POSSIBLE INDICES FOR THE GALOIS IMAGE OF ELLIPTIC CURVES
OVER \( \mathbb{Q} \)

DAVID ZYWINA

Abstract. For a non-CM elliptic curve \( E/\mathbb{Q} \), the Galois action on its torsion points can be expressed in terms of a Galois representation \( \rho_E: \text{Gal}_\mathbb{Q} \to \text{GL}_2(\hat{\mathbb{Z}}) \). A well-known theorem of Serre says that the image of \( \rho_E \) is open and hence has finite index in \( \text{GL}_2(\mathbb{Z}) \). We will study what indices are possible assuming that we are willing to exclude a finite number of possible \( j \)-invariants from consideration. For example, we will show that there is a finite set \( J \) of rational numbers such that if \( E/\mathbb{Q} \) is a non-CM elliptic curve with \( j \)-invariant not in \( J \) and with surjective mod \( \ell \) representations for all \( \ell > 37 \) (which conjecturally always holds), then the index \([\text{GL}_2(\hat{\mathbb{Z}}): \rho_E(\text{Gal}_\mathbb{Q})]\) lies in the set
\[
I = \{ 2, 4, 6, 8, 10, 12, 16, 20, 24, 30, 32, 36, 40, 48, 54, 60, 72, 84, 108, 112, 120, 144, 192, 220, 240, 288, 336, 360, 384, 504, 576, 768, 864, 1152, 1200, 1296, 1536 \}.
\]
Moreover, \( I \) is the minimal set with this property.

1. Introduction

1.1. Main results. Let \( E \) be an elliptic curve defined over \( \mathbb{Q} \). For each integer \( N > 1 \), let \( E[N] \) be the \( N \)-torsion subgroup of \( E(\overline{\mathbb{Q}}) \). The group \( E[N] \) is a free \( \mathbb{Z}/N\mathbb{Z} \)-module of rank 2 and has natural action of the absolute Galois group \( \text{Gal}_\mathbb{Q} := \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \). This Galois action on \( E[N] \) may be expressed in terms of a Galois representation
\[
\rho_{E,N}: \text{Gal}_\mathbb{Q} \to \text{Aut}_{\mathbb{Z}/N\mathbb{Z}}(E[N]) \cong \text{GL}_2(\mathbb{Z}/N\mathbb{Z});
\]
it is uniquely determined up to conjugacy by an element of \( \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) \). By choosing bases compatibly for all \( N \), we may combine the representations \( \rho_{E,N} \) to obtain a single Galois representation
\[
\rho_E: \text{Gal}_\mathbb{Q} \to \text{GL}_2(\hat{\mathbb{Z}})
\]
that describes the Galois action on all the torsion points of \( E \), where \( \hat{\mathbb{Z}} \) is the profinite completion of \( \mathbb{Z} \). If \( E \) is non-CM, then the following theorem of Serre [Ser72] says that the image is, up to finite index, as large as possible.

Theorem 1.1 (Serre). If \( E/\mathbb{Q} \) is a non-CM elliptic curve, then \( \rho_E(\text{Gal}_\mathbb{Q}) \) has finite index in \( \text{GL}_2(\hat{\mathbb{Z}}) \).

Serre’s theorem is qualitative, and it natural to ask what the possible values for the index \([\text{GL}_2(\hat{\mathbb{Z}}): \rho_E(\text{Gal}_\mathbb{Q})]\) are. Our theorems address this question assuming that we are willing to exclude a finite number of exceptional \( j \)-invariants from consideration; we will see later that the index \([\text{GL}_2(\hat{\mathbb{Z}}): \rho_E(\text{Gal}_\mathbb{Q})]\) depends only on the \( j \)-invariant \( j_E \) of \( E \).

The most difficult part of Serre’s proof of Theorem 1.1 is to show that there is an integer \( c_E \) such that \( \rho_{E,\ell}(\text{Gal}_\mathbb{Q}) = \text{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \) for all \( \ell > c_E \). In [Ser72, §4.3], Serre asks whether one can choose \( c_E \) independent of the elliptic curve (moreover, he asked whether this holds with \( c_E = 37 \) [Ser81, p. 399]). We formulate this as a conjecture.

2020 Mathematics Subject Classification. Primary 11G05; Secondary 11F80.
Conjecture 1.2. There is an absolute constant \( c \) such that for every non-CM elliptic curve \( E \) over \( \mathbb{Q} \), we have \( \rho_{E,\ell}(\text{Gal}_{\mathbb{Q}}) = \text{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \) for all \( \ell > c \).

Define the set
\[
I := \left\{ 2, 4, 6, 8, 10, 12, 16, 20, 24, 30, 32, 36, 40, 48, 54, 60, 72, 84, 96, 108, 112, 120, 144, \right. \\
\left. 192, 220, 240, 288, 336, 360, 384, 504, 576, 768, 864, 1152, 1200, 1296, 1536 \right\}.
\]

Theorem 1.3. Fix an integer \( c \). There is a finite set \( J \), depending only on \( c \), such that if \( E/\mathbb{Q} \) is an elliptic curve with \( j_E \notin J \) and \( \rho_{E,\ell} \) surjective for all primes \( \ell > c \), then \( [\text{GL}_2(\hat{\mathbb{Z}}) : \rho_{E}(\text{Gal}_{\mathbb{Q}})] \) is an element of \( I \).

Assuming Conjecture 1.2, we can describe all possible indices \( [\text{GL}_2(\hat{\mathbb{Z}}) : \rho_{E}(\text{Gal}_{\mathbb{Q}})] \) after first excluding elliptic curves with a finite number of exceptional \( j \)-invariants.

Theorem 1.4. Conjecture 1.2 holds if and only if there exists a finite set \( J \subseteq \mathbb{Q} \) such that
\[
[\text{GL}_2(\hat{\mathbb{Z}}) : \rho_{E}(\text{Gal}_{\mathbb{Q}})] \in I
\]
for every elliptic curve \( E \) over \( \mathbb{Q} \) with \( j_E \notin J \).

For each integer \( n \geq 1 \), let \( J_n \) be the set of \( j \in \mathbb{Q} \) that occur as the \( j \)-invariant of some elliptic curve \( E \) over \( \mathbb{Q} \) with \( [\text{GL}_2(\hat{\mathbb{Z}}) : \rho_{E}(\text{Gal}_{\mathbb{Q}})] = n \). The following theorem shows that in Theorems 1.3 and 1.4, we cannot replace \( I \) by a smaller set.

Theorem 1.5. For any integer \( n \geq 1 \), the set \( J_n \) is infinite if and only if \( n \in I \).

Remark 1.6.

(i) Assuming Conjecture 1.2, Theorem 1.4 and Serre’s theorem implies that there is an absolute constant \( C \) such that \( [\text{GL}_2(\hat{\mathbb{Z}}) : \rho_{E}(\text{Gal}_{\mathbb{Q}})] \leq C \) for all non-CM elliptic curves \( E \) over \( \mathbb{Q} \).

(ii) The set \( J \) in Theorem 1.4 contains more than the thirteen \( j \)-invariants coming from those elliptic curves over \( \mathbb{Q} \) with complex multiplication. For example, the set \( J \) contains \(-7 \cdot 11^3\) and \(-7 \cdot 17^3 \cdot 2083^3\) which arise from the two non-cuspidal rational points of \( X_0(37) \), see [Vél74]. If \( E/\mathbb{Q} \) is an elliptic curve with \( j \)-invariant \(-7 \cdot 11^3\) or \(-7 \cdot 17^3 \cdot 2083^3\), then one can show that \( [\text{GL}_2(\hat{\mathbb{Z}}) : \rho_{E}(\text{Gal}_{\mathbb{Q}})] \geq 2736 \).

(iii) In our proofs of Theorems 1.3 and 1.4, the finite set \( J \) that arises is ineffective. The ineffectiveness arises from an application of Faltings’ theorem to a finite number of modular curves of genus at least 2.

1.2. Overview. In §2, we show that the index of \( \rho_{E}(\text{Gal}_{\mathbb{Q}}) \) in \( \text{GL}_2(\hat{\mathbb{Z}}) \) depends only on its commutator subgroup. In §3, we give some background on modular curves; for a fixed group \( G \) of \( \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) \) containing \(-I\), its rational points will describe the elliptic curves \( E/\mathbb{Q} \) with \( j_E \notin \{0,1728\} \) for which \( \rho_{E,N}(\text{Gal}_{\mathbb{Q}}) \) is conjugate to a subgroup of \( G \).

In §4, we prove a version of Theorem 1.3 with \( I \) replaced by another finite set \( \mathcal{I} \) that is defined in terms of the congruence subgroups of \( \text{SL}_2(\mathbb{Z}) \) with genus 0 or 1. Here we use Faltings’ theorem to deal with rational points of several modular curves with genus at least 2.

In §5, we describe how to compute the set \( \mathcal{I} \); it agrees with our set \( I \). Here, and throughout the paper, we avoid computing models for modular curves. For a genus 0 modular curve, we use the Hasse principle to determine whether it is isomorphic to \( \mathbb{P}^1_{\mathbb{Q}} \). We compute the Jacobian of genus 1 modular curves, up to isogeny, by counting their \( \mathbb{F}_l \)-points via the moduli interpretation. We also make use of the classification of genus 0 and 1 congruence subgroups due to Cummin and Pauli.

Finally, in §6 we complete the proofs of Theorems 1.3, 1.4 and 1.5.
1.3. Notation. Fix a positive integer $m$. Let $\mathbb{Z}_m$ be the ring that is the inverse limit of the rings $\mathbb{Z}/m^i\mathbb{Z}$ with respect to the reduction maps; equivalently, the inverse limit of $\mathbb{Z}/NZ$, where $N$ divides some power of $m$. We will make frequent use of the identifications $\mathbb{Z}_m = \prod_{p|m} \mathbb{Z}_p$ and $\hat{\mathbb{Z}} = \prod \mathbb{Z}_\ell$, where $\ell$ denotes a prime. In particular, $\mathbb{Z}_m$ depends only on the primes dividing $m$.

For a subgroup $G$ of $\text{GL}_2(\mathbb{Z}/m\mathbb{Z})$, $\text{GL}_2(\mathbb{Z}_m)$ or $\text{GL}_2(\hat{\mathbb{Z}})$ and an integer $N$ dividing $m$, we denote by $G(N)$ the image of the group $G$ in $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ under reduction modulo $N$.

All profinite groups will be considered with their profinite topologies. The *commutator subgroup* of a profinite group $G$ is the closed subgroup $G'$ generated by its commutators.

For each prime $p$, let $v_p: \mathbb{Q}^\times \to \mathbb{Z}$ be the $p$-adic valuation.

Acknowledgments. Thanks to Andrew Sutherland and David Zureick-Brown. We have made use of some of the *Magma* code from [Sut15].

The computations in §5 were performed using the *Magma* computer algebra system [BCP97]; code can be found at [https://github.com/davidzywina/PossibleIndices](https://github.com/davidzywina/PossibleIndices).

2. The commutator subgroup of the image of Galois

Let $E$ be a non-CM elliptic curve defined over $\mathbb{Q}$. Using the Weil pairing on the groups $E[N]$, one can show that the homomorphism $\text{det}_p: \text{Gal}_Q \to \hat{\mathbb{Z}}^\times$ is equal to the cyclotomic character $\chi$. Recall that $\chi: \text{Gal}_Q \to \hat{\mathbb{Z}}^\times$ satisfies $\sigma(\zeta) = \chi(\sigma) \mod n$ for any integer $n \geq 1$, where $\zeta \in \overline{\mathbb{Q}}$ is an $n$-th root of unity and $\sigma \in \text{Gal}_Q$.

We first show that index of $\rho_E(\text{Gal}_Q)$ in $\text{GL}_2(\hat{\mathbb{Z}})$ is determined by its commutator subgroup.

**Proposition 2.1.** We have $[\text{GL}_2(\hat{\mathbb{Z}}): \rho_E(\text{Gal}_Q)] = [\text{SL}_2(\hat{\mathbb{Z}}): \rho_E(\text{Gal}_Q)']$.

**Proof.** The character $\chi$ is surjective, so $\text{det}(\rho_E(\text{Gal}_Q)) = \hat{\mathbb{Z}}^\times$ and hence $\rho_E(\text{Gal}_Q) \cap \text{SL}_2(\hat{\mathbb{Z}}) = \rho_E(\text{Gal}_Q)_{\text{cyc}}$, where $\mathbb{Q}^{\text{cyc}}$ is the cyclotomic extension of $\mathbb{Q}$. We thus have

$$[\text{GL}_2(\hat{\mathbb{Z}}): \rho_E(\text{Gal}_Q)] = [\text{SL}_2(\hat{\mathbb{Z}}): \rho_E(\text{Gal}_Q) \cap \text{SL}_2(\hat{\mathbb{Z}})] = [\text{SL}_2(\hat{\mathbb{Z}}): \rho_E(\text{Gal}_Q^{\text{cyc}})].$$

It thus suffices to show that $\rho_E(\text{Gal}_Q^{\text{cyc}})$ equals $\rho_E(\text{Gal}_Q^{\text{ab}}) = \rho_E(\text{Gal}_Q)^{\prime}$, where $\mathbb{Q}^{\text{ab}} \subseteq \overline{\mathbb{Q}}$ is the maximal abelian extension of $\mathbb{Q}$. This follows from the Kronecker-Weber theorem which says that $\mathbb{Q}^{\text{cyc}} = \mathbb{Q}^{\text{ab}}$. \( \square \)

**Remark 2.2.**

(i) One can show that there are infinitely many different groups of the form $\rho_E(\text{Gal}_Q)$ as $E$ varies over non-CM elliptic curves over $\mathbb{Q}$; moreover, there are infinitely many such groups with index 2 in $\text{GL}_2(\hat{\mathbb{Z}})$. One consequence of Proposition 2.1 is that to compute the index $[\text{GL}_2(\hat{\mathbb{Z}}): \rho_E(\text{Gal}_Q)]$ one does not need to know the full group $\rho_E(\text{Gal}_Q)$, only $\rho_E(\text{Gal}_Q)^{\prime}$.

Conjecturally, there are only a finite number of subgroups of $\text{SL}_2(\hat{\mathbb{Z}})$ of the form $\rho_E(\text{Gal}_Q)^{\prime}$ with a non-CM $E/\mathbb{Q}$. Indeed, suppose that Conjecture 1.2 holds. Remark 1.6(i) and Proposition 2.1 implies that the index of $[\text{SL}_2(\hat{\mathbb{Z}}): \rho_E(\text{Gal}_Q)^{\prime}]$ is uniformly bounded for non-CM $E/\mathbb{Q}$. The finite number of possible groups of the form $\rho_E(\text{Gal}_Q)^{\prime}$ follows from their only being finitely many open subgroup of $\text{SL}_2(\hat{\mathbb{Z}})$ of a given index.

(ii) For a non-CM elliptic curve $E$ over a number field $K$, a similar argument shows that

$$[\text{GL}_2(\hat{\mathbb{Z}}): \rho_E(\text{Gal}_K)] \leq [\hat{\mathbb{Z}}^\times: \chi(\text{Gal}_K)] \cdot [\text{SL}_2(\hat{\mathbb{Z}}): \rho_E(\text{Gal}_K)^{\prime}].$$

The inequality may be strict if $K \neq \mathbb{Q}$ (the cyclotomic extension of $K$ does not agree with the maximal abelian extension of $K$).
The following corollary show that for an elliptic curve $E/\mathbb{Q}$, the index of $\rho_E(\text{Gal}_\mathbb{Q})$ in $\text{GL}_2(\mathbb{Z})$ depends only on the $\mathbb{Q}$-isomorphism class of $E$. In particular, the $j$-invariant is the correct notion to use in Theorems 1.4 and 1.5.

**Corollary 2.3.** For an elliptic curve $E$ over $\mathbb{Q}$, the index $[\text{GL}_2(\mathbb{Z}) : \rho_E(\text{Gal}_\mathbb{Q})]$ depends only on the $j$-invariant of $E$.

**Proof.** Suppose that $E_1$ and $E_2$ are elliptic curves over $\mathbb{Q}$ with the same $j$-invariant (and hence isomorphic over $\overline{\mathbb{Q}}$). If $E_1$ (and hence $E_2$) has complex multiplication, then both indices are infinite. We may thus assume that $E_1$ and $E_2$ are non-CM. Since they have the same $j$-invariant, $E_1$ and $E_2$ are isomorphic over a quadratic extension $L$ of $\mathbb{Q}$. Fixing such an isomorphism, we can identify the representations $\rho_{E_1}|_{\text{Gal}_L}$ and $\rho_{E_2}|_{\text{Gal}_L}$. We have $L \subseteq \mathbb{Q}^{ab}$, so the groups $\rho_{E_1}(\text{Gal}_{\mathbb{Q}^{ab}}) = \rho_{E_1}(\text{Gal}_\mathbb{Q})'$ and $\rho_{E_2}(\text{Gal}_{\mathbb{Q}^{ab}}) = \rho_{E_2}(\text{Gal}_\mathbb{Q})'$ are equal under this identification. The corollary then follows immediately from Proposition 2.1. 

\[ \square \]

3. Modular curves

Fix a positive integer $N$ and a subgroup $G$ of $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ containing $-I$ that satisfies $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$. Denote by $Y_G$ and $X_G$, the $\mathbb{Z}[1/N]$-schemes that are the coarse space of the algebraic stacks $\mathscr{M}_G[1/N]$ and $\mathscr{M}_G[1/N]$, respectively, from [DR73, IV §3]. We refer to [DR73, IV] for further details.

The $\mathbb{Z}[1/N]$-scheme $X_G$ is smooth and proper and $Y_G$ is an open subscheme of $X_G$. The complement of $Y_G$ in $X_G$, which we denote by $X_G^\infty$, is a finite étale scheme over $\mathbb{Z}[1/N]$, see [DR73, IV §5.2]. The fibers of $X_G$ are geometrically irreducible, see [DR73, IV Corollaire 5.6]; this uses our assumption that $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$.

In later sections, we will mostly work with the generic fiber of $X_G$, which we will also denote by $X_G$, which is a smooth, projective and geometrically irreducible curve over $\mathbb{Q}$ (similarly, we will work with the generic fiber of $Y_G$ which will be a non-empty open subvariety of $X_G$).

Fix a field $k$ whose characteristic does not divide $N$; for simplicity, we will also assume that $k$ is perfect. Choose an algebraic closure $\overline{k}$ of $k$ and set $\text{Gal}_k := \text{Gal}(\overline{k}/k)$.

In §3.1, we use the moduli property of $\mathscr{M}_G[1/N]$ to give a description of the sets $Y_G(k)$ and $Y_G(\overline{k})$. In §3.2, we describe the natural morphism from $Y_G$ to the $j$-line. In §3.3, we give a way to compute the cardinality of the finite set $X_G^\infty(k)$ of cusps of $X_G$ that are defined over $k$. In §3.4, we determine when the set $Y_G(\mathbb{R})$ is non-empty. In §3.5, we will observe that $Y_G(\mathbb{C})$ as a Riemann surface is isomorphic to the quotient of the upper-half plane by the congruence subgroup $\Gamma_G$ consisting of $A \in \text{SL}_2(\mathbb{Z})$ for which $A$ modulo $N$ lies $G$. Finally in §3.6, we explain how to compute the cardinality of $X_G(\mathbb{F}_p)$ for primes $p \nmid 6N$.

3.1. **Points of $Y_G$.** For an elliptic curve $E$ over $\overline{k}$, let $E[N]$ be the $N$-torsion subgroup of $E(\overline{k})$. A $G$-level structure for $E$ is an equivalence class $[\alpha]_G$ of group isomorphisms $\alpha : E[N] \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^2$, where we say that $\alpha$ and $\alpha'$ are equivalent if $\alpha = g \circ \alpha'$ for some $g \in G$. We say that two pairs $(E, [\alpha]_G)$ and $(E', [\alpha']_G)$, both consisting of an elliptic curve over $\overline{k}$ and a $G$-level structure, are **isomorphic** if there is an isomorphism $\phi : E \rightarrow E'$ of elliptic curves such that $[\alpha]_G = [\alpha' \circ \phi]_G$, where we also denote by $\phi$ the isomorphism $E[N] \rightarrow E'[N]$, $P \mapsto \phi(P)$.

From [DR73, IV Definition 3.2], $\mathscr{M}_G[1/N](\overline{k})$ is the category with objects $(E, [\alpha]_G)$, i.e., elliptic curves over $\overline{k}$ with a $G$-level structure, and morphisms being the isomorphisms between such pairs. Since $Y_G$ is the coarse space of $\mathscr{M}_G[1/N]$, we find that $Y_G(\overline{k})$ is the set of isomorphisms classes in $\mathscr{M}_G[1/N](\overline{k})$. 

4
The functoriality of \( \mathcal{M}_\mathbb{Z}[1/N] \), gives an action of the group \( \text{Gal}_k \) on \( Y_G(\bar{k}) \). Take any \( \sigma \in \text{Gal}_k \). Let \( E^\sigma \) be the base extension of \( E/\bar{k} \) by the morphism \( \text{Spec} \bar{k} \to \text{Spec} \bar{k} \) coming from \( \sigma \). The natural morphism \( E^\sigma \to E \) of schemes induces a group isomorphism \( E^\sigma[N] \to E[N] \) which, by abuse of notation, we will denote by \( \sigma \). More explicitly, if \( E \) is given by a Weierstrass equation \( y^2 + a_1xy + a_3y = x^3 + a_2x + a_6 \) with \( a_i \in \bar{k} \), we may take \( E^\sigma \) to be the curve defined by \( y^2 + \sigma(a_1)xy + \sigma(a_3)y = x^3 + \sigma(a_2)x + \sigma(a_6) \); the isomorphism \( E^\sigma[N] \to E[N] \) is then given by \( (x, y) \mapsto (\sigma^{-1}(x), \sigma^{-1}(y)) \). For a point \( P \in Y_G(\bar{k}) \) represented by a pair \( (E, [\alpha]_G) \), the point \( \sigma(P) \in Y_G(\bar{k}) \) is represented by \( (E^\sigma, [\alpha \circ \sigma^{-1}]_G) \).

Since \( k \) is perfect, \( Y_G(k) \) is the subset of \( Y_G(\bar{k}) \) stable under the action of \( \text{Gal}_k \). The following lemma describes \( Y_G(k) \). For an elliptic curve \( E \) over \( k \), let \( E[N] \) be the \( N \)-torsion subgroup of \( E(\bar{k}) \). Each \( \sigma \in \text{Gal}_k \) gives an isomorphism \( E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2 \) for some \( \phi \in \text{Aut}(E) \) and \( g \in G \).

**Lemma 3.1.**

(i) Every point \( P \in Y_G(k) \) is represented by a pair \( (E, [\alpha]_G) \) with \( E \) defined over \( k \).

(ii) Let \( P \in Y_G(\bar{k}) \) be a point represented by a pair \( (E, [\alpha]_G) \) with \( E \) defined over \( k \). Then \( P \) is an element of \( Y_G(k) \) if and only if for all \( \sigma \in \text{Gal}_k \), we have an equality

\[
\alpha \circ \sigma^{-1} = g \circ \alpha \circ \phi
\]

of isomorphisms \( E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2 \) for some \( \phi \in \text{Aut}(E) \) and \( g \in G \).

**Proof.** First suppose that \( (E, [\alpha]_G) \) represents a point \( P \in Y_G(k) \). To prove (i) it suffices to show that \( E \) is isomorphic over \( \bar{k} \) to an elliptic curve defined over \( k \). So we need only show that \( j_E \) is an element of \( k \). For any \( \sigma \in \text{Gal}_k \), the point \( P = \sigma(P) \) is also represented by \( (E^\sigma, [\alpha \circ \sigma^{-1}]_G) \). This implies that \( E \) and \( E^\sigma \) are isomorphic and hence \( \sigma(j_E) = j_E \). We thus have \( j_E \in k \) since \( k \) is perfect.

We now prove (ii). Let \( P \in Y_G(\bar{k}) \) be a point represented by a pair \( (E, [\alpha]_G) \) with \( E \) defined over \( k \). Take any \( \sigma \in \text{Gal}_k \). The point \( \sigma(P) \) is represented by \( (E^\sigma, [\alpha \circ \sigma^{-1}]_G) \); we can make the identification \( E = E^\sigma \) since \( E \) is defined over \( k \). We have \( \sigma(P) = P \) if and only if there is an automorphism \( \phi \in \text{Aut}(E) \) such that \( [\alpha \circ \sigma^{-1}]_G = [\alpha \circ \phi]_G \). Since \( k \) is perfect, we have \( P \in Y_G(k) \) if and only if for all \( \sigma \in \text{Gal}_k \), we have \([\alpha \circ \sigma^{-1}]_G = [\alpha \circ \phi]_G \) for some \( \phi \in \text{Aut}(E) \); this is a reformulation of part (ii). \( \square \)

3.2. **Morphism to the \( j \)-line.** If \( G = \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) \), then there is only a single \( G \)-level structure for each elliptic curve. There is an isomorphism \( Y_{\text{GL}_2(\mathbb{Z}/N\mathbb{Z})} = \mathbb{A}^1_{\mathbb{Z}[1/N]} \) on \( \bar{k} \)-points, it takes a point represented by a pair \( (E, [\alpha]_G) \) to the \( j \)-invariant \( j_E \in \bar{k} \).

If \( G' \) is a subgroup of \( \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) \) containing \( G \), then there is a natural morphism \( Y_G \to Y_{G'} \). In particular, \( G' = \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) \) gives a morphism

\[
\pi_G : Y_G \to \mathbb{A}^1_{\mathbb{Z}[1/N]}
\]

that maps a \( \bar{k} \)-point represented by a pair \( (E, [\alpha]_G) \) to the \( j \)-invariant of \( E \).

Fix an elliptic curve \( E \) over \( k \). By choosing a basis for \( E[N] \) as a \( \mathbb{Z}/N\mathbb{Z} \)-module, the Galois action on \( E[N] \) can be expressed in terms of a representation \( \rho_{E,N} : \text{Gal}_k \to \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) \); this is the same as the earlier definition with \( k = \mathbb{Q} \). The representation \( \rho_{E,N} \) is uniquely determined up to conjugation by an element of \( \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) \).

**Proposition 3.2.** Let \( E \) be an elliptic curve over \( k \) with \( j_E \notin \{0, 1728\} \). The group \( \rho_{E,N}(\text{Gal}_k) \) is conjugate in \( \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) \) to a subgroup of \( G \) if and only if \( j_E \) is an element of \( \pi_G(Y_G(k)) \).
Proof. First suppose that $\rho_{E,N}(\text{Gal}_k)$ is conjugate to a subgroup of $G$. There is thus an isomorphism $\alpha: E[N] \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^2$ such that $\alpha \circ \sigma \circ \alpha^{-1} \in G$ for all $\sigma \in \text{Gal}_k$. By Lemma 3.1(ii), with $\phi = 1$, the pair $(E,[\alpha]_G)$ represents a point $P \in Y_G(k)$. Therefore, $j_E = \pi_G(P)$ is an element of $\pi_G(Y_G(k))$.

Now suppose that $j_E = \pi_G(P)$ for some point $P \in Y_G(k)$. Lemma 3.1 implies that $P$ is represented by a pair $(E,[\alpha]_G)$, where for all $\sigma \in \text{Gal}_k$, we have $\alpha \circ \sigma^{-1} \circ \phi \circ \alpha^{-1} \in G$ for some automorphism $\phi$ of $E$. The assumption $j_E \notin \{0,1728\}$ implies that $\text{Aut}(E \bar{F}_k) = \{\pm 1\}$. In particular, every automorphism of $E \bar{F}_k$ acts on $E[N]$ as $\pm I$. Since $G$ contains $-I$, we deduce that $\alpha \circ \sigma^{-1} \circ \alpha^{-1} \in G$ for all $\sigma \in \text{Gal}_k$. We may choose $\rho_{E,N}$ so that $\rho_{E,N}(\sigma) = \alpha \circ \sigma \circ \alpha^{-1}$ for all $\sigma \in \text{Gal}_k$, and hence $\rho_{E,N}(\text{Gal}_k)$ is a subgroup of $G$. \hfill \Box

Take any $j \in k$ and fix an elliptic curve $E$ over $k$ with $j_E = j$. Let $M$ be the group of isomorphisms $E[N] \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^2$. Composition gives an action of the groups $G$ and $\text{Aut}(E \bar{F}_k)$ on $M$; they are left and right actions, respectively. The map $\alpha \in M \mapsto (E,[\alpha]_G)$ induces a bijection

$$G \backslash M / \text{Aut}(E \bar{F}_k) \xrightarrow{\sim} \{P \in Y_G(k) : \pi_G(P) = j\}.$$ 

The group $\text{Gal}_k$ acts on $M$ by the map $\text{Gal}_k \times M \rightarrow M$, $(\sigma,\alpha) \mapsto \alpha \circ \sigma^{-1}$, from the description of the Galois action in §3.1, we find that the bijection (3.1) respects the $\text{Gal}_k$-actions. The following lemma is now immediate (again we are using that $k$ is perfect).

Lemma 3.3. The set $\{P \in Y_G(k) : \pi_G(P) = j\}$ has the same cardinality as the subset of $G \backslash M / \text{Aut}(E \bar{F}_k)$ fixed by the $\text{Gal}_k$-action.

3.3. Cusps. In this section, we state an analogue of Lemma 3.3 for $X_G^\infty(k)$. Let $M$ be the group of isomorphisms $\mu_N \times \mathbb{Z}/N\mathbb{Z} \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^2$, where $\mu_N$ is the group of $N$-th roots of unity in $\mathbb{F}$. The group $\text{Gal}_k$ acts on $M$ by the map $\text{Gal}_k \times M \rightarrow M$, $(\sigma,\alpha) \mapsto \alpha \circ \sigma^{-1}$, where $\sigma^{-1}$ acts on $\mu_N$ as usual and trivially on $\mathbb{Z}/N\mathbb{Z}$. Let $U$ be the subgroup of $\text{Aut}(\mu_N \times \mathbb{Z}/N\mathbb{Z})$ given by the matrices $\pm \left( \begin{smallmatrix} u & 1 \\ 0 & 1 \end{smallmatrix} \right)$ with $u \in \text{Hom}(\mathbb{Z}/N\mathbb{Z},\mu_N)$. Composition gives an action of the groups $G$ and $U$ on $M$; they are left and right actions, respectively. Construction 5.3 of [DR73, VI] shows that there is a bijection

$$X_G^\infty(\mathbb{F}) \xrightarrow{\sim} G \backslash M / U$$

that respects the actions of $\text{Gal}_k$. We thus have a bijection between $X_G^\infty(k)$ and the subset of $G \backslash M / U$ fixed by the action of $\text{Gal}_k$.

Observe that the cardinality of $X_G^\infty(k)$ depends only on $G$ and the image of the character $\chi_N: \text{Gal}_k \rightarrow (\mathbb{Z}/N\mathbb{Z})^\times$ describing the Galois action on $\mu_N$, i.e., $\sigma(\zeta) = \zeta^{\chi_N(\sigma)}$ for all $\sigma \in \text{Gal}_k$ and all $\zeta \in \mu_N$. Let $B$ be the subgroup of $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ consisting of matrices of the form $\left( \begin{smallmatrix} b & 0 \\ 0 & 1 \end{smallmatrix} \right)$ with $b \in \chi_N(\text{Gal}_k)$. Let $U$ be the subgroup of $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ generated by $-I$ and $\left( \begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} \right)$. The group $B$ normalizes $U$ and hence right multiplication gives a well-defined action of $B$ on $X_G^\infty(\mathbb{F})$. The following lemma is now immediate.

Lemma 3.4. The set $X_G^\infty(k)$ has the same cardinality as the subset of $G \backslash \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) / U$ fixed by right multiplication by $B$.

3.4. Real points. The following proposition tells us when $Y_G(\mathbb{R})$ is non-empty.

Proposition 3.5. The set $Y_G(\mathbb{R})$ is non-empty if and only if $G$ contains an element that is conjugate in $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ to $\left( \begin{smallmatrix} 0 & 0 \\ 1 & -1 \end{smallmatrix} \right)$ or $\left( \begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix} \right)$.

Proof. Let $E$ be any elliptic curve over $\mathbb{R}$. As a topological group, the identity component of $E(\mathbb{R})$ is isomorphic to $\mathbb{R}/\mathbb{Z}$. So there is a point $P_1 \in E(\mathbb{R})$ of order $N$. Choose a second point $P_2 \in E(\mathbb{C})$ so that $\{P_1,P_2\}$ is a basis of $E[N]$ as a $\mathbb{Z}/N\mathbb{Z}$-module. Define $\rho_{E,N}$ with respect to this basis.

Let $\sigma \in \text{Aut}(\mathbb{C}/\mathbb{R})$ be the complex conjugation automorphism. We have $\sigma(P_1) = P_1$ and $\sigma(P_2) = bP_1 + dP_2$ for some $b,d \in \mathbb{Z}/N\mathbb{Z}$, i.e., $\rho_{E,N}(\sigma) := \left( \begin{smallmatrix} b & 0 \\ d & 1 \end{smallmatrix} \right) \in \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Using the Weil pairing, we find that $\det(\rho_{E,N}(\sigma))$ describes how $\sigma$ acts on the $N$-th roots of unity. Since complex conjugation
contains an element that is conjugate in \( GL \)
inverts roots of unity, we have \( \det(\rho_{E,N}(\sigma)) = -1 \) and hence \( d = -1 \). For a fixed \( m \in \mathbb{Z}/\mathbb{N} \), define points \( P'_1 := P_1 \) and \( P'_2 := P_2 + mP_1 \). The points \( \{P'_1, P'_2\} \) are a basis for \( E[\mathbb{N}] \), and we have
\[
\sigma(P'_1) = \sigma(P'_2) = (bP_1 - P_2) + mP_1 = -(P_2 + mP_1) + (b + 2m)P_1 = -P'_2 + (b + 2m)P'_1.
\]

We can choose \( m \) so that \( b + 2m \) is congruent to 0 or 1 modulo \( N \); with such an \( m \) and the choice of basis \( \{P'_1, P'_2\} \), the matrix \( \rho_{E,N}(\sigma) \) will be \( \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \) or \( \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \).

We claim that both of the matrices \( \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \) and \( \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \) are conjugate to \( \rho_{E,N}(\sigma) \) for some \( E/\mathbb{R} \) with \( j_E \not\in \{0,1728\} \). This is clear if \( N \) is odd since the two matrices are then conjugate (we could have solved for \( m \) in either of the congruences above). If \( N \) is even, then it suffices to show that both possibilities occur when \( N = 2 \); this is easy (if \( E/\mathbb{Q} \) is given by a Weierstrass equation \( y^2 = x^3 + ax + b \), the two possibilities are distinguished by the number of real roots that \( x^3 + ax + b \) has).

Using Proposition 3.2, we deduce that \( \pi_G(Y_G(\mathbb{R})) - \{0,1728\} \) is non-empty if and only if \( G \) contains an element that is conjugate in \( GL_2(\mathbb{Z}/\mathbb{N} \mathbb{Z}) \) to \( \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \) or \( \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \). To complete the proof of the proposition, we need to show that if \( \pi_G(Y_G(\mathbb{R})) \subseteq \{0,1728\} \), then \( \pi_G(Y_G(\mathbb{R})) \) is empty. So suppose that \( \pi_G(Y_G(\mathbb{R})) \subseteq \{0,1728\} \) and hence \( Y_G(\mathbb{R}) \) is finite. However, since \( Y_G \) over \( \mathbb{Q} \) is a smooth, geometrically irreducible curve, the set \( Y_G(\mathbb{R}) \) is either empty or infinite. \( \square \)

3.5. Complex points. The complex points \( Y_G(\mathbb{C}) \) form a Riemann surface. In this section, we describe it as a familiar quotient of the upper half plane by a congruence subgroup.

Let \( \mathfrak{H} \) be the complex upper half plane. For \( z \in \mathfrak{H} \) and \( \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \), set \( \gamma(z) := (az + b)/(cz + d) \). We let \( SL_2(\mathbb{Z}) \) act on the right of \( \mathfrak{H} \) by \( SL_2(\mathbb{Z}) \to \mathfrak{H}, (z, \gamma) \mapsto \gamma z \), where \( \gamma^t \) is the transpose of \( \gamma \). For a congruence subgroup \( \Gamma \), the quotient \( \mathcal{H}/\Gamma \) is a smooth Riemann surface.

We define the genus of a congruence subgroup \( \Gamma \) to be the genus of the Riemann surface \( \mathcal{H}/\Gamma \).

Remark 3.6. One could also consider the quotient \( \Gamma \backslash \mathfrak{H} \) of \( \mathfrak{H} \) under the left action given by \( (\gamma, z) \mapsto \gamma z \); it is isomorphic to the Riemann surface \( \mathcal{H}/\Gamma \) (use that \( \gamma^t = B \gamma^{-1} B^{-1} \) for all \( \gamma \in \Gamma \), where \( B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \)). In particular, the genus of \( \Gamma \backslash \mathfrak{H} \) agrees with the genus of \( \Gamma \).

Let \( \Gamma_G \) be the congruence subgroup consisting of matrices \( \gamma \in SL_2(\mathbb{Z}) \) whose image modulo \( N \) lies in \( G \). The image of \( \Gamma_G \) modulo \( N \) is \( G \cap SL_2(\mathbb{Z}/\mathbb{N} \mathbb{Z}) \) since the reduction map \( SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/\mathbb{N} \mathbb{Z}) \) is surjective. In particular, \( \Gamma_G \) depends only on the group \( G \cap SL_2(\mathbb{Z}/\mathbb{N} \mathbb{Z}) \) and we have
\[
[SL_2(\mathbb{Z}) : \Gamma_G] = [SL_2(\mathbb{Z}/\mathbb{N} \mathbb{Z}) : G \cap SL_2(\mathbb{Z}/\mathbb{N} \mathbb{Z})].
\]

Proposition 3.7. The Riemann surfaces \( Y_G(\mathbb{C}) \) and \( \mathcal{H}/\Gamma_G \) are isomorphic. In particular, the genus of \( Y_G \) is equal to the genus of \( \mathcal{H}/\Gamma_G \).

Proof. Set \( X^\pm := \mathbb{C} - \mathbb{R} \); we let \( GL_2(\mathbb{Z}) \) act on the right in the same manner \( SL_2(\mathbb{Z}) \) acts on \( \mathfrak{H} \). We also let \( GL_2(\mathbb{Z}) \) act on the right of \( G \backslash GL_2(\mathbb{Z}/\mathbb{N} \mathbb{Z}) \) by right multiplication. From [DR73, IV §5.3], we have an isomorphism
\[
Y_G(\mathbb{C}) \cong (X^\pm \times (G \backslash GL_2(\mathbb{Z}/\mathbb{N} \mathbb{Z}))) / GL_2(\mathbb{Z}).
\]

Using that \( \det(G) = (\mathbb{Z}/\mathbb{N} \mathbb{Z})^\times \) and setting \( H := G \cap SL_2(\mathbb{Z}/\mathbb{N} \mathbb{Z}) \), we find that the natural maps
\[
(\mathcal{H} \times (G \backslash GL_2(\mathbb{Z}/\mathbb{N} \mathbb{Z}))) / SL_2(\mathbb{Z}) \to (X^\pm \times (G \backslash GL_2(\mathbb{Z}/\mathbb{N} \mathbb{Z}))) / GL_2(\mathbb{Z})
\]
and
\[
(\mathcal{H} \times (H \backslash SL_2(\mathbb{Z}/\mathbb{N} \mathbb{Z}))) / SL_2(\mathbb{Z}) \to (\mathcal{H} \times (G \backslash GL_2(\mathbb{Z}/\mathbb{N} \mathbb{Z}))) / SL_2(\mathbb{Z})
\]
are isomorphisms of Riemann surfaces. It thus suffices to show that \( \mathcal{H}/\Gamma_G \) and \( (\mathcal{H} \times (H \backslash SL_2(\mathbb{Z}/\mathbb{N} \mathbb{Z}))) / SL_2(\mathbb{Z}) \) are isomorphic. Define the map
\[
\varphi : \mathcal{H}/\Gamma_G \to (\mathcal{H} \times (H \backslash SL_2(\mathbb{Z}/\mathbb{N} \mathbb{Z}))) / SL_2(\mathbb{Z})
\]
that takes a class containing \( z \) to the class represented by \( (z, H \cdot I) \). For \( \gamma \in \text{SL}_2(\mathbb{Z}) \), the pairs \( (z, H \cdot I) \) and \( (\gamma'(z), H \cdot \gamma^{-1}) \) lies in the same class of \( (\mathfrak{g} \times (\text{SL}_2(\mathbb{Z})/\mathbb{N}\mathbb{Z}))/\text{SL}_2(\mathbb{Z}) \); from this one readily deduced that \( \varphi \) is well-defined and injective. It is straightforward to check that \( \varphi \) is an isomorphism of Riemann surfaces. \( \square \)

3.6. \( \mathbb{F}_p \)-points. Fix a prime \( p \nmid 6N \) and an algebraic closure \( \overline{\mathbb{F}}_p \) of \( \mathbb{F}_p \). The Galois group \( \text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \) is topologically generated by the automorphism \( \text{Frob}_p \colon x \mapsto x^p \). In this section, we will describe how to compute \( |X_G(\mathbb{F}_p)| \).

For an imaginary quadratic order \( \mathcal{O} \) of discriminant \( D \), the \( j \)-invariant of the complex elliptic curve \( \mathbb{C}/\mathcal{O} \) is an algebraic integer; its minimal polynomial \( P_D(x) \in \mathbb{Z}[x] \) is the Hilbert class polynomial of \( \mathcal{O} \). For an integer \( D < 0 \) which is not the discriminant of a quadratic order, we set \( P_D(x) = 1 \).

Fix an elliptic curve \( E \) over \( \mathbb{F}_p \) with \( j_E \notin \{0, 1728\} \). Let \( a_E \) be the integer \( p + 1 - |E(\mathbb{F}_p)| \). Set \( \Delta_E := a_E^2 - 4p \); we have \( \Delta_E \neq 0 \) by the Hasse inequality. Let \( b_E \) be the largest integer \( b \geq 1 \) such that \( b^2|\Delta_E \) and \( P_{\Delta_E/b^2}(j_E) = 0 \); this is well-defined since we will always have \( P_{\Delta_E}(j_E) = 0 \). Define the matrix
\[
\Phi_E := \begin{pmatrix} (a_E - \Delta_E/b_E)/2 & \Delta_E/b_E \cdot (1 - \Delta_E/b_E^2)/4 \\ b_E & (a_E + \Delta_E/b_E)/2 \end{pmatrix};
\]
it has integer entries since \( \Delta_E/b_E^2 \) is an integer congruent to 0 or 1 modulo 4 (it is the discriminant of a quadratic order) and \( \Delta_E \equiv a_E \pmod{2} \). One can check that \( \Phi_E \) has trace \( a_E \) and determinant \( p \). In practice, \( \Phi_E \) is straightforward to compute; there are many good algorithms to compute \( a_E \) and \( P_D(x) \).

The following proposition shows that \( \Phi_E \) describes \( \rho_{E,N}(\text{Frob}_p) \), and hence also \( \rho_{E,N} \), up to conjugacy.

**Proposition 3.8.** With notation as above, the reduction of \( \Phi_E \) modulo \( N \) is conjugate in \( \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) \) to \( \rho_{E,N}(\text{Frob}_p) \).

**Proof.** It suffices to prove the proposition when \( N \) is a prime power. For \( N \) a prime power, it is then a consequence of Theorem 2 in [Cen16]. \( \square \)

We now explain how to compute \( |X_G(\mathbb{F}_p)| \). We can compute \( |X_G^\mathbb{F}_p(\mathbb{F}_p)| \) using Lemma 3.4 (with \( k = \mathbb{F}_p \), the subgroup \( \chi_N(\text{Gal}_{\mathbb{F}_p}) \) of \( (\mathbb{Z}/N\mathbb{Z})^\times \) is generated by \( p \) modulo \( N \)). So we need only describe how to compute \( |Y_G(\mathbb{F}_p)| \); it thus suffices to compute each term in the sum
\[
|Y_G(\mathbb{F}_p)| = \sum_{j \in \mathbb{F}_p} |\{P \in Y_G(\mathbb{F}_p) : \pi_G(P) = j\}|.
\]
Take any \( j \in \mathbb{F}_p \) and fix an elliptic curve \( E \) over \( \mathbb{F}_p \) with \( j_E = j \).

First suppose that \( j \notin \{0, 1728\} \). We have \( \text{Aut}(E_{\mathbb{F}_p}) = \{\pm I\} \) and hence each automorphism acts on \( E[N] \) by \( I \) or \( -I \). Let \( M \) be the group of isomorphisms \( E[N] \stackrel{\sim}{\to} (\mathbb{Z}/N\mathbb{Z})^2 \). Since \( -I \in G \), we have \( G/M/\text{Aut}(E_{\mathbb{F}_p}) = G \setminus M \). Lemma 3.3 implies that \( |\{P \in Y_G(\mathbb{F}_p) : \pi_G(P) = j\}| \) is equal to cardinality of the subset of \( G \setminus M \) fixed by the action of \( \text{Frob}_p \). By Proposition 3.8 and choosing an appropriate basis of \( E[N] \), we deduce that \( |\{P \in Y_G(\mathbb{F}_p) : \pi_G(P) = j\}| \) is equal to the cardinality of the subset of \( G \setminus \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) \) fixed by right multiplication by \( \Phi_E \). In particular, note that we can compute \( |\{P \in Y_G(\mathbb{F}_p) : \pi_G(P) = j\}| \) without having to compute \( E[N] \).

Now suppose that \( j \in \{0, 1728\} \) and recall that \( p \nmid 6 \). When \( j = 0 \), we take \( E/\mathbb{F}_p \) to be the curve defined by \( y^2 = x^3 - 1 \); the group \( \text{Aut}(E_{\mathbb{F}_p}) \) is cyclic of order 6 and generated by \( (x, y) \mapsto (\zeta x, -y) \),
where $\zeta \in \mathbb{F}_p$ is a cube root of unity. When $j = 1728$, we take $E/\mathbb{F}_p$ to be the curve defined by $y^2 = x^3 - x$; the group $\text{Aut}(E/\mathbb{F}_p)$ is cyclic of order 6 and generated by $(x, y) \mapsto (-x, \zeta y)$, where $\zeta \in \mathbb{F}_p$ is a fourth root of unity.

One can compute an explicit basis of $E[N]$. With respect to this basis, the action of $\text{Aut}(E/\mathbb{F}_p)$ on $E[N]$ corresponds to a subgroup $\mathcal{A}$ of $GL_2(\mathbb{Z}/N\mathbb{Z})$ and the action of Frobenius on $E[N]$ corresponds to a matrix $\Phi_{E,N} \in GL_2(\mathbb{Z}/N\mathbb{Z})$. Lemma 3.3 implies that $|\{P \in Y_G(\mathbb{F}_p) : \pi_G(P) = j\}|$ equals the number of elements in $G \setminus GL_2(\mathbb{Z}/N\mathbb{Z})/\mathcal{A}$ that are fixed by right multiplication by $\Phi_{E,N}$.

4. Preliminary work

Take any congruence subgroup $\Gamma$ of $SL_2(\mathbb{Z})$ and denote its level by $N_0$. Let $\pm \Gamma$ be the congruence subgroup generated by $\Gamma$ and $-I$. Let $N$ be the integer $N_0$, $4N_0$ or $2N_0$ when $v_2(N_0)$ is 0, 1 or at least 2, respectively.

**Definition 4.1.** We define $\mathcal{I}(\Gamma)$ to be the set of integers

$$[SL_2(\mathbb{Z}/N) : G'] \cdot 2/\gcd(2, N),$$

where $G$ varies over the open subgroups of $GL_2(\mathbb{Z}/N)$ that are the inverse image by the reduction map $GL_2(\mathbb{Z}/N) \to GL_2(\mathbb{Z}/N \mathbb{Z})$ of a subgroup $G(N) \subseteq GL_2(\mathbb{Z}/N \mathbb{Z})$ which satisfies the following conditions:

(a) $G(N) \cap SL_2(\mathbb{Z}/N \mathbb{Z})$ is equal to $\pm \Gamma$ modulo $N$,

(b) $G(N) \supseteq (\mathbb{Z}/N \mathbb{Z})^\times \cdot I$,

(c) $\det(G(N)) = (\mathbb{Z}/N \mathbb{Z})^\times$,

(d) $G(N)$ contains a matrix that is conjugate to $(1 0^{-1})$ or $(1 1^{-1})$ in $GL_2(\mathbb{Z}/N \mathbb{Z})$,

(e) the set $X_{G(N)}(\mathbb{Q})$ is infinite.

The set $\mathcal{I}(\Gamma)$ is finite since there are only finitely many possible $G(N)$ for a fixed $N$. In the special case $N = 1$, we view $GL_2(\mathbb{Z}/1)$ and $SL_2(\mathbb{Z}/1)$ as trivial groups and hence we find that $\mathcal{I}(SL_2(\mathbb{Z})) = \{2\}$. Define the set of integers

$$\mathcal{I} := \bigcup_{\Gamma} \mathcal{I}(\Gamma),$$

where the union is over the congruence subgroups of $SL_2(\mathbb{Z})$ that have genus 0 or 1. The set $\mathcal{I}$ is finite since there are only finitely many congruence subgroups of genus 0 or 1, see [CP03].

The goal of this section is to prove the following theorem.

**Theorem 4.2.** Fix an integer $c$. There is a finite set $J$, depending only on $c$, such that if $E/\mathbb{Q}$ is an elliptic curve with $j_E \notin J$ and $\rho_{E,\ell}$ surjective for all primes $\ell > c$, then $[GL_2(\mathbb{Z}) : \rho_E(\text{Gal}_{\mathbb{Q}})]$ is an element of $\mathcal{I}$.

In §5, we will compute $\mathcal{I}$ and show that it is equal to the set $\mathcal{I}$ from §1; this will prove Theorem 1.3.

4.1. The congruence subgroup $\Gamma_E$. Fix a non-CM elliptic curve $E$ over $\mathbb{Q}$. Define the subgroup

$$G := \hat{\mathbb{Z}}^\times \cdot \rho_E(\text{Gal}_{\mathbb{Q}})$$

of $GL_2(\mathbb{Z})$. For each positive integer $n$, let $G_n$ be the image of $G$ under the projection map $GL_2(\mathbb{Z}) \to GL_2(\mathbb{Z}/n)$. By Serre’s theorem, $G$ is an open subgroup of $GL_2(\mathbb{Z})$. We have an equality $G' = \rho_E(\text{Gal}_{\mathbb{Q}})'$ of commutator subgroups and hence

$$[GL_2(\mathbb{Z}) : \rho_E(\text{Gal}_{\mathbb{Q}})] = [SL_2(\mathbb{Z}) : G']$$

(4.1)
Proposition 4.3. The subgroup $\Gamma = \Gamma_0$ of $\text{SL}_2(\mathbb{Z})$ obtained by Proposition 2.1. There is no harm in working with the larger group $G$ since we are only concerned about the index $[\text{GL}_2(\mathbb{Z}) : \rho_E(\text{Gal}_\mathbb{Q})]$.

Let $m$ be the product of the primes $\ell$ for which $\ell \leq 5$ or for which $\rho_{E,\ell}$ is not surjective. The group $G_m \cap \text{SL}_2(\mathbb{Z}_m)$ is open in $\text{SL}_2(\mathbb{Z}_m)$. Let $N_0 \geq 1$ be the smallest positive integer dividing some power of $m$ for which

$$G_m \cap \text{SL}_2(\mathbb{Z}_m) \supseteq \{ A \in \text{SL}_2(\mathbb{Z}_m) : A \equiv I \pmod{N_0} \}. \tag{4.2}$$

Let $N$ be the integer $N_0$, $4N_0$ or $2N_0$ when $v_2(N_0)$ is 0, 1 or at least 2, respectively.

Define $\Gamma_E := \Gamma_{G(N)}$; it is the congruence subgroup consisting of matrices in $\text{SL}_2(\mathbb{Z})$ whose image modulo $N$ lies in $G(N)$. Note that the congruence subgroup $\Gamma_E$ has level $N_0$ and contains $-I$.

**Proposition 4.3.** The subgroup $G(N)$ of $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ satisfies conditions (a), (b), (c) and (d) of Definition 4.1 with $\Gamma = \Gamma_E$.

**Proof.** Our congruence subgroup $\Gamma_E$ contains $-I$ and was chosen so that $\Gamma_E$ modulo $N$ equals $G(N) \cap \text{SL}_2(\mathbb{Z}/N\mathbb{Z})$. We have $G \supseteq \hat{\mathbb{Z}}^\times \cdot I$, so $G(N) \supseteq (\mathbb{Z}/N\mathbb{Z})^\times \cdot I$. We have $\det(\rho_E(\text{Gal}_\mathbb{Q})) = \hat{\mathbb{Z}}^\times$, so $\det(G(N)) = (\mathbb{Z}/N\mathbb{Z})^\times$.

It remains to show that condition (d) holds. Since $E/\mathbb{Q}$ is non-CM and $\rho_{E,N}(\text{Gal}_\mathbb{Q})$ is a subgroup of $G(N)$, we have $Y_{G(N)}(\mathbb{Q}) \not\equiv 0$ by Proposition 3.2. In particular, $Y_{G(N)}(\mathbb{R}) \not\equiv 0$. Proposition 3.5 implies that $G$ contains an element that is conjugate in $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ to $\left( \begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix} \right)$ or $\left( \begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix} \right)$. \hfill $\square$

The following lemma shows that $G_N$ is determined by $G(N)$.

**Lemma 4.4.** The group $G_N$ is the inverse image of $G(N)$ under the reduction modulo $N$ map $\text{GL}_2(\mathbb{Z}_N) \to \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

**Proof.** Take any $A \in \text{GL}_2(\mathbb{Z}_N)$ satisfying $A \equiv I \pmod{N}$; we need only verify that $A$ is an element of $G_N$. Our integer $N$ has the property that $(1 + N_0\mathbb{Z}_N)^2 = 1 + N\mathbb{Z}_N$. Since $\det(A) \equiv 1 \pmod{N}$, we have $\det(A) = \lambda^2$ for some $\lambda \in 1 + N_0\mathbb{Z}_N$. Define $B := \lambda^{-1}A$; it is an element of $\text{SL}_2(\mathbb{Z}_N)$ that is congruent to $I$ modulo $N_0$. Using (4.2), we deduce that $B$ is an element of $G_N$. From the definition of $G$, it is clear that $G_N$ contains the scalar matrix $\lambda I$. Therefore, $A = \lambda I \cdot B$ is an element of $G_N$. \hfill $\square$

The following group theoretical lemma will be proved in §4.4.

**Lemma 4.5.** We have

$$[\text{SL}_2(\mathbb{Z}_N) : G'] = [\text{SL}_2(\mathbb{Z}_m) : G'_m] = [\text{SL}_2(\mathbb{Z}_N) : G_N'] \cdot 2 / \gcd(2, N).$$

Moreover, $G' = G'_m \times \prod_{\ell | m} \text{SL}_2(\mathbb{Z}_\ell)$.

The following lemma motivates our definition of $\mathcal{I}$.

**Lemma 4.6.** If $X_{G(N)}(\mathbb{Q})$ is infinite, then $[\text{GL}_2(\mathbb{Z}) : \rho_E(\text{Gal}_\mathbb{Q})]$ is an element of $\mathcal{I}$.

**Proof.** By Lemma 4.5 and (4.1), we have $[\text{GL}_2(\mathbb{Z}) : \rho_E(\text{Gal}_\mathbb{Q})] = [\text{SL}_2(\mathbb{Z}_N) : G_N'] \cdot 2 / \gcd(2, N)$.

The group $G(N)$ satisfies conditions (a), (b), (c) and (d) of Definition 4.1 with $\Gamma = \Gamma_E$ by Lemma 4.4. The group $G(N)$ satisfies (e) by assumption. Using Lemma 4.4, we deduce that $[\text{SL}_2(\mathbb{Z}_N) : G_N'] \cdot 2 / \gcd(2, N)$ is an element of $\mathcal{I}(\Gamma_E)$.

To complete the proof of the lemma, we need to show that $\Gamma_E$ has genus 0 or 1 since then $\mathcal{I}(\Gamma_E) \subseteq \mathcal{I}$. The genus of $\Gamma_E$ is equal to the genus of $X_{G(N)}$ by Proposition 3.7. Since $X_{G(N)}$ has infinitely many rational point, it must have genus 0 or 1 by Faltings’ theorem. \hfill $\square$
4.2. Exceptional rational points on modular curves. Let $S$ be the set of pairs $(N, G)$ with $N \geq 1$ an integer not divisible by any prime $\ell > 13$ and with $G$ a subgroup of $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ satisfying the following conditions:

- $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$ and $-I \in G$,
- $X_G$ has genus at least 2 or $X_G(\mathbb{Q})$ is finite.

Define the set

$$J : = \bigcup_{(N, G) \in S} \pi_G(Y_G(\mathbb{Q})).$$

We will prove that $J$ is finite. We will need the following lemma.

Lemma 4.7. Fix an integer $m \geq 2$. An open subgroup $H$ of $\text{GL}_2(\mathbb{Z}_m)$ has only a finite number of closed maximal subgroups and they are all open.

Proof. The lemma follows from the proposition in [Ser97, §10.6] which gives a condition for the Frattini subgroup of $H$ to be open; note that $H$ contains a normal subgroup of the form $I + m^e M_2(\mathbb{Z}_m)$ for some $e \geq 1$ and that $I + m^e M_2(\mathbb{Z}_m)$ is the product of pro-$\ell$ groups with $\ell | m$. □

Proposition 4.8. The set $J$ is finite.

Proof. Fix pairs $(N, G), (N', G') \in S$ such that $N$ is a divisor of $N'$ and such that reduction modulo $N$ gives a well-defined map $G' \to G$. This gives rise to a morphism $\varphi : Y_{G'} \to Y_G$ of curves over $\mathbb{Q}$ such that $\pi_G \circ \varphi = \pi_{G'}$. In particular, $\pi_{G'}(Y_{G'}(\mathbb{Q})) \subseteq \pi_G(Y_G(\mathbb{Q}))$. Therefore,

$$J = \bigcup_{(N, G) \in S'} \pi_G(Y_G(\mathbb{Q})),
$$

where $S'$ is the set of pairs $(N, G) \in S$ for which there is no pair $(N', G') \in S - \{(N, G)\}$ with $N'$ a divisor of $N$ so that the reduction modulo $N'$ defines a map $G \to G'$. For each pair $(N, G) \in S'$, the set $Y_G(\mathbb{Q})$, and hence also $\pi_G(Y_G(\mathbb{Q}))$, is finite. The finiteness is immediate from the definition of $S$ when $Y_G$ has genus 0 or 1. If $Y_G$ has genus at least 2, then $Y_G(\mathbb{Q})$ is finite by Faltings’ theorem. So to prove that $J$ is finite, it suffices to show that $S'$ is finite.

Let $m$ be the product of primes $\ell \leq 13$. For each pair $(N, G) \in S'$, let $\bar{G}$ be the open subgroup of $\text{GL}_2(\mathbb{Z}_m)$ that is the inverse image of $G$ under the reduction map $\text{GL}_2(\mathbb{Z}_m) \to \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Note that we can recover the pair $(N, G)$ from $\bar{G}; N \geq 1$ is the smallest integer (not divisible by primes $\ell > 13$) such that $\bar{G}$ contains $\{A \in \text{GL}_2(\mathbb{Z}_m) : A \equiv I \mod{N}\}$ and $G$ is the image of $\bar{G}$ in $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Define the set

$$G := \{\bar{G} : (N, G) \in S'\}.$$

We have $|G| = |S'|$, so it suffices to show that the set $G$ is finite.

Suppose that $G$ is infinite. We now recursively define a sequence $\{M_i\}_{i \geq 0}$ of open subgroups of $\text{GL}_2(\mathbb{Z}_m)$ such that

$$M_0 \supseteq M_1 \supseteq M_2 \supseteq M_3 \supseteq \ldots$$

and such that each $M_i$ has infinitely many subgroups in $G$. Set $M_0 := \text{GL}_2(\mathbb{Z}_m)$. Take an $i \geq 0$ for which $M_i$ has been defined and has infinitely many subgroups in $G$. Since $M_i$ has only finite many open maximal subgroups by Lemma 4.7, one of the them contains infinitely many subgroups in $G$; denote such a maximal subgroup by $M_{i+1}$.

Take any $i \geq 0$. Since there are elements of $G$ that are proper subgroups of $M_i$, we deduce that $M_i \supseteq \bar{G}$ for some pair $(N, G) \in S'$. The group $G = \bar{G}(N)$ is thus a proper subgroup of $M_i(N) \subseteq \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$. We have $\det(M_i(N)) = (\mathbb{Z}/N\mathbb{Z})^\times$ and $-I \in M_i(N)$ since $G$ has these properties. We have $(N, M_i(N)) \notin S$ since otherwise $(N, G)$ would not be an element of $S'$. Therefore, the modular curve $X_{M_i(N)}$ has genus 0 or 1. By Proposition 3.7, the congruence subgroup
\[ \Gamma_i := \Gamma_{M_i(N)} \] (which consists of \( A \in \text{SL}_2(\mathbb{Z}) \) with \( A \) modulo \( N \) in \( M_i(N) \)) has genus 0 or 1. We have

\[ [\text{SL}_2(\mathbb{Z}) : \Gamma_i] = [\text{SL}_2(\mathbb{Z}/N\mathbb{Z}) : M_i(N) \cap \text{SL}_2(\mathbb{Z}/N\mathbb{Z})] = [\text{GL}_2(\mathbb{Z}/N\mathbb{Z}) : M_i(N)] = [\text{GL}_2(\mathbb{Z}_m) : M_i], \]

so \([\text{SL}_2(\mathbb{Z}) : \Gamma_i] \to \infty \) as \( i \to \infty \) by the proper inclusions (4.3). In particular, there are infinitely many congruence subgroup of genus 0 or 1. However, there are only finitely many congruence subgroups of \( \text{SL}_2(\mathbb{Z}) \) of genus 0 and 1; moreover, the level of such congruence subgroups is at most \( 52 \) by [CP03]. This contradiction implies that \( \mathcal{G} \), and hence \( \mathcal{G}' \), is finite. \( \square \)

For each prime \( \ell \), let \( \mathcal{J}_\ell \) be the set of \( j \)-invariants of elliptic curves \( E/\mathbb{Q} \) for which \( \rho_{E,\ell} \) is not surjective.

**Proposition 4.9.** The set \( \mathcal{J}_\ell \) is finite for all primes \( \ell > 13 \).

**Proof.** Fix a prime \( \ell > 13 \). By Proposition 3.2, it suffices to show that \( X_G(\mathbb{Q}) \) is finite for each of the maximal subgroups \( G \) of \( \text{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \) that satisfy \( \text{det}(G) = (\mathbb{Z}/\ell\mathbb{Z})^\times \). Fix such a group \( G \) and let \( \Gamma = \text{G} \) be the congruence subgroup consisting of \( A \in \text{SL}_2(\mathbb{Z}) \) for which \( A \) modulo \( N \) lies in \( G \). The curve \( X_G \) has the same genus as \( \Gamma \) by Proposition 3.7. If \( \Gamma \) has genus at least 2, then \( X_G(\mathbb{Q}) \) is finite by Faltings’ theorem.

We may thus suppose that \( \Gamma \) has genus 0 or 1. From the description of congruence subgroups of genus 0 and 1 in [CP03], we find that \( \ell \in \{17, 19\} \) and that \( \Gamma \) modulo \( \ell \) contains an element of order \( \ell \). Therefore, after replacing \( G \) by a conjugate in \( \text{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \), we may assume that \( G \) is the subgroup of upper-triangular matrices. So we are left to consider the modular curve \( X_0(\ell) := X_G \) with \( \ell \in \{17, 19\} \). The curve \( X_0(\ell) \), with \( \ell \in \{17, 19\} \), indeed has finitely many points (it has a rational cusp, so it is an elliptic curve of conductor \( \ell \in \{17, 19\} \)); all such elliptic curves have rank 0. \( \square \)

4.3. **Proof of Theorem 4.2.** Let \( \mathcal{J} \) and \( \mathcal{J}_\ell \) (with \( \ell > 13 \)) be the sets from §4.2. Define the set

\[ J := \mathcal{J} \cup \bigcup_{13 < \ell \leq c} \mathcal{J}_\ell; \]

it is finite by Propositions 4.8 and 4.9.

Take any elliptic curve \( E/\mathbb{Q} \) with \( j_E \notin J \) for which \( \rho_{E,\ell} \) is surjective for all \( \ell > c \). Since \( j_E \notin \mathcal{J}_\ell \) for \( 13 < \ell \leq c \), the representation \( \rho_{E,\ell} \) is surjective for all \( \ell > 13 \).

Let \( \Gamma_E \) be the congruence subgroup from §4.1; denote its level by \( N_0 \) and define \( N \) as in the beginning of the section. Let \( G(N) \) be the subgroup of \( \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) \) from §4.1 associated to \( E/\mathbb{Q} \).

**Lemma 4.10.** The set \( X_{G(N)}(\mathbb{Q}) \) is infinite.

**Proof.** Take \( \mathcal{S} \) as in §4.2. The integer \( N \) is not divisible by any prime \( \ell > 13 \) since \( \rho_{E,\ell} \) is surjective for all \( \ell > 13 \). If \( (N, G(N)) \in \mathcal{S} \), then \( j_E \in \pi_{G(N)}(Y_{G(N)}(\mathbb{Q})) \subseteq J \subseteq \mathcal{J} \). Since \( j_E \notin J \) by assumption, we have \( (N, G(N)) \notin \mathcal{S} \). We have \( \text{det}(G(N)) = (\mathbb{Z}/N\mathbb{Z})^\times \) and \( -I \in G(N) \), so \( (N, G(N)) \notin \mathcal{S} \) implies that \( X_{G(N)} \) has genus 0 or 1, and that \( X_{G(N)}(\mathbb{Q}) \) is infinite. \( \square \)

Lemmas 4.6 and 4.10 together imply that \([\text{GL}_2(\mathbb{Z}) : \rho_{E,\text{Gal}(\mathbb{Q})}]\) is an element of \( \mathcal{J} \).

4.4. **Proof of Lemma 4.5.** Let \( d \) be the product of primes that divide \( m \) but not \( N \); it divides \( 2 \cdot 3 \cdot 5 \). Since \( G_m \cap \text{SL}_2(\mathbb{Z}_m) \) contains \( \{A \in \text{SL}_2(\mathbb{Z}_m) : A \equiv I \pmod{N_0}\} \), we have

\[ G_m \cap \text{SL}_2(\mathbb{Z}_m) = W \times \text{SL}_2(\mathbb{Z}_d). \]

for a subgroup \( W \) of \( \text{SL}_2(\mathbb{Z}_N) \) containing \( \{A \in \text{SL}_2(\mathbb{Z}_N) : A \equiv I \pmod{N_0}\} \). Since \( G_m \cap \text{SL}_2(\mathbb{Z}_m) \) is a normal subgroup of \( G_m \), the group \( W \) is normal in \( G_N \). We have \( G_d = \text{GL}_2(\mathbb{Z}_d) \), since \( G_d \subseteq \text{SL}_2(\mathbb{Z}_d) \) and \( \text{det}(G_d) = \mathbb{Z}_d^\times \) (note that \( \text{det}(\rho_{E,\text{Gal}(\mathbb{Q})}) = \mathbb{Z}_d^\times \)).
Now consider the quotient map
\[ \varphi : G_N \times G_d \to G_N/W \times G_d/SL_2(\mathbb{Z}_d). \]

We can view \( G_m \) as an open subgroup of \( G_N \times G_d \); it projects surjectively on both of the factors. The group \( G_m \) contains \( W \times SL_2(\mathbb{Z}_d) \), so there is an open subgroup \( Y \) of \( G_N/W \times G_d/SL_2(\mathbb{Z}_d) \) for which \( G_m = \varphi^{-1}(Y) \).

For part (i) and (ii), see [Zyw10, Lemma A.1]. To verify (iii), it suffices by (ii) to show that the topological group generated by the set \( C \) contains \( SL_2(\mathbb{Z}_p) \) of profinite groups. Similarly, we have

---

**Proof.** We proceed by induction on \( n \). The case \( n = 1 \) is trivial, so assume that \( n = 2 \). The kernel of \( p_1|_H \) is a closed subgroup of \( H \) of the form \( \{ I \} \times N_2 \), and similarly the kernel of \( p_2|_H \) is of the form \( N_1 \times \{ I \} \). The group \( N = N_1 \times N_2 \) is a closed normal subgroup of \( H \). Since \( p_1|_H \) is surjective, we find that \( N_1 = p_1(N) \) is a closed normal subgroup of \( B_1 \); this gives an isomorphism \( H/N \cong B_1/N_1 \) of profinite groups. Similarly, we have \( H/N \cong B_2/N_2 \) and thus \( B_1/N_1 \) and \( B_2/N_2 \) are isomorphism.
Since we have assumed that \( B_1 \) and \( B_2 \) have no common finite simple quotients, we deduce that \( B_1 = N_1 \) and \( B_2 = N_2 \). This proves the \( n = 2 \) case since \( H \) contains \( N_1 \times N_2 = B_1 \times B_2 \).

Now fix an \( n \geq 3 \) and assume that the \( n - 1 \) case of the lemma has been proved. Then the image \( \bar{H} \) of \( H \) in \( C := \prod_{i=1}^{n-1} B_i \) is a closed subgroup such that the projection \( \bar{H} \rightarrow B_i \) is surjective for all \( 1 \leq i \leq n - 1 \). By our inductive hypothesis, we have \( \bar{H} = C \). So \( H \) is a closed subgroup of \( C \times B_n \) and the projections \( H \rightarrow C \) and \( H \rightarrow B_n \) are surjective. By the \( n = 2 \) case, it suffices to show any finite simple quotient of \( C \) is not a quotient of \( B_n \). Take any open normal subgroup \( U \) of \( C \) such that \( C/U \) is a finite simple group. There is an integer \( 1 \leq j \leq n - 1 \) for which the projection \( U \rightarrow B_j \) is not surjective (if not, then we could use our inductive hypothesis to show that \( U = C \)). For simplicity, suppose \( j = 1 \); then \( U \) is of the form \( N_1 \times B_2 \times \cdots \times B_{n-1} \) where \( N_1 \) is an open normal subgroup of \( B_1 \). Since \( C/U \cong B_1/N_1 \), we deduce from the hypothesis on the \( B_i \) that \( C/U \) is not a quotient of \( B_n \).

We claim that \( G'_\ell = \SL_2(\mathbb{Z}_\ell) \) for every prime \( \ell \nmid m \). We have the easy inclusions \( G'_\ell \subseteq \GL_2(\mathbb{Z}_\ell)' \subseteq \SL_2(\mathbb{Z}_\ell) \). By [Ser89, IV Lemma 3] and \( \ell > 5 \) (since \( \ell \nmid m \)), we have \( G'_\ell = \SL_2(\mathbb{Z}_\ell) \) if and only if the image of \( G'_\ell \) in \( \SL_2(\mathbb{Z}/\ell\mathbb{Z}) \) is \( \SL_2(\mathbb{Z}/\ell\mathbb{Z}) \). Thus it suffices to show that \( \rho_{E,\ell}(\text{Gal}_Q)' = \SL_2(\mathbb{Z}/\ell\mathbb{Z}) \). Since \( \ell \nmid m \), we have \( \rho_{E,\ell}(\text{Gal}_Q)' = \SL_2(\mathbb{Z}/\ell\mathbb{Z}) \) and hence \( \rho_{E,\ell}(\text{Gal}_Q)' = \SL_2(\mathbb{Z}/\ell\mathbb{Z}) \) by Lemma 4.11(i); this proves our claim.

We can view \( G' \) as a subgroup of \( G'_m \times \prod_{\ell|m} \SL_2(\mathbb{Z}_\ell) \). The projection of \( G' \) to the the factors \( G'_m \) and \( \SL_2(\mathbb{Z}_\ell) = G'_\ell \) with \( \ell \nmid m \) are all surjective.

Fix a prime \( \ell \geq 5 \). The simple group \( \PSL_2(\mathbb{F}_\ell) \) is a quotient of \( \SL_2(\mathbb{Z}_\ell) \). Since \( \ell \)-groups are solvable and \( \SL_2(\mathbb{Z}_\ell)' = \SL_2(\mathbb{Z}_\ell) \) by Lemma 4.11(i), we find that \( \PSL_2(\mathbb{F}_\ell) \) is the only simple group that is a quotient of \( \SL_2(\mathbb{Z}_\ell) \). Note that the groups \( \PSL_2(\mathbb{F}_\ell) \) are non-isomorphic for different \( \ell \); in fact, they have different cardinalities.

Take any prime \( \ell \nmid m \), and hence \( \ell > 5 \). We claim that the simple group \( \PSL_2(\mathbb{F}_\ell) \) is not isomorphic to a quotient of \( G'_m \). Indeed, any closed subgroup \( H \) of \( \SL_2(\mathbb{Z}_m) \) has no quotients isomorphic to \( \PSL_2(\mathbb{F}_\ell) \) with \( \ell > 5 \) and \( \ell \nmid m \) (this follows from the calculation of the groups \( \text{Occ}(\SL_2(\mathbb{Z}_\ell)) \) in [Ser98, IV-25]). We can now apply Goursat’s lemma (Lemma 4.12) to deduce that

\[
G' = G'_m \times \prod_{\ell|m} \SL_2(\mathbb{Z}_\ell).
\]

Therefore, \( [\SL_2(\mathbb{Z}) : G'] = [\SL_2(\mathbb{Z}_m) : G'_m] \). By (4.4), we have

\[
[\SL_2(\mathbb{Z}_m) : G'_m] = [\SL_2(\mathbb{Z}_N) : G'_N] \cdot [\SL_2(\mathbb{Z}_d) : \GL_2(\mathbb{Z}_d)]'.
\]

By Lemma 4.11, \( [\SL_2(\mathbb{Z}_d) : \GL_2(\mathbb{Z}_d)]' = \prod_{d|d} [\SL_2(\mathbb{Z}_d) : \GL_2(\mathbb{Z}_d)]' \) is equal to 1 if \( d \) is odd and 2 if \( d \) is even. Since \( N \) and \( d \) have opposite parities, we conclude that \( [\SL_2(\mathbb{Z}_m) : G'_m] \) is equal to \( [\SL_2(\mathbb{Z}_N) : G'_N] \) if \( N \) is even and \( [\SL_2(\mathbb{Z}_N) : G'_N] \cdot 2 \) if \( N \) is odd. The lemma is now immediate.

5. INDEX COMPUTATIONS

In §1.1, we defined the set

\[
I = \{ 2, 4, 6, 8, 10, 12, 16, 20, 24, 30, 32, 36, 40, 48, 54, 60, 72, 84, 96, 108, 112, 120, 144, 192, 220, 240, 288, 336, 360, 384, 504, 576, 768, 864, 1152, 1200, 1296, 1536 \}.
\]

In §4, we defined the set of integers

\[
\mathcal{J} := \bigcup_{\Gamma} \mathcal{J}(\Gamma),
\]

where \( \Gamma \) runs over the congruence subgroups of \( \SL_2(\mathbb{Z}) \) of genus 0 or 1. The goal of this section is to outline the computations needed to verify the following.
Proposition 5.1. We have $\mathcal{I} = \mathcal{I}$.

The computations in this section were performed with Magma [BCP97]; code for the computations can be found at  
https://github.com/davidzywina/PossibleIndices

Let $S_0$ and $S_1$ be sets of representatives of the congruence subgroups of $\text{SL}_2(\mathbb{Z})$ containing $-I$, up to conjugacy in $\text{GL}_2(\mathbb{Z})$, with genus 0 and 1, respectively. Set $S := S_0 \cup S_1$. Since the set $\mathcal{I}(\Gamma)$ does not change if we replace $\Gamma$ by $\pm \Gamma$ or by a conjugate subgroup in $\text{GL}_2(\mathbb{Z})$, we have

$$\mathcal{I} = \bigcup_{\Gamma \in S} \mathcal{I}(\Gamma).$$

Cummin and Pauli [CP03] have classified the congruence subgroups of $\text{PSL}_2(\mathbb{Z})$ with genus 0 or 1, up to conjugacy in $\text{PGL}_2(\mathbb{Z})$. We thus have a classification of the congruence subgroups $\Gamma$ of $\text{SL}_2(\mathbb{Z})$, up to conjugacy in $\text{GL}_2(\mathbb{Z})$, of genus 0 or 1 that contain $-I$. Moreover, they have made available an explicit list1 of such congruence subgroups; each congruence subgroup is given by a level $N$ and set of generators of its image in $\text{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$. In our computations, we will let $S_0$ and $S_1$ consist of congruence subgroups from the explicit list of Cummin and Pauli.

5.1. Computing indices. Fix a congruence subgroup $\Gamma$ of $\text{SL}_2(\mathbb{Z})$ that contains $-I$ and has level $N_0$. Let $N$ be the integer $N_0$, $4N_0$ or $2N_0$ when $v_2(N_0)$ is 0, 1 or at least 2, respectively. For simplicity, we will assume that $N > 1$.

We first explain how we computed the subgroups $G(N)$ of $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that satisfy conditions (a), (b) and (c) of Definition 4.1. Instead of directly looking for subgroups in $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$, we will search for certain abelian subgroups in a smaller group.

Let $H$ be the the image of $\pm \Gamma = \Gamma$ in $\text{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Define the subgroup $\tilde{H} := (\mathbb{Z}/N\mathbb{Z})^\times \cdot H$ of $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$. We may assume that $H = \tilde{H} \cap \text{SL}_2(\mathbb{Z}/N\mathbb{Z})$; otherwise, conditions (a) and (b) are incompatible.

Let $\mathcal{N}$ be the normalizer of $\tilde{H}$ (equivalently, of $H$) in $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and set $\mathcal{C} := \mathcal{N}/\tilde{H}$. Since $\det(\tilde{H}) = ((\mathbb{Z}/N\mathbb{Z})^\times)^2$, the determinant induces a homomorphism

$$\det : \mathcal{C} \to (\mathbb{Z}/N\mathbb{Z})^\times/((\mathbb{Z}/N\mathbb{Z})^\times)^2 =: Q_N.$$

Lemma 5.2. The subgroups $G(N)$ of $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that satisfy conditions (a), (b) and (c) of Definition 4.1 are precisely the groups obtained by taking the inverse image under $\mathcal{N} \to \mathcal{C}$ of the subgroups $W$ of $\mathcal{C}$ for which the determinant induces an isomorphism $W \xrightarrow{\sim} Q_N$.

Proof. Let $B := G(N)$ be a subgroup of $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that satisfies conditions (a), (b) and (c). The group $B$ contains $\tilde{H}$ by (a) and (b). For any matrix $A \in B$ with $\det(A)$ a square, there is a scalar $\lambda \in (\mathbb{Z}/N\mathbb{Z})^\times$ such that $\det(\lambda A) = 1$. Since $B \cap \text{SL}_2(\mathbb{Z}/N\mathbb{Z}) = H$ by (a), we deduce that $\tilde{H}$ consists precisely of the element of $B$ with square determinant. The determinant thus gives rise to an exact sequence

$$1 \to \tilde{H} \hookrightarrow B \xrightarrow{\det} Q_N \to 1. \tag{5.1}$$

Therefore, $\tilde{H}$ is a normal subgroup of $B$, and hence $B \subseteq \mathcal{N}$, and the determinant map induces an isomorphism $B/\tilde{H} \xrightarrow{\sim} Q_N$. Let $W$ be the image of the natural injection $B/\tilde{H} \hookrightarrow \mathcal{N}/\tilde{H} = \mathcal{C}$; it satisfies the conditions for $W$ in the statement of the lemma.

Now take any subgroup $W$ of $\mathcal{C}$ for which the determinant gives an isomorphism $W \xrightarrow{\sim} Q_N$. Let $B$ be the inverse image of $W$ under the map $\mathcal{N} \to \mathcal{C}$. The short exact sequence (5.1) holds. Therefore, $B \cap \text{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is equal to $\tilde{H} \cap \text{SL}_2(\mathbb{Z}/N\mathbb{Z}) = H$. We have $B \supseteq (\mathbb{Z}/N\mathbb{Z})^\times \cdot I$ since

\[\text{See http://www.uncg.edu/mat/faculty/pauli/congruence/congruence.html}\]
$B \geq \bar{H}$. So $\det(B) \geq (\mathbb{Z}/N\mathbb{Z})^2$; with $\det(B/\bar{H}) = Q_N$, this implies that $\det(B) = (\mathbb{Z}/N\mathbb{Z})^2$. We have verified that $G(N) := B$ satisfies conditions (a), (b) and (c). \qed

We first compute the subgroups $W$ of $\mathcal{C}$ for which the determinant map $\mathcal{N}/\bar{H} \rightarrow Q_N$ gives an isomorphism $W \sim Q_N$. By Lemma 5.2, the subgroups $G(N)$ of $\text{GL}_2(\mathbb{Z}/\mathbb{N}\mathbb{Z})$ that satisfy the conditions (a), (b) and (c) of Definition 4.1 are precisely the inverse images of the groups $W$ under the quotient map $\mathcal{N} \rightarrow \mathcal{C}$. We can then check condition (d) for each of the groups $G(N)$. We shall now describe how to compute the index $[\text{SL}_2(\mathbb{Z}_N) : G']$; this is needed in order to compute $\mathcal{I} (\Gamma)$. We remark that $G' (M) = G(M)'$. \smallskip

**Lemma 5.3.** The group $G'$ contains $\{ A \in \text{SL}_2(\mathbb{Z}_N) : A \equiv I \pmod{N^2} \}$. In particular, we have $[\text{SL}_2(\mathbb{Z}_N) : G'] = [\text{SL}_2(\mathbb{Z}/N^2\mathbb{Z}) : G(N^2)' \}$. \smallskip

**Proof.** Since $G \geq I + NM_2(\mathbb{Z}_N)$, it suffices to prove that $(I + NM_2(\mathbb{Z}_N))' = \text{SL}_2(\mathbb{Z}_N) \cap (I + N^2M_2(\mathbb{Z}_N))$. So it suffices to prove that $(I + qM_2(\mathbb{Z}_q))' = \text{SL}_2(\mathbb{Z}_q) \cap (I + q^2M_2(\mathbb{Z}_q))$ for any prime power $q > 1$; this is Lemma 1 of [LT76, p.163]. \qed

Lemma 5.3 allows us to compute $[\text{SL}_2(\mathbb{Z}_N) : G']$ by computing the finite group $G(N^2)'$. In practice, we will use the following to reduce the computation to finding $G(M)'$ for some, possibly smaller, divisor $M$ of $N^2$. \smallskip

**Lemma 5.4.** Let $r$ be the product of the primes dividing $N$. Let $M > 1$ be an integer having the same prime divisors as $N$. If $G(rM)'$ contains $\{ A \in \text{SL}_2(\mathbb{Z}/rM\mathbb{Z}) : A \equiv I \pmod{M} \}$, then $[\text{SL}_2(\mathbb{Z}_N) : G'] = [\text{SL}_2(\mathbb{Z}/M\mathbb{Z}) : G(M)']$. \smallskip

**Proof.** For each positive integer $m$, define the group $S_m := \{ A \in \text{SL}_2(\mathbb{Z}_m) : A \equiv I \pmod{m} \}$. Let $H$ be a closed subgroup of $\text{SL}_2(\mathbb{Z}_N)$ whose image in $\text{SL}_2(\mathbb{Z}/rM\mathbb{Z})$ contains $\{ A \in \text{SL}_2(\mathbb{Z}/rM\mathbb{Z}) : A \equiv I \pmod{M} \}$. We claim that $H \geq S_M$; the lemma will follow from the claim with $H = G'$. By replacing $H$ with $H \cap S_M$, we may assume that $H$ is a closed subgroup of $S_M$. Since $S_M$ is a product of the pro-$\ell$ groups $S_{\ell^e(M)}$ with $\ell | M$, we may further assume that $M$ is a power of a prime $\ell$ and hence $r = \ell$. \smallskip

So fix a prime power $\ell e > 1$ and let $H$ be a closed subgroup of $S_{\ell^e}$ for which $H(\ell^{e+1}) = \{ A \in \text{SL}_2(\mathbb{Z}/\ell^{e+1}\mathbb{Z}) : A \equiv I \pmod{\ell^e} \}$; we need to prove that $H = S_{\ell^e}$. For each integer $i \geq 1$, define $H_i := H \cap (I + \ell^iM_2(\mathbb{Z}_\ell))$ and $h_i := H_i/H_{i+1}$. For any $A \in M_2(\mathbb{Z}_\ell)$ with $I + \ell^iA \in \text{SL}_2(\mathbb{Z}_\ell)$, we have $\text{tr}(A) \equiv 0 \pmod{\ell}$. The map $H_i \rightarrow M_2(\mathbb{Z}_\ell)$, $I + \ell^iA \mapsto A$ thus induces a homomorphism $\varphi_i : h_i \hookrightarrow \text{sl}_2(\mathbb{F}_\ell)$, where $\text{sl}_2(\mathbb{F}_\ell)$ is the subgroup of trace 0 matrices in $M_2(\mathbb{F}_\ell)$. Using that $H$ is closed, we deduce that $H = S_{\ell^e}$ if and only if $\varphi_i$ is surjective for all $i \geq e$. \smallskip

We now show that $\varphi_i$ is surjective for all $i \geq e$. We proceed by induction on $i$; the homomorphism $\varphi_e$ is surjective by our initial assumption on $H$. Now suppose that $\varphi_i$ is surjective for a fixed $i \geq e$. Take any matrix $B$ in the set $\mathcal{B} := \{ (0 1, 1 0), (\frac{1}{2} 1, 1 2) \}$. The matrix $I + \ell^iB$ has determinant 1, so the surjectivity of $\varphi_i$ implies that there is a matrix $A \in M_2(\mathbb{Z}_\ell)$ with $A \equiv B \pmod{\ell}$ such that $h := I + \ell^iA$ is an element of $H$. \smallskip

16
Working modulo $\ell^{2i+1}$, we find that $(\ell^iA)^2 = \ell^{2i}A^2 \equiv \ell^{2i}B^2 = 0$, where the last equality uses \( \ell^{2i} \). In particular, $(\ell^iA)^2 \equiv 0 \pmod{\ell^{i+2}}$. Therefore,
\[
h^\ell \equiv I + (\ell^i) \ell^i A \equiv I + \ell^i A \equiv I + \ell^{i+1}B \pmod{\ell^{i+2}}.
\]
Since $h^\ell \in H$, we find that $B$ modulo $\ell$ lies in the image of $\varphi_{i+1}$. Since $\mathfrak{s}_2(F_\ell)$ is generated by the $B \in B$, we deduce that $\varphi_{i+1}$ is surjective. $\Box$

5.2. Genus 0 computations. In this section, we compute the set of integers
\[
I_0 := \bigcup_{\Gamma \in S_0} \mathcal{I}(\Gamma).
\]
Instead of computing $\mathcal{I}(\Gamma)$, we will compute two related quantities. Let $\mathcal{I}'(\Gamma)$ be the set of integers as in Definition 4.1 but with condition (e) excluded. Let $\mathcal{I}''(\Gamma)$ be the set of integers as in Definition 4.1 with condition (e) excluded and satisfying the additional condition that $X^\infty_{G(N)}(\mathbb{Q}_p)$ is empty for at most one prime $p|N$.

**Lemma 5.5.** For a congruence subgroup $\Gamma$ of genus 0, we have $\mathcal{I}''(\Gamma) \subseteq \mathcal{I}(\Gamma) \subseteq \mathcal{I}'(\Gamma)$.

**Proof.** The inclusion $\mathcal{I}(\Gamma) \subseteq \mathcal{I}'(\Gamma)$ is obvious. So assume that $G(N)$ is any group satisfying conditions (a)-(d) of Definition 4.1 and that $X^\infty_{G(N)}(\mathbb{Q}_p)$ is empty for at most one prime $p|N$. To prove the inclusion $\mathcal{I}''(\Gamma) \subseteq \mathcal{I}(\Gamma)$, we need to verify that $X := X_{G(N)}$ has infinitely many $\mathbb{Q}$-points. Note that the curve $X_{\mathbb{Q}}$ is smooth and projective; it has genus 0 by our assumption on $\Gamma$ and Proposition 3.7.

We claim that $X(Q_v)$ is non-empty for all places $v$ of $\mathbb{Q}$; the places corresponds to the primes $p$ or to $\infty$ where $Q_\infty = \mathbb{R}$. Condition (d) and Proposition 3.5 imply that $X(\mathbb{R})$ is non-empty. Now take any prime $p \nmid N$. As an $\mathbb{Z}[1/N]$-scheme $X$ has good reduction at $p$ and hence the fiber $X$ over $\mathbb{F}_p$ is a smooth and projective curve of genus 0. Therefore, $X(\mathbb{F}_p)$ is non-empty and any of the points can be lifted by Hensel’s lemma to a point in $X(Q_p)$. By our hypothesis on the sets $X^\infty_{G(N)}(\mathbb{Q}_p)$ with $p|N$, we deduce that there is at most one prime $p_0$ such that $X(Q_{p_0})$ is empty.

So suppose that there is precisely one prime $p_0$ for which $X(Q_{p_0})$ is empty. The curve $X_{\mathbb{Q}}$ has a model given by a conic of the form $ax^2 + by^2 - z^2 = 0$ with $a, b \in \mathbb{Q}^\times$. The Hilbert symbol $(a, b)_v$ for a place $v$, is equal to +1 if $X(Q_v) \neq \emptyset$ and −1 otherwise. Therefore, $\prod_v (a, b) = (a, b)_{p_0} = -1$. However, we have $\prod_v (a, b) = 1$ by reciprocity. This contradiction proves our claim that $X(Q_v)$ is non-empty for all places $v$ of $\mathbb{Q}$.

The curve $X_{\mathbb{Q}}$ has genus 0 so it satisfies the Hasse principle, and hence has a $\mathbb{Q}$-rational point. The curve $X_{\mathbb{Q}}$ is thus isomorphic to $\mathbb{P}_1^1$ and has infinitely many $\mathbb{Q}$-points.

We shall use the explicit set $S_0$ due to Cummin and Pauli. For each $\Gamma \in S_0$, it is straightforward to compute the set $\mathcal{I}(\Gamma)$ using the method in §5.1.

Using Lemma 3.4 and the discussion in §5.1, we can also compute $\mathcal{I}''(\Gamma)$. Fix a prime $p$ dividing $N$. Take $e$ so that $p^e \| N$ and set $M = N/p^e$. The image of the character $\chi_N : \text{Gal}_{\mathbb{Q}_p} \to (\mathbb{Z}/N\mathbb{Z})^\times = (\mathbb{Z}/p^e\mathbb{Z})^\times \times (\mathbb{Z}/M\mathbb{Z})^\times$ arising from the Galois action on the $N$-th roots of unity is $(\mathbb{Z}/p^e\mathbb{Z})^\times \times (p)$.

Our Magma computations show that $\bigcup_{\Gamma \in S_0} \mathcal{I}''(\Gamma) = I_0$ and $\bigcup_{\Gamma \in S_0} \mathcal{I}'(\Gamma) = I_0$, where
\[
I_0 := \{ 2, 4, 6, 8, 10, 12, 16, 20, 24, 30, 32, 36, 40, 48, 54, 60, 72, 84, 96, 108, 112, 120, 144, 192, 288, 336, 384, 576, 768, 864, 1152, 1200, 1296, 1536 \}.
\]
Using the inclusions of Lemma 5.5, we deduce that $\mathcal{I}_0 = I_0$.

**Remark 5.6.** From our genus 0 computations, we find that $S_0$ has cardinality 121 which led to 331 total groups $G(N)$ that satisfied (a)-(d) with respect to some $\Gamma \in S_0$. 17
5.3. Genus 1 computations. Now define the set of integers

$$\mathcal{I}_1 := \bigcup_{\Gamma \in \mathcal{S}_1} (\mathcal{I}(\Gamma) - \mathcal{I}_0),$$

where $\mathcal{I}_0$ is the set from §5.2.

Instead of computing $\mathcal{I}(\Gamma)$, we will compute a related quantity. We define $\mathcal{I}''(\Gamma)$ to be the set of integers as in Definition 4.1 with condition (e) excluded and satisfying the additional condition that the Mordell-Weil group of the Jacobian $J$ of the curve $X_{G(N)}$ over $\mathbb{Q}$ has positive rank. For a congruence subgroup $\Gamma$ of genus 1, we have an inclusion $\mathcal{I}(\Gamma) \subseteq \mathcal{I}''(\Gamma)$ since a genus 1 curve over $\mathbb{Q}$ that has a $\mathbb{Q}$-point is isomorphic to its Jacobian. Therefore,

$$\mathcal{I}_1 \subseteq \bigcup_{\Gamma \in \mathcal{S}_1} (\mathcal{I}''(\Gamma) - \mathcal{I}_0).$$

We now explain how to compute $\mathcal{I}''(\Gamma) - \mathcal{I}_0$ for a fixed congruence subgroup $\Gamma$ of genus 1. As described in §5.1, we can compute the subgroups $G(N)$ satisfying the conditions (a)–(d). For each group $G(N)$, it is described in §5.1 how to compute $[\text{SL}_2(\mathbb{Z}_N) : G']$, where $G$ is the inverse image of $G(N)$ under the reduction map $\text{GL}_2(\mathbb{Z}_N) \to \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$. We may assume that $[\text{SL}_2(\mathbb{Z}_N) : G'] \cdot 2/\gcd(2, N) \notin \mathcal{I}_0$ since otherwise it does not contribute to $\mathcal{I}''(\Gamma) - \mathcal{I}_0$.

Let $J$ be the Jacobian of the curve $X_{G(N)}$ over $\mathbb{Q}$; it is an elliptic curve since $\Gamma$ has genus 1. Let us now explain how to compute the rank of $J(\mathbb{Q})$ (and hence finish our method for computing $\mathcal{I}''(\Gamma) - \mathcal{I}_0$) without having to compute a model for $X_{G(N)}$. Moreover, we shall determine the elliptic curve $J$ up to isogeny (defined over $\mathbb{Q}$); note that the Mordell rank is an isogeny invariant.

The curve $J$ has good reduction at all primes $p \nmid N$ since the $\mathbb{Z}[1/N]$-scheme $X_{G(N)}$ is smooth. If $E/\mathbb{Q}$ is an elliptic curve with good reduction at all primes $p \nmid N$, then its conductor divides $N_{\text{max}} := \prod_{p|N} p^{e_p}$, where $e_2 = 8$, $e_3 = 5$ and $e_p = 2$ otherwise. One can compute a finite list of elliptic curves

$$E_1, \ldots, E_n$$

over $\mathbb{Q}$ that represent the isogeny classes of elliptic curves over $\mathbb{Q}$ with good reduction at $p \nmid N$. In our computations, we will have $N_{\text{max}} \leq 2^8 \cdot 3^5 = 62208$ and hence the representative curves $E_i$ can all be found in Cremona’s database [Cre] of elliptic curves which are included in Magma (it currently contains all elliptic curves over $\mathbb{Q}$ with conductor at most $500000$). It remains to determine which curve $E_i$ is isogenous to $J$.

Take any prime $p \nmid N$. Using the methods of §3.6, we can compute the cardinality of $X_{G(N)}(\mathbb{F}_p)$ and hence also the trace of Frobenius

$$a_p(J) = p + 1 - |J(\mathbb{F}_p)| = p + 1 - |X_{G(N)}(\mathbb{F}_p)|.$$

If $a_p(E_i) \neq a_p(J)$, then $E_i$ and $J$ are not isogenous elliptic curves over $\mathbb{Q}$. By computing $a_p(J)$ for enough primes $p \nmid N$, one can eventually eliminate all but one curve $E_{i_0}$ which then must be isogenous to $J$. There are then known methods to determine the Mordell rank of $E_{i_0}$; the rank is also part of Cremona’s database. Therefore, we can compute the rank of $J(\mathbb{Q})$.

Our Magma computations show that

$$\bigcup_{\Gamma \in \mathcal{S}_1} (\mathcal{I}''(\Gamma) - \mathcal{I}_0) = \{220, 240, 360, 504\}.$$

In particular, $\mathcal{I}_1 \subseteq \{220, 240, 360, 504\}$.

We now describe how the values 220, 240, 360 and 504 arise in our computations.

For an odd prime $\ell$, let $\mathcal{N}_\ell^{-}$ be the normalizer in $\text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ of a non-split Cartan subgroup and let $\mathcal{N}_\ell^{+}$ be the normalizer in $\text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ of a split Cartan subgroup. Define $G_1 := \mathcal{N}_1^{-}$. We can
identify $\mathcal{N}_3^− \times \mathcal{N}_5^−$ and $\mathcal{N}_3^− \times \mathcal{N}_7^+$ with subgroups $G_2$ and $G_3$, respectively, of $\text{GL}_2(\mathbb{Z}/15\mathbb{Z})$. We can identify $\mathcal{N}_7^+ \times \mathcal{N}_7^−$ with a subgroup $G_4$ of $\text{GL}_2(\mathbb{Z}/21\mathbb{Z})$.

Fix an $n \in \{220, 240, 360, 504\}$. Let $\Gamma \in S_1$ be any congruence subgroup such that $n \in \mathcal{I}(\Gamma)$. Let $G(N)$ be one of the groups such that the following hold:

- it satisfies conditions (a), (b), (c) and (d) of Definition 4.1,
- the Jacobian $J$ of the curve $X_{G(N)}$ over $\mathbb{Q}$ has positive rank,
- we have $[\text{SL}_2(\mathbb{Z}_N) : G'] \cdot 2 / \gcd(2, N) = n$, where $G$ is the inverse image of $G(N)$ under the reduction $\text{GL}_2(\mathbb{Z}_N) \to \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

Our computations show that one of the following hold:

- We have $n = 220$, $N = 11$ and $G(N)$ is conjugate in $\text{GL}_2(\mathbb{Z}/11\mathbb{Z})$ to $G_1$.
- We have $n = 240$, $N = 15$ and $G(N)$ is conjugate in $\text{GL}_2(\mathbb{Z}/15\mathbb{Z})$ to $G_2$.
- We have $n = 360$, $N = 15$ and $G(N)$ is conjugate in $\text{GL}_2(\mathbb{Z}/15\mathbb{Z})$ to $G_3$.
- We have $n = 504$, $N = 21$ and $G(N)$ is conjugate in $\text{GL}_2(\mathbb{Z}/21\mathbb{Z})$ to $G_4$.

For later, we note that the index $[\text{GL}_2(\mathbb{Z}/N\mathbb{Z}) : G_i]$ is 55, 30, 45 or 63 for $i = 1, 2, 3$ or 4, respectively.

**Lemma 5.7.** We have $\mathcal{I}_1 = \{220, 240, 360, 504\}$.

**Proof.** We already know the inclusion $\mathcal{I}_1 \subseteq \{220, 240, 360, 504\}$. It thus suffices to show that the set $X_{G_i}(\mathbb{Q})$ is infinite for all $1 \leq i \leq 4$. So for a fixed $i \in \{1, 2, 3, 4\}$, it suffices to show that $X_{G_i}(\mathbb{Q})$ is non-empty, since it then becomes isomorphic to its Jacobian which we know has infinitely many rational points. By Proposition 3.2, it suffices to find a single elliptic curve $E/\mathbb{Q}$ with $j_E \not\in \{0, 1728\}$ for which $\rho_{E, N}(\text{Gal}_\mathbb{Q})$ is conjugate to a subgroup of $G_i$.

Let $E/\mathbb{Q}$ be a CM elliptic curve. Define $R := \text{End}(E)$; it is an order in the imaginary quadratic field $K := R \otimes \mathbb{Q}$. Take any odd prime $\ell$ that does not divide the discriminant of $R$. One can show that $\rho_{E, \ell}(\text{Gal}_\mathbb{Q})$ is contained in the normalizer of a Cartan subgroup $C \subseteq \text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^\times$, cf. [Ser97, Appendix A.5]. The Cartan group $C$ is split if and only if $\ell$ splits in $K$.

Consider the CM curve $E_1/\mathbb{Q}$ defined by $y^2 = x^3 - 11x + 14$; $R$ is an order in $\mathbb{Q}(i)$ of discriminant $-16$. The primes 3, 7 and 11 are inert in $\mathbb{Q}(i)$ and 5 is split in $\mathbb{Q}(i)$. Therefore, $\rho_{E_1, 11}(\text{Gal}_\mathbb{Q})$, $\rho_{E_1, 15}(\text{Gal}_\mathbb{Q})$ and $\rho_{E_1, 21}(\text{Gal}_\mathbb{Q})$ are conjugate to subgroups of $G_1$, $G_3$ and $G_4$, respectively.

Consider the CM curve $E_2/\mathbb{Q}$ defined by $y^2 + xy = x^3 - x^2 - 2x - 1$; $R$ is an order in $\mathbb{Q}(\sqrt{-7})$ of discriminant $-7$. The primes 3 and 5 are inert in $\mathbb{Q}(\sqrt{-7})$. Therefore, $\rho_{E_2, 15}(\text{Gal}_\mathbb{Q})$ is conjugate to a subgroup of $G_2$. \qed

**Remark 5.8.** From our genus 1 computations, we find that $S_1$ has cardinality 163 which led to 805 total groups $G(N)$ that satisfied (a)–(d) with respect to some $\Gamma \in S_1$. We needed to determine the Jacobian of $X_{G(N)}$, up to isogeny, for 63 of these groups $G(N)$.

5.4. **Proof of Proposition 5.1.** In §5.2, we found that $\bigcup_{\Gamma \in S_0} \mathcal{I}(\Gamma) = \mathcal{I}_0$. By Lemma 5.7, we have

$$\left( \bigcup_{\Gamma \in S_1} \mathcal{I}(\Gamma) \right) \cap \mathcal{I}_0 = \bigcup_{\Gamma \in S_1} (\mathcal{I}(\Gamma) \cap \mathcal{I}_0) = \{220, 240, 360, 504\}.$$

Therefore, $\mathcal{I}$ is equal to $\mathcal{I}_0 \cup \{220, 240, 360, 504\} = \mathcal{I}$.

6. **Proof of main theorems**

6.1. **Proof of Theorem 1.3.** The theorem follows immediately from Theorem 4.2 and Proposition 5.1.
6.2. Proof of Theorem 1.4.

Lemma 6.1. Let $E/Q$ be a non-CM elliptic curve and suppose $\ell > 37$ is a prime for which $\rho_{E,\ell}$ is not surjective. Then $\ell \leq [\text{GL}_2(\hat{\mathbb{Z}}) : \rho_E(\text{Gal}_{\mathbb{Q}})]$.

Proof. From [Ser81, §8.4], we find that $\rho_{E,\ell}(\text{Gal}_{\mathbb{Q}})$ is contained in the normalizer of a Cartan subgroup of $\text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. In particular, we have $[\text{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \rho_{E,\ell}(\text{Gal}_{\mathbb{Q}})] \geq \ell(\ell - 1)/2 \geq \ell$. Therefore, $\ell \leq [\text{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \rho_{E,\ell}(\text{Gal}_{\mathbb{Q}})] \leq [\text{GL}_2(\hat{\mathbb{Z}}) : \rho_E(\text{Gal}_{\mathbb{Q}})]$. \hfill $\square$

First suppose that there is a finite set $J$ such that if $E/Q$ is an elliptic curve with $j_E \notin J$, then $[\text{GL}_2(\hat{\mathbb{Z}}) : \rho_E(\text{Gal}_{\mathbb{Q}})] \in J$. There is thus an integer $c > 37$ such that for any non-CM $E/Q$, we have $[\text{GL}_2(\hat{\mathbb{Z}}) : \rho_E(\text{Gal}_{\mathbb{Q}})] \leq c$, this uses Serre’s theorem (and Lemma 2.3) to deal with the finite number of $j$-invariants of CM elliptic curves over $\mathbb{Q}$. By Lemma 6.1, we deduce that $\rho_{E,\ell}$ is surjective for all primes $\ell > c$; this gives Conjecture 1.2.

Now suppose that Conjecture 1.2 holds for some constant $c$. Let $J$ be the finite set from Theorem 1.3 with this constant $c$. After possibly increasing $J$, we may assume that it contains the finite number of $j$-invariants of CM elliptic curves over $\mathbb{Q}$. Theorem 1.3 then implies that for any elliptic curve $E/Q$ with $j_E \notin J$, we have $[\text{GL}_2(\hat{\mathbb{Z}}) : \rho_E(\text{Gal}_{\mathbb{Q}})] \in J$.

6.3. Proof of Theorem 1.5. First take any $n \geq 1$ so that $J_n$ is infinite. Let $E/Q$ be an elliptic curve with $j_E \in J_n$, equivalently, with $[\text{GL}_2(\hat{\mathbb{Z}}) : \rho_E(\text{Gal}_{\mathbb{Q}})] = n$. Lemma 6.1 implies that $\rho_{E,\ell}$ is surjective for all primes $\ell > \max\{37, n\}$. Let $J$ be the set from Theorem 1.3 with $c := \max\{37, n\}$. Now take any elliptic curve $E/Q$ with $j_E \in J_n - J$; note that $J_n - J$ is non-empty since $J_n$ is infinite and $J$ is finite. The representation $\rho_{E,\ell}$ is surjective for all $\ell > c$ and $j_E \notin J$, so $[\text{GL}_2(\hat{\mathbb{Z}}) : \rho_E(\text{Gal}_{\mathbb{Q}})]$ is an element of $J$ by Theorem 1.3. Therefore, $n \in J$.

Now take any integer $n \in J$. To complete the proof of the theorem, we need to show that $J_n$ is infinite. By Proposition 5.1, we have $n \in \mathcal{I}(\Gamma)$ for some congruence subgroup $\Gamma$ of $\text{SL}_2(\mathbb{Z})$ of genus 0 or 1. From our computation of $\mathcal{I}_0$ in §5.2, we may assume that $\Gamma$ has genus 0 when $n \notin \{220, 240, 360, 504\}$.

Denote the level of $\Gamma$ by $N_0$. Let $N$ be the integer $N_0, 4N_0$ or $2N_0$ when $v_2(N_0)$ is 0, 1 or at least 2, respectively. The integer $N$ is not divisible by any prime $\ell > 13$ (if $\Gamma$ has genus 0, this follows from the classification of genus 0 congruence subgroups in [CP03]; if $\Gamma$ has genus 1, then we saw in §5.3 that $N \in \{11, 15, 21\}$).

Since $n \in \mathcal{I}(\Gamma)$, there is a subgroup $G(N)$ of $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that satisfies conditions (a), (b), (c), (d) and (e) of Definition 4.1 and also satisfies $n = [\text{SL}_2(\mathbb{Z}/N\mathbb{Z}) : G(N)] = 2/gcd(2, N)$, where $G(N)$ is the inverse image of $G(N)$ under the reduction map $\text{GL}_2(\mathbb{Z}/N\mathbb{Z}) \to \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Let $G$ be the inverse image of $G(N)$ under $\text{GL}_2(\hat{\mathbb{Z}}) \to \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

Let $m$ be the product of the primes $\ell \leq 13$; note that $N$ divides some power of $m$. Let $G_m$ be the image of $G$ under the projection map $\text{GL}_2(\hat{\mathbb{Z}}) \to \text{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Lemma 4.7 implies that there is a positive integer $M$, dividing some power of $m$, such that if $H$ is an open subgroup of $G_m \subseteq \text{GL}_2(\mathbb{Z}/m\mathbb{Z})$, then $H$ equals $G_m$ if and only if $H(M) = G(M)$.

Take any proper subgroup $B \subseteq G(M)$ for which $\det(B) = (\mathbb{Z}/M\mathbb{Z})^\times$ and $-I \in B$. We have a morphism $\varphi_B : Y_B \to Y_{G(M)} = Y_{G(N)}$ of curves over $\mathbb{Q}$ such that $\pi_B = \pi_{G(N)} \circ \varphi_B$. The morphism $\varphi_B$ has degree $[G(M) : B] > 1$. Define $W := \bigcup_B \varphi_B(Y_B(\mathbb{Q}))$. 

20
where $B$ varies over the proper subgroups of $G(M)$ for which $\det(B) = (\mathbb{Z}/M\mathbb{Z})^\times$ and $-I \in B$. We have $W \subseteq Y_{G(N)}(\mathbb{Q})$.

**Lemma 6.2.** If $E/\mathbb{Q}$ is a non-CM elliptic curve with $j_E \in \pi_{G(N)}(Y_{G(N)}(\mathbb{Q}) - W)$, then $\pm \rho_{E,M}(\text{Gal}_{\mathbb{Q}})$ is conjugate in $\text{GL}_2(\mathbb{Z}/M\mathbb{Z})$ to $G(M)$.

**Proof.** Fix a non-CM elliptic curve $E/\mathbb{Q}$ with $j_E \in \pi_{G(N)}(Y_{G(N)}(\mathbb{Q}) - W) = \pi_{G(M)}(Y_{G(M)}(\mathbb{Q}) - W)$. There is a point $P \in Y_{G(Q)} - W$ for which $\pi_{G(M)}(P) = j_E$.

With notation as in §3, there is an isomorphism $\alpha : E[M] \cong (\mathbb{Z}/M\mathbb{Z})^2$ such that the pair $(E, [\alpha]_G)$ represents $P$. Since $j_E \notin \{0, 1728\}$, the automorphisms of $E_{/\mathbb{Q}}$ act on $E[N]$ by $I$ or $-I$. By Lemma 3.1(ii) and $-I \in G(M)$, we have $\alpha \circ \sigma^{-1} \circ \alpha^{-1} \in G(M)$ for all $\sigma \in \text{Gal}_{\mathbb{Q}}$. We may assume that $\rho_{E,M}$ was chosen so that $\rho_{E,M}(\sigma) = \alpha \circ \sigma \circ \alpha^{-1}$ for all $\sigma \in \text{Gal}_{\mathbb{Q}}$. Since $-I \in G(M)$, we deduce that $B := \pm \rho_{E,M}(\text{Gal}_{\mathbb{Q}})$ is a subgroup of $G(M)$. Note that $\det(B) = (\mathbb{Z}/M\mathbb{Z})^\times$ and $-I \in B$.

Suppose that $B$ is a proper subgroup of $G(M)$. We have $\alpha \circ \sigma^{-1} \circ \alpha^{-1} \in B$ for all $\sigma \in \text{Gal}_{\mathbb{Q}}$, so $(E, [\alpha]_B)$ represents a point $P' \in Y_B(\mathbb{Q})$ by Lemma 3.1(ii). We have $\varphi_B(P') = P$, so $P \in W$. This contradicts $P \in Y_{G(Q)} - W$ and hence $B = G(M)$. □

**Lemma 6.3.** If $E/\mathbb{Q}$ is an elliptic curve with $j_E \in \pi_{G(N)}(Y_{G(N)}(\mathbb{Q}) - W)$, then

$$[\text{GL}_2(\hat{\mathbb{Z}}) : \rho_E(\text{Gal}_{\mathbb{Q}})] = n$$

or $\rho_{E,\ell}$ is not surjective for some prime $\ell > 13$.

**Proof.** Let $E/\mathbb{Q}$ be an elliptic curve with $j_E \in \pi_{G(N)}(Y_{G(N)}(\mathbb{Q}) - W)$ such that $\rho_{E,\ell}$ is surjective for all $\ell > 13$. We need to show that $[\text{GL}_2(\hat{\mathbb{Z}}) : \rho_E(\text{Gal}_{\mathbb{Q}})] = n$. The curve $E$ is non-CM since $\rho_{E,\ell}$ is surjective for $\ell > 13$. Define the subgroup

$$H := \hat{\mathbb{Z}}^\times \cdot \rho_E(\text{Gal}_{\mathbb{Q}})$$

of $\text{GL}_2(\hat{\mathbb{Z}})$. By Lemma 6.2, we may assume that $\pm \rho_{E,M}(\text{Gal}_{\mathbb{Q}}) = G(M)$. Since $G(M)$ contains the scalar matrices in $\text{GL}_2(\mathbb{Z}/M\mathbb{Z})$, we have $H(M) = G(M)$ and an inclusion $H \subseteq G$. In particular, $H' \subseteq G'$.

Let $m_0$ be the product of the primes $\ell$ for which $\ell \leq 5$ or for which $\rho_{E,\ell}$ is not surjective. Let $H_m$ and $H'_m$ be the image of $H$ under the projection to $\text{GL}_2(\mathbb{Z}_m)$ and $\text{GL}_2(\mathbb{Z}_m)$, respectively. The integer $m_0$ divides $m$ since $\rho_{E,\ell}$ is surjective for all $\ell > 13$.

Lemma 4.5 applied with $G$ and $m$ replaced by $H$ and $m_0$, respectively, implies that $H' = H'_m \times \prod_{\ell|m_0} \text{SL}_2(\mathbb{Z}_\ell)$. Therefore, we have

$$H' = H'_m \times \prod_{\ell|m} \text{SL}_2(\mathbb{Z}_\ell).$$

Since $H' \subseteq G' \subseteq \text{SL}_2(\hat{\mathbb{Z}})$, we deduce that

$$G' = G'_m \times \prod_{\ell|m} \text{SL}_2(\mathbb{Z}_\ell).$$

We have $H_m \subseteq G_m$ and $H(M) = G(M)$, and thus $H_m = G_m$ by our choice of $M$. Therefore, $H'_m = G'_m$ and hence $H' = G'$. The groups $H$ and $\rho_E(\text{Gal}_{\mathbb{Q}})$ have the same commutator subgroup, so by Proposition 2.1, we have

$$[\text{GL}_2(\hat{\mathbb{Z}}) : \rho_E(\text{Gal}_{\mathbb{Q}})] = [\text{SL}_2(\hat{\mathbb{Z}}) : H'] = [\text{SL}_2(\hat{\mathbb{Z}}) : G'].$$

It remains to show that $[\text{SL}_2(\hat{\mathbb{Z}}) : G'] = n$. We have $G = G_N \times \prod_{\ell|N} \text{GL}_2(\mathbb{Z}_\ell)$, so $G' = G'_N \times \prod_{\ell|N} \text{GL}_2(\mathbb{Z}_\ell)'$. By Lemma 4.11, the index $[\text{SL}_2(\mathbb{Z}_\ell) : \text{GL}_2(\mathbb{Z}_\ell)]$ is 1 or 2 when $\ell \neq 2$ or $\ell = 2$, and so $[\text{SL}_2(\hat{\mathbb{Z}}) : G'] = n$. □
respectively. Therefore,
\[ |\text{SL}_2(\mathbb{Z}) : G'| = |\text{SL}_2(\mathbb{Z}_N) : G'_N| \prod_{\ell \in \mathbb{N}} |\text{SL}_2(\mathbb{Z}_\ell) : \text{GL}_2(\mathbb{Z}_\ell)'| = |\text{SL}_2(\mathbb{Z}_N) : G'_N| \cdot 2/\gcd(2, N) = n. \]

Recall that a subset \( S \) of \( \mathbb{P}^1(\mathbb{Q}) \) has \textit{density} \( \delta \) if
\[ \frac{|\{P \in S : h(P) \leq x\}|}{|\{P \in \mathbb{P}^1(\mathbb{Q}) : h(P) \leq x\}|} \to \delta \]
as \( x \to \infty \), where \( h \) is the height function. If \( X_{G(N)} \) has genus 0, then it is isomorphic to \( \mathbb{P}^1(\mathbb{Q}) \) (from our assumptions on \( G(N) \), the curve \( X_{G(N)} \) has infinitely many \( \mathbb{Q} \)-points). Choosing such an isomorphism \( X_{G(N)} \cong \mathbb{P}^1(\mathbb{Q}) \) allows us to define the density of a subset of \( X_{G(N)}(\mathbb{Q}) \); the existence and value of the density does not depend on the choice of isomorphism.

\textbf{Lemma 6.4.} There is an infinite subset \( S \) of \( Y_{G(N)}(\mathbb{Q}) \), with positive density if \( X_{G(N)} \) has genus 0, such that if \( E/\mathbb{Q} \) is an elliptic curve with \( j_E \in \pi_{G(N)}(S) \), then \( \rho_{E, \ell} \) is surjective for all \( \ell > 13 \).

\textit{Proof.} We claim that for any place \( v \) of \( \mathbb{Q} \), the set \( X_{G(N)}(\mathbb{Q}) \) has no isolated points in \( X_{G(N)}(\mathbb{Q}_v) \), i.e., there is no open subset \( U \) of \( X_{G(N)}(\mathbb{Q}_v) \) with respect to the \( v \)-adic topology, for which \( U \cap X_{G(N)}(\mathbb{Q}) \) consists of a single point. If \( X_{G(N)} \) has genus 0, then the claim follows since no point in \( \mathbb{P}^1(\mathbb{Q}) \) is isolated in \( \mathbb{P}^1(\mathbb{Q}_v) \). Now consider the case where \( X_{G(N)} \) has genus 1. If one point of \( X_{G(N)}(\mathbb{Q}) \) was isolated in \( X_{G(N)}(\mathbb{Q}_v) \), then using the group law of \( X_{G(N)}(\mathbb{Q}) \) (by first fixing a rational point), we find that every point is isolated. So suppose that for each \( P \in X_{G(N)}(\mathbb{Q}) \), there is an open subset \( U_P \subseteq X_{G(N)}(\mathbb{Q}_v) \) such that \( U_P \cap X_{G(N)}(\mathbb{Q}) = \{P\} \). The sets \( \{U_P\}_{P \in X_{G(N)}(\mathbb{Q})} \) along with the complement of the closure of \( X_{G(N)}(\mathbb{Q}) \) in \( X_{G(N)}(\mathbb{Q}_v) \) form an open cover of \( X_{G(N)}(\mathbb{Q}_v) \) that has no finite subcover. This contradicts the compactness of \( X_{G(N)}(\mathbb{Q}_v) \) and proves the claim.

Since \( \pi_{G(N)} : Y_{G(N)}(\mathbb{R}) \to \mathbb{R} \) is continuous, the above claim with \( v = \infty \) implies that the set \( \pi_{G(N)}(Y_{G(N)}(\mathbb{Q})) \) is not a subset of \( \mathbb{Z} \). Choose a rational number \( j \in \pi_{G(N)}(Y_{G(N)}(\mathbb{Q})) \) that is \textit{not} an integer.

There is a prime \( p \) such that \( v_p(j) \) is negative; set \( e := -v_p(j) \). Let \( \mathcal{U} \) be the set of points \( P \in Y_{G(N)}(\mathbb{Q}_p) \) for which \( v_{G(N)}(P) \neq 0 \) and \( v_p(\pi_{G(N)}(P)) = -e \); it is an open subset of \( Y_{G(N)}(\mathbb{Q}_p) \). Define \( S := \mathcal{U} \cap Y_{G(N)}(\mathbb{Q}) = \mathcal{U} \cap X_{G(N)}(\mathbb{Q}) \); it is non-empty by our choice of \( e \) (in particular, \( \mathcal{U} \) is non-empty). The set \( S \) is infinite since otherwise there would be an isolated point of \( X_{G(N)}(\mathbb{Q}) \) in \( X_{G(N)}(\mathbb{Q}_v) \). If \( X_{G(N)} \) has genus 0, then \( S \) clearly has positive density.

Now take any elliptic curve \( E/\mathbb{Q} \) with \( j_E \in \pi_{G(N)}(S) \) and any prime \( \ell > \max\{37, e\} \); it is non-CM since its \( j \)-invariant is not an integer. We claim that \( \rho_{E, \ell} \) is surjective. The lemma will follow from the claim after using Proposition 4.9 to remove a finite subset from \( S \) to ensure the surjectivity of \( \rho_{E, \ell} \) for \( 13 < \ell \leq \max\{37, e\} \).

Suppose that \( \rho_{E, \ell} \) is not surjective. From Lemmas 16, 17 and 18 in [Ser81], we find that \( \rho_{E, \ell}(\text{Gal}_{\mathbb{Q}}) \) is contained in the normalizer of a Cartan subgroup of \( \text{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \). In particular, the order of \( \rho_{E, \ell}(\text{Gal}_{\mathbb{Q}}) \) is not divisible by \( \ell \).

We have \( v_p(j_E) = -e < 0 \) since \( j_E \in \pi_{G(N)}(S) \). Let \( E'/\mathbb{Q}_p \) be the Tate curve with \( j \)-invariant \( j_E \); see [Ser98, IV Appendix A.1] for details. From the proposition in [Ser98, IV Appendix A.1.5] and our assumption \( \ell > e \), we find that \( \rho_{E', \ell}(\text{Gal}_{\mathbb{Q}_p}) \) contains an element of order \( \ell \). Since \( E' \) and \( E \) have the same \( j \)-invariant, they become isomorphic over some quadratic extension of \( \mathbb{Q}_p \). Since \( \ell \) is odd, we deduce that \( \rho_{E, \ell}(\text{Gal}_{\mathbb{Q}}) \) contains an element of order \( \ell \). This contradicts that the order of \( \rho_{E, \ell}(\text{Gal}_{\mathbb{Q}}) \) is not divisible by \( \ell \). Therefore, \( \rho_{E, \ell} \) is surjective as claimed.

Let \( W \) and \( S \) be the sets from Lemma 6.3 and Lemma 6.4, respectively. Take any elliptic curve \( E/\mathbb{Q} \) with \( j_E \in \pi_{G(N)}(S - W) \). Lemma 6.4 implies that the representation \( \rho_{E, \ell} \) is surjective for all

22
\( \ell > 13. \) Lemma 6.3 then implies that \( [\text{GL}_2(\hat{\mathbb{Z}}) : \rho_E(\text{Gal}_\mathbb{Q})] = n. \) Therefore, \( J_n \supseteq \pi_{G(N)}(S - W). \) So to prove that \( J_n \) is infinite, it suffices to show that the set \( S - W \) is infinite.

First suppose that \( X_{G(N)} \) has genus 0. The set \( W \) is a thin subset of \( X_{G(N)}(\mathbb{Q}) \cong \mathbb{P}^1(\mathbb{Q}) \) in the language of [Ser97, §9.1]; this uses that the union defining \( W \) is finite and that the morphisms \( \varphi_B \) are dominant with degree at least 2. From [Ser97, §9.7], we find that \( W \) has density 0. Since \( S \) has positive density, we deduce that \( S - W \) is infinite.

Finally suppose that \( X_{G(N)} \) has genus 1. Since \( S \) is infinite, it suffices to show that \( W \) is finite. So take any proper subgroup \( B \) of \( G(M) \) satisfying \( \det(B) = (\mathbb{Z}/M\mathbb{Z})^\times \) and \( -I \in B. \) It thus suffices to show that the set \( X_B(\mathbb{Q}) \) is finite. The morphism \( \varphi_B : X_B \to X_{G(N)} \) is dominant, so \( X_B \) has genus at least 1. If \( X_B \) has genus greater than 1, then \( X_B(\mathbb{Q}) \) is finite by Faltings' theorem. We are left to consider the case where \( X_B \) has genus 1. Let \( \Gamma_B \) be the congruence subgroup associated to \( X_B; \) it has genus 1. We have \( \Gamma_B \subseteq \Gamma \) and hence the level of \( \Gamma_B \) is divisible by \( N_0. \) We have \( [\text{SL}_2(\mathbb{Z}) : \Gamma_B] = [\text{GL}_2(\mathbb{Z}/M\mathbb{Z}) : B] \) and hence \( b := [\text{GL}_2(\mathbb{Z}/M\mathbb{Z}) : G(M)] = [\text{GL}_2(\mathbb{Z}/N\mathbb{Z}) : G(N)] \) is a proper divisor of \( [\text{SL}_2(\mathbb{Z}) : \Gamma_B]. \) From the computations in §5.3, we may assume that \( G(N) \) is equal to one of the groups denoted \( G_1, G_2, G_3 \) or \( G_4. \) In particular, we have \( (N_0, b) \in \{(11, 55), (15, 30), (15, 45), (21, 63)\}. \) From the classification in [CP03], we find that there are no genus 1 congruence subgroups of \( \text{SL}_2(\mathbb{Z}) \) containing \( -I \) whose level is divisible by \( N_0 \) and whose index in \( \text{SL}_2(\mathbb{Z}) \) has \( b \) as a proper divisor. So the case where \( X_B \) has genus 1 does not occur and we are done.

**References**

[BCP97] Web 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).

[Cen16] Tommaso Giorgio Centeleghe, *Integral Tate modules and splitting of primes in torsion fields of elliptic curves*, Int. J. Number Theory 12 (2016), no. 1, 237–248. MR3455277

[Cre] J. E. Cremona, *Elliptic Curve Data* (webpage). http://johncremona.github.io/ecdata/.

[CP03] C. J. Cummins and S. Pauli, *Congruence subgroups of PSL(2, Z) of genus less than or equal to 24*, Experiment. Math. 12 (2003), no. 2, 243–255. MR2016709

[DR73] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Inst. Hautes Études Sci. Publ. Math. 24 (1961–63), 143–221. Distribution of Frobenius automorphisms in \( \text{GL}_2 \)-extensions, Lecture Notes in Mathematics, Vol. 504, Springer-Verlag, Berlin, 1976. Distribution of Frobenius automorphisms in \( \text{GL}_2 \)-extensions of the rational numbers. MR0568299 (58 #27900)

[Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points fini des courbes elliptiques*, Invent. Math. 15 (1972), no. 4, 259–331. MR0387283

[Ser81] ______, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. 54 (1981), 323–401. MR644559

[Ser89] ______, *Abelian l-adic representations and elliptic curves*, Second, Advanced Book Classics, Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1989. With the collaboration of Willem Kuyk and John Labute. MR1043865

[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

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

[Vé74] Jacques Vélu, *Les points rationnels de \( X_0(37) \)*, Journées Arithmétiques (Grenoble, 1973), 1974, pp. 169–179. Bull. Soc. Math. France Mém., 37. MR0366930 (51 #3176)
[Zyw10] David Zywina, *Elliptic curves with maximal Galois action on their torsion points*, Bull. London Math. Soc. 42 (2010), no. 5, 811–826. ↑4.4

Department of Mathematics, Cornell University, Ithaca, NY 14853, USA

Email address: zywina@math.cornell.edu

URL: http://www.math.cornell.edu/~zywina