. Multiplying $y^2 + y = x^3 - x^2 - 7x + 10$ by a^2, we deduce that $(JA-b)^2 + a(JA-b) - a^2(x^3 - x^2 - 7x + 10) = 0$. Therefore, $A^2J^2 + (-2b + a)AJ + b^2 - ba - a^2(x^3 - x^2 - 7x + 10) = 0$. Our polynomials B and C satisfy $B = -2b + a$ and $C = (b^2 - ba - a^2(x^3 - x^2 - 7x + 10))/A$. We thus have

$$A(x)J(x,y)^2 + B(x)J(x,y) + C(x) = 0 \tag{4.10}$$

for all $(x,y) \in \mathcal{E} - \{\mathcal{O}\}$.

First suppose that $j = J(x_0,y_0)$ for some $(x_0,y_0) \in \mathcal{E}(\mathbb{Q}) - \{\mathcal{O}\}$. Then $0 = A(x_0)J(x_0,y_0)^2 + B(x_0)J(x_0,y_0) + C(x_0) = A(x_0)j^2 + B(x_0)j + C(x_0)$ and hence $A(x)j^2 + B(x)j + C(x)$ has a rational root.

Now fix $j \in \mathbb{Q}$ and suppose that there is an $x_0 \in \mathbb{Q}$ such that $A(x_0)j^2 + B(x_0)j + C(x_0) = 0$. Define $\Delta(x) := B(x)^2 - 4A(x)C(x)$. A computation shows that $\Delta(x) = D(x)^2(x^3 - x^2 - 7x + 41/4)$

for a polynomial $D \in \mathbb{Q}[x]$ that has no rational roots. The rational number $\Delta(x_0) = D(x_0)^2(x_0^3 - x_0^2 - 7x_0 + 41/4)$ is a square since j is a root of $A(x_0)X^2 + B(x_0)X + C(x_0) \in \mathbb{Q}[X]$. Therefore, $v^2 = x_0^3 - x_0^2 - 7x_0 + 41/4$ for some $v \in \mathbb{Q}$. With $y_0 = v - 1/2$, we have $y_0^2 + y_0 = x_0^3 - x_0^2 - 7x_0 + 10$ and hence $P := (x_0, y_0)$ is a point in $\mathcal{E}(\mathbb{Q}) - \{\mathcal{O}\}$. We could have chose v with a different sign, so $P' := (x_0, -v - 1/2) = (x_0, -y_0 - 1)$ also belongs to $\mathcal{E}(\mathbb{Q}) - \{\mathcal{O}\}$.

We claim that $J(P) \neq J(P')$. Suppose that they are in fact equal. Using that $J(x, y)A(x) = a(x)y + b(x)$, we find that $a(x_0)y_0 = a(x_0)(-y_0 - 1)$. Since $a(x)$ has no rational roots, we must have $y_0 = -1/2$ and hence $v = 0$. However, this is impossible since $x^3 - x^2 - 7x + 41/4$ has no rational roots, so the claim follows. From (4.10), we find that $J(P)$ and $J(P')$ are distinct roots of $A(x_0)X^2 + B(x_0)X + C(x_0)$. Since j is also a root of this quadratic polynomial, we deduce that $j = J(P)$ or $j = J(P')$. □

4.6. $\ell = 13$. We shall prove parts (i) and (ii) of Theorem 1.8 (part (iv) was explained in the introduction); so we will focus on $B(13)$ and its subgroups. We first rule out subgroups of $C_s(13)$.

Lemma 4.7. *There are no non-CM elliptic curves $E/\mathbb{Q}$ for which $\rho_{E,13}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_{13})$ to a subgroup of $C_s(13)$.*

Proof. Kenku has proved that the only rational points of $X_0(13^2)$ are cusps, cf. [Ken80, Ken81]. By Lemma 3.6, we deduce that the only rational points of the modular curve $X_{C_s(13)}$ are cusps. □

One can show that the applicable subgroups of $B(13) = G_6$ that are not subgroups of $C_s(13)$ are G_1, G_2, G_3, G_4, G_5, and $G_i \cap G_j$ with $i \in \{1, 2\}$ and $j \in \{3, 4, 5\}$. Note that these subgroups are normal in $B(13)$.

We now describe several modular function constructed by Lecacheux [Lec89, p.56]. Define

$$f(\tau) = \frac{\wp(\frac{1}{13};\tau) - \wp(\frac{2}{13};\tau)}{\wp(\frac{1}{13};\tau) - \wp(\frac{3}{13};\tau)} \quad \text{and} \quad g(\tau) = \frac{\wp(\frac{1}{13};\tau) - \wp(\frac{2}{13};\tau)}{\wp(\frac{1}{13};\tau) - \wp(\frac{5}{13};\tau)}$$

where $\wp(z;\tau)$ is the Weierstrass $\wp$-function at z of the lattice $\mathbb{Z}\tau + \mathbb{Z} \subseteq \mathbb{C}$. Define the functions

$$h_5 := \frac{(g-1)(g(g-1)+1-f)}{(f-1)(f-g)} \quad \text{and} \quad h_2 := \frac{f-1}{g-1}.$$

The functions h_5 and h_2 belong to $\mathcal{F}_{13}$ and satisfy $F_2(h_2) = F_5(h_5)$, where

$$F_2(t) = t+(t-1)/t-1/(t-1)-4 = (t^3-4t^2+t+1)/(t^2-t) \quad \text{and} \quad F_5(t) = t-1/t-3 = (t^2-3t-1)/t;$$

this follows from [Lec89, p.56–57] with $H = h_5$ and $h = h_2$.

Let h_6 be the function $F_2(h_2) = F_5(h_5)$; it is called $a - 3$ in [Lec89] and satisfies $J_6(h_6) = j$, cf. [Lec89, p.62]. Since $J_2(t) = J_6(F_2(t))$ and $J_5(t) = J_6(F_5(t))$, we have $J_2(h_2) = j$ and $J_5(h_5) = j$.

Define $\alpha := -\zeta_{13}^{11} - \zeta_{13}^{10} - \zeta_{13}^{3} - \zeta_{13}^{2} + 1$. Define the rational functions

$$F_1(t) = 13(t^2 - t)/(t^3 - 4t^2 + t + 1) \quad \text{and} \quad \phi_1(t) = (\alpha t + 1 - \alpha)/(t - \alpha);$$

Define the modular function $h_1 := \phi_1(h_2) \in \mathcal{F}_{13}$. One can check that $F_1(\phi_1(t)) = F_2(t)$ and hence $F_1(h_1) = F_2(h_2) = h_6$. Since $J_1(t) = J_6(F_1(t))$, we have $J_1(h_1) = j$.

Define $\beta := \zeta_{13}^{11} + \zeta_{13}^{10} + \zeta_{13}^{9} + \zeta_{13}^{7} + \zeta_{13}^{6} + \zeta_{13}^{4} + \zeta_{13}^{3} + \zeta_{13}^{2} + 2$. Define the rational functions

$$F_3(t) = (-5t^3 + 7t^2 + 8t - 5)/(t^3 - 4t^2 + t + 1) \quad \text{and} \quad \phi_3(t) = (\beta t - 1)/(t + \beta - 1).$$

Define the modular function $h_3 := \phi_3(h_2) \in \mathcal{F}_{13}$. One can check that $F_3(\phi_3(t)) = F_2(t)$ and hence $F_3(h_3) = F_2(h_2) = h_6$. Since $J_3(t) = J_6(F_3(t))$, we have $J_3(h_3) = j$.

Define $\gamma = (1+\sqrt{13})/2$; it belongs to $\mathbb{Q}(\zeta_{13})$ and moreover equals $\gamma = -\zeta_{13}^{11} - \zeta_{13}^{8} - \zeta_{13}^{7} - \zeta_{13}^{6} - \zeta_{13}^{5} - \zeta_{13}^{2}$. Define the rational functions

$$F_4(t) = 13t/(t^2 - 3t - 1) \quad \text{and} \quad \phi_4(t) = ((2-\gamma)t + 1)/(t - 2 + \gamma)).$$

Define the modular function $h_4 := \phi_4(h_5) \in \mathcal{F}_{13}$. One can check that $F_4(\phi_4(t)) = F_5(t)$ and hence $F_4(h_4) = F_5(h_5) = h_6$. Since $J_4(t) = J_6(F_4(t))$, we have $J_4(h_4) = j$.

For $1 \le i \le 6$, let H_i be the subgroup of $\mathrm{GL}_2(\mathbb{F}_7)$ that fixes h_i. We have shown that $J_i(h_i) = j$. By Lemma 3.4, we find that H_i is an applicable subgroup and that the morphism $\pi_{H_i} \colon X_{H_i} \to \mathbb{P}^1_{\mathbb{Q}}$ is described by the rational function $J_i(t)$.

Lemma 4.8. *The groups H_i and G_i are conjugate in $\mathrm{GL}_2(\mathbb{F}_{13})$ for all $1 \le i \le 6$.*

Proof. The index of H_6 in $\mathrm{GL}_2(\mathbb{F}_{13})$ is equal to 14, i.e., the degree of J_6 as a morphism. Therefore, H_6 must be conjugate to $B(13)$. The index $[H_6 : H_i]$ equals the degree of $F_i(t)$, and is thus 3 if $i \in \{1,2,3\}$ and 2 if $i \in \{4,5\}$.

The groups H_1, H_2 and H_3 are not conjugate in $\mathrm{GL}_2(\mathbb{F}_{13})$ since one can show that the images of $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$ under J_1, J_2 and J_3 are distinct. Therefore, H_1, H_2 and H_3 are conjugate to G_1, G_2 and G_3 which are the applicable subgroups of $B(13)$ of index 2; however, we still need to determine which group is conjugate to which.

Let $E/\mathbb{Q}$ be the elliptic curve defined by $y^2 = x^3 - 338x + 2392$. The group $\rho_{E,13}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to a subgroup of H_3 since $j_E = J_3(0)$. One can check that $E/\mathbb{Q}$ has good reduction at 3 and that $a_3(E) = 0$. Since $x^2 - a_3(E) + 3 \equiv (x-6)(x+6) \pmod{13}$, we deduce that the eigenvalues of the matrix $\rho_{E,13}(\mathrm{Frob}_3)$ are 6 and -6. For every matrix in G_1 or G_2 has an eigenvalue in $(\mathbb{F}_{13}^{\times})^3 = \{\pm 1, \pm 5\}$. Since 6 and -6 do not belong to $(\mathbb{F}_{13}^{\times})^3$, we deduce that H_3 is not conjugate to G_1 and G_2. Therefore, H_3 is conjugate to G_3.

Let $E/\mathbb{Q}$ be the elliptic curve defined by $y^2 = x^3 - 2227x - 59534$. We have $j_E = J_2(2)$ and $j_E \notin J_1(\mathbb{Q} \cup \{\infty\})$. Therefore, $\rho_{E,13}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to a subgroup of H_2 and not conjugate to a subgroup of H_1. By computing the division polynomial of E at the prime 13, we find that E has a point P of order 13 whose x-coordinate is $17 + 8\sqrt{17}$. So with respect to a basis of $E[13]$ whose first element is P, we find that $\rho_{E,13}(\mathrm{Gal}_{\mathbb{Q}})$ is a subgroup of G_2. Therefore, H_2 is conjugate to G_2, and hence H_1 is conjugate to G_1.

The groups H_4 and H_5 are not conjugate in $\mathrm{GL}_2(\mathbb{F}_{13})$ since one can show that the images of $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$ under J_4 and J_5 are distinct. Therefore, H_4 and H_5 are conjugate to G_4 and G_5 which are the applicable subgroups of $B(13)$ of index 3; however, we still need to determine which group is conjugate to which.

Let $E/\mathbb{Q}$ be the elliptic curve defined by $y^2 = x^3 - 3024x - 69552$. We have $j_E = J_5(2)$ and $j_E \notin J_4(\mathbb{Q} \cup \{\infty\})$. Therefore, $\rho_{E,13}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to a subgroup of H_5 and not conjugate to a subgroup of H_4. By computing the division polynomial of E at the prime 13, we find that E has a point P of order 13 whose x-coordinate w is a root of $x^3 - 3024x + 12096$. The cubic extension $\mathbb{Q}(w)$ of $\mathbb{Q}$ is Galois, so with respect to a basis of $E[13]$ whose first element is P, we find that $\rho_{E,13}(\mathrm{Gal}_{\mathbb{Q}})$ is a subgroup of G_5. Therefore, H_5 is conjugate to G_5, and hence H_4 is conjugate to G_4. □

We have thus completed the proof of Theorem 1.8(ii); we can ignore $t = \infty$ since $J_i(\infty) = \infty$ for $i \neq 3$ and $J_3(\infty) = J_3(0)$. If H is a proper subgroup of G_i satisfying $\pm H = G_i$, then one can show that $i \in \{4,5\}$ and H is one of the groups $H_{i,j}$.

To complete the proof of Theorem 1.8(i), we need only show that the modular curves $X_{G_i \cap G_j}$, with fixed $i \in \{1,2\}$ and $j \in \{3,4,5\}$, have no rational points other than cusps. It suffices to prove the same thing for the modular curves $X_{H_i \cap H_j}$.

The function field of $X_{H_i \cap H_j}$ is $\mathbb{Q}(h_i, h_j)$ and the generators h_i and h_j satisfy the relation $F_i(h_i) = h_6 = F_j(h_j)$. The smooth projective (and geometrically irreducible) curve over $\mathbb{Q}$ arising from the equation $F_i(x) = F_j(y)$ is thus a model of $X_{H_i \cap H_j}$.

The following `Magma` code shows that if $(x, y) \in \mathbb{Q}^2$ is a solution of $F_i(x) = F_j(y)$ (where we say that both sides equal ∞ if the denominators vanish), then $y = 0$. The code considers the projective (and possibly singular) curve $C_{i,j}$ in $\mathbb{P}^2_{\mathbb{Q}}$ defined by the affine equation $F_i(x) = F_j(y)$ (we first clear denominators and homogenize). We then find a genus 2 curve C that is birational with $C_{i,j}$ and is defined by some Weierstrass equation $y^2 = f(x)$ with $f(x) \in \mathbb{Q}[x]$ a separable polynomial of degree 5 or 6. We then check that the Jacobian J of C has rank 0, equivalently, that $J(\mathbb{Q})$ is a finite group (`Magma` accomplishes this by computing the 2-Selmer group of J). Using that $J(\mathbb{Q})$ has rank 0, the function `Chabauty0` finds all the rational points on C. Using the birational isomorphism between C and $C_{i,j}$, we can determine the rational points of C.

```
K<t>:=FunctionField(Rationals());
F:=[13*(t^2-t)/(t^3-4*t^2+t+1), (t^3-4*t^2+t+1)/(t^2-t),
    (-5*t^3+7*t^2+8*t-5)/(t^3-4*t^2+t+1), 13*t/(t^2-3*t-1), (t^2-3*t-1)/t ];
P2<x,y,z>:=ProjectiveSpace(Rationals(),2);
for i in [1,2,3], j in [4,5] do
    f:=Numerator(Evaluate(F[i],x/z)- Evaluate(F[j],y/z));
    while Evaluate(f,z,0) eq 0 do  f:= f div z; end while;
    C0:=Curve(P2,f);
    b,C1,f1:=IsHyperelliptic(C0); C2,f2:=SimplifiedModel(C1);
    Jac:=Jacobian(C2);   RankBound(Jac) eq 0;
    S:=Chabauty0(Jac);
    b,g1:=IsInvertible(f1); b,g2:=IsInvertible(f2);
    T:=g1(g2(S) join SingularPoints(C1)) join SingularPoints(C0);
    {P: P in T | P[2] ne 0 and P[3] ne 0} eq {};
end for;
```

We find that if $F_i(x) = F_i(y)$ for some $x, y \in \mathbb{Q} \cup \{\infty\}$, then $y = 0$ or $y = \infty$. Thus the only rational points of $X_{H_i \cap H_j}$ are cusps since $J_j(0) = J_j(\infty) = \infty$ for $j \in \{4, 5\}$.

4.7. $\ell = 17$. We now prove Theorem 1.10(i). Let $E/\mathbb{Q}$ be the elliptic curve defined by the Weierstrass equation $y^2 + xy + y = x^3 - 190891x - 36002922$; it has j-invariant $-17 \cdot 373^3/2^{17}$ and conductor $2 \cdot 5^2 \cdot 17^2$. The division polynomial of E at 17 factors as a product of $f(x) = x^4 + 482x^3 + 1144x^2 - 15809842x - 958623689$ with irreducible polynomials of degree 4 and $8 \cdot 17$. Fix a point $P \in E(\overline{\mathbb{Q}})$ whose x-coordinate w is a root of $f(x)$; it is a 17-torsion point. Let C be the cyclic group of order 17 generated by P; it is stable under the $\mathrm{Gal}_{\mathbb{Q}}$ action. Let $\chi_1 \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathbb{F}_{17}^{\times}$ be the homomorphism such that $\sigma(P) = \chi_1(\sigma) \cdot P$ for $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$. One can show that the degree 4 extension $\mathbb{Q}(w)/\mathbb{Q}$ is Galois, so $\chi_1(\mathrm{Gal}_{\mathbb{Q}})$ has cardinality 4 or 8. There is a second character $\chi_2 \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathbb{F}_{17}^{\times}$ such that, with respect to an appropriate change of basis, we have

$$\rho_{E,17}(\sigma) = \begin{pmatrix} \chi_1(\sigma) & * \\ 0 & \chi_2(\sigma) \end{pmatrix}.$$

The cardinality of $\rho_{E,17}(\mathrm{Gal}_{\mathbb{Q}})$ is divisible by 17 since the division polynomial of E at 17 has an irreducible factor whose degree is divisible by 17. We have $\chi_1\chi_2 = \omega$ where $\omega \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathbb{F}_{17}^{\times}$ is the character describing the Galois action on the 17-th roots of unity (we have $\omega(\mathrm{Frob}_p) = p$ for primes $p \neq 17$). The characters χ_1 and χ_2 are unramified at primes $p \nmid 2 \cdot 5 \cdot 17$, so $\chi_1 = \omega^a \chi$ and $\chi_2 = \omega^{17-a}\chi^{-1}$ for some integer $0 \leq a < 16$ and some character $\chi \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathbb{F}_{17}^{\times}$ unramified at $p \nmid 2 \cdot 5$.

Let H_1 and H_2 be the subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ consisting of matrices of the form

$$\begin{pmatrix} \omega(\sigma)^a & 0 \\ 0 & \omega(\sigma)^{17-a} \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} \chi_1(\sigma) & 0 \\ 0 & \chi_1(\sigma)^{-1} \end{pmatrix},$$

respectively, with $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$. Since ω and χ are ramified at different primes, we find that the image of $\rho_{E,\ell}$ is generated by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and the groups H_1 and H_2.

The character χ is unramified at $p \nmid 2 \cdot 5$ and has image in a cyclic group of order 16. Therefore, χ must factor through the group $\mathrm{Gal}(\mathbb{Q}(\zeta_{64}, \zeta_5)/\mathbb{Q})$. Since $641 \equiv 1 \pmod{64 \cdot 5}$, we have $\chi(\mathrm{Frob}_{641}) = 1$. Therefore, $\chi_1(\mathrm{Frob}_{641}) = \omega(\mathrm{Frob}_{641})^a \cdot 1 \equiv 641^a \pmod{17}$ is a root of

$$x^2 - a_{641}(E)x + 641 = x^2 - (-9)x + 641 \equiv (x - 641^6)(x - 641^{11}) \pmod{17},$$

and hence $a \in \{6, 11\}$ since 641 is a primitive root modulo 17. If $a = 11$, then $\chi_1(\mathrm{Gal}_{\mathbb{Q}}) = \mathbb{F}_{17}^{\times}$ which is impossible since the cardinality of $\chi_1(\mathrm{Gal}_{\mathbb{Q}})$ is 4 or 8. Therefore, $a = 6$. The group H_1 thus consists of matrices of the form $\left(\begin{smallmatrix} c^6 & 0 \\ 0 & c^{11} \end{smallmatrix}\right)$ with $c \in \mathbb{F}_{17}^{\times}$, and in particular is generated by $\left(\begin{smallmatrix} 5^6 & 0 \\ 0 & 5^{11} \end{smallmatrix}\right) = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 11 \end{smallmatrix}\right)$.

To complete the proof that $\rho_{E,17}(\mathrm{Gal}_{\mathbb{Q}})$ is G_1, it suffices to show that H_2 is generated by $\left(\begin{smallmatrix} 4 & 0 \\ 0 & -4 \end{smallmatrix}\right)$; equivalently, to show that the image of χ is cyclic of order 4. As noted earlier, χ factors through the group $\mathrm{Gal}(\mathbb{Q}(\zeta_{64}, \zeta_5)/\mathbb{Q}) \cong (\mathbb{Z}/64 \cdot 5\mathbb{Z})^{\times}$. One can then show that $\mathrm{Gal}(\mathbb{Q}(\zeta_{64}, \zeta_5)/\mathbb{Q})$ is generated by Frob_{103}, Frob_{137} and Frob_{307}. The primes $p \in \{103, 137, 307\}$ were chosen to be congruent to 1 modulo 17, and hence $\chi(\mathrm{Frob}_p) = \chi_1(\mathrm{Frob}_p)$ is a root of $x^2 - a_p(E)x + p$ modulo 17. It is then straightforward to check that $\chi(\mathrm{Frob}_{103})$, $\chi(\mathrm{Frob}_{137})$ and $\chi(\mathrm{Frob}_{307})$ all have order 4.

The elliptic curve $E'/\mathbb{Q}$ defined by the Weierstrass equation $y^2 + xy + y = x^3 - 3041x + 64278$; it has j-invariant $-17^2 \cdot 101^3/2$. One can show that E/C is isomorphic to E'. The group $\rho_{E',17}(\mathrm{Gal}_{\mathbb{Q}})$ is thus conjugate to G_2 in $\mathrm{GL}_2(\mathbb{F}_{17})$.

Finally we note that G_1 and G_2 have no index 2 subgroups that do not contain $-I$.

4.8. $\ell = 37$**.** We now prove Theorem 1.10(ii). Let $E/\mathbb{Q}$ be the elliptic curve defined by the equation $y^2 + xy + y = x^3 + x^2 - 8x + 6$; it has j-invariant $-7 \cdot 11^3$ and conductor $5^2 \cdot 7^2$. The division polynomial of E at 17 factors as a product of $f(x) := x^6 - 15x^5 - 90x^4 - 50x^3 + 225x^2 + 125x - 125$ with irreducible polynomials of degree 6, 6 and $18 \cdot 37$. Fix a point $P \in E(\overline{\mathbb{Q}})$ whose x-coordinate w is a root of $f(x)$; it is a 37-torsion point. Let C be the cyclic group of order 37 generated by P; it is stable under the $\mathrm{Gal}_{\mathbb{Q}}$ action.

Let $\chi_1 \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathbb{F}_{37}^{\times}$ be the homomorphism such that $\sigma(P) = \chi_1(\sigma) \cdot P$ for $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$. One can show that the degree 6 extension $\mathbb{Q}(w)/\mathbb{Q}$ is Galois, so $\chi_1(\mathrm{Gal}_{\mathbb{Q}})$ has cardinality 6 or 12; in particular $\chi_1(\mathrm{Gal}_{\mathbb{Q}})$ is a subgroup of $(\mathbb{F}_{37}^{\times})^3$. There is a second character $\chi_2 \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathbb{F}_{37}^{\times}$ such that, with respect to an appropriate change of basis, we have

$$\rho_{E,37}(\sigma) = \begin{pmatrix} \chi_1(\sigma) & * \\ 0 & \chi_2(\sigma) \end{pmatrix}.$$

The cardinality of $\rho_{E,37}(\mathrm{Gal}_{\mathbb{Q}})$ is divisible by 37 since the division polynomial of E at 37 has an irreducible factor whose degree is divisible by 37. So to prove that $\rho_{E,37}(\mathrm{Gal}_{\mathbb{Q}}) = G_3$, it suffices to show that the homomorphism $\chi_1 \times \chi_2 \colon \mathrm{Gal}_{\mathbb{Q}} \to (\mathbb{F}_{37}^{\times})^3 \times \mathbb{F}_{37}^{\times}$ is surjective.

The characters χ_1 and χ_2 are unramified at primes $p \nmid 5 \cdot 7 \cdot 37$. By Proposition 11 of [Ser72], we have $\{\chi_1, \chi_2\} = \{\alpha, \alpha^{-1} \cdot \omega\}$ where $\alpha \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathbb{F}_{37}^{\times}$ is a character unramified at primes $p \nmid 5 \cdot 7$ and $\omega \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathbb{F}_{37}^{\times}$ is the character describing the Galois action on the 37-th roots of unity. Since α is unramified at 37, we find that the character $\alpha^{-1} \cdot \omega$ is surjective and that $(\alpha \times (\alpha^{-1} \cdot \omega))(\mathrm{Gal}_{\mathbb{Q}}) = \alpha(\mathrm{Gal}_{\mathbb{Q}}) \times \mathbb{F}_{37}^{\times}$. Since χ_1 is not surjective, we must have $\chi_1 = \alpha$ and $\chi_2 = \alpha^{-1} \cdot \omega$. It thus suffices to show that the image of α contains an element of order 12. The fixed field of the kernel of α is contained in $\mathbb{Q}(\zeta_5, \zeta_7)$ since it is unramified at $p \nmid 5 \cdot 7$ and has image relatively prime to $5 \cdot 7$. Since $107 \equiv 2 \pmod{35}$, we have $\alpha(\mathrm{Frob}_2) = \alpha(\mathrm{Frob}_{107})$. Therefore, $\alpha(\mathrm{Frob}_2)$ is a common root of $x^2 - a_2(E)x + 2 = x^2 + x + 2$ and $x^2 - a_{107}(E)x + 107 = x^2 + 11x + 107$ modulo 37. This implies that $\alpha(\mathrm{Frob}_2)$ equals $8 \in \mathbb{F}_{37}^{\times}$ which has order 12.

One can show that the quotient of E by C is the elliptic curve $E'/\mathbb{Q}$ defined by $y^2 + xy + y = x^3 + x^2 - 208083x - 36621194$; it has j-invariant $-7 \cdot 137^3 \cdot 2083^3$. The group $\rho_{E',37}(\mathrm{Gal}_{\mathbb{Q}})$ is thus conjugate in $\mathrm{GL}_2(\mathbb{F}_{37})$ to G_4.

Finally we note that G_3 and G_4 have no index 2 subgroups that do not contain $-I$.

5. Quadratic twists

Fix an elliptic curve $E/\mathbb{Q}$ with $j_E \notin \{0, 1728\}$ and an integer $N \geq 3$.

Define the group $G := \pm\rho_{E,N}(\mathrm{Gal}_{\mathbb{Q}})$ and let $\mathcal{H}$ be the set of proper subgroups H of G that satisfy $\pm H = G$. For each group $H \in \mathcal{H}$, we obtain a character

$$\chi_{E,H} \colon \mathrm{Gal}_{\mathbb{Q}} \to \{\pm 1\}$$

by composing $\rho_{E,N}$ with the quotient map $G \to G/H \cong \{\pm 1\}$. The fixed field of the kernel of the character $\chi_{E,H}$ is of the form $\mathbb{Q}(\sqrt{d_{E,H}})$ for a unique squarefree integer $d_{E,H}$. Define the set

$$\mathcal{D}_E := \{d_{E,H} \colon H \in \mathcal{H}\}.$$

Using $\pm\rho_{E,N}(\mathrm{Gal}_{\mathbb{Q}}) = G$, we find that different groups $H \in \mathcal{H}$ give rise to distinct characters $\chi_{E,H}$ and thus $|\mathcal{D}_E| = |\mathcal{H}|$.

5.1. **Twists with smaller image.** For a squarefree integer d, let $E_d/\mathbb{Q}$ be a quadratic twist of $E/\mathbb{Q}$ by d. By choosing an appropriate basis of $E_d[\ell]$, we may assume that $\rho_{E_d,N} \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ satisfies

$$\rho_{E_d,N} = \chi_d \cdot \rho_{E,N},$$

where $\chi_d \colon \mathrm{Gal}_{\mathbb{Q}} \to \{\pm 1\}$ is the character corresponding to the extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$. We have $\pm\rho_{E_d,N}(\mathrm{Gal}_{\mathbb{Q}}) = \pm\rho_{E,N}(\mathrm{Gal}_{\mathbb{Q}}) = G$. Therefore, $\rho_{E_d,N}(\mathrm{Gal}_{\mathbb{Q}})$ is equal to either G or to one of the subgroups $H \in \mathcal{H}$.

We now show that $\mathcal{D}_E$ is precisely the set of squarefree integers d for which the image of $\rho_{E_d,N}$ is not conjugate to G.

Lemma 5.1. *Take any squarefree integer d.*

(i) *We have $d \in \mathcal{D}_E$ if and only if the group $\rho_{E_d,N}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ to a proper subgroup of G.*

(ii) *If $d = d_{E,H}$ for some $H \in \mathcal{H}$, then $\rho_{E_d,N}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ to H.*

Proof. Take any group $H \in \mathcal{H}$. Composing $\rho_{E_d,N} \colon \mathrm{Gal}_{\mathbb{Q}} \to G$ with the quotient map $G \to G/H \cong \{\pm 1\}$ gives the character $\chi_d \cdot \chi_{E,H}$. Therefore, $\rho_{E_d,N}(\mathrm{Gal}_{\mathbb{Q}})$ is a subgroup of H (and hence equal to H) if and only if $\chi_{E,H} = \chi_d$; equivalently, $d = d_{E,H}$. Parts (i) and (ii) are now immediate. □

Since $|\mathcal{D}_E| = |\mathcal{H}|$, we deduce from Lemma 5.1 that the map

$$\mathcal{H} \to \mathcal{D}_E, \quad H \mapsto d_{E,H}$$

is a bijection.

Remark 5.2. Observe that $\rho_{E_d,N}(\mathrm{Gal}_{\mathbb{Q}})$ being conjugate to H in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ need not imply that $d = d_{E,H}$. For example, it is possibly for distinct groups in $\mathcal{H}$ to be conjugate in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

5.2. **Computing $\mathcal{D}_E$.** Now assume that $N \geq 3$ is odd; we shall explain how to compute $\mathcal{D}_E$ (we will later be interested in the case where N is an odd prime). Let M_E be set of squarefree integers that are divisible only by primes p such that $p|N$ or such that E has bad reduction at p.

For each $r \geq 1$, let $\mathcal{D}_r$ be the set of $d \in M_E$ such that

$$a_p(E) \not\equiv -2\left(\tfrac{d}{p}\right) \pmod{N} \tag{5.1}$$

holds for all primes $p \leq r$ for which E has good reduction and $p \equiv 1 \pmod{N}$.

Lemma 5.3. *Suppose that N is odd. We have $\mathcal{D}_E \subseteq \mathcal{D}_r$ with equality holding for all sufficiently large r.*

Proof. Define $\mathscr{D} := \cap_r \mathcal{D}_r$; it is the set of $d \in M_E$ such that (5.1) holds for all primes $p \equiv 1 \pmod N$ for which E has good reduction. We have $\mathcal{D}_r \subseteq \mathcal{D}_{r'}$ if $r \geq r'$, so it suffices to prove that $\mathscr{D} = \mathcal{D}_E$.

Take any $d \in \mathscr{D}$. We have $a_p(E_d) = \left(\frac{d}{p}\right) a_p(E) \not\equiv -2 \pmod N$ for all primes $p \equiv 1 \pmod N$ for which E has good reduction. By the Chebotarev density theorem, there are no elements $g \in \rho_{E_d,N}(\mathrm{Gal}_{\mathbb{Q}})$ satisfying $\det(g) = 1$ and $\mathrm{tr}(g) = -2$. In particular, the group $\rho_{E_d,N}(\mathrm{Gal}_{\mathbb{Q}})$ does not contain $-I$ and hence $d \in \mathcal{D}_E$ by Lemma 5.1(i). Therefore, $\mathscr{D} \subseteq \mathcal{D}_E$.

We have $\mathcal{D}_E \subseteq M_E$ since each character $\chi_{E,H}$ factors through $\rho_{E,N}$ (and is hence unramified at all primes $p \nmid N$ for which E has good reduction).

Now take any $d \in \mathcal{D}_E - \mathscr{D}$. There is thus a prime $p \equiv 1 \pmod N$ for which E has good reduction and $a_p(E_d) = \left(\frac{d}{p}\right) a_p(E) \equiv -2 \pmod N$. Define $g := \rho_{E_d,N}(\mathrm{Frob}_p)$; it has trace -2 and determinant 1. Since N is odd, some power of g is equal to $-I$. Therefore, $\rho_{E_d,N}(\mathrm{Gal}_{\mathbb{Q}}) = \pm\rho_{E_d,N}(\mathrm{Gal}_{\mathbb{Q}}) = G$ which contradicts that $d \in \mathcal{D}_E$. Therefore, $\mathcal{D}_E - \mathscr{D}$ is empty and hence $\mathcal{D}_E \subseteq \mathscr{D}$. □

One can compute the finite sets $\mathcal{D}_r$ for larger and larger values of r until $|\mathcal{D}_r| = |\mathcal{H}|$ and then $\mathcal{D}_E = \mathcal{D}_r$. This works since we always have an inclusion $\mathcal{D}_E \subseteq \mathcal{D}_r$ by Lemma 5.3, and equality holds when $|\mathcal{D}_r| = |\mathcal{H}|$ since $|\mathcal{D}_E| = |\mathcal{H}|$.

When N is a prime, the integers in $\mathcal{D}_E$ come in pairs.

Lemma 5.4. *Suppose $N = \ell$ is an odd prime. Let $\mathcal{D}'_E$ be the set of $d \in \mathcal{D}_E$ for which $\ell \nmid d$. Then*

$$\mathcal{D}_E = \bigcup_{d \in \mathcal{D}'_E} \{d, (-1)^{(\ell-1)/2}\ell \cdot d\}.$$

Proof. Define $\ell^* := (-1)^{(\ell-1)/2}\ell$. Take any $d \in \mathcal{D}_E$. We need to show that $d\ell^*$ or d/ℓ^* belong to $\mathcal{D}_E$ (whichever one is a squarefree integer). After possibly replacing E by E_d, we may assume that $d = 1$ and hence we need only verify that $\ell^* \in \mathcal{D}_E$.

So assume that $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is a proper subgroup of G and hence is equal to one of the $H \in \mathcal{H}$. We need to show that $\rho_{E',\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is also a proper subgroup of G, where $E' := E_{\ell^*}$.

The field $\mathbb{Q}(\sqrt{\ell^*}) \subseteq \mathbb{Q}(\zeta_\ell)$ is a subfield of both $\mathbb{Q}(E[\ell])$ and $\mathbb{Q}(E'[\ell])$. Since E and E' are isomorphic over $\mathbb{Q}(\sqrt{\ell^*})$, we deduce that $[\mathbb{Q}(E'[\ell]) : \mathbb{Q}] = [\mathbb{Q}(E[\ell]) : \mathbb{Q}]$. Therefore,

$$|\rho_{E',\ell}(\mathrm{Gal}_{\mathbb{Q}})| = [\mathbb{Q}(E'[\ell]) : \mathbb{Q}] = [\mathbb{Q}(E[\ell]) : \mathbb{Q}] = |\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})| = |H| = |G|/2.$$

By cardinality assumption, we deduce that $\rho_{E',\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to a proper subgroup of G. □

Remark 5.5. One could also use the methods of this section to help determine $\mathcal{H}$. For example, if $\mathcal{D}_r = \emptyset$ for some r, then $\mathcal{H} = \emptyset$. Suppose we are in the setting, like what happens often in the introduction, where we know that $|\mathcal{H}| \geq 2$ because we have two explicit elements of $\mathcal{H}$. Then to verify that $|\mathcal{H}| = 2$, one need only find an r such that $|\mathcal{D}_r| = 2$.

5.3. **Some examples.**

5.3.1. Take $\ell = 7$. Let $E/\mathbb{Q}$ be the elliptic curve defined by $y^2 = x^3 - 5^3 7^3 x - 5^4 7^2 106$; it has j-invariant $3^3 \cdot 5 \cdot 7^5/2^7$ and conductor $2 \cdot 5^2 \cdot 7^2$. From the part of Theorem 1.5 proved in §4.4, we know that $\pm\rho_{E,7}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to the group G_1 of §1.4. Let $\mathcal{H}$ be the set of proper subgroups H of G_1 such that $\pm H = G_1$. The set $\mathcal{H}$ consists of two groups; they are both conjugate in $\mathrm{GL}_2(\mathbb{F}_7)$ to the group $H_{1,1}$ of §1.4. The curve E is denoted by $\mathcal{E}_1$ in §1.4.

We have $\mathcal{D}_E \subseteq M_E = \{\pm 1, \pm 2, \pm 5, \pm 7, \pm 10, \pm 14, \pm 35, \pm 70\}$. The primes 211, 239 and 337 are congruent to 1 modulo ℓ. One can check that

$$a_{211}(E) = 16 \equiv 2 \pmod 7, \quad a_{239}(E) = -5 \equiv 2 \pmod 7, \quad a_{337}(E) = -5 \equiv 2 \pmod 7.$$

So if $d \in \mathcal{D}_{337}$, then $\left(\frac{d}{211}\right) = 1$, $\left(\frac{d}{239}\right) = 1$ and $\left(\frac{d}{337}\right) = 1$. Checking the $d \in M_E$, we find that $\mathcal{D}_{337} \subseteq \{1, -7\}$. Since $|\mathcal{H}| = 2$, we deduce that $\mathcal{D}_E = \{1, -7\}$.

Now let $E'/\mathbb{Q}$ be any elliptic curve with j-invariant $3^3 \cdot 5 \cdot 7^5/2^7$. Using Lemma 5.1, we deduce that $\rho_{E',7}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to G_1 if and only if E' is not isomorphic to E or its quadratic twist by -7. When $\rho_{E',7}(\mathrm{Gal}_{\mathbb{Q}})$ is not conjugate to G_1 it must be conjugate to $H_{1,1}$ in $\mathrm{GL}_2(\mathbb{F}_7)$.

5.3.2. Take $\ell = 11$. Let G_1, $H_{1,1}$ and $H_{1,2}$ be the groups from §1.5. The set $\mathcal{H}$ of proper subgroups H of G_1 for which $\pm H = G_1$ is equal to $\{H_{1,1}, H_{1,2}\}$.

Let $E/\mathbb{Q}$ be the elliptic curve defined by $y^2+xy+y = x^3+x^2-305x+7888$; it has j-invariant -11^2 and is isomorphic to the curve $\mathcal{E}_1$ of §1.5. In §4.5.4, we showed that $\rho_{E,11}(\mathrm{Gal}_{\mathbb{Q}})$ and $\pm\rho_{E,11}(\mathrm{Gal}_{\mathbb{Q}})$ are conjugate in $\mathrm{GL}_2(\mathbb{F}_{11})$ to $H_{1,1}$ and G_1, respectively.

Using Lemma 5.4 and $|\mathcal{D}_E| = |\mathcal{H}|$, we deduce that $\mathcal{D}_E = \{1, -11\}$. Lemma 5.1 implies that if $E'/\mathbb{Q}$ has j-invariant -11^2, then $\rho_{E',11}(\mathrm{Gal}_{\mathbb{Q}})$ is not conjugate to G_1 if and only if E' is isomorphic to E or its quadratic twist by -11. If E' is isomorphic to E or its twist by -11, then $\rho_{E',11}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_{11})$ to $H_{1,1}$ or $H_{1,2}$, respectively.

5.3.3. Take $\ell = 11$. Let G_2, $H_{2,1}$ and $H_{2,2}$ be the subgroups of $\mathrm{GL}_2(\mathbb{F}_{11})$ from §1.5. The set $\mathcal{H}$ of proper subgroups H of G_2 for which $\pm H = G_2$ is equal to $\{H_{2,1}, H_{2,2}\}$.

Let $E/\mathbb{Q}$ be the elliptic curve defined by $y^2 + xy = x^3 + x^2 - 3632x + 82757$; it has j-invariant $-11 \cdot 131^3$ and is isomorphic to the curve $\mathcal{E}_2$ of §1.5. In §4.5.4, we showed that $\rho_{E,11}(\mathrm{Gal}_{\mathbb{Q}})$ and $\pm\rho_{E,11}(\mathrm{Gal}_{\mathbb{Q}})$ are conjugate in $\mathrm{GL}_2(\mathbb{F}_{11})$ to $H_{2,1}$ and G_2, respectively.

Using Lemma 5.4 and $|\mathcal{D}_E| = |\mathcal{H}|$, we deduce that $\mathcal{D}_E = \{1, -11\}$. Lemma 5.1 implies that if $E'/\mathbb{Q}$ has j-invariant $-11 \cdot 131^3$, then $\rho_{E',11}(\mathrm{Gal}_{\mathbb{Q}})$ is not conjugate to G_2 if and only if E' is isomorphic to E or its quadratic twist by -11. If E' is isomorphic to E or its twist by -11, then $\rho_{E',11}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_{11})$ to $H_{2,1}$ or $H_{2,2}$, respectively.

6. Quadratic twists of families

In this section, we complete the proof of the theorems from §1.

6.1. **General setting.** Fix an integer $N \geq 3$ and an applicable subgroup G of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Let $\mathcal{H}$ be the set of proper subgroups H of G that satisfy $\pm H = G$.

Assume that the morphism $\pi_G \colon X_G \to \mathbb{P}^1_{\mathbb{Q}}$ arises from a rational function $J(t) \in \mathbb{Q}(t)$, i.e., the function field of X_G is of the form $\mathbb{Q}(h)$ where $j = J(h)$.

Let $g(t)$ be a rational function $\mathbb{Q}(t)$ such that

$$a(t) := -3g(t)^2J(t)/(J(t) - 1728) \quad \text{and} \quad b(t) := -2g(t)^3J(t)/(J(t) - 1728)$$

belong to $\mathbb{Z}[t]$, and for which there is no irreducible element π of the ring $\mathbb{Z}[t]$ such that π^2 divides a and π^3 divides b. After possibly changing g by a sign, we may assume that g is the quotient of two polynomials with positive leading coefficient; the function $g(t)$ is now uniquely determined. Define $\Delta := -16(4a^3 + 27b^2)$; it is a polynomial in $\mathbb{Z}[t]$ and equals $2^{12}3^6J(t)^2/(J(t) - 1728)^3g(t)^6$. Let $\mathscr{M}$ be the set of squarefree $f(t) \in \mathbb{Z}[t]$ which divide $N\Delta(t)$.

Take any $u \in \mathbb{Q}$ for which $J(u) \notin \{0, 1728, \infty\}$. We have $\Delta(u) \neq 0$ and hence $f(u) \neq 0$ for all $f \in \mathscr{M}$. Let $E_u/\mathbb{Q}$ be the elliptic curve defined by the Weierstrass equation $y^2 = x^3 + a(u)x + b(u)$; note that $\Delta(u) \neq 0$ since $J(u) \notin \{0, 1728, \infty\}$. One can readily check that the curve E_u has j-invariant $J(u)$. *Warning*: this is not to be confused with the quadratic twist notation we used in §5.

Proposition 6.1. *There is an injective map*

$$\mathcal{H} \to \mathscr{M}, \quad H \mapsto f_H$$

such that for any $u \in \mathbb{Q}$ with $J(u) \notin \{0, 1728, \infty\}$ and $\pm\rho_{E_u,N}(\mathrm{Gal}_{\mathbb{Q}})$ conjugate to G in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, the following hold:

(a) *If $E'/\mathbb{Q}$ is an elliptic curve with j-invariant $J(u)$, then $\rho_{E',N}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to G in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ if and only if E' is not isomorphic to the quadratic twist of E_u by $f_H(u)$ for all $H \in \mathcal{H}$.*

(b) *If $E'/\mathbb{Q}$ is isomorphic to the quadratic twist of E_u by $f(u)$ for some $H \in \mathcal{H}$, then $\rho_{E',N}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to H in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.*

The sets $\{f_H(u) : H \in \mathcal{H}\}$ and $\mathcal{D}_{E_u}$ represent the same cosets in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, with $\mathcal{D}_{E_u}$ defined as in §5.

Proof. Define the scheme $U := \operatorname{Spec} \mathbb{Z}[t, N^{-1}, \Delta(t)^{-1}]$. By taking the square root of a polynomial $f \in \mathscr{M}$, we obtain an étale extension of U of degree 1 or 2; we denote the corresponding quadratic character by $\chi_f \colon \pi_1(U) \to \{\pm 1\}$. Conversely, every (continuous) character $\pi_1(U) \to \{\pm 1\}$ is of the form χ_f for a unique $f \in \mathscr{M}$. (Note that 2 always divides $\Delta(t)$).

The Weierstrass equation

$$y^2 = x^3 + a(t)x + b(t)$$

defines a relative elliptic curve $E \to U$. Let $E[N]$ be the N-torsion subscheme of E. The morphism $E[N] \to U$ allows us to view $E[N]$ as a lisse sheaf of $\mathbb{Z}/N\mathbb{Z}$-modules on U that is free of rank 2. The sheaf $E[N]$ then gives rise to a representation

$$\rho_N \colon \pi_1(U) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

that is uniquely defined up to conjugacy (we will suppress the base point in our fundamental group since we are only interested in ρ_N up to conjugacy).

We now consider specializations of E. Take any $u \in U(\mathbb{Q})$, i.e., an element $u \in \mathbb{Q}$ with $\Delta(u) \neq 0$. One can show that elements $u \in U(\mathbb{Q})$ can also be described as those $u \in \mathbb{Q}$ for which $J(u) \notin \{0, 1728, \infty\}$. We can specialize E at u to obtain the elliptic curve that we have denoted $E_u/\mathbb{Q}$; it is defined by $y^2 = x^3 + a(u)x + b(u)$ and has j-invariant $J(u)$.

Let $\rho_{u,N} \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be the specialization of ρ_N at u; it is obtained by composing the homomorphism $u_* \colon \mathrm{Gal}_{\mathbb{Q}} \to \pi_1(U)$ coming from $u \in U(\mathbb{Q})$ with ρ_N. The homomorphism $\rho_{u,N}$ agrees, up to conjugacy, with the representation $\rho_{E_u,N}$ that describes the Galois action on the N-torsion points of E_u. So taking $\rho_{E_u,N} = \rho_{u,N}$, specialization gives an inclusion $\rho_{E_u,N}(\mathrm{Gal}_{\mathbb{Q}}) \subseteq \rho_N(\pi_1(U))$.

We claim that $\pm\rho_N(\pi_1(U))$ and G are conjugate in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. By Lemma 3.5, the group $\pm\rho_{E_u,N}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to G in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ for "most" $u \in \mathbb{Q}$. By Hilbert's irreducibility theorem, the group $\pm\rho_{E_u,N}(\mathrm{Gal}_{\mathbb{Q}})$ equals $\pm\rho_N(\pi_1(U))$ for "most" $u \in \mathbb{Q}$. This proves the claim.

We may thus assume that $G = \pm\rho_N(\pi_1(U))$ and hence we have a representation $\rho_N \colon \pi_1(U) \to G$. Specializations thus give inclusions $\rho_{E_u,N}(\mathrm{Gal}_{\mathbb{Q}}) \subseteq G$. Take any $H \in \mathcal{H}$ and let $\chi_H \colon \pi_1(U) \to \{\pm 1\}$ be the character obtained by composing ρ_N with the quotient map $G \to G/H \cong \{\pm 1\}$. We thus have $\chi_H = \chi_{f_H}$ for a unique polynomial $f_H \in \mathscr{M}$.

Specializing χ_H at u, we obtain the character $\chi_{E_u,H} \colon \mathrm{Gal}_{\mathbb{Q}} \to \{\pm 1\}$ from §5. With notation as in §5, we find that the integer $d_{E_u,H}$ lies in the same class in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ as $f_H(u)$. Therefore, the classes of $\mathcal{D}_{E_u}$ in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ are represented by the set $\{f_H(u) : H \in \mathcal{H}\}$. Parts (a) and (b) are now immediate consequences of Lemma 5.1. □

We claim that the set of polynomials

$$\mathscr{F} := \{f_H : H \in \mathcal{H}\}$$

is uniquely determined and has cardinality $|\mathcal{H}|$. By Hilbert irreducibility, one can chose $u \in U(\mathbb{Q})$ such that $\pm\rho_{E_u,N}(\mathrm{Gal}_{\mathbb{Q}}) = G$ and such that the map $\mathscr{M} \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, $f \mapsto f(u)\cdot(\mathbb{Q}^\times)^2$ is injective. The uniqueness of $\mathscr{F}$ then follows from part (a) of Proposition 6.1.

6.2. **Computing $\mathscr{F}$.** We now focus on the case where N is a prime $\ell \in \{3, 5, 7, 13\}$. Fix notation as in the subsection of §1 for the given ℓ.

Let G be one of the subgroups G_i of $\mathrm{GL}_2(\mathbb{F}_\ell)$ in §1 for which there is a corresponding rational function $J(t) := J_i(t) \in \mathbb{Q}(t) - \mathbb{Q}$. The group G is applicable and in particular contains $-I$.

We take notation as in §6.1. In particular, $\mathcal{H}$ is the set of proper subgroups H of G such that $\pm H = G$. We shall assume that $\mathcal{H} \neq \emptyset$ (otherwise $\mathscr{F} = \emptyset$); this holds when

$$(\ell, i) \in \big\{(3,1),(3,3),(5,1),(5,5),(5,6),(7,1),(7,3),(7,4),(7,5),(7,7),(13,4),(13,5)\big\}.$$

In each of these cases, one can check that $|\mathcal{H}| = 2$.

We now explain how to compute the set $\mathscr{F} = \{f_H : H \in \mathcal{H}\}$; it has cardinality $|\mathcal{H}| = 2$. Take any $u \in \mathbb{Q}$ with $J(u) \notin \{0, 1728, \infty\}$ such that $J(u) \notin J_j(\mathbb{Q})$ for all $j < i$. From the parts of the main theorems proved in §4, this implies that $\pm\rho_{E_u,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to G. Let $\mathcal{D}_{E_u}$ be the (computable!) set from §5. From Proposition 6.1, we find that

$$\mathscr{F} \subseteq \{f \in \mathscr{M} : f(u) \in d(\mathbb{Q}^\times)^2 \text{ for some } d \in \mathcal{D}_{E_u}\}. \tag{6.1}$$

By considering (6.1) with many such $u \in \mathbb{Q}$, one is eventually left with only $|\mathcal{H}|$ candidates $f \in \mathscr{F}$ to be of the form f_H; this then produces the set $\{f_H : H \in \mathcal{H}\}$ of order $|\mathcal{H}|$ (for our examples, one only needs to check $u \in \{1, 2, 3, 4\}$). One could also work with a single $u \in \mathbb{Q}$ chosen so that the map $\mathscr{F} \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, $f \mapsto f(u) \cdot (\mathbb{Q}^\times)^2$ is injective. This method thus produces $\mathscr{F}$.

Doing the above computations, we find that

$$\{f_H : H \in \mathcal{H}\} = \{f_1, \ell^* f_1\}$$

for a unique polynomial $f_1 \in \mathscr{F}$, where $\ell^* := (-1)^{(\ell-1)/2} \cdot \ell$; this can also be deduced from $|\mathcal{H}| = 2$ and Lemma 5.4. We thus have $f_1 = f_{M_1}$ and $\ell^* f_1 = f_{M_2}$, where $\mathcal{H} = \{M_1, M_2\}$.

Let h be the largest element of $\mathbb{Z}[t]$, in terms of divisibility, with positive leading coefficient such that h^4 divides af_1^2 and h^6 divides bf_1^3; define $A := (af_1^2)/h^4$ and $B := (bf_1^3)/h^6$ in $\mathbb{Z}[t]$. The Weierstrass equation

$$y^2 = x^3 + A(t)x + B(t)$$

is precisely the equation given for $\mathcal{E}_{i,t}$ in the subsection of §1 corresponding to the prime ℓ. (For code verifying these claims, see the link given in §1.10.)

For $u \in \mathbb{Q}$ with $J(u) \notin \{0, 1728, \infty\}$, let $\mathcal{E}_{i,u}$ be the elliptic curve over $\mathbb{Q}$ defined by setting t equal to u. Let $E'/\mathbb{Q}$ be any elliptic curve with $j_{E'} \notin \{0, 1728\}$ for which $\pm\rho_{E',\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to G in $\mathrm{GL}_2(\mathbb{F}_\ell)$. From the parts of the main theorems proved in §4, we have $j_{E'} = J(u)$ for some $u \in \mathbb{Q}$. The curve $E_u/\mathbb{Q}$ also has j-invariant $J(u)$. The twist of E_u by $f_1(u)$ is isomorphic to the the curve $\mathcal{E}_{i,u}/\mathbb{Q}$. By Proposition 6.1, we deduce that $\rho_{E',\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to G if and only if E' is not isomorphic to $\mathcal{E}_{i,u}$ and not isomorphic to the quadratic twist of $\mathcal{E}_{i,u}$ by ℓ^*. By Proposition 6.1, $\rho_{E',\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to M_1 or M_2 when E' is isomorphic to $\mathcal{E}_{i,u}$ or the quadratic twist of $\mathcal{E}_{i,u}$ by ℓ^*, respectively.

It thus remains to determine M_1 and M_2.

If $(\ell, i) \in \{(3,1),(7,1)\}$, then M_1 and M_2 are both conjugate to $H_{i,1}$ since the two groups in $\mathcal{H}$ are conjugate in $\mathrm{GL}_2(\mathbb{F}_\ell)$. We shall now assume that $(\ell, i) \notin \{(3,1),(7,1)\}$. We then have

$\mathcal{H} = \{H_{i,1}, H_{i,2}\}$. It thus remains to prove that $M_1 = H_{i,1}$ (and hence $M_2 = H_{i,2}$).

Suppose that $(\ell, i) \in \big\{(5,1),(5,5),(5,6),(7,3),(7,4),(13,4),(13,5)\big\}$. Take u, p and a as in Table 2 below for the pair (ℓ, i).

(ℓ, i)	$(5,1)$	$(5,5)$	$(5,6)$	$(7,3)$	$(7,4)$	$(13,4)$	$(13,5)$
u	1	2	1	2	2	1	1
p	2	3	2	3	3	2	2
a	-2	-1	-2	-3	-3	2	2

TABLE 2.

The element $u \in \mathbb{Q}$ is chosen so that $J_i(u) \notin \{0, 1728, \infty\}$ and such that $J_i(u) \notin J_j(\mathbb{Q} \cup \{\infty\})$ for all $j < i$. Define the elliptic curve $E := \mathcal{E}_{i,u}/\mathbb{Q}$. By our choice of u, the group $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_\ell)$ to M_1.

The curve has good reduction at the prime p and we have $a = a_p(E)$. Let t_p be the image of (a,p) in $\mathbb{F}_\ell^2$; it equals $(\mathrm{tr}(A), \det(A))$ with $A := \rho_{E,\ell}(\mathrm{Frob}_p) \in M_1$. A direct computation shows that $t_p \notin \{(\mathrm{tr}(A), \det(A)) : A \in H_{i,2}\}$. Therefore, M_1 is not conjugate to $H_{i,2}$. So M_1 must be conjugate to $H_{i,1}$ and hence M_2 is conjugate to $H_{i,2}$.

Finally, consider the remaining pairs $(\ell, i) \in \{(3,3),(7,5),(7,7)\}$.

Consider $(\ell, i) = (3,3)$. The pair $(3(u+1)^2, 4u(u+1)^2)$ is a point of order 3 of $\mathcal{E}_{3,u}$ for all u. This implies that M_1 is conjugate in $\mathrm{GL}_2(\mathbb{F}_3)$ to a subgroup of $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$. So $M_1 \neq H_{i,2}$ and hence $M_1 = H_{i,1}$.

We may now suppose that $\ell = 7$ and $i \in \{5, 7\}$.

Take $i = 5$. Let $E'/\mathbb{Q}$ be the elliptic curve defined by $y^2 = x^3 - 2835(-7)^2 x - 71442(-7)^3$; it is the quadratic twist of $\mathcal{E}_{5,0}$ by -7. Using Theorem 1.5(ii), which we proved in §4, we find that $\pm\rho_{E',7}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to G_5. The group $\rho_{E',7}(\mathrm{Gal}_{\mathbb{Q}})$ is thus conjugate to M_2. So to prove that $M_2 = H_{i,2}$, and hence $M_1 = H_{i,1}$, we need only verify that E' has a 7-torsion point defined over some cubic field. Let $w \in \overline{\mathbb{Q}}$ be a root of the irreducible polynomial $x^3 - 441x^2 - 83349x + 22754277$. The pair $(w, 21w - 1323)$ is a point of order 7 on E'.

Finally, take $i = 7$. Let $E'/\mathbb{Q}$ be the elliptic curve defined by $y^2 = x^3 - 17870609043(-7)^2 x - 919511455160466(-7)^3$; it is the quadratic twist of $\mathcal{E}_{7,1}$ by -7. Using Theorem 1.5(ii), which we proved in §4, we find that $\pm\rho_{E',7}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to G_7. The group $\rho_{E',7}(\mathrm{Gal}_{\mathbb{Q}})$ is thus conjugate to M_2. So to prove that $M_2 = H_{i,2}$, and hence $M_1 = H_{i,1}$, we need only verify that E' has a 7-torsion point defined over some cubic field. Let $w \in \overline{\mathbb{Q}}$ be a root of the irreducible polynomial $x^3 - 1750329x^2 + 1015924207851x - 195667237639563291$. The pair $(w, 1323w - 714884373)$ is a point of order 7 on E'.

7. Proof of Propositions from §1.9

Let E be an elliptic curve defined over $\mathbb{Q}$ that has complex multiplication. Let R be the ring of endomorphisms of $E_{\overline{\mathbb{Q}}}$. Let $k \subseteq \overline{\mathbb{Q}}$ be the minimal extension of $\mathbb{Q}$ over which all the endomorphisms of $E_{\overline{\mathbb{Q}}}$ are defined; it is an imaginary quadratic field. Moreover, we can identify k with $R \otimes_{\mathbb{Z}} \mathbb{Q}$ (the action of R on the Lie algebra of E_k gives a ring homomorphism $R \to k$ that extends to an isomorphism $R \otimes_{\mathbb{Z}} \mathbb{Q} \to k$). The field k has discriminant $-D$.

Take any *odd* prime ℓ. For each integer $n \geq 1$, let $E[\ell^n]$ be the ℓ^n-torsion subgroup of $E(\overline{\mathbb{Q}})$. The ℓ-adic Tate module $T_\ell(E)$ of E is the inverse limit of the groups $E[\ell^n]$ with multiplication by ℓ giving transition maps $E[\ell^{n+1}] \to E[\ell]$; it is a free $\mathbb{Z}_\ell$-module of rank 2. The natural Galois action

on $T_\ell(E)$ can be expressed in terms of a representation

$$\rho_{E,\ell^\infty}\colon \mathrm{Gal}_k \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(E)).$$

The ring R acts on each of the $E[\ell^n]$ and this induces a faithful action of R on $T_\ell(E)$.

The Tate module $T_\ell(E)$ is actually a free module over $R_\ell := R \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ of rank 1 (see the remarks at the end of §4 of [ST68]). We can thus make an identification $\mathrm{Aut}_{R_\ell}(T_\ell(E)) = R_\ell^\times$. The actions of $\mathrm{Gal}_k = \mathrm{Gal}(\overline{\mathbb{Q}}/k)$ and R_ℓ on $T_\ell(E)$ commute, so the restriction of ρ_{E,ℓ^∞} to Gal_k gives a representation

$$\mathrm{Gal}_k \to \mathrm{Aut}_{R_\ell}(T_\ell(E)) = R_\ell^\times.$$

Lemma 7.1.

(i) *If E has good reduction at ℓ, then $\rho_{E,\ell^\infty}(\mathrm{Gal}_k) = R_\ell^\times$.*

(ii) *If $j_E \neq 0$, then $\rho_{E,\ell^\infty}(\mathrm{Gal}_k)$ is an open subgroup of $R_\ell^\times$ whose index is a power of 2.*

Proof. Since $R_\ell^\times$ is commutative, we can factor $\rho_{E,\ell^\infty}|_{\mathrm{Gal}_k}$ through the maximal abelian quotient of Gal_k. Composing with the reciprocity map of class field theory, we obtain a continuous representation $\varrho_{E,\ell^\infty}\colon \mathbb{A}_k^\times \to R_\ell^\times$, where $\mathbb{A}_k^\times$ is the group of ideles of k. Define $k_\ell := k \otimes_{\mathbb{Z}} \mathbb{Q}_\ell = \prod_{v|\ell} k_v$, where the product is over the places v of k lying over ℓ and k_v is the completion of k at v. For an idele $a \in \mathbb{A}_k^\times$, let a_ℓ be the component of a in $k_\ell^\times$. From [ST68, Theorems 10 & 11], there is a unique homomorphism $\varepsilon\colon \mathbb{A}_k^\times \to k^\times$ such that $\varrho_{E,\ell^\infty}(a) = \varepsilon(a)a_\ell^{-1}$ for $a \in \mathbb{A}_k^\times$. The homomorphism ε satisfies $\varepsilon(x) = x$ for all $x \in k^\times$ and its kernel is open in $\mathbb{A}_k^\times$. We identify $R_\ell^\times = \prod_{v|\ell} \mathcal{O}_v^\times$, where $\mathcal{O}_v$ is the valuation ring of k_v, with a subgroup of $\mathbb{A}_k^\times$ (by letting the coordinates at the places $v \nmid \ell$ of k be 1). Let B be the kernel of $\varepsilon|_{R_\ell^\times}$.

First suppose that E has good reduction at ℓ, and hence at all places $v|\ell$ of k. By the first corollary of Theorem 11 in [ST68], we deduce that that ε is unramified at all $v|\ell$. Therefore, $B = R_\ell^\times$ and hence $\varrho_{E,\ell^\infty}(R_\ell^\times) = R_\ell^\times$. Therefore, $\rho_{E,\ell^\infty}(\mathrm{Gal}_k)$ contains, and hence is equal to, $R_\ell^\times$.

Now suppose that $j_E \neq 0$. Since ℓ is odd and $j_E \neq 0$, the subgroup of $R[\ell^{-1}]^\times$ consisting of roots of unity has order 2 or 4. By Theorem 11(ii) and Theorem 6(b) in [ST68], we find that B is an open subgroup of $R_\ell^\times$ with index a power of 2. So $\varrho_{E,\ell^\infty}(B) = B$ and hence $\rho_{E,\ell^\infty}(\mathrm{Gal}_k) \supseteq B$. Therefore, $\rho_{E,\ell^\infty}(\mathrm{Gal}_k)$ is an open subgroup of $R_\ell^\times$ whose index is a power of 2. □

The following gives constraints on the elements of $\rho_{E,\ell^\infty}(\mathrm{Gal}_\mathbb{Q} - \mathrm{Gal}_k)$. Since R is a quadratic order, there is an element $\beta \in R - \mathbb{Z}$ such that $\beta^2 \in \mathbb{Z}$; note that β is not defined over $\mathbb{Q}$. We can view β as an endomorphism of $T_\ell(E)$.

Lemma 7.2. *For any $\sigma \in \mathrm{Gal}_\mathbb{Q} - \mathrm{Gal}_k$, we have $\rho_{E,\ell^\infty}(\sigma)\beta = -\beta\rho_{E,\ell^\infty}(\sigma)$ and $\mathrm{tr}(\rho_{E,\ell^\infty}(\sigma)) = 0$.*

Proof. Take any $\sigma \in \mathrm{Gal}_\mathbb{Q} - \mathrm{Gal}_k$. The group $\mathrm{Gal}_\mathbb{Q}$ acts on R and we have $\sigma(\beta) = -\beta$ since $\beta^2 \in \mathbb{Z}$ and β is not defined over $\mathbb{Q}$ (but is defined over k). So for each $P \in E[\ell^n]$, we have $\sigma(\beta(P)) = \sigma(\beta)(\sigma(P)) = -\beta(\sigma(P))$. Taking an inverse limit, we deduce that $\rho_{E,\ell^\infty}(\sigma)\beta = -\beta\rho_{E,\ell^\infty}(\sigma)$. In $\mathrm{Aut}_{\mathbb{Q}_\ell}(T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell) \cong \mathrm{GL}_2(\mathbb{Q}_\ell)$, we have $\rho_{E,\ell^\infty}(\sigma) = -\beta\rho_{E,\ell^\infty}(\sigma)\beta^{-1}$. Taking traces we deduce that $\mathrm{tr}(\rho_{E,\ell^\infty}(\sigma)) = -\mathrm{tr}(\rho_{E,\ell^\infty}(\sigma))$ and hence $\mathrm{tr}(\rho_{E,\ell^\infty}(\sigma)) = 0$. □

Lemma 7.3. *Suppose that $\ell \nmid D$ and that E has good reduction at ℓ.*

(i) *If ℓ splits in k, then $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_\ell)$ to $N_s(\ell)$.*

(ii) *If ℓ is inert in k, then $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_\ell)$ to $N_{ns}(\ell)$.*

Proof. Lemma 7.1 implies that the group $C := \rho_{E,\ell}(\mathrm{Gal}_k)$ is isomorphic to $(R/\ell R)^\times$. The ring $R/\ell R$ is isomorphic to $\mathbb{F}_\ell \times \mathbb{F}_\ell$ or $\mathbb{F}_{\ell^2}$ when ℓ splits or is inert in k, respectively. Therefore, C is a Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$; it is split if and only if ℓ splits in k. Let N be the normalizer of C in $\mathrm{GL}_2(\mathbb{F}_\ell)$. The group $C = \rho_{E,\ell}(\mathrm{Gal}_k)$ is normal in $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ since $k/\mathbb{Q}$ is a Galois extension, so $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q}) \subseteq N$.

It remains to show that $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}}) = N$. Suppose that $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}}) \neq N$, and hence $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}}) = C = \rho_{E,\ell}(\mathrm{Gal}_k)$. This implies that the actions of $\mathrm{Gal}_{\mathbb{Q}}$ and R on $E[\ell]$ commute. However, this contradicts Lemma 7.2 which implies that the actions of $\sigma \in \mathrm{Gal}_{\mathbb{Q}} - \mathrm{Gal}_k$ and β on $E[\ell]$ anti-commute. Therefore, $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}}) = N$. □

We now describe the commutator subgroup of the normalizer N of a Cartan subgroup C of $\mathrm{GL}_2(\mathbb{F}_\ell)$. Let $\varepsilon\colon N \to N/C \cong \{\pm 1\}$ be the quotient map, and define the homomorphism

$$\varphi\colon N \to \{\pm 1\} \times \mathbb{F}_\ell^\times, \quad A \mapsto (\varepsilon(A), \det(A));$$

it is surjective.

Lemma 7.4.

(i) *The commutator subgroup of N is $\ker\varphi$, i.e., the subgroup of C consisting of matrices with determinant 1.*

(ii) *If H is a subgroup of N satisfying $\pm H = N$, then $H = N$.*

Proof. The kernel of φ contains the commutator subgroup of N since the image of φ is abelian. It suffices to show that every element in $\ker\varphi$ is a commutator. If N is conjugate to $N_s(\ell)$, this is immediate since $\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)\left(\begin{smallmatrix}1&0\\0&a\end{smallmatrix}\right)\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)^{-1}\left(\begin{smallmatrix}1&0\\0&a\end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix}a&0\\0&a^{-1}\end{smallmatrix}\right)$.

We now consider the non-split case. We may take $C = C(\ell)$, $N = N(\ell)$ and with the explicit $\epsilon \in \mathbb{F}_\ell^\times$ as given in the notation section of §1. Fix $\beta \in \mathbb{F}_{\ell^2}$ for which $\beta^2 = \epsilon$. The map $C(\ell) \to \mathbb{F}_{\ell^2}^\times$, $\left(\begin{smallmatrix}a&b\epsilon\\b&a\end{smallmatrix}\right) \to a + b\beta$ is a group isomorphism. Fix any $B \in N(\ell) - C(\ell)$. One can check that the map

$$C(\ell) \to C(\ell), \quad A \mapsto BAB^{-1}A^{-1} \tag{7.1}$$

corresponds to the homomorphism $\mathbb{F}_{\ell^2}^\times \to \mathbb{F}_{\ell^2}^\times$, $\alpha \mapsto \alpha^{\ell-1}$. In particular, the image of the map (7.1) is the unique (cyclic) subgroup of $C(\ell)$ of order $\ell + 1$; these are the matrices in $C(\ell)$ with determinant 1. This completes the proof of (i).

Finally, let H be a subgroup of N satisfying $\pm H = N$. The group H is normal in N and N/H is abelian, so H contains the commutator subgroup of N. From (i), the commutator subgroup of N, and hence H, contains $-I$. Therefore, $H = \pm H = N$. □

7.1. **Proof of Proposition 1.14(i) and (ii).** Let $E/\mathbb{Q}$ be an CM elliptic curve with $j_E \neq 0$. The curve E is thus a twist of one of the curves $E_{D,f}/\mathbb{Q}$ from Table 1. Take any odd prime $\ell \nmid D$. The curve $E_{D,f}$ has good reduction at ℓ. By Lemma 7.3, the group $\rho_{E_{D,f},\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is the normalizer N of a Cartan subgroup C of $\mathrm{GL}_2(\mathbb{F}_\ell)$. Also the Cartan subgroup C is split or non-split if ℓ is split or inert, respectively, in k.

First suppose that $j_E \neq 1728$. Since $j_E \notin \{0, 1728\}$, the curve E is a quadratic twist of $E_{D,f}$. As noted in the introduction, this implies that $\pm\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ and $\pm\rho_{E_{D,f},\ell}(\mathrm{Gal}_{\mathbb{Q}}) = N$ are conjugate in $\mathrm{GL}_2(\mathbb{F}_\ell)$. After first conjugating $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$, we may assume that $N = \pm\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$. By Lemma 7.4, we have $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}}) = N$.

Now suppose that $j_E = 1728$. Let μ_4 be the group of 4-th roots of unity in R. The elliptic curve $E/\mathbb{Q}$ can be defined by an equation of the form $y^2 = x^3 + dx$ for some non-zero integer d, i.e., E is a quartic twist of $E_{4,1}$. There is thus a character $\alpha\colon \mathrm{Gal}_k \to \mu_4 \subseteq R^\times$ such that the representations ρ_{E,ℓ^∞} and $\alpha \cdot \rho_{E_{4,1},\ell^\infty}\colon \mathrm{Gal}_k \to R_\ell^\times$ are equal. We have $\rho_{E_{4,1},\ell^\infty}(\mathrm{Gal}_k) = R_\ell^\times$ by Lemma 7.1(i), so the image of $\rho_{E,\ell^\infty}(\mathrm{Gal}_k)$ in $R_\ell^\times/\{\pm 1\}$ has index 1 or 2. Therefore, the image of $\rho_{E,\ell}(\mathrm{Gal}_k)$ in $C/\{\pm I\}$ has index 1 or 2. We have $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}}) \not\subseteq C$ since otherwise the actions of $\mathrm{Gal}_{\mathbb{Q}}$ and R on $E[\ell]$ would commute (which is impossible by Lemma 7.2). Therefore, the image of $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ in $N/\{\pm I\}$ is an index 1 or 2 subgroup.

The group $G := \pm\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ thus has index 1 or 2 in N. Since $\rho_{E,\ell}(\mathrm{Gal}_k) \subseteq C$ and $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}}) \not\subseteq C$, the quadratic character $\varepsilon \circ \rho_{E,\ell}\colon \mathrm{Gal}_{\mathbb{Q}} \to \{\pm 1\}$ corresponds to the extension $k = \mathbb{Q}(i)$ of $\mathbb{Q}$. The homomorphism $\det \circ \rho_{E,\ell}\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathbb{F}_\ell^\times$ is surjective and factors through $\mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q})$. We have

$\mathbb{Q}(i)\cap\mathbb{Q}(\zeta_\ell)=\mathbb{Q}$ since ℓ is odd, so $\varphi(\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q}))=\{\pm1\}\times\mathbb{F}_\ell^\times$ and hence $\varphi(G)=\{\pm1\}\times\mathbb{F}_\ell^\times$. Since $[N:G]\le 2$, the group G is normal in N with abelian quotient N/G. In particular, G contains the commutator subgroup of N. By Lemma 7.4, we deduce that G contains the kernel of φ. Since G contains the kernel of φ and $\varphi(G)=\{\pm1\}\times\mathbb{F}_\ell^\times$, we have $G=N$. By Lemma 7.4, we conclude that $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})=N$.

7.2. **Proof of Proposition 1.14(iii).** We first consider the elliptic curve $E=E_{D,f}$ over $\mathbb{Q}$ from Table 1 with $D=\ell$, where ℓ is an odd prime and $j_E\neq 0$. We have $k=\mathbb{Q}(\sqrt{-\ell})$.

Lemma 7.5. *The group $\pm\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ is conjugate to G.*

Proof. Let $\overline{\beta}$ be the image of $f\sqrt{-D}$ in $R/\ell R$. Since ℓ is odd, the $\mathbb{F}_\ell$-module $R/\ell R$ has basis $\{\overline{\beta},1\}$ and $\overline{\beta}^2=0$. Using this basis, we find that $R/\ell R$ is isomorphic to the subring $A:=\mathbb{F}_\ell\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right)\oplus\mathbb{F}_\ell\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$ of $M_2(\mathbb{F}_\ell)$. Using that $\rho_{E,\ell^\infty}(\mathrm{Gal}_k)\subseteq R_\ell^\times$, we deduce that $\rho_{E,\ell}(\mathrm{Gal}_k)$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_\ell)$ to a subgroup of $A^\times$. We may thus assume that

$$\rho_{E,\ell}(\mathrm{Gal}_k)\subseteq A^\times=\left\{\left(\begin{smallmatrix}a&b\\0&a\end{smallmatrix}\right):a\in\mathbb{F}_\ell^\times,b\in\mathbb{F}_\ell\right\}.$$

By Lemma 7.1(ii), we deduce that $[A^\times:\rho_{E,\ell}(\mathrm{Gal}_k)]$ is a power of 2 and hence $\rho_{E,\ell}(\mathrm{Gal}_k)$ contains the order ℓ group $\langle\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\rangle$. The order of $\rho_{E,\ell}(\mathrm{Gal}_k)$ is divisible by $(\ell-1)/2$ since $\det(\rho_{E,\ell}(\mathrm{Gal}_k))=(\mathbb{F}_\ell^\times)^2$, so $\rho_{E,\ell}(\mathrm{Gal}_k)$ contains $\left\{\left(\begin{smallmatrix}a&b\\0&a\end{smallmatrix}\right):a\in(\mathbb{F}_\ell^\times)^2,b\in\mathbb{F}_\ell\right\}$. Therefore, $\pm\rho_{E,\ell}(\mathrm{Gal}_k)=A^\times$ since -1 is not a square in $\mathbb{F}_\ell$ (we have $\ell\equiv 3 \pmod 4$).

Fix any $\sigma\in\mathrm{Gal}_\mathbb{Q}-\mathrm{Gal}_k$. The matrix $g=\rho_{E,\ell}(\sigma)$ is upper triangular since the Borel subgroup $B(\ell)$ is the normalizer of $A^\times=\pm\rho_{E,\ell}(\mathrm{Gal}_k)$ in $\mathrm{GL}_2(\mathbb{F}_\ell)$. We have $\mathrm{tr}(g)=0$ by Lemma 7.2, so $g=\left(\begin{smallmatrix}a&b\\0&-a\end{smallmatrix}\right)$ for some $a\in\mathbb{F}_\ell^\times$ and $b\in\mathbb{F}_\ell$. The group $\pm\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ is generated by g and $A^\times$ and is thus G. □

The subgroups H of G that satisfy $\pm H=G$ are H_1, H_2 and G.

Lemma 7.6. *The groups $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ and H_1 are conjugate in $\mathrm{GL}_2(\mathbb{F}_\ell)$.*

Proof. By Lemma 7.5, we may assume that $\pm\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})=G$. There are thus unique characters $\psi_1,\psi_2\colon\mathrm{Gal}_\mathbb{Q}\to\mathbb{F}_\ell^\times$ such that $\rho_{E,\ell}=\left(\begin{smallmatrix}\psi_1&*\\0&\psi_2\end{smallmatrix}\right)$. Let $f\in\mathbb{Q}[x]$ be the ℓ-th division polynomial of $E/\mathbb{Q}$; it is a polynomial of degree $(\ell^2-1)/2$ whose roots in $\overline{\mathbb{Q}}$ are the x-coordinates of the non-zero points in $E[\ell]$. Since $\pm\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})=G$, we find that $f=f_1f_2$ where the polynomials $f_1,f_2\in\mathbb{Q}[x]$ are irreducible, and f_1 has degree $(\ell-1)/2$. We may take f_1 so that it is monic. Take any root $a\in\overline{\mathbb{Q}}$ of f_1 and choose a point $P=(a,b)$ in $E[\ell]$. We have $\sigma(P)=\psi_1(\sigma)P$ for all $\sigma\in\mathrm{Gal}_\mathbb{Q}$. Therefore, $\mathbb{Q}(a,b)$ is the fixed field in $\overline{\mathbb{Q}}$ of $\ker\psi_1$.

Suppose that $\ell=3$. The point $(3,-2)$ of $E_{3,2}$ has order 3. The point $(12,-4)$ of $E_{3,3}$ has order 3. Therefore, $\mathbb{Q}(a,b)=\mathbb{Q}$.

Suppose that $\ell=7$. For the curve $E_{7,1}$ we have computed that $f_1=x^3-441x^2+59339x-2523451$. If $a\in\overline{\mathbb{Q}}$ is a root of f_1, then one can check that $(a,-7a+49)$ belongs to E. For the curve $E_{7,2}$ we have computed that $f_1=x^3-49x^2-1029x+31213$. If $a\in\overline{\mathbb{Q}}$ is a root of f_1, then one can check that $(a,21a-2107)$ belongs to E. In both cases, we have $[\mathbb{Q}(a,b):\mathbb{Q}]=3$.

Suppose that $\ell>7$. Dieulefait, González-Jiménez and Jiménez-Urroz have computed $\mathbb{Q}(a,b)$ and found it to be equal to the maximal totally real subfield $\mathbb{Q}(\zeta_\ell)^+$ of $\mathbb{Q}(\zeta_\ell)$, cf. Lemma 4 of [DGJJU11]. They also give a link to files containing an explicit polynomial f_1. In particular, $[\mathbb{Q}(a,b):\mathbb{Q}]=(\ell-1)/2$. (However, note that the conclusions on the image of $\rho_{E,\ell}$ in Proposition 9 of [DGJJU11] are not correct.)

In all cases, the image of ψ_1 has order $[\mathbb{Q}(a,b):\mathbb{Q}]=(\ell-1)/2$, so the group $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ cannot be G or H_2. Therefore, $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})=H_1$. □

Take any elliptic curve $E'/\mathbb{Q}$ with the same j-invariant as $E = E_{D,f}$; it is a quadratic twist. Now take $\mathcal{D}_E$ as in §5. Since $\#\mathcal{D}_E = \#\{H_1, H_2\} = 2$, we deduce from Lemma 5.4 (and $\ell \equiv 3 \pmod 4$) that $\mathcal{D}_E = \{1, -\ell\}$.

Since $\mathcal{D}_E = \{1, -\ell\}$, we deduce from Lemma 7.6 that if $E'/\mathbb{Q}$ is not isomorphic to E or its quadratic twist by $-\ell$, then $\rho_{E',\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to $\pm\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}}) = \pm H_1 = G$. If E' is isomorphic to E or its quadratic twist by $-\ell$, then $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to H_1 or H_2, respectively.

7.3. **Proof of Proposition 1.15.** If $E/\mathbb{Q}$ is given by $y^2 = f(x)$ with $f(x) \in \mathbb{Q}[x]$ a separable cubic, then $\rho_{E,2}(\mathrm{Gal}_{\mathbb{Q}})$ is isomorphic to the groups $\mathrm{Gal}(f)$, i.e., the Galois group of the splitting field of f over $\mathbb{Q}$. Observe that $\mathrm{GL}_2(\mathbb{F}_2) \cong \mathfrak{S}_3$. It thus suffices to compute $\mathrm{Gal}(f)$ since the cardinality of a subgroup of $\mathfrak{S}_3$ determines it up to conjugacy.

For the $j_E = 1728$ case, we have $f(x) = x^3 - dx = x(x^2 - d)$. We have $\mathrm{Gal}(f) = \mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$ which has order 1 or 2 when d is a square or non-square, respectively.

For the $j_E = 0$ case, we have $f(x) = x^3 + d$. We have $\mathrm{Gal}(f) = \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{d}, \zeta_3)/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{d}, \sqrt{-3})$ which has order 2 or 6 when d is a cube or non-cube, respectively.

For $j_E \notin \{0, 1728\}$, the group $\rho_{E,2}(\mathrm{Gal}_{\mathbb{Q}})$ does not change if we replace E by a quadratic twist (since $-I \equiv I \pmod \ell$), so one need only consider the specific curve $E = E_{D,f}$. Using the $f(x)$ of Table 1, one can check that $\mathrm{Gal}(f)$ has order 2 for the j-invariants listed in (i) and otherwise has order 6.

Proposition 1.15 is now a direct consequence of the above computations.

7.4. **Proof of Proposition 1.16.** Take any prime $\ell \geq 5$; we will deal with $\ell = 3$ in §7.4.1. We first consider an elliptic curve $E_d/\mathbb{Q}$ defined by the equation

$$y^2 = x^3 + 16d^2$$

for a fixed *cube-free* integer $d \geq 1$. We have $R = \mathbb{Z}[\omega]$ and $k = \mathbb{Q}(\omega)$, where $\omega := (-1 + \sqrt{-3})/2$ is a cube root of unity in k. The ring R is a PID.

If ℓ is congruent to 1 or 2 modulo 3, define $C(\ell)$ be the Cartan subgroup $C_s(\ell)$ or $C_{ns}(\ell)$, respectively. Let $N(\ell)$ be the normalizer of $C(\ell)$ in $\mathrm{GL}_2(\mathbb{F}_\ell)$.

Lemma 7.7. *After replacing $\rho_{E_d,\ell}$ by a conjugate representation, we will have $\rho_{E_d,\ell}(\mathrm{Gal}_{\mathbb{Q}}) \subseteq N(\ell)$ and $\rho_{E_d,\ell}(\mathrm{Gal}_k) \subseteq C(\ell)$ with*

$$[N(\ell) : \rho_{E_d,\ell}(\mathrm{Gal}_{\mathbb{Q}})] = [C(\ell) : \rho_{E_d,\ell}(\mathrm{Gal}_k)] \in \{1, 3\}.$$

Proof. We have $E_1 = E_{3,1}$. By Lemma 7.3, we have $\rho_{E_1,\ell}(\mathrm{Gal}_{\mathbb{Q}}) = N(\ell)$. The curves E_d and E_1 are isomorphic over $\mathbb{Q}(\sqrt[3]{d})$, so $\rho_{E_d,\ell}(\mathrm{Gal}_{\mathbb{Q}(\sqrt[3]{d})})$ is conjugate to a subgroup of $N(\ell)$ of index 1 or 3. Therefore, $\rho_{E_d,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate to a subgroup of $N(\ell)$ of index 1 or 3. Since $\rho_{E,d,\ell}(\mathrm{Gal}_{\mathbb{Q}}) \not\subseteq C(\ell)$ and $\rho_{E,d,\ell}(\mathrm{Gal}_k) \subseteq C(\ell)$, we deduce that $[N(\ell) : \rho_{E_d,\ell}(\mathrm{Gal}_{\mathbb{Q}})] = [C(\ell) : \rho_{E_d,\ell}(\mathrm{Gal}_k)]$. □

To determine the index in Lemma 7.7, we first compute some cubic residue symbols. Recall that we have already defined a representation $\rho_{E_d,\ell^\infty} \colon \mathrm{Gal}_k \to R_\ell^\times$.

Lemma 7.8. *Let λ be a prime of R dividing ℓ that satisfies $\lambda \equiv 2 \pmod{3R}$. Take any non-zero prime ideal $\mathfrak{p} \nmid 6d\ell$ of R. We have $\mathfrak{p} = R\pi$ for some $\pi \equiv 2 \pmod{3R}$. Then*

$$\left(\frac{\rho_{E_d,\ell^\infty}(\mathrm{Frob}_{\mathfrak{p}})}{\lambda}\right)_3 = \left(\frac{d^{\frac{2(\ell^e-1)}{3}}\lambda}{\pi}\right)_3,$$

where we are using cubic residue characters and the field $R/\lambda R$ has order ℓ^e.

Proof. By Example 10.6 of [Sil94, II §10], we have $\rho_{E_d,\ell^\infty}(\mathrm{Frob}_\mathfrak{p}) = -\overline{\left(\frac{4\cdot 16d^2}{\pi}\right)_6}\cdot\pi$, where we are using the 6-th power residue symbol. Therefore,

$$\rho_{E_d,\ell^\infty}(\mathrm{Frob}_\mathfrak{p}) = -\overline{\left(\frac{d}{\pi}\right)}_6^2\pi = -\overline{\left(\frac{d}{\pi}\right)}_3\pi = -\left(\frac{d}{\pi}\right)_3^2\cdot\pi$$

and hence

$$\left(\frac{\rho_{E_d,\ell^\infty}(\mathrm{Frob}_\mathfrak{p})}{\lambda}\right)_3 = \left(\frac{-\left(\frac{d^2}{\pi}\right)_3\cdot\pi}{\lambda}\right)_3 = \left(\frac{d^2}{\pi}\right)_3^{\frac{\ell^e-1}{3}}\left(\frac{\pi}{\lambda}\right)_3 = \left(\frac{d^2}{\pi}\right)_3^{\frac{\ell^e-1}{3}}\left(\frac{\lambda}{\pi}\right)_3 = \left(\frac{d^{\frac{2(\ell^e-1)}{3}}\lambda}{\pi}\right)_3,$$

where we have used cubic reciprocity. □

Lemma 7.9. *Suppose that $\ell\equiv 2 \pmod 3$. Then the group $\rho_{E_d,\ell}(\mathrm{Gal}_k)$ has index 3 in $C(\ell)$ if and only if $\ell\equiv 2 \pmod 9$ and $d=\ell$, or $\ell\equiv 5 \pmod 9$ and $d=\ell^2$. Note that $C(\ell)$ has a unique index 3 subgroup.*

Proof. Using Lemma 7.7 and $\ell\geq 5$, we find that $\rho_{E_d,\ell}(\mathrm{Gal}_k)$ is an index 3 subgroup of $C(\ell)$ if and only if $\rho_{E_d,\ell^\infty}(\mathrm{Gal}_k)$ lies in a closed subgroup of $R_\ell^\times$ of index 3. We have $C(\ell)=C_{ns}(\ell)$ since $\ell\equiv 2 \pmod 3$, so $R_\ell^\times$ has a unique index 3 closed subgroup, i.e., the group of $a\in R_\ell^\times$ with $\left(\frac{a}{\ell}\right)_3 = 1$.

By the Chebotarev density theorem and Lemma 7.8 with $\lambda=\ell$, we deduce that $\rho_{E_d,\ell}(\mathrm{Gal}_k)$ is an index 3 subgroup of $C(\ell)$ if and only if $d^{2(\ell^2-1)/3}\ell$ is a cube in $R/\mathfrak{p}$ for all primes $\mathfrak{p}\nmid 6d\ell$ of R; equivalently, $d^{2(\ell^2-1)/3}\ell$ is a cube in R. Since $d^{2(\ell^2-1)/3}\ell$ is a rational integer, it is a cube in R if and only if it is a cube in $\mathbb{Z}$.

We have $2(\ell^2-1)/3\equiv 2(\ell+1)/3 \pmod 3$, so we need only determine when the integer $d^{2(\ell+1)/3}\ell$ is a cube. In the following, we use that $d\geq 1$ is cube-free and that $\mathbb{Z}$ has unique factorization. If $\ell=2+9m$, then $d^{2+6m}\ell$ is a cube if and only if $d=\ell$. If $\ell=5+9m$, then $d^{4+6m}\ell$ is a cube if and only if $d=\ell^2$. If $\ell=8+9m$, then $d^{6+6m}\ell$ is never a cube. □

Lemma 7.10. *Suppose that $\ell\equiv 1 \pmod 3$. Then the group $\rho_{E_d,\ell}(\mathrm{Gal}_k)$ has index 3 in $C(\ell)$ if and only if $\ell\equiv 4 \pmod 9$ and $d=\ell^2$, or $\ell\equiv 7 \pmod 9$ and $d=\ell$.*

The group $\rho_{E_d,\ell}(\mathrm{Gal}_k)$ is conjugate to $C(\ell)=C_s(\ell)$ or the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} a & 0\\ 0 & b\end{smallmatrix}\right)$ with $a/b\in\mathbb{F}_\ell^\times$ a cube.

Proof. Using Lemma 7.7 and $\ell\geq 5$, we find that $\rho_{E_d,\ell}(\mathrm{Gal}_k)$ is an index 3 subgroup of $C(\ell)$ if and only if $\rho_{E_d,\ell^\infty}(\mathrm{Gal}_k)$ lies in a closed subgroup of $R_\ell^\times$ of index 3. Let us describe the index 3 subgroups of $R_\ell^\times$. Since $\ell\equiv 1 \pmod 3$, we have $\ell=\lambda_1\lambda_2$ for irreducibles $\lambda_i\in R$ that we may choose to be congruent to 2 modulo $3R$. We have $R_\ell^\times = R_{\lambda_1}^\times\times R_{\lambda_2}^\times$. The cubic residue symbol $\left(\frac{\cdot}{\lambda_i}\right)$ defines a homomorphism $\varphi_i\colon R_\ell^\times\to\mu_3:=\langle\omega\rangle$. Since $\ell\geq 5$, we find that every non-trivial homomorphism $R_\ell^\times\to\mu_3$ is of the form $\varphi_e:=\varphi_1^{e_1}\varphi_2^{e_2}$ with $e=(e_1,e_2)\in\{0,1,2\}^2-\{(0,0)\}$. Therefore, $\rho_{E_d,\ell}(\mathrm{Gal}_k)$ is an index 3 subgroup of $C(\ell)$ if and only if $\rho_{E_d,\ell^\infty}(\mathrm{Gal}_k)\subseteq\ker\varphi_e$ for some $e\neq(0,0)$.

By Lemma 7.8, we have $\left(\frac{\rho_{E_d,\ell^\infty}(\mathrm{Frob}_\mathfrak{p})}{\lambda_i}\right)_3 = \left(\frac{d^{\frac{2(\ell-1)}{3}}\lambda_i}{\pi}\right)_3$ and hence

$$\varphi_e(\rho_{E_d,\ell^\infty}(\mathrm{Frob}_\mathfrak{p})) = \left(\frac{d^{\frac{2(\ell-1)}{3}}\lambda_1}{\pi}\right)_3^{e_1}\left(\frac{d^{\frac{2(\ell-1)}{3}}\lambda_2}{\pi}\right)_3^{e_2} = \left(\frac{d^{\frac{2(\ell-1)(e_1+e_2)}{3}}\lambda_1^{e_1}\lambda^{e_2}}{\pi}\right)_3 \tag{7.2}$$

for all $\mathfrak{p}\nmid 6d\ell$. Using the Chebotarev density theorem, we deduce that $\rho_{E_d,\ell^\infty}(\mathrm{Gal}_k)\subseteq\ker\varphi_e$ if and only if $\beta:=d^{\frac{2(\ell-1)(e_1+e_2)}{3}}\lambda_1^{e_1}\lambda^{e_2}$ is a cube in R.

First suppose that $e_1\neq e_2$. Let $v_{\lambda_i}\colon R^\times\twoheadrightarrow\mathbb{Z}$ be the valuation for the prime λ_i and let $v_\ell\colon\mathbb{Q}^\times\twoheadrightarrow\mathbb{Z}$ be the valuation for ℓ. We have

$$v_{\lambda_i}(\beta) = e_i + \tfrac{2(\ell-1)(e_1+e_2)}{3}v_{\lambda_i}(d) = e_i + \tfrac{2(\ell-1)(e_1+e_2)}{3}v_\ell(d).$$

We have $e_1 \not\equiv e_2 \pmod 3$ since $e_1 \neq e_2$, so $v_{\lambda_i}(\beta) \not\equiv 0 \pmod 3$ for some $i \in \{1,2\}$. Therefore, $\beta \in R$ is not a cube.

Now suppose that $e_1 = e_2$. We may assume that $e_1 = e_2 = 1$ since $\varphi_{(2,2)}$ is the square of $\varphi_{(1,1)}$ and hence have the same kernel. So $\beta = d^{4(\ell-1)/3}\ell$. Since β is a rational integer, it is a cube in $\mathbb{Z}$ if and only if it is a cube in R. If $\ell = 1 + 9m$, then $\beta = (d^{4m})^3\ell$ is not a cube. If $\ell = 4 + 9m$, then $\beta = (d^{4m+1})^3 \cdot d\ell$ which is a cube if and only if $d = \ell^2$ (recall that d is positive and cube-free). If $\ell = 7 + 9m$, then $\beta = (d^{4m+2})^3 \cdot d^2\ell$ which is a cube if and only if $d = \ell$.

Finally, suppose we are in the case where $\rho_{E_d,\ell}(\mathrm{Gal}_k)$ is an index 3 subgroup of $C_s(\ell)$. There are 4 index 3 subgroups of $C_s(\ell)$. Two of the groups consist of the matrices $A := \left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ for which a is a cube (or b is a cube); these groups cannot equal $\rho_{E_d,\ell}(\mathrm{Gal}_k)$ since it would correspond to the case where $e_1 = 0$ or $e_2 = 0$ (and hence $e_1 \neq e_2$). Another index 3 subgroup of $C_s(\ell)$ is the subgroup of matrices whose determinant is a cube; this is impossible since $\det(\rho_{E_d,\ell}(\mathrm{Gal}_k)) = \mathbb{F}_\ell^\times$. Therefore, the only possibility for the image of $\rho_{E_d,\ell}$ is the group of A with a/b a cube. □

We now complete the proof of the proposition for the curve $E_d/\mathbb{Q}$. From Lemmas 7.7, 7.9 and 7.10, we deduce that $\rho_{E_d}(\mathrm{Gal}_\mathbb{Q})$ has index 1 or 3 in $N(\ell)$, with index 3 occurring if and only if one of the following hold:

- $\ell \equiv 2 \pmod 9$ and $d = \ell$,
- $\ell \equiv 5 \pmod 9$ and $d = \ell^2$,
- $\ell \equiv 4 \pmod 9$ and $d = \ell^2$,
- $\ell \equiv 7 \pmod 9$ and $d = \ell$.

Set $M := \rho_{E_d,\ell}(\mathrm{Gal}_k)$; we may assume that it is the index 3 subgroup of $C(\ell)$ from Lemma 7.9 or 7.10. The group M is normal in $N(\ell)$. We have $[N(\ell) : M] = 6$ and $\det(M) = \mathbb{F}_\ell^\times$, so $N(\ell)/M$ is non-abelian by Lemma 7.4(i). So $N(\ell)/M$ is isomorphic to $\mathfrak{S}_3$ and hence, up to conjugation, $N(\ell)$ has a unique index 3 subgroup G' satisfying $G' \subseteq M$. Therefore, G' is conjugate in $\mathrm{GL}_2(\mathbb{F}_\ell)$ to both $\rho_{E_d,\ell}(\mathrm{Gal}_\mathbb{Q})$ and the group G from part (iii) or (iv) of Lemma 1.16. This finishes the proof of Proposition 1.16 for the curve $E_d/\mathbb{Q}$ and $\ell > 3$.

Finally suppose that $E/\mathbb{Q}$ is any elliptic curve with j-invariant 0; it is defined by a Weierstrass equation $y^2 = x^3 + dm^3$ for some integer $m \neq 0$ and cube-free integer d. It suffices to show that $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ is conjugate to $\rho_{E_d,\ell}(\mathrm{Gal}_\mathbb{Q})$ in $\mathrm{GL}_2(\mathbb{F}_\ell)$. The curves E and E_d are quadratic twists, so $\pm\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ is conjugate to $\pm\rho_{E_d,\ell}(\mathrm{Gal}_\mathbb{Q})$. The general case of Proposition 1.16 is thus a consequence of the following lemma.

Lemma 7.11. *There are no proper subgroups $\pm\rho_{E_d,\ell}(\mathrm{Gal}_\mathbb{Q})$ has no proper subgroups H such that $\pm H = \pm\rho_{E_d,\ell}(\mathrm{Gal}_\mathbb{Q})$.*

Proof. If $\pm\rho_{E_d,\ell}(\mathrm{Gal}_\mathbb{Q})$ is conjugate to $N(\ell)$, then the lemma follows immediately from Lemma 7.4(ii). From the case of Proposition 1.16 we have already proved (i.e., for the curve E_d and prime $\ell > 3$), we need only show that the group G from parts (iii) and (iv) of Lemma 1.16 have no proper subgroups H satisfying $\pm H = G$. Equivalently, we need to show that $-I$ is a commutator of such a subgroup G. With G as in Lemma 1.16(iii), this follows from $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)^{-1}\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. So we may take G as in Lemma 1.16(iv).

Fix any $B \in G - C(\ell)$. As noted in the proof of Lemma 7.4, the map $\varphi\colon C(\ell) \to C(\ell)$, $A \mapsto BABA^{-1}$ is a homomorphism whose image is cyclic of order $\ell + 1$. Therefore, $\varphi(G \cap C(\ell))$ is the cyclic subgroup of $C(\ell)$ of order $(\ell+1)/3$. In particular, $\varphi(G \cap C(\ell))$ contains $-I$ which is the unique element of order 2 in $C(\ell)$. Therefore, $-I$ is a commutator of G. □

7.4.1. $\ell = 3$ *case.* We now consider the prime $\ell = 3$ with $E/\mathbb{Q}$ defined by the elliptic curve $y^2 = x^3 + d$. The division polynomial of $E/\mathbb{Q}$ at 3 is $3x(x^3 + 4d)$. The points of order 3 in $E(\overline{\mathbb{Q}})$ are thus $(0, \pm\sqrt{d})$ and $(-\sqrt[3]{4d}\omega^e, \pm\sqrt{-3}\sqrt{d})$ with $e \in \{0, 1, 2\}$. The points $P_1 = (0, \sqrt{d})$ and $P_2 = (-\sqrt[3]{4d}, \sqrt{-3}\sqrt{d})$ form a basis of $E[3]$. With respect to this basis, we have

$$\rho_{E,3} = \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix},$$

with characters $\psi_1, \psi_2 \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathbb{F}_3^\times$. The quadratic character ψ_1 describes the Galois action on P_1 and it thus corresponds to the extension $\mathbb{Q}(\sqrt{d})$ of $\mathbb{Q}$. The quadratic character $\psi_1\psi_2 = \det \circ \rho_{E,3} \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathbb{F}_3^\times$ corresponds to the extension $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ of $\mathbb{Q}$. Therefore,

$$(\psi_1 \times \psi_2)(\mathrm{Gal}_{\mathbb{Q}}) = \begin{cases} \{1\} \times \mathbb{F}_3^\times & \text{if } d \text{ is a square,} \\ \mathbb{F}_3^\times \times \{1\} & \text{if } -3d \text{ is a square,} \\ \mathbb{F}_3^\times \times \mathbb{F}_3^\times & \text{otherwise.} \end{cases}$$

To compute the image of $\rho_{E,3}(\mathrm{Gal}_{\mathbb{Q}})$ it remains to determine when its cardinality is divisible by 3 or not. From P_1 and P_2, it is clear that $\rho_{E,3}(\mathrm{Gal}_{\mathbb{Q}})$ is divisible by 3 if and only if $4d$ is not a cube.

8. Proof of Proposition 1.13

By Theorem 1.11, we may assume that $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is a subgroup of $N_{ns}(\ell)$. Let I_ℓ be an inertia subgroup of $\mathrm{Gal}_{\mathbb{Q}}$ for the prime ℓ. We will show that $\rho_{E,\ell}$ has large image by showing that the group $\rho_{E,\ell}(I_\ell)$ is large. The cardinality of $\rho_{E,\ell}(I_\ell)$ is not divisible by ℓ since it is a subgroup of $N_{ns}(\ell)$. The group $\rho_{E,\ell}(I_\ell)$ is thus cyclic since the *tame inertia group* at ℓ is pro-cyclic, cf. [Ser72, §1.3].

Let v_ℓ be the ℓ-adic valuation on $\mathbb{Q}_\ell$ normalized so that $v_\ell(\ell) = 1$. Let $\mathbb{Q}_\ell^{\mathrm{un}}$ be the maximal unramified extension of $\mathbb{Q}_\ell$ in a fixed algebraic closed field $\overline{\mathbb{Q}}_\ell$. An embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$ allows us to identify I_ℓ with the subgroup $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell^{\mathrm{un}})$ of $\mathrm{Gal}_{\mathbb{Q}_\ell} := \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$. Let Δ_E be the minimal discriminant of $E/\mathbb{Q}$.

• First suppose that $v_\ell(j_E) \geq 0$ and that $v_\ell(\Delta_E)$ is not congruent to 2 and 10 modulo 12.

Let L be the smallest extension of $\mathbb{Q}_\ell^{\mathrm{un}}$ for which E base extended to L has good reduction. Define $e = [L : \mathbb{Q}_\ell^{\mathrm{un}}]$. There is thus a finite extension $K/\mathbb{Q}_\ell$ such that E base extended to K has good reduction and that $v_\ell(K^\times) = e^{-1}\mathbb{Z}$, where v_ℓ is the valuation on K that extends v_ℓ. From [Ser72, §5.6], we find that $e \in \{1, 2, 3, 4\}$; this uses our assumption on $v_\ell(\Delta_E)$.

Let $\mathcal{I}$ be the inertia subgroup of $\mathrm{Gal}_K := \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/K)$; it is a subgroup of I_ℓ. The action of $\mathcal{I}$ on $E[\ell]$ is semi-simple since the cardinality of $\rho_{E,\ell}(\mathcal{I})$ is relatively prime to ℓ (the group $N_{ns}(\ell)$ has this property). Let $\theta_1 \colon \mathcal{I} \twoheadrightarrow \mathbb{F}_\ell^\times$ and $\theta_2 \colon \mathcal{I} \twoheadrightarrow \mathbb{F}_{\ell^2}^\times$ be *fundamental characters* of level 1 and 2, respectively, cf. [Ser72, §1.7].

Lemma 8.1. *The representation $\rho_{E,\ell}|_{\mathcal{I}} \colon \mathcal{I} \to \mathrm{GL}_2(\mathbb{F}_\ell)$ is irreducible.*

Proof. Suppose that $\rho_{E,\ell}|_{\mathcal{I}}$ is reducible. The representation $\rho_{E,\ell}|_{\mathcal{I}}$ is given by a pair of characters $\theta_1^{e_1}$ and $\theta_1^{e_2}$ with $0 \leq e_1 \leq e_2 < \ell - 1$. From Proposition 11 of [Ser72], we can take $e_1 = 0$ and $e_2 = e$. The image of $\rho_{E,\ell}(\mathcal{I})$ in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is thus isomorphic to $\theta_1^e(\mathcal{I})$ and hence is cyclic of order $(\ell - 1)/\gcd(\ell - 1, e)$.

The matrix A^2 is scalar for all $A \in N_{ns}(\ell) - C_{ns}(\ell)$. Therefore, the order of every element in the image of $N_{ns}(\ell) \to \mathrm{PGL}_2(\mathbb{F}_\ell)$ divides $\ell + 1$. Since $\gcd(\ell + 1, \ell - 1) = 2$, we deduce that $(\ell - 1)/\gcd(\ell - 1, e)$ equals 1 or 2. This is a contradiction since $\ell \geq 17$. □

Scalar multiplication and a choice of $\mathbb{F}_\ell$-basis for $\mathbb{F}_{\ell^2}$ allows us to identify $\mathbb{F}_{\ell^2}^\times$ with a subgroup of $\mathrm{Aut}_{\mathbb{F}_\ell}(\mathbb{F}_{\ell^2}) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$. Since $\rho_{E,\ell}|_{\mathcal{I}}$ is irreducible by Lemma 8.1, it is isomorphic to $\theta_2^{e_1 + e_2\ell} \colon \mathcal{I} \to$

$\mathbb{F}_{\ell^2}^\times \hookrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)$ for some $0 \leq e_1, e_2 \leq \ell - 1$. As an $\mathbb{F}_\ell[\mathcal{I}]$-module, $E[\ell]$ is isomorphic to the dual of the étale cohomology group $H^1_{\text{ét}}(E_{\overline{K}}, \mathbb{F}_\ell)$. By Théorème 1.2 of [Car08], we may take $0 \leq e_1, e_2 \leq e$ (when E has good reduction at ℓ, and hence $e = 1$, this follows from [Ser72, Prop. 12]). We have $e_1 \neq e_2$ since otherwise $\theta_2^{e_1+e_2\ell} = (\theta_2^{\ell+1})^{e_1}$ is not irreducible.

Let g be the greatest common divisor of $e_1 + e_2\ell$ and $\ell + 1$. We have $(e_1 + e_2\ell) - e_2(\ell + 1) = e_1 - e_2 \in \{\pm 1, \pm 2, \pm 3, \pm 4\}$ since $0 \leq e \leq 4$, so $g \in \{1, 2, 3, 4\}$. Therefore, $\rho_{E,\ell}(\mathcal{I})$ contains a cyclic group of order $(\ell + 1)/g$.

Lemma 8.2. *The group $\rho_{E,\ell}(I_\ell)$ is a subgroup of $C_{ns}(\ell)$ with index 1 or 3.*

Proof. Set $H := \rho_{E,\ell}(I_\ell)$; it is cyclic. We claim that H is a subgroup of $C_{ns}(\ell)$. Suppose not, then the order of H divides $2(\ell - 1)$ since A^2 is a scalar matrix for any $A \in N_{ns}(\ell) - C_{ns}(\ell)$. Therefore, $(\ell+1)/g$ divides $2(\ell-1)$ since $\rho_{E,\ell}(\mathcal{I}) \subseteq H$ contains an element of order $(\ell+1)/g$. Since $\gcd(\ell+1, \ell-1) = 2$, we deduce that $(\ell+1)/g$ divides 4. This is impossible since $\ell \geq 17$ and $g \leq 4$.

It remains to bound the index of H in $C_{ns}(\ell)$. We have $\det(H) = \mathbb{F}_\ell^\times$ since $\det \circ \rho_{E,\ell}$ describes the Galois action on the ℓ-th roots of unity. Therefore, the group H is cyclic and its order is divisible by $\ell - 1$ and $(\ell + 1)/g$. Since $\gcd(\ell + 1, \ell - 1) = 2$, we deduce that the order of H is divisible by $(\ell - 1)(\ell + 1)/(2g)$. Therefore, the index $b := [C_{ns}(\ell) : H]$ divides $2g$.

Suppose b is even. Since $C_{ns}(\ell)$ is cyclic, the group H must be contained in $\{A \in C_{ns}(\ell) : \det(A) \in (\mathbb{F}_\ell^\times)^2\}$; this is the unique index 2 subgroup of $C_{ns}(\ell)$. However, this is impossible since $\det(H) = \mathbb{F}_\ell^\times$. So b is odd and divides $2g \in \{2, 4, 6, 8\}$. Therefore, b is 1 or 3. □

Now define $H := \rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q}) \cap C_{ns}(\ell)$. We have $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q}) \not\subseteq C_{ns}(\ell)$ since $C_{ns}(\ell)$ is not applicable; it does not contain an element with trace 0 and determinant -1. So if $H = C_{ns}(\ell)$, then $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q}) = N_{ns}(\ell)$.

We are thus left to consider the case where H is the (unique) index 3 subgroup of $C_{ns}(\ell)$. The group H is a normal subgroup of $N_{ns}(\ell)$ of index 6.

Lemma 8.3. *We have $\ell \equiv 2 \pmod 3$ and the quotient group $N_{ns}(\ell)/H$ is isomorphic to $\mathfrak{S}_3$.*

Proof. If $\ell \equiv 1 \pmod 3$, then $\det(H) = (\mathbb{F}_\ell^\times)^3 \subsetneq \mathbb{F}_\ell^\times$. This is impossible since $\det(\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})) = \mathbb{F}_\ell^\times$ and $[\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q}) : H] = 2$. Therefore, $\ell \equiv 2 \pmod 3$. One can now verify that $N_{ns}(\ell)$ quotiented out by the scalar matrices is isomorphic to a dihedral group. It is then easy to check that $N_{ns}(\ell)/H$ is the dihedral group of order $2 \cdot 3$; it is thus isomorphic to $\mathfrak{S}_3$. □

The index 3 subgroups of $\mathfrak{S}_3$ are all conjugate so, up to conjugacy, G (as in the statement of Proposition 1.13) is the unique index 3 subgroup of $N_{ns}(\ell)$ that contains H. Therefore, $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ and G are conjugate subgroups.

• Suppose that $v_\ell(j_E) \geq 0$.

By twisting $E/\mathbb{Q}$ by 1 or ℓ, we obtain an elliptic curve $E'/\mathbb{Q}$ with $v_\ell(\Delta_{E'})$ not congruent to 2 and 10 modulo 12. The group $\pm\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ is conjugate to $\pm\rho_{E',\ell}(\mathrm{Gal}_\mathbb{Q})$. The previous case applies and shows that $\pm\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ is conjugate to $\pm G = G$ or $\pm N_{ns}(\ell) = N_{ns}(\ell)$ in $\mathrm{GL}_2(\mathbb{F}_\ell)$.

It remains to show that $\pm\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q}) = \rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$; if not then there is an index 2 subgroup H of G or $N_{ns}(\ell)$ such that $-I \notin H$. The group $H \cap C_{ns}(\ell)$ is then an index 2 or 6 subgroup of $C_{ns}(\ell)$ that does not contain $-I$. However, the cardinality of $H \cap C_{ns}(\ell)$ is even, so it contains an element of order 2 which most be $-I$.

• Finally suppose that $v_\ell(j_E) < 0$.

There exists an element $q \in \mathbb{Q}_\ell$ with $v_\ell(q) = -v_\ell(j_E) > 0$ such that

$$j_E = (1 + 240\sum\nolimits_{n\geq 1} n^3 q^n/(1 - q^n))^3/(q\prod\nolimits_{n\geq 1}(1 - q^n)^{24}).$$

Let $\mathcal{E}/\mathbb{Q}_\ell$ be the Tate curve associated to q, cf. [Sil94, V§3]; it is an elliptic curve with j-invariant j_E and the group $\mathcal{E}(\overline{\mathbb{Q}}_\ell)$ is isomorphic to $\overline{\mathbb{Q}}_\ell^\times/\langle q\rangle$ as a $\mathrm{Gal}_{\mathbb{Q}_\ell}$-module. In particular, the ℓ-torsion subgroup $\mathcal{E}[\ell]$ is isomorphic as an $\mathbb{F}_\ell[\mathrm{Gal}_{\mathbb{Q}_\ell}]$-module to the subgroup of $\overline{\mathbb{Q}}_\ell^\times/\langle q\rangle$ generated by an ℓ-th root of unity ζ and a chosen ℓ-th root $q^{1/\ell}$ of q. Let $\alpha\colon \mathrm{Gal}_{\mathbb{Q}_\ell}\to\mathbb{F}_\ell^\times$ and $\beta\colon \mathrm{Gal}_{\mathbb{Q}_\ell}\to\mathbb{F}_\ell$ be the maps defined so that $\sigma(\zeta)=\zeta^{\alpha(\sigma)}$ and $\sigma(q^{1/\ell})=\zeta^{\beta(\sigma)}q^{1/\ell}$. So with respect to the basis $\{\zeta, q^{1/\ell}\}$ for $\mathcal{E}[\ell]$, we have $\rho_{\mathcal{E},\ell}(\sigma)=\left(\begin{smallmatrix}\alpha(\sigma) & \beta(\sigma)\\ 0 & 1\end{smallmatrix}\right)$ for $\sigma\in\mathrm{Gal}_{\mathbb{Q}_\ell}$. The curves E and $\mathcal{E}$ are quadratic twists of each other over $\mathbb{Q}_\ell$ (the curve E is non-CM since its j-invariant is not an integer). So there is a character $\chi\colon \mathrm{Gal}_{\mathbb{Q}_\ell}\to\{\pm1\}$ such that, after an appropriate choice of basis for $E[\ell]$, we have

$$\rho_{E,\ell}(\sigma)=\chi(\sigma)\left(\begin{smallmatrix}\alpha(\sigma) & \beta(\sigma)\\ 0 & 1\end{smallmatrix}\right)$$

for all $\sigma\in\mathrm{Gal}_{\mathbb{Q}_\ell}$. Since α is surjective, we find that the image of $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ contains a cyclic group of order $\ell-1$. However, the image of $N_{ns}(\ell)$ in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ has order $2(\ell+1)$. Since $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})\subseteq N_{ns}(\ell)$, we find that $\ell-1$ divides $2(\ell+1)$; this is impossible since $\gcd(\ell-1,\ell+1)=2$ and $\ell\geq 17$.

References

[Bar14] Burcu Baran, *An exceptional isomorphism between modular curves of level 13*, J. Number Theory **145** (2014), 273–300, DOI 10.1016/j.jnt.2014.05.017. MR3253304 ↑1.6

[BC14] Barinder S. Banwait and John E. Cremona, *Tetrahedral elliptic curves and the local-global principle for isogenies*, Algebra Number Theory **8** (2014), no. 5, 1201–1229. MR3263141 ↑1.6

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Computational algebra and number theory (London, 1993). ↑1.10

[BK75] B. J. Birch and W. Kuyk (eds.), *Modular functions of one variable. IV*, Lecture Notes in Mathematics, Vol. 476, Springer-Verlag, Berlin, 1975. MR0376533 (51 #12708) ↑4.5.4

[BPR11] Yu. Bilu, P. Parent, and M. Rebolledo, *Rational points on $X_0^+(p^r)$*, 2011. arXiv:1104.4641. ↑1.7, 4.5.2

[CC06] Bryden Cais and Brian Conrad, *Modular curves and Ramanujan's continued fraction*, J. Reine Angew. Math. **597** (2006), 27–104. MR2264315 (2007j:11079) ↑4.3

[Car08] Xavier Caruso, *Conjecture de l'inertie modérée de Serre*, Invent. Math. **171** (2008), no. 3, 629–699. MR2372809 (2008j:14034) ↑8

[DFGS14] Valerio Dose, Julio Fernández, Josep González, and René Schoof, *The automorphism group of the non-split Cartan modular curve of level* 11, Journal of Algebra **417** (2014), 95–102. ↑4.5.3

[DGJJU11] Luis Dieulefait, Enrique González-Jiménez, and Jorge Jiménez Urroz, *On fields of definition of torsion points of elliptic curves with complex multiplication*, Proc. Amer. Math. Soc. **139** (2011), no. 6, 1961–1969. MR2775372 (2012a:11067) ↑7.2

[DR73] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), 1973, pp. 143–316. Lecture Notes in Math., Vol. 349. MR0337993 (49 #2762) ↑3

[Duk05] W. Duke, *Continued fractions and modular functions*, Bull. Amer. Math. Soc. (N.S.) **42** (2005), no. 2, 137–162. MR2133308 (2006c:11042) ↑4.3

[Elk01] Noam D. Elkies, *Explicit modular towers*, 2001. arXiv:math/0103107 [math.NT]. ↑3.3

[Elk99] ———, *The Klein quartic in number theory*, The eightfold way, 1999, pp. 51–101. MR1722413 (2001a:11103) ↑4.4, 4.4, 4.4

[Hal98] Emmanuel Halberstadt, *Sur la courbe modulaire $X_{ndép}(11)$*, Experiment. Math. **7** (1998), no. 2, 163–174. MR1677158 (99m:11062) ↑1.7, 4.5.3

[Ken80] M. A. Kenku, *The modular curve $X_0(169)$ and rational isogeny*, J. London Math. Soc. (2) **22** (1980), no. 2, 239–244. MR588271 (81m:10048) ↑4.6

[Ken81] ———, *Corrigendum: "The modular curve $X_0(169)$ and rational isogeny" [J. London Math. Soc. (2) **22** (1980), no. 2, 239–244; MR 81m:10048]*, J. London Math. Soc. (2) **23** (1981), no. 3, 428. MR616547 (82h:10039) ↑4.6

[Lec89] Odile Lecacheux, *Unités d'une famille de corps cycliques réeles de degré* 6 *liés à la courbe modulaire $X_1(13)$*, J. Number Theory **31** (1989), no. 1, 54–63. MR978099 (90i:11062) ↑4.6

[Lig77] Gérard Ligozat, *Courbes modulaires de niveau* 11, Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), 1977, pp. 149–237. Lecture Notes in Math., Vol. 601. MR0463118 (57 #3079) ↑4.5.1

[Maz78] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162. MR482230 (80h:14022) ↑1.7

[RZB14] Jeremy Rouse and David Zureick-Brown, *Elliptic curves over* $\mathbb{Q}$ *and* 2*-adic images of Galois*, 2014. arXiv:1402.5997 (to appear: Research in Number Theory). ↑1.8

[Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331. MR0387283 (52 #8126) ↑1, 4.8, 8, 8

[Ser81] ———, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. **54** (1981), 323–401. MR644559 (83k:12011) ↑1.7

[Ser97] ———, *Lectures on the Mordell-Weil theorem*, Third, Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre. MR1757192 (2000m:11049) ↑3.2

[Shi94] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1. MR1291394 (95e:11048) ↑3, 3.4, 3.4

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, Second, Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094 (2010i:11005) ↑3.4

[Sil94] ———, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR1312368 (96b:11074) ↑1.9, 7.4, 8

[ST68] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517. MR0236190 (38 #4488) ↑7, 7

[Sut12] Andrew V. Sutherland, *A local-global principle for rational isogenies of prime degree*, J. Théor. Nombres Bordeaux **24** (2012), no. 2, 475–485 (English, with English and French summaries). MR2950703 ↑4.3

[Sut15] Andrew V. Sutherland, *Computing images of Galois representations attached to elliptic curves*, 2015. arXiv:1504.07618. ↑1.8

[Zyw10] David Zywina, *Elliptic curves with maximal Galois action on their torsion points*, Bull. Lond. Math. Soc. **42** (2010), no. 5, 811–826. MR2721742 (2012a:11073) ↑2

[Zyw15] ———, *On the surjectivity of mod* ℓ *representations associated to elliptic curves* (2015). preprint. ↑1.8

Department of Mathematics, Cornell University, Ithaca, NY 14853, USA
E-mail address: zywina@math.cornell.edu
URL: http://www.math.cornell.edu/~zywina