# EXPLICIT OPEN IMAGES FOR ELLIPTIC CURVES OVER $\mathbb{Q}$

DAVID ZYWINA

ABSTRACT. For a non-CM elliptic curve $E$ defined over $\mathbb{Q}$, the Galois action on its torsion points gives rise to a Galois representation $\rho_E\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$ that is unique up to isomorphism. A renowned theorem of Serre says that the image of $\rho_E$ is an open, and hence finite index, subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. We describe an algorithm that computes the image of $\rho_E$ up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$; this algorithm is practical and has been implemented. Up to a positive answer to a uniformity question of Serre and finding all the rational points on a finite number of explicit modular curves of genus at least 2, we give a complete classification of the groups $\rho_E(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ and the indices $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))]$ for non-CM elliptic curves $E/\mathbb{Q}$. Much of the paper is dedicated to the efficient computation of modular curves via modular forms expressed in terms of Eisenstein series.

## 1. INTRODUCTION

1.1. **Serre's open image theorem.** Consider an elliptic curve $E$ defined over $\mathbb{Q}$. For each integer $N > 1$, let $E[N]$ be the $N$-torsion subgroup of $E(\overline{\mathbb{Q}})$, where $\overline{\mathbb{Q}}$ is a fixed algebraic closure of $\mathbb{Q}$. The group $E[N]$ is a free $\mathbb{Z}/N\mathbb{Z}$-module of rank 2. There is a natural action of the absolute Galois group $\mathrm{Gal}_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E[N]$ that respects the group structure and which we may express in terms of a representation

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

By choosing compatible bases and taking the inverse limit, we can combine these representations into a single representation

$$\rho_E\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$$

that encodes the Galois action on all the torsion points of $E$. Here the ring $\widehat{\mathbb{Z}}$ is the profinite completion of $\mathbb{Z}$. The representation $\rho_E$ is uniquely determined up to isomorphism and hence the image $\rho_E(\mathrm{Gal}_{\mathbb{Q}})$ is uniquely determined up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

With respect to the profinite topology, we find that $\rho_E(\mathrm{Gal}_{\mathbb{Q}})$ is a closed subgroup of the compact group $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. In [Ser72], Serre proved the following theorem which says that, up to finite index, the image of $\rho_E$ is as large as possible when $E$ is non-CM (it was actually shown for elliptic curves over general number fields, but we will restrict our attention to the rationals).

**Theorem 1.1** (Serre's open image theorem)**.** *Let $E$ be a non-CM elliptic curve defined over $\mathbb{Q}$. Then $\rho_E(\mathrm{Gal}_{\mathbb{Q}})$ is an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. Equivalently, $\rho_E(\mathrm{Gal}_{\mathbb{Q}})$ is a finite index subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.*

The group $\rho_E(\mathrm{Gal}_{\mathbb{Q}})$, when known, will have a simple description since it is open in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, i.e., it is given by its level $N$ and a set of generators for its image modulo $N$ in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. For a definition of the level and other conventions see §1.12. Unfortunately, Serre's proof is in general ineffective.

The goal of this work is to explain how, given a non-CM elliptic curve $E/\mathbb{Q}$, we can compute the group $\rho_E(\mathrm{Gal}_{\mathbb{Q}})$ up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. The algorithm we obtain is practical. For example, we have used it to compute the image of $\rho_E$, up to conjugacy, for all non-CM elliptic curves $E/\mathbb{Q}$ with conductor up to 500000 (on the machine we ran it on, it took on average 0.015 seconds per

curve). We have implemented our algorithms in `Magma` [BCP97] and our code can be found in the public repository [Zyw22].

A large part of Serre's paper [Ser72] is dedicated to showing that $\rho_{E,\ell}$ is surjective for all sufficiently large primes $\ell$. Serre asked whether there is a constant $C$, not depending on $E$, such that $\rho_{E,\ell}$ is surjective for all primes $\ell > C$, cf. [Ser72, §4.3]. Moreover, he asks whether $\rho_{E,\ell}$ is surjective for all $\ell > 37$ [Ser81, p. 399]. We pose as a conjecture a slightly stronger version (it was conjectured independently in [Zyw15b] and [Sut16]). We denote the $j$-invariant of $E$ by $j_E$.

**Conjecture 1.2.** *If $E$ is a non-CM elliptic curve over $\mathbb{Q}$ and $\ell > 13$ is a prime, then either $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ or*

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

Assuming Conjecture 1.2, one can show that the indices $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(\mathrm{Gal}_{\mathbb{Q}})]$ are uniformly bounded as we vary over all non-CM elliptic curves $E/\mathbb{Q}$, cf. [Zyw15a, Theorem 1.3]. Based on the computations arising in this paper, we make the following prediction.

**Conjecture 1.3.** *We have $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(\mathrm{Gal}_{\mathbb{Q}})] \leq 2736$ for all non-CM elliptic curve $E$ over $\mathbb{Q}$.*

*Remark* 1.4. An elliptic curve $E/\mathbb{Q}$ with $j$-invariant $-7\cdot 11^3$ or $-7\cdot 137^3\cdot 2083^3$ satisfies $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(\mathrm{Gal}_{\mathbb{Q}})] = 2736$. Such non-CM elliptic curves $E/\mathbb{Q}$ are special because they have an isogeny of degree 37 defined over $\mathbb{Q}$. In particular, the upper bound in Conjecture 1.3 would be best possible.

We now make a braver conjecture on the possible values of the index $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(\mathrm{Gal}_{\mathbb{Q}})]$. This conjecture holds assuming Conjecture 1.2 and assuming that we have not missed any rational points on the high genus modular curves that arise in our computations.

**Conjecture 1.5.** *If $E$ is a non-CM elliptic curve defined over $\mathbb{Q}$, then the index $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(\mathrm{Gal}_{\mathbb{Q}})]$ lies in the set*

$$\left\{ \begin{array}{c} 2, 4, 6, 8, 10, 12, 16, 20, 24, 30, 32, 36, 40, 48, 54, 60, 72, 80, 84, 96, 108, \\ 112, 120, 128, 144, 160, 182, 192, 200, 216, 220, 224, 240, 288, 300, 336, \\ 360, 384, 480, 504, 576, 768, 864, 1152, 1200, 1296, 1536, 2736 \end{array} \right\}.$$

*Remark* 1.6. All of the integers in the set from Conjecture 1.5 actually occur as an index $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(\mathrm{Gal}_{\mathbb{Q}})]$ for some non-CM elliptic curve $E/\mathbb{Q}$.

In our arguments, it will often be convenient to work with the dual representation

$$\rho_E^*\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$$

of $\rho_E$, i.e., $\rho_E^*(\sigma)$ is the transpose of $\rho_E(\sigma^{-1})$. Similarly, we can define $\rho_{E,N}^*(\sigma)$ to be the transpose of $\rho_{E,N}(\sigma^{-1})$. Of course, computing the images of $\rho_E^*$ and $\rho_E$ are equivalent problems and their images have the same index in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

For a prime $\ell$, let $\rho_{E,\ell^\infty}\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ be the representation obtained by taking the inverse limit of the $\rho_{E,\ell^n}$; equivalently, $\rho_{E,\ell^\infty}$ is the composition of $\rho_E$ with the $\ell$-adic projection.

1.2. **The Kronecker–Weber constraint on the image.** For a fixed non-CM elliptic curve $E/\mathbb{Q}$, consider the group $G_E := \rho_E^*(\mathrm{Gal}_{\mathbb{Q}}) \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$. The group $G_E$ is open in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ by Theorem 1.1. We have $\det(G_E) = \widehat{\mathbb{Z}}^\times$ since $\det\circ\rho_E^* = \chi_{\mathrm{cyc}}^{-1}$, where $\chi_{\mathrm{cyc}}\colon \mathrm{Gal}_{\mathbb{Q}} \to \widehat{\mathbb{Z}}^\times$ is the cyclotomic character, cf. §2.

We also have the following important constraint on $G_E$ that arises from the Kronecker–Weber theorem. For a group $G$, we will denote its commutator subgroup by $[G, G]$.

**Lemma 1.7.** *We have* $G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = [G_E, G_E]$. *In particular,*

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E] = [\mathrm{SL}_2(\widehat{\mathbb{Z}}) : [G_E, G_E]].$$

*Proof.* Let $\mathbb{Q}^{\mathrm{ab}} \subseteq \overline{\mathbb{Q}}$ be the maximal abelian extension of $\mathbb{Q}$. Since $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}})$ is the commutator subgroup of $\mathrm{Gal}_{\mathbb{Q}}$, we have $\rho_E^*(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}})) = [G_E, G_E]$. By the Kronecker–Weber theorem, $\mathbb{Q}^{\mathrm{ab}}$ is the cyclotomic extension of $\mathbb{Q}$. Since $\chi_{\mathrm{cyc}}^{-1} = \det \circ \rho_E^*$, we deduce that $G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = \rho_E^*(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}}))$. We obtain $G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = [G_E, G_E]$ by comparing our two descriptions of $\rho_E^*(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}}))$. Since $\det(G_E) = \widehat{\mathbb{Z}}^\times$, we have $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E] = [\mathrm{SL}_2(\widehat{\mathbb{Z}}) : G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})]$. The lemma is now immediate. □

*Example* 1.8. The commutator subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ is an index 2 subgroup of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$, cf. Lemma 7.7, so the index of $[G_E, G_E]$ in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ is even. Therefore, the index of $G_E$ in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ is even by Lemma 1.7. In particular, $G_E \neq \mathrm{GL}_2(\widehat{\mathbb{Z}})$; this was first observed by Serre, cf. Proposition 22 of [Ser72]. Moreover, the image of $G_E$ lies in a specific index 2 subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, cf. §1.6.

1.3. **Modular curves.** Let $E/\mathbb{Q}$ be a non-CM elliptic curve and set $G_E := \rho_E^*(\mathrm{Gal}_{\mathbb{Q}})$. Our main tool for studying the group $G_E$ is the theory of *modular curves*.

Consider any open subgroup $G$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ that satisfies $\det(G) = \widehat{\mathbb{Z}}^\times$ and $-I \in G$. Associated to $G$, we will define a modular curve $X_G$, cf. §3. The modular curve $X_G$ is a smooth, projective and geometrically irreducible curve defined over $\mathbb{Q}$ that comes with a morphism

$$\pi_G \colon X_G \to \mathbb{P}^1_{\mathbb{Q}} = \mathbb{A}^1_{\mathbb{Q}} \cup \{\infty\}.$$

For our applications to Serre's open image theorem, the key property of the curve $X_G$ is that $G_E$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a subgroup of $G$ if and only if the $j$-invariant $j_E$ of $E$ lies in the set $\pi_G(X_G(\mathbb{Q})) \subseteq \mathbb{Q} \cup \{\infty\}$. We say that a point $P \in X_G(\mathbb{Q})$ is non-CM if $\pi_G(P) \in \mathbb{Q} \cup \{\infty\}$ is the $j$-invariant of a non-CM elliptic curve.

The pairs $(X_G, \pi_G)$, as we vary over all $G$, will thus determine the image of $G_E$ in $\mathrm{GL}_2(\widehat{\mathbb{Z}})/\{\pm I\}$ up to conjugacy. However, this is an impractical approach for finding $G_E$ since there are *infinitely many* groups $G$ to consider. In fact, infinitely many open subgroups of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ arise as $G_E$ for a non-CM elliptic curve $E/\mathbb{Q}$.

In §5, we will describe a method for computing an explicit model for the modular curve $X_G$ given a group $G$. We are also interested in computing $\pi_G$ in terms of our model. Our approach to computing modular curves is via related spaces of modular forms that we study in §4. Our application involves computing thousands of modular curves, so we are especially interested in finding efficient techniques.

1.4. **Agreeable closures.** Instead of computing $G_E = \rho_E^*(\mathrm{Gal}_{\mathbb{Q}})$ directly, we first find a larger and friendlier group. We say that a subgroup $\mathcal{G}$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ is agreeable if it is open in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, has full determinant, contains all the scalar matrices, and the levels of $\mathcal{G}$ and $\mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and $\mathrm{SL}_2(\widehat{\mathbb{Z}})$, respectively, have the same odd prime divisors.

There is a unique minimal agreeable subgroup $\mathcal{G}_E$ satisfying $G_E \subseteq \mathcal{G}_E$ which we call the agreeable closure of $G_E$, cf. §8. The group $G_E$ is normal in $\mathcal{G}_E$ and the quotient group $\mathcal{G}_E/G_E$ is finite and abelian, cf. Proposition 8.1.

We claim that $[G_E, G_E] = [\mathcal{G}_E, \mathcal{G}_E]$. We have $[\mathcal{G}_E, \mathcal{G}_E] \subseteq G_E$ since $\mathcal{G}_E/G_E$ is abelian and hence $[\mathcal{G}_E, \mathcal{G}_E] \subseteq G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. By Lemma 1.7, this gives the inclusion $[\mathcal{G}_E, \mathcal{G}_E] \subseteq [G_E, G_E]$. The claim follows since the other inclusion is a consequence of $G_E \subseteq \mathcal{G}_E$.

In particular, the agreeable group $\mathcal{G}_E$ determines $G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = [\mathcal{G}_E, \mathcal{G}_E]$, up to conjugation in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, and also determines the index $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E] = [\mathrm{SL}_2(\widehat{\mathbb{Z}}) : [\mathcal{G}_E, \mathcal{G}_E]]$. The advantage of agreeable groups is that are far fewer of them to consider. In fact, if Conjecture 1.2 holds for $E$,

then any prime dividing the level of $\mathcal{G}_E$ in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ must lie in the set

$$\mathcal{L} := \{2, 3, 5, 7, 11, 13, 17, 37\},$$

cf. Lemma 10.1. From this, one can show that there are only *finitely many* agreeable groups of the form $\mathcal{G}_E$ as we vary over *all* non-CM elliptic curves $E/\mathbb{Q}$ for which Conjecture 1.2 holds.

The following theorem summarizes some details of our computations.

**Theorem 1.9.** *We can compute a finite set $\mathscr{A}$ of agreeable subgroups that are pairwise non-conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and satisfy the following conditions:*

(a) *For every group $\mathcal{G} \in \mathscr{A}$, the level of $\mathcal{G}$ is not divisible by any prime $\ell \notin \mathcal{L}$.*

(b) *Let $G$ be any agreeable subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ for which the level of $G$ is divisible only by primes in the set $\mathcal{L}$ and for which $X_G(\mathbb{Q})$ has a non-CM point.*
- *If $X_G(\mathbb{Q})$ is infinite, then $G$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to some group $\mathcal{G} \in \mathscr{A}$.*
- *If $X_G(\mathbb{Q})$ is finite, then $G$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a subgroup of some $\mathcal{G} \in \mathscr{A}$ with $X_{\mathcal{G}}(\mathbb{Q})$ finite.*

(c) *If $\mathcal{G} \in \mathscr{A}$ is a group for which $X_{\mathcal{G}}(\mathbb{Q})$ is finite, then $X_G(\mathbb{Q})$ is infinite for all agreeable groups $\mathcal{G} \subsetneq G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$.*

(d) *If $\mathcal{G} \in \mathscr{A}$ is a group for which $X_{\mathcal{G}}(\mathbb{Q})$ has genus at most 1, then $X_{\mathcal{G}}(\mathbb{Q})$ has a non-CM point.*

(e) *For any group $\mathcal{G} \in \mathscr{A}$ for which $X_{\mathcal{G}}$ has genus at most 1, we can compute a model for the curve $X_{\mathcal{G}}$ and, with respect to this model, compute the morphism $\pi_{\mathcal{G}}$ from $X_{\mathcal{G}}$ to the $j$-line.*

(f) *For any group $\mathcal{G} \in \mathscr{A}$ and rational number $j \in \mathbb{Q} - \{0, 1728\}$, we can determine whether $\pi_{\mathcal{G}}(P) = j$ for some $P \in X_{\mathcal{G}}(\mathbb{Q})$.*

Our set $\mathscr{A}$ contains 315 groups $\mathcal{G}$ for which $X_{\mathcal{G}}$ has genus 0 (and hence $X_{\mathcal{G}}$ is isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$ since it has a rational point). Our set $\mathscr{A}$ contains 139 and 17 groups $\mathcal{G}$ for which $X_{\mathcal{G}}$ has genus 1 and $X_{\mathcal{G}}(\mathbb{Q})$ is infinite or finite, respectively.

Our original set $\mathscr{A}$ constructed contained thousands of groups $\mathcal{G}$ for which $X_{\mathcal{G}}$ has genus at least 2. For each such group $\mathcal{G}$, $X_{\mathcal{G}}(\mathbb{Q})$ is finite by Faltings; unfortunately, $X_{\mathcal{G}}(\mathbb{Q})$ can sometimes be extremely difficult to compute. Observe that whenever one can show that $X_{\mathcal{G}}(\mathbb{Q})$ has no non-CM points, then we can remove $\mathcal{G}$ from $\mathscr{A}$. In our set $\mathscr{A}$, we know of 53 groups $\mathcal{G}$ so that $X_{\mathcal{G}}$ has genus at least 2 and $X_{\mathcal{G}}(\mathbb{Q})$ has a non-CM point; these give rise to 81 exceptional $j$-invariants of non-CM elliptic curves.

We will now outline how to compute $\mathcal{G}_E$, up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, for a fixed non-CM elliptic curve $E/\mathbb{Q}$. Again recall that once we know $\mathcal{G}_E$, we can then compute $G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = [\mathcal{G}_E, \mathcal{G}_E]$ up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, cf. §7.3.1 for how to compute commutator subgroups. We can thus also compute the index $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(\mathrm{Gal}_{\mathbb{Q}})] = [\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E] = [\mathrm{SL}_2(\widehat{\mathbb{Z}}) : [\mathcal{G}_E, \mathcal{G}_E]]$.

Consider the case where Conjecture 1.2 holds for $E/\mathbb{Q}$ and $j_E$ is not in the finite set

$$\mathcal{J} := \bigcup_{G \in \mathscr{A},\, X_G(\mathbb{Q}) \text{ finite}} \pi_G(X_G(\mathbb{Q})).$$

We can verify whether $E/\mathbb{Q}$ satisfies these condition by using the algorithm from [Zyw20b] and Theorem 1.9(f). (For non-CM elliptic curves over $\mathbb{Q}$ that do not satisfy these conditions, we will take any alternate and more direct approach later.)

Let us now explain how Theorem 1.9 allows us to compute the group $\mathcal{G}_E$ up to conjugacy; more details can be found in §10. We have $j_E \in \pi_{\mathcal{G}_E}(X_{\mathcal{G}_E}(\mathbb{Q}))$ since $\rho_E^*(\mathrm{Gal}_{\mathbb{Q}}) \subseteq \mathcal{G}_E$. In particular, $X_{\mathcal{G}_E}(\mathbb{Q})$ contains a non-CM point. Our assumption that Conjecture 1.2 holds for $E$ implies that

the level of $\mathcal{G}_E$ is not divisible by any prime $\ell \notin \mathcal{L}$, cf. §10.1. If $\mathcal{G}_E$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a subgroup of some group $\mathcal{G} \in \mathscr{A}$ with $X_{\mathcal{G}}(\mathbb{Q})$ finite, then we have $j_E \in \pi_{\mathcal{G}}(X_{\mathcal{G}}(\mathbb{Q}))$ which contradicts $j_E \notin \mathcal{J}$. Therefore, $\mathcal{G}_E$ is not conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a subgroup of any $\mathcal{G} \in \mathscr{A}$ with $X_{\mathcal{G}}(\mathbb{Q})$ finite. Applying Theorem 1.9(b), we deduce that $\mathcal{G}_E$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a unique group $\mathcal{G} \in \mathscr{A}$. So let $\mathcal{G}$ be a group in $\mathscr{A}$ with maximal index in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ amongst those that satisfy $j_E \in \pi_{\mathcal{G}}(X_{\mathcal{G}}(\mathbb{Q}))$; this can be found using Theorem 1.9(f). Then the explicit group $\mathcal{G}$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to the agreeable closure $\mathcal{G}_E$ of $G_E$.

1.5. **Finding the image of Galois.** Let $E$ be a non-CM elliptic curve over $\mathbb{Q}$. Suppose that we have found an agreeable subgroup $\mathcal{G}$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ such that, after possibly conjugating $G_E := \rho_E^*(\mathrm{Gal}_{\mathbb{Q}})$ in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, $G_E$ is a subgroup of $\mathcal{G}$ satisfying $G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = [\mathcal{G}, \mathcal{G}]$. In particular, $G_E$ is a normal subgroup of $\mathcal{G}$ and $\mathcal{G}/G_E$ is finite and abelian. As noted in §1.4, the agreeable closure $\mathcal{G}_E$ of $G_E$ will satisfy these properties and is computable.

Choose an open subgroup $G$ of $\mathcal{G}$ satisfying $\det(G) = \widehat{\mathbb{Z}}^\times$ and $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = [\mathcal{G}, \mathcal{G}]$. Note that such a subgroup $G$ exists since the (unknown) group $G_E$ will have these properties. In practice, we choose $G$ with minimal possible level. Note that $G$ is a normal subgroup of $\mathcal{G}$ and that $\mathcal{G}/G$ is finite and abelian.

Let $\alpha_E\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathcal{G}/G$ be the homomorphism that is the composition of $\rho_E^*\colon \mathrm{Gal}_{\mathbb{Q}} \to G_E \subseteq \mathcal{G}$ with the quotient map $\mathcal{G} \to \mathcal{G}/G$. Since $\mathcal{G}/G$ is abelian, there is a unique homomorphism

$$\gamma_E\colon \widehat{\mathbb{Z}}^\times \to \mathcal{G}/G$$

satisfying $\gamma_E(\chi_{\mathrm{cyc}}(\sigma)^{-1}) = \alpha_E(\sigma)$ for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$. Now define

$$\mathcal{H}_E := \{g \in \mathcal{G} : g \cdot G = \gamma_E(\det g)\}; \tag{1.1}$$

it is a subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and the following lemma shows that it is the image of $\rho_E^*$ up to conjugacy.

**Lemma 1.10.** *The groups $G_E = \rho_E^*(\mathrm{Gal}_{\mathbb{Q}})$ and $\mathcal{H}_E$ are conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.*

*Proof.* For any $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$, we have

$$\rho_E^*(\sigma) \cdot G = \alpha_E(\sigma) = \gamma_E(\chi_{\mathrm{cyc}}(\sigma)^{-1}) = \gamma_E(\det(\rho_E^*(\sigma))).$$

In particular, $G_E$ is a subgroup of $\mathcal{H}_E$. By assumption, we have $G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = [\mathcal{G}, \mathcal{G}]$ and hence

$$\mathcal{H}_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = [\mathcal{G}, \mathcal{G}] = G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}).$$

Since $G_E$ is a subgroup of $\mathcal{H}_E$ with $G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = \mathcal{H}_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ and $\det(G_E) = \widehat{\mathbb{Z}}^\times$, we deduce that $G_E = \mathcal{H}_E$. □

Since $G_E$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to the group $\mathcal{H}_E$, computing the image of $\rho_E^*$ reduces to the problem of finding $\gamma_E$.

*Remark* 1.11. The notation $\alpha_E$, $\gamma_E$ and $\mathcal{H}_E$ suppresses the dependence on the choice of conjugate of $\rho_E^*$ for which $\rho_E^*(\mathrm{Gal}_{\mathbb{Q}}) \subseteq \mathcal{G}$. However, the group $\mathcal{H}_E$, up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, depends only on $E$.

We now give an alternate description of $\gamma_E$ and an overview of how we will compute it.

Define the open subvariety $U_{\mathcal{G}} := X_{\mathcal{G}} - \pi_{\mathcal{G}}^{-1}(\{0, 1728, \infty\})$ of $X_{\mathcal{G}}$. In §11, we shall describe a particular étale cover $\phi\colon Y \to U_{\mathcal{G}}$ that is Galois with group $\mathcal{G}/G$. When $-I \in G$, we will have $Y = U_G \subseteq X_G$ and $\phi$ will be the natural morphism. The main task in §11 is computing models for $Y$ and $U_{\mathcal{G}}$, with the action of $\mathcal{G}/G$ on $Y$, and finding the corresponding $\phi$ with respect to these models. Note that from §1.4, we need only consider a finite number of agreeable groups $\mathcal{G}$ if we restrict to non-CM $E/\mathbb{Q}$ for which Conjecture 1.2 holds.

Since $G_E$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a subgroup of $\mathcal{G}$ and we have a model for $U_{\mathcal{G}}$, we can choose an explicit rational point $u \in U_{\mathcal{G}}(\mathbb{Q})$ such that $\pi_{\mathcal{G}}(u) = j_E$. The fiber $\phi^{-1}(u) \subseteq Y(\overline{\mathbb{Q}})$ has a simply transitive $\mathcal{G}/G$-action. We also have a $\mathrm{Gal}_{\mathbb{Q}}$-action on $\phi^{-1}(u)$ since $\phi$ and $u$ are defined over $\mathbb{Q}$. The actions of $\mathcal{G}/G$ and $\mathrm{Gal}_{\mathbb{Q}}$ on $\phi^{-1}(u)$ commute. Fix an element $y \in Y(\overline{\mathbb{Q}})$ with $\phi(y) = u$. For each $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$, we have

$$\sigma(y) = \alpha_u(\sigma) \cdot y$$

for a unique $\alpha_u(\sigma) \in \mathcal{G}/G$. In this manner, we obtain a homomorphism $\alpha_u \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathcal{G}/G$. Since $\mathcal{G}/G$ is abelian, $\alpha_u$ does not depend on the choice of $y$. Our models produce an explicit description of $\alpha_u$. For any sufficiently large prime $p$, by reducing our models modulo $p$ we will be able to verify that $\alpha_u$ is unramified at $p$ and also compute $\alpha_u(\mathrm{Frob}_p) \in \mathcal{G}/G$.

After possibly replacing $\rho_E^*$ by an isomorphic representation that still satisfies $G_E := \rho_E^*(\mathrm{Gal}_{\mathbb{Q}}) \subseteq \mathcal{G}$ and $G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = [\mathcal{G}, \mathcal{G}]$, we will show in §11.2 that $\alpha_E = \chi_d \cdot \alpha_u$, where $\chi_d \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \hookrightarrow \{\pm 1\}$ is the quadratic character arising from a certain squarefree integer $d$ (the $d$ is chosen so that the quadratic twist of $E$ by $d$ is isomorphic to an explicit elliptic curve over $\mathbb{Q}$ with the same $j$-invariant). With this $\alpha_E$ and any sufficiently large prime $p$, we can verify that $\chi_d$ and $\alpha_u$ are unramified at $p$ and compute $\alpha_E(\mathrm{Frob}_p) = \chi_d(\mathrm{Frob}_p)\alpha_u(\mathrm{Frob}_p)$.

The homomorphism $\alpha_E$ factors through $\rho_{E,N}^*$, where $N$ is the level of $G$. Therefore, $\alpha_E$ is unramified at all primes $p \nmid M$, where $M$ is the product of $N$ and the primes $p$ for which $E$ has bad reduction. So the corresponding $\gamma_E$ factors through a homomorphism

$$\overline{\gamma}_E \colon \mathbb{Z}_M^\times/(\mathbb{Z}_M^\times)^e \to \mathcal{G}/G,$$

where $e$ is the exponent of the group $\mathcal{G}/G$ and $\mathbb{Z}_M = \prod_{\ell \mid M} \mathbb{Z}_\ell$. So to compute $\gamma_E$, it suffices to find $\overline{\gamma}_E(p \cdot (\mathbb{Z}_M^\times)^e) = \alpha_E(\mathrm{Frob}_p)^{-1} \in \mathcal{G}/G$ for a finite set of primes $p \nmid M$ that generate the finite group $\mathbb{Z}_M^\times/(\mathbb{Z}_M^\times)^e$.

So by computing $\alpha_E(\mathrm{Frob}_p)$ for enough primes $p \nmid M$, we obtain $\gamma_E$ and hence can compute the group $\mathcal{H}_E$. This will complete the computation of $\rho_E^*(\mathrm{Gal}_{\mathbb{Q}})$, up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, since it is conjugate to $\mathcal{H}_E$.

*Remark* 1.12. . Let us make clear what we mean that $\mathcal{H}_E$ is computable. That we have computed $\gamma_E$ means we have a positive integer $D \geq 1$ such that $\gamma_E$ factors through a homomorphism $(\mathbb{Z}/D\mathbb{Z})^\times \to \mathcal{G}/G$. We also know the groups $\mathcal{G}$ and $G$, i.e., we have an integer $N \geq 1$ that is divisible by the levels of $\mathcal{G}$ and $G$, and we have a set of generators for the image in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ of $\mathcal{G}$ and $G$. Let $N'$ be the least common multiple of $N$ and $D$. Then $\mathcal{H}_E$ is an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ whose level divides $N'$ and we can find explicit generators for the image of $\mathcal{H}_E$ in $\mathrm{GL}_2(\mathbb{Z}/N'\mathbb{Z})$ under reduction modulo $N'$.

1.6. **Example: Serre curves.** Let us consider the largest agreeable group $\mathcal{G} := \mathrm{GL}_2(\widehat{\mathbb{Z}})$. The commutator subgroup $[\mathcal{G}, \mathcal{G}]$ is the unique subgroup of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ with level 2 and index 2, cf. Lemma 7.7. Let $G$ be the unique subgroup of $\mathcal{G} = \mathrm{GL}_2(\widehat{\mathbb{Z}})$ with level 2 and index 2. We have $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = [\mathcal{G}, \mathcal{G}]$, $\det(G) = \widehat{\mathbb{Z}}^\times$, and $\mathcal{G}/G$ is cyclic of order 2.

For a squarefree integer $d$, let $\gamma_d \colon \widehat{\mathbb{Z}}^\times \to \mathcal{G}/G$ be the unique homomorphism for which $\mathrm{Gal}_{\mathbb{Q}} \to \mathcal{G}/G$, $\sigma \mapsto \gamma_d(\chi_{\mathrm{cyc}}(\sigma)^{-1})$ factors through $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \hookrightarrow \mathcal{G}/G$. After fixing an isomorphism $\mathcal{G}/G \xrightarrow{\sim} \{\pm 1\}$, $\gamma_d$ factors through the *Kronecker character* of $\mathbb{Q}(\sqrt{d})$. Define the group

$$G_{\gamma_d} := \{g \in \mathcal{G} : g \cdot G = \gamma_d(\det g)\}.$$

Observe that $G_{\gamma_d}$ is an open subgroup of $\mathcal{G} = \mathrm{GL}_2(\widehat{\mathbb{Z}})$ with index 2 that satisfies $\det(G_{\gamma_d}) = \widehat{\mathbb{Z}}^\times$ and $G_{\gamma_d} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = [\mathcal{G}, \mathcal{G}]$. We have $G_{\gamma_1} = G$.

Now consider any non-CM elliptic curve $E/\mathbb{Q}$ and set $G_E := \rho_E^*(\mathrm{Gal}_\mathbb{Q})$. As noted in Remark 1.8, the index of $G_E$ in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ is always divisible by 2. Moreover, we can show that $G_E$ is contained in an explicit index 2 subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. Let $\alpha_E\colon \mathrm{Gal}_\mathbb{Q} \to \mathcal{G}/G$ be the composition of $\rho_E^*$ with the obvious quotient map. Let $\gamma_E\colon \widehat{\mathbb{Z}}^\times \to \mathcal{G}/G$ be the homomorphism satisfying $\gamma_E(\chi_{\mathrm{cyc}}(\sigma)^{-1}) = \alpha_E(\sigma)$ for all $\sigma \in \mathrm{Gal}_\mathbb{Q}$. We have $\gamma_E = \gamma_d$ for a unique squarefree integer $d$ and hence

$$G_E \subseteq G_{\gamma_d}$$

since $\rho_E^*(\sigma) \cdot G = \alpha_E(\sigma) = \gamma_E(\chi_{\mathrm{cyc}}(\sigma)^{-1}) = \gamma_d(\det \rho_E^*(\sigma))$. Since $G$ has level 2, the integer $d$ can be found by studying the 2-torsion of $E$. A direct computation shows that $d \in \Delta \cdot (\mathbb{Q}^\times)^2$, where $\Delta$ is the discriminant of a Weierstrass model of $E/\mathbb{Q}$. One can show that $\Delta \cdot (j_E - 1728)$ is always a square in $\mathbb{Q}$ so $d \in (j_E - 1728) \cdot (\mathbb{Q}^\times)^2$.

Following Lang and Trotter [LT76], we say that a (non-CM) $E/\mathbb{Q}$ is a Serre curve if $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E] = 2$. Thus Serre curves are elliptic curves $E/\mathbb{Q}$ for which the image of $\rho_E$ is as "large as possible". Equivalently, a non-CM elliptic curve $E/\mathbb{Q}$ is a Serre curve if and only if $G_E = G_{\gamma_d}$ for the unique squarefree integer $d \in (j_E - 1728) \cdot (\mathbb{Q}^\times)^2$. The first examples of such curves were given by Serre, see the end of §5.5 of [Ser72].

Now consider a Serre curve $E/\mathbb{Q}$. We have $G_E = G_{\gamma_d}$ for a unique squarefree integer $d$. If $d$ is divisible by an odd prime, then $G_{\gamma_d}$ is not agreeable since the level of $G_E$ is divisible by an odd prime and the level of $G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ is 2. So for $d \notin \{\pm 1, \pm 2\}$, the agreeable closure of $G_E$ is $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. For $d \in \{\pm 1, \pm 2\}$, the group $G_{\gamma_d}$ is agreeable (and so $G_E$ is its own agreeable closure). However, we cannot have $G_E = G_{\gamma_d}$ for $d \in \{\pm 1\}$, since in these cases $[G_{\gamma_d}, G_{\gamma_d}] \subsetneq G_{\gamma_d} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$.

**Proposition 1.13.** *For a non-CM elliptic curve $E/\mathbb{Q}$, let $\mathcal{G}_E$ be the agreeable closure of $G_E$. Then $E$ is a Serre curve if and only if $\mathcal{G}_E$ is equal to $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, $G_{\gamma_2}$ or $G_{\gamma_{-2}}$.*

*Proof.* One direction we have already proved. Now suppose that $\mathcal{G}_E$ is $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, $G_{\gamma_2}$ or $G_{\gamma_{-2}}$. In all three cases, we have $[\mathcal{G}_E, \mathcal{G}_E] = [\mathcal{G}, \mathcal{G}]$. So $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E] = [\mathrm{SL}_2(\widehat{\mathbb{Z}}) : [\mathcal{G}, \mathcal{G}]] = 2$. □

*Remark* 1.14.

(i) With notation as in §1.5, there should be a related étale cover $\phi\colon Y \to U_\mathcal{G}$ of degree $|\mathcal{G}/G| = 2$. We have $U_\mathcal{G} = \mathbb{A}^1_\mathbb{Q} - \{0, 1728\}$ and $Y = U_G$.

There is a model $U_G = \{t \in \mathbb{A}^1_\mathbb{Q} : t(t^2+1728) \neq 0\}$ with morphism $\phi\colon U_G \to U_\mathcal{G}$ given by $\phi(t) = t^2 + 1728$. For each $j \in U_\mathcal{G}(\mathbb{Q}) = \mathbb{Q} - \{0, 1728\}$, the fiber $\phi^{-1}(j) \subseteq U_G(\overline{\mathbb{Q}})$ consists of two points and the action of $\mathrm{Gal}_\mathbb{Q}$ on it factors through a faithful action of $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$, where $d$ is the unique squarefree integer in $(j - 1728) \cdot (\mathbb{Q}^\times)^2$.

(ii) "Most" elliptic curves over $\mathbb{Q}$ are Serre curves, cf. [Jon10].

(iii) For number fields $K \neq \mathbb{Q}$ that contain no nontrivial abelian extension of $\mathbb{Q}$, one can show that there are elliptic curves $E$ over $K$ with $\rho_E^*(\mathrm{Gal}_K) = \mathrm{GL}_2(\widehat{\mathbb{Z}})$, cf. [Zyw10]. Note that when $K \neq \mathbb{Q}$, the maximal abelian extension of $K$ is strictly larger than the cyclotomic extension and hence the constraint of Lemma 1.7 need not hold.

1.7. **An example with largest known index.** Let $E/\mathbb{Q}$ be the non-CM elliptic curve defined by the Weierstrass equation $y^2 + xy + y = x^3 + x^2 - 8x + 6$; it has $j$-invariant $-7 \cdot 11^3$ and conductor $5^2 \cdot 7^2$. This curve $E$ is special since it has an isogeny of degree 37 defined over $\mathbb{Q}$. Without giving all the details, we now explain what goes into computing the group $G_E := \rho_E^*(\mathrm{Gal}_\mathbb{Q})$. In particular, this elliptic curve arises from a rational point on a modular curve of genus 2, i.e., $X_0(37)$.

For every prime $\ell \neq 37$, we have $\rho_{E,\ell^\infty}(\mathrm{Gal}_\mathbb{Q}) = \mathrm{GL}_2(\mathbb{Z}_\ell)$. After choosing bases appropriately, the image of $\rho_{E,37}^*$ will lie in the group of upper triangular matrices in $\mathrm{GL}_2(\mathbb{Z}/37\mathbb{Z})$. Therefore,

$G_E$ is a subgroup of

$$\mathcal{G} := \left\{ g \in \mathrm{GL}_2(\widehat{\mathbb{Z}}) : g \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \pmod{37} \right\}.$$

Making use our our explicit modular curves from Theorem 1.9, we find that $\mathcal{G}_E = \mathcal{G}$, i.e., $\mathcal{G}$ is the agreeable closure of $G_E$.

The commutator subgroup $[\mathcal{G}, \mathcal{G}]$ is the level $2 \cdot 37$ subgroup of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ consisting of matrices whose image modulo 2 lies in the unique index 2 subgroup of $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ and whose image modulo 37 is of the form $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$. As noted in §1.4, since $\mathcal{G}$ is the agreeable closure of $G_E$ we will have $G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = [\mathcal{G}, \mathcal{G}]$ and

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E] = [\mathrm{SL}_2(\widehat{\mathbb{Z}}) : [\mathcal{G}, \mathcal{G}]] = 2 \cdot |\mathrm{SL}_2(\mathbb{Z}/37\mathbb{Z})|/37 = 2736.$$

Let $G$ be the open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ of level $2 \cdot 37$ consisting of matrices whose image modulo 2 lies in the unique index 2 subgroup of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ and whose image modulo 37 is of the form $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$. Note that $G$ is an open subgroup of $\mathcal{G}$ that satisfies $\det(G) = \widehat{\mathbb{Z}}^\times$ and $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = [\mathcal{G}, \mathcal{G}]$.

Let $\chi_1 \colon \mathcal{G} \to \{\pm 1\}$ be the homomorphism obtained by composing reduction modulo 2 with the only nontrivial homomorphism $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \twoheadrightarrow \{\pm 1\}$. Let $\chi_2 \colon \mathcal{G} \to (\mathbb{Z}/37\mathbb{Z})^\times$ be the homomorphism that takes a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ to $d$ modulo 37. The kernel of the homomorphisms $\chi_1$ and $\chi_2$ both contain $G$ and together they induce an isomorphism

$$\mathcal{G}/G \xrightarrow{\sim} \{\pm 1\} \times (\mathbb{Z}/37\mathbb{Z})^\times. \tag{1.2}$$

Let $\alpha_E \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathcal{G}/G$ be the homomorphism obtained by composing $\rho_E^* \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathcal{G}$ with the quotient map $\mathcal{G}/G$. Since $\mathcal{G}/G$ is abelian, there is a unique homomorphism $\gamma_E \colon \widehat{\mathbb{Z}}^\times \to \mathcal{G}/G$ satisfying $\gamma_E(\chi_{\mathrm{cyc}}(\sigma)^{-1}) = \alpha_E(\sigma)$ for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$. Once we have found $\gamma_E$, Lemma 1.10 implies that $G_E$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to the explicit group $\mathcal{H}_E := \{g \in \mathcal{G} : g \cdot G = \gamma_E(\det g)\}$.

Let $\gamma_1 \colon \widehat{\mathbb{Z}}^\times \to \{\pm 1\}$ and $\gamma_2 \colon \widehat{\mathbb{Z}}^\times \to (\mathbb{Z}/37\mathbb{Z})^\times$ be the homomorphism obtained by composing $\gamma_E$ with $\chi_1$ and $\chi_2$, respectively.

We first describe $\gamma_1$. The extension $\mathbb{Q}(E[2])/\mathbb{Q}$ is a Galois extension with group isomorphic to $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$. So $\mathbb{Q}(E[2])$ contains a unique quadratic extension; it is $\mathbb{Q}(\sqrt{\Delta})$, where $\Delta = -5^3 7^2$ is the discriminant of the Weierstrass model of $E$. Therefore, $\mathbb{Q}(\sqrt{-5})$ is the unique quadratic extension of $\mathbb{Q}$ in $\mathbb{Q}(E[2])$. Using this, we find that $\gamma_1 \circ \chi_{\mathrm{cyc}} \colon \mathrm{Gal}_{\mathbb{Q}} \to \{\pm 1\}$ factors through $\mathrm{Gal}(\mathbb{Q}(\sqrt{-5})/\mathbb{Q}) \hookrightarrow \{\pm 1\}$. Therefore, $\gamma_1$ is obtained by composing the reduction modulo 20 homomorphism $\widehat{\mathbb{Z}}^\times \to (\mathbb{Z}/20\mathbb{Z})^\times$ with the unique Dirichlet character $(\mathbb{Z}/20\mathbb{Z})^\times \to \{\pm 1\}$ of conductor 20.

We now describe $\gamma_2$. There is a unique subgroup $H \subseteq E[37]$ of order 37 that is stable under the action of $\mathrm{Gal}_{\mathbb{Q}}$; the $x$-coordinates of the nonzero elements of $H$ are the roots of a degree 18 polynomial $f(x) \in \mathbb{Z}[x]$ that can be found by factoring the 37-th division polynomial of $E$. Let $\beta \colon \mathrm{Gal}_{\mathbb{Q}} \to (\mathbb{Z}/37\mathbb{Z})^\times$ be the the homomorphism for which $\sigma(P) = \beta(\sigma) \cdot P$ for all $P \in H$ and $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$. We have

$$\rho_{E,37}^*(\sigma) = \left(\begin{smallmatrix} * & * \\ 0 & \beta(\sigma)^{-1} \end{smallmatrix}\right)$$

for $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$. From this, we find that $\gamma_2(\chi_{\mathrm{cyc}}(\sigma)) = \beta(\sigma)$ for $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$. The representation $\rho_{E,37}^*$, and hence also $\beta$, is unramified at all primes $p \nmid 5 \cdot 7 \cdot 37$ since the conductor of $E$ is $5^2 \cdot 7^2$. Therefore, $\gamma_2$ factors through a homomorphism $\overline{\gamma}_2 \colon (\mathbb{Z}/(5 \cdot 7 \cdot 37)\mathbb{Z})^\times = (\mathbb{Z}/1295\mathbb{Z})^\times \to (\mathbb{Z}/37\mathbb{Z})^\times$ satisfying $\overline{\gamma}_2(p) = \beta(\mathrm{Frob}_p)$ for all primes $p \nmid 5 \cdot 7 \cdot 37$. We can compute $\beta(\mathrm{Frob}_p)$ for any prime $p \nmid 5 \cdot 7 \cdot 37$ by working modulo $p$ (for any point $P \in E(\overline{\mathbb{F}}_p)$ whose $x$-coordinate is a root of $f$, we have $\mathrm{Frob}_p(P) = \beta(\mathrm{Frob}_p) \cdot P$). In particular, we find that:

$$\beta(\mathrm{Frob}_{13}) = 6, \quad \beta(\mathrm{Frob}_{19}) = 26, \quad \beta(\mathrm{Frob}_{29}) = 36. \tag{1.3}$$

Since 13, 19 and 29 generate $(\mathbb{Z}/1295\mathbb{Z})^\times$, the values (1.3) determine $\overline{\gamma}_2$ and hence also $\gamma_2$.

The homomorphism $\gamma_E\colon \widehat{\mathbb{Z}}^\times \to \mathcal{G}/G$ is thus the map $a \mapsto (\gamma_1(a), \gamma_2(a))$ composed with the inverse of (1.2). Now that we know $\mathcal{G}$ and $\gamma_E$, we can compute $\mathcal{H}_E$ which gives the image of $\rho_E^*$ up to conjugacy. A direct calculation shows that $\mathcal{H}_E$ has level $4 \cdot 5 \cdot 7 \cdot 37 = 5180$ and the image of $\mathcal{H}_E$ modulo 5180 is generated by the matrices:

$$\left(\begin{smallmatrix} 1 & 38 \\ 0 & 1 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} 1 & 1 \\ 37 & 38 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} 13 & 0 \\ 0 & 2391 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} 64 & 3737 \\ 37 & 2970 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} 70 & 851 \\ 37 & 5038 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} 42 & 1961 \\ 37 & 4318 \end{smallmatrix}\right).$$

Note that the first two matrices generate the image of $[\mathcal{G}, \mathcal{G}]$ modulo 5180 while the other matrices are chosen to have determinants 3, 11, 13 and 19, respectively (these primes generate the group $(\mathbb{Z}/5180\mathbb{Z})^\times$).

1.8. **An involved example.** We now give a more complicated example involving the étale morphism $\phi\colon Y \to U_{\mathcal{G}}$ from §1.5; it will arise from our computations.

Let $\mathcal{G}$ be the open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ of level 27 whose image modulo 27 is generated by the matrices: $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 2 \\ 3 & 2 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 2 & 1 \\ 9 & 5 \end{smallmatrix}\right)$. We have $\det(\mathcal{G}) = \widehat{\mathbb{Z}}^\times$, $-I \in \mathcal{G}$, and $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathcal{G}] = 36$.

The curve $X_{\mathcal{G}}$ is isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$ and $\mathcal{G}$ is one of the agreeable groups in our set $\mathscr{A}$ from Theorem 1.9. Moreover, $\mathbb{Q}(X_{\mathcal{G}}) = \mathbb{Q}(t)$ for some $t$ so that the map $\pi_{\mathcal{G}}$ to the $j$-line is given by the rational function

$$\pi(t) := \frac{(t^3+3)^3(t^9+9t^6+27t^3+3)^3}{t^3(t^6+9t^3+27)}.$$

We have $\pi(t) - 1728 = (t^{18}+18t^{15}+135t^{12}+504t^9+891t^6+486t^3-27)^2/(t^3(t^6+9t^3+27))$. So

$$U_{\mathcal{G}} = \operatorname{Spec} \mathbb{Q}[t, 1/f] \subseteq \operatorname{Spec} \mathbb{Q}[t] = \mathbb{A}^1_{\mathbb{Q}},$$

where $f := t(t^3+3)(t^9+9t^6+27t^3+3)(t^{18}+18t^{15}+135t^{12}+504t^9+891t^6+486t^3-27)$.

Let $G$ be the open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ of level 54 whose image modulo 54 is generated by the matrices: $\left(\begin{smallmatrix} 7 & 0 \\ 36 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 7 & 16 \\ 0 & 25 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 16 & 7 \\ 3 & 5 \end{smallmatrix}\right)$. We have $\det(G) = \widehat{\mathbb{Z}}^\times$, $-I \notin G$, $G \subseteq \mathcal{G}$, and $[\mathcal{G} : G] = 36$. The group $G$ is normal in $\mathcal{G}$ and $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = [\mathcal{G}, \mathcal{G}]$. The quotient group $\mathcal{G}/G$ is abelian of order 36.

As mentioned in §1.5, in §11 we describe a particular étale cover $\phi\colon Y \to U_{\mathcal{G}}$ that is Galois with group $\mathcal{G}/G$; it is used for computing groups $\rho_E^*(\mathrm{Gal}_{\mathbb{Q}})$ whose agreeable closure is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to $\mathcal{G}$. We now state $\phi$ with respect to the explicit models that occur in our computations.

For each $1 \le i \le 9$, define a homogeneous polynomial $F_i \in \mathbb{Z}[x_1, \dots, x_8]$ and a polynomial $c_i \in \mathbb{Z}[t]$ as follows:

$$\begin{aligned}
F_1 &:= x_1^2 + x_1x_4 + x_2^2 + x_2x_5 + x_3^2 + x_3x_6 + x_4^2 + x_5^2 + x_6^2,\\
F_2 &:= x_1x_3 - x_1x_5 + x_2x_4 - x_2x_6 + x_3x_4 + x_3x_5 + x_4x_6,\\
F_3 &:= x_1x_2 - x_1x_6 + x_2x_3 + x_2x_4 + x_3x_4 + x_3x_5 + x_4x_5 + x_5x_6,\\
F_4 &:= x_1^2x_4 + x_1x_4^2 + x_2^2x_5 + x_2x_5^2 + x_3^2x_6 + x_3x_6^2,\\
F_5 &:= x_1^2x_3 + x_1^2x_6 - x_1x_2^2 + 2x_1x_3x_4 + x_1x_5^2 - x_2x_3^2 + 2x_2x_4x_5 + x_2x_6^2 + 2x_3x_5x_6 - x_4^2x_6 + x_4x_5^2 + x_5x_6^2,\\
F_6 &:= x_1^3 + 3x_1^2x_4 + x_2^3 + 3x_2^2x_5 + x_3^3 + 3x_3^2x_6 - x_4^3 - x_5^3 - x_6^3,\\
F_7 &:= x_1^2x_2 + x_1^2x_5 + 2x_1x_2x_4 - x_1x_3^2 + x_1x_6^2 + x_2^2x_3 + x_2^2x_6 + 2x_2x_3x_5 + 2x_3x_4x_6 - x_4^2x_5 + x_4x_6^2 - x_5^2x_6,\\
F_8 &:= x_7^2,\\
F_9 &:= x_8^2,
\end{aligned}$$

$c_1 := 2(t^6 + 9t^3 + 27)$,

$c_2 := -(t^6 + 9t^3 + 27)$,

$c_3 := -(t^6 + 9t^3 + 27)$,

$c_4 := -(2t^2 + 2t - 3)(t^6 + 9t^3 + 27)$,

$c_5 := 3(t - 1)(t + 2)(t^6 + 9t^3 + 27)$,

$c_6 := -(2t - 3)(t^2 + 3t + 3)(t^6 + 9t^3 + 27)$,

$c_7 := (3t^2 + 4t - 3)(t^6 + 9t^3 + 27)$,

$c_8 := t(t^6 + 9t^3 + 27)$,

$c_9 := -3t(t^3 + 3)(t^6 + 9t^3 + 27)(t^9 + 9t^6 + 27t^3 + 3)(t^{18} + 18t^{15} + 135t^{12} + 504t^9 + 891t^6 + 486t^3 - 27)$.

Let $Y$ be the closed subvariety of $\operatorname{Spec} \mathbb{Q}[x_1, \dots, x_8, t, 1/f]$ defined by the equations

$$F_i(x_1, \dots, x_8) = c_i(t)$$

with $1 \le i \le 9$. Let $\phi\colon Y \to U_{\mathcal{G}}$ be the morphism given by $(x_1, \dots, x_8, t) \mapsto t$.

We now describe an action of $\mathcal{G}/G$ on $Y$. Choose matrices $g_1$, $g_2$ and $g_3$ in $\mathcal{G}$ that are congruent modulo 54 to $\left(\begin{smallmatrix} 31 & 44 \\ 36 & 25 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 28 & 27 \\ 27 & 28 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, respectively. We have a unique isomorphism of abelian groups

$$\iota\colon \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \xrightarrow{\sim} \mathcal{G}/G$$

for which $(1,0,0) \mapsto g_1G$, $(0,1,0) \mapsto g_2G$ and $(0,0,1) \mapsto g_3G$. So it suffices to describe the action of each $g_iG$ on $Y$. For any point $y = (a_1, \dots, a_9) \in Y(\overline{\mathbb{Q}})$, we have

$$\begin{aligned} g_1G \cdot y &:= (a_2, a_3, a_4, a_5, a_6, -a_1 - a_4, a_7, a_8, a_9), \\ g_2G \cdot y &:= (a_1, a_2, a_3, a_4, a_5, a_6, -a_7, a_8, a_9), \\ g_2G \cdot y &:= (a_1, a_2, a_3, a_4, a_5, a_6, a_7, -a_8, a_9). \end{aligned}$$

The action of $\mathcal{G}/G$ on $Y$ is faithful and does not affect the morphism $\phi$. In fact, $\phi\colon Y \to U_{\mathcal{G}}$ is an étale morphism of degree 36 that is Galois with the action of $\mathcal{G}/G$ giving its Galois group. The curve $Y$ is defined over $\mathbb{Q}$ and is smooth and geometrically irreducible. This completes our explicit description of $\phi\colon Y \to U_{\mathcal{G}}$.

As an example of how to use these equations, consider the elliptic curve $E/\mathbb{Q}$ give by the Weierstrass equation

$$y^2 + y = x^3 + x^2 + x.$$

The curve $E$ has $j$-invariant 32768/19 and conductor 19. We have $j_E = \pi(-1) \in \pi_{\mathcal{G}}(X_{\mathcal{G}}(\mathbb{Q}))$, so $G_E := \rho_E^*(\operatorname{Gal}_{\mathbb{Q}})$ is conjugate in $\operatorname{GL}_2(\widehat{\mathbb{Z}})$ to a subgroup of $\mathcal{G}$. So after replacing $\rho_E^*$ by an isomorphic representation, we may assume that $G_E \subseteq \mathcal{G}$. In particular, the agreeable closure $\mathcal{G}_E$ of $G_E$ is a subgroup of $\mathcal{G}$. Using our groups and modular curves from Theorem 1.9, we find that $\mathcal{G}_E = \mathcal{G}$.

Fix $u := -1 \in U_{\mathcal{G}}(\mathbb{Q}) = \mathbb{Q} - \{0\}$. The fiber $\phi^{-1}(u)$ is the subscheme of $\mathbb{A}^8_{\mathbb{Q}} = \operatorname{Spec} \mathbb{Q}[x_1, \dots, x_8]$ defined by the equations $F_i(x_1, \dots, x_8) = c_i(-1)$ with $1 \le i \le 9$; it is reduced of dimension 0, has degree 36, and $\mathcal{G}/G$ acts faithfully on the $\overline{\mathbb{Q}}$-points. Let $\alpha_u\colon \operatorname{Gal}_{\mathbb{Q}} \to \mathcal{G}/G$ be the homomorphism such that $\sigma(y) = \alpha_u(\sigma) \cdot y$ for any $\sigma \in \operatorname{Gal}_{\mathbb{Q}}$ and any $y \in Y(\overline{\mathbb{Q}})$ with $\phi(y) = u$.

Take any prime $p \nmid 6$ for which the $\mathbb{Z}_p$-subscheme $Z \subseteq \mathbb{A}^8_{\mathbb{Z}_p} = \operatorname{Spec} \mathbb{Z}_p[x_1, \dots, x_8]$ defined by the equations $F_i(x_1, \dots, x_8) = c_i(-1)$ with $1 \le i \le 9$, is smooth and $Z_{\mathbb{F}_p}$ has degree 36. The action of $\mathcal{G}/G$ on $Z(\overline{\mathbb{F}}_p)$ is simply transitive. Using Hensel's lemma and the smoothness of $Z$, we find that $\operatorname{Frob}_p(y) = \alpha_u(\operatorname{Frob}_p) \cdot y$ for all $y \in Z(\overline{\mathbb{F}}_p)$. This gives our computable description

of $\alpha_u(\mathrm{Frob}_p)$; find a point $y \in Z(\overline{\mathbb{F}}_p)$, raise its coordinates to the $p$-th power and find the unique $\alpha_u(\mathrm{Frob}_p) \in \mathcal{G}/G$ for which $\mathrm{Frob}_p(y) = \alpha_u(\mathrm{Frob}_p) \cdot y$. In this way, one can show that:

$$\alpha_u(\mathrm{Frob}_5) = \iota((2,0,1)), \quad \alpha_u(\mathrm{Frob}_{11}) = \iota((6,0,1)), \quad \alpha_u(\mathrm{Frob}_{13}) = \iota((4,1,1)). \tag{1.4}$$

With notation as in §11.2, we define $\alpha_E := \chi \cdot \alpha_u \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathcal{G}/G$, where $\chi \colon \mathrm{Gal}_{\mathbb{Q}} \to \{\pm 1\}$ is the homomorphism that factors through $\mathrm{Gal}(\mathbb{Q}(\sqrt{-19})/\mathbb{Q}) \hookrightarrow \{\pm 1\}$. By Lemma 11.1, after replacing $\rho_E^*$ by an isomorphic representation, we may assume that $G_E \subseteq \mathcal{G}$ and that the composition of $\rho_E^*$ with the quotient map $\mathcal{G} \to \mathcal{G}/G$ is $\alpha_E$.

Let

$$\gamma_E \colon \widehat{\mathbb{Z}}^\times \to \mathcal{G}/G$$

be the homomorphism such that $\gamma_E(\chi_{\mathrm{cyc}}(\sigma)^{-1}) = \alpha_E(\sigma)$ for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$. With $M = 2 \cdot 3 \cdot 19$ and $e = 18$, we can argue as in §1.5 that $\gamma_E$ factors through a homomorphism $\overline{\gamma}_E \colon \mathbb{Z}_M^\times/(\mathbb{Z}_M^\times)^e \to \mathcal{G}/G$ such that $p \cdot (\mathbb{Z}_M^\times)^e \mapsto \alpha_E(\mathrm{Frob}_p)^{-1}$ for all primes $p \nmid M$. In particular,

$$\overline{\gamma}_E(5) = \iota((7,0,1)), \quad \overline{\gamma}_E(11) = \iota((3,0,1)), \quad \overline{\gamma}_E(13) = -\iota((5,1,1)) = \iota((5,1,0)). \tag{1.5}$$

Since the primes 5, 11 and 13 generate $\mathbb{Z}_M^\times/(\mathbb{Z}_M^\times)^e$, we deduce that $\gamma_E$ is determined by $M$ and the values (1.5). Using this, we can show that $\gamma_E$ is the composition of the reduction homomorphism $\widehat{\mathbb{Z}}^\times \to (\mathbb{Z}/57\mathbb{Z})^\times$ with the unique homomorphism $(\mathbb{Z}/57\mathbb{Z})^\times \to \mathcal{G}/G$ for which $5 \mapsto \iota((7,0,1))$ and $13 \mapsto \iota((5,1,0))$.

Now that we know $\mathcal{G}$ and $\gamma_E$, we can compute the group $\mathcal{H}_E$ from (1.1). The group $\mathcal{H}_E$ is an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ with level $2 \cdot 27 \cdot 19 = 1026$ and its image modulo 1026 is generated by the matrices:

$$\left(\begin{smallmatrix} 31 & 198 \\ 10 & 97 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} 1 & 0 \\ 18 & 1 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} 28 & 729 \\ 27 & 703 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} 149 & 681 \\ 271 & 448 \end{smallmatrix}\right), \quad \left(\begin{smallmatrix} 994 & 9 \\ 689 & 790 \end{smallmatrix}\right);$$

the first three matrices also generate the image of $\mathcal{H}_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ modulo 1026. By Lemma 1.10, this gives the image of $\rho_E^*$ up to conjugacy.

1.9. **Some related results.** There has been much research on modular curves and the image of Galois representations associated to non-CM elliptic curves over $\mathbb{Q}$. We now give a brief and incomplete description of some related recent progress.

Given a fixed non-CM elliptic curve $E/\mathbb{Q}$, we can determine the (finite) set of primes $\ell$ for which $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}}) \neq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ using the algorithm in [Zyw20b] (it is based on Serre's original proof in [Ser72]). For each prime $\ell$ for which $\rho_{E,\ell}$ is not surjective, we can also compute the subgroup $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}}) \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ up to conjugacy using [Zyw15b] or [Sut16] (the first reference uses explicit modular curves while the second reference uses Frobenius matrices to give a probabilistic algorithm).

Consider primes $\ell > 13$. There has been much progress towards Conjecture 1.2. If $\rho_{E,\ell}$ is not surjective for a non-CM elliptic curve $E/\mathbb{Q}$, then $E$ gives rise to a rational non-CM point on a modular curve $X_G$ with $G$ a maximal subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ satisfying $\det(G) = (\mathbb{Z}/\ell\mathbb{Z})^\times$. When $G$ is the subgroup of upper triangular matrices, Mazur [Maz78] has found the rational points of $X_0(\ell) := X_G$. The curve $X_0(\ell)$ has no non-CM rational points for $\ell > 17$ and $\ell \neq 37$ (for $\ell \in \{17, 37\}$, there are non-CM rational points which lead to the $j$-invariants in the statement of Conjecture 1.2). When $G$ is the normalizer of a split Cartan subgroup, Bilu, Parent and Rebolledo [BPR13] have shows that $X_G$ has no non-CM points. When the image of $G$ in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})/((\mathbb{Z}/\ell\mathbb{Z})^\times \cdot I)$ is isomorphic to $\mathfrak{S}_4$, the modular curve $X_G(\mathbb{Q})$ has no non-CM points, see the remarks on page 36 of [Maz77b]. The remaining modular curves to consider are the curves $X_{\mathrm{ns}}^+(\ell) := X_G$, where $G$ is the normalizer of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

There has been recent progress on finding the rational points on $X_{\mathrm{ns}}^+(\ell)$ for small $\ell$ using generalized versions of Chabauty's method, cf. [BDM+19, BDM+21], but the general case remains open.

Now consider the images of the $\ell$-adic representations $\rho_{E,\ell^\infty}$. If $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for a non-CM elliptic $E/\mathbb{Q}$ and a prime $\ell \geq 5$, then we have $\rho_{E,\ell^\infty}(\mathrm{Gal}_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{Z}_\ell)$, cf. §7.9. Taking Conjecture 1.2 and our above discussion of modulo $\ell$ representations into account, it makes sense to focus on $\ell$-adic projections for the primes $\ell \in \{2, 3, 5, 7, 11, 13, 17, 37\}$. For the prime $\ell = 2$, Rouse and Zureick-Brown [RZB15] gave a complete description of the images $\rho_{E,\ell^\infty}(\mathrm{Gal}_{\mathbb{Q}}) \subseteq \mathrm{GL}_2(\mathbb{Z}_\ell)$, up to conjugacy, for all non-CM elliptic curves $E/\mathbb{Q}$ (they found models of all relevant modular curves and computed their rational points). For each prime $\ell$, Sutherland and Zywina [SZ17] described all open subgroups $G$ of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ with $\det(G) = \mathbb{Z}_\ell^\times$ for which $X_G(\mathbb{Q})$ infinite and then computed a model for $X_G$ along with the morphism to the $j$-line. In [RSZB22], Rouse, Sutherland and Zureick-Brown gave a complete description of $\ell$-adic images up to possible counterexamples to Conjecture 1.2 and determining the rational points on a finite number of explicit modular curves $X_G$ of genus at least 2.

Once one gets a handle on the $\ell$-adic Galois images, it is natural to consider the image modulo integers divisible by several distinct primes. There has been much recent work on understanding and classifying "entanglements"; for example, see [DLRM21, DM22, JM22, Mor19, BJ16]. For relative prime positive integers $m$ and $n$, we say that $E$ has a $(m, n)$-entanglement if $\mathbb{Q}(E[m]) \cap \mathbb{Q}(E[n]) \neq \mathbb{Q}$; equivalently, $\rho_{E,mn}(\mathrm{Gal}_{\mathbb{Q}})$ can be viewed as a *proper* subgroup of $\rho_{E,m}(\mathrm{Gal}_{\mathbb{Q}}) \times \rho_{E,n}(\mathrm{Gal}_{\mathbb{Q}})$. In particular, entanglements describe constraints on the image $\rho_E(\mathrm{Gal}_{\mathbb{Q}})$.

While the work in this paper does give some information, we have avoided a general study of possible entanglements. What may seem surprising at first, is that to compute the group $\rho_E(\mathrm{Gal}_{\mathbb{Q}})$ we do not first compute the $\ell$-adic projections $\rho_{E,\ell^\infty}(\mathrm{Gal}_{\mathbb{Q}})$; even though they can be found using [RSZB22]. The approach of computing the $\ell$-adic images and then describing all the possible entanglements seems to lead to an excessive number of cases. Of course once we have found $\rho_E(\mathrm{Gal}_{\mathbb{Q}})$, up to conjugacy, we can then easily compute the $\ell$-adic projections $\rho_{E,\ell^\infty}(\mathrm{Gal}_{\mathbb{Q}})$.

There has also been some more general study on the image of $\rho_E$. Jones has produced upper bounds for the level of $\rho_E(\mathrm{Gal}_{\mathbb{Q}})$ in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ for non-CM elliptic curves $E/\mathbb{Q}$, cf. [Jon20, Jon09]. The paper [Jon15] of Jones contains a lot of group theoretic information about the image of $\rho_E$; in particular, he generalizes the notion of a Serre curve, cf. Remark 14.3. The doctoral thesis of Brau Avilo [BA15] appears to be the first place to explicitly point out that there is an algorithm to compute $\rho_E(\mathrm{Gal}_{\mathbb{Q}})$. His algorithm first find the level $m$ of $\rho_E(\mathrm{Gal}_{\mathbb{Q}})$ and then computes $\rho_{E,m}(\mathrm{Gal}_{\mathbb{Q}})$ by making use of division polynomials; it it not practical in general.

Define the set of integers

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

In [Zyw15a], it is shown that there is a finite set $J \subseteq \mathbb{Q}$ such that for any elliptic curve $E/\mathbb{Q}$ with $j_E \notin J$ and $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all primes $\ell > 37$, we have $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(\mathrm{Gal}_{\mathbb{Q}})] \in \mathcal{I}$. Moreover, $\mathcal{I}$ is the smallest set with this property. The results of this paper can be used to give an elaborate alternate proof of this result (in [Zyw15a], modular curves are used but no models are computed). Note that the only new integers that arise in Conjecture 1.5 are: 80, 128, 160, 182, 200, 216, 224, 300, 480, 2736.

Rakvi [Rak21] has recently given a description of the pairs $(X_G, \pi_G)$, up to a suitable notion of isomorphism, as we vary over all open subgroups $G$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ satisfying $\det(G) = \widehat{\mathbb{Z}}^\times$, $-I \in G$,

and $X_G \cong \mathbb{P}^1_{\mathbb{Q}}$ (see the end of §14 for details).

The above results, and similar ones, are often phrased in the context of progress towards the following overarching program:

**Mazur's Program B.** [Maz77a] *Given a number field $K$ and a subgroup $H$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}}) = \prod_p \mathrm{GL}_2(\mathbb{Z}_p)$ classify all elliptic curves $E/K$ whose associated Galois representation on torsion points map $\mathrm{Gal}(\overline{K}/K)$ into $H \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$.*

1.10. **Overview.** We briefly outline the structure of the paper. In §2, we recall the connection between $\rho_E^*$ with the cyclotomic character and explain how the image of $\rho_E^*$ changes when we replace $E$ by a quadratic twist.

Consider a subgroup $G \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ satisfying $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$ and $-I \in G$. In §3, we give a quick definition of modular curves $X_G$ in terms of their function fields (which will be fields consisting of modular functions). The curve comes with a non-constant morphism $\pi_G\colon X_G \to \mathbb{P}^1_{\mathbb{Q}} = \mathbb{A}^1_{\mathbb{Q}} \cup \{\infty\}$ from $X_G$ to the $j$-line.

In §4, we will define a finite dimensional $\mathbb{Q}$-vector space $M_{k,G}$ consisting of modular forms for each integer $k \geq 2$. There will be a natural isomorphism $M_{k,G} \otimes_{\mathbb{Q}} \mathbb{C} \xrightarrow{\sim} M_k(\Gamma_G)$, where $\Gamma_G$ is the congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ consisting of matrices whose image modulo $N$ lies in $G$ and $M_k(\Gamma_G)$ is the usual space of weight $k$ modular forms on $\Gamma_G$. Much of §4 is dedicated to describing how to compute an explicit basis of $M_{k,G}$; our approach makes use of Eisenstein series and a theorem of Khuri-Makdisi. Our modular forms will be expressed in terms of their $q$-expansion at every cusp (and for which we can compute arbitrarily many terms of each $q$-expansion).

In §5, we explain how to compute a model for the modular curve $X_G$ and in some cases compute the morphism $\pi_G$. The key observation is that our space of modular forms $M_{k,G}$ is the global sections of a line bundle on the modular curve $X_G$ for even $k$. For $k$ even and sufficiently large, this line bundle will be very ample and a basis for $M_{k,G}$ will allow us to compute an explicit model of $X_G$ in some projective space $\mathbb{P}^n_{\mathbb{Q}}$.

Let $U_G$ be the open subvariety $X_G - \pi_G^{-1}(\{0, 1728, \infty\})$ of $X_G$. In §6, we use modular functions to construct an explicit representation $\varrho\colon \pi_1(U_G) \to G$ of the étale fundamental group of $U_G$. For each rational point $u \in U_G(\mathbb{Q})$, the specialization of $\varrho$ at $u$ will be a Galois representation $\mathrm{Gal}_{\mathbb{Q}} \to G \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that is isomorphic to $\rho^*_{E,N}\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ for a certain elliptic curve $E/\mathbb{Q}$ with $j$-invariant $\pi_G(u)$.

After recalling group theoretic results concerning subgroups and quotients of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ and $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ in §7, we will study agreeable groups in §8. In particular, in §8 we will prove the existence of agreeable closures and we will also explain how to find the maximal agreeable subgroups of an agreeable group.

In §9, we prove Theorem 1.9. In §10, we explain how to find the agreeable closure of $G_E := \rho_E^*(\mathrm{Gal}_{\mathbb{Q}})$, up to conjugacy, for a non-CM elliptic curve $E/\mathbb{Q}$. In §12, we finally explain how to compute $G_E$, up to conjugacy, after understanding how to construct a certain homomorphism $\gamma_E$ in §11.

In §13, we give some insight into computing universal elliptic curves; this will follow quickly from earlier sections but we state it separately for easy reference. Finally in §14, we make some remarks concerning "families" of groups.

1.11. **Implementation.** As already noted, our algorithms have been implemented in `Magma` [BCP97] and code can be found in the repository [Zyw22]:

https://github.com/davidzywina/OpenImage

This also include files containing all the relevant groups and modular curves (unfortunately, the number of cases makes it infeasible to express in a reasonable length table).

This motivation to have a practical algorithm underlies much of the exposition and structure of this paper. At the onset of the project, it was unclear if the approach presented here was going to be computationally feasible; for example, some modular curves took hours to find models for, using known approaches, and we had thousands of curves to study. The precomputation required for our algorithms, which are not especially optimized, took less than half a day.

1.12. **Notation.** We now set some notation that will hold throughout. All profinite groups will be viewed as topological groups with their profinite topology. In particular, finite groups will have the discrete topology. For a topological group $G$, we define its commutator subgroup $[G, G]$ to be the smallest closed normal subgroup of $G$ for which $G/[G, G]$ is abelian. Equivalently, $[G, G]$ is the topological subgroup of $G$ generated by the set of commutators $\{ghg^{-1}h^{-1} : g, h \in G\}$.

For each integer $N > 1$, we let $\mathbb{Z}_N$ be the ring obtained by taking the inverse limit of the $\mathbb{Z}/N^e\mathbb{Z}$ with $e \geq 1$. Let $\widehat{\mathbb{Z}}$ be the ring obtained taking the inverse limit of $\mathbb{Z}/n\mathbb{Z}$ over all positive integers $n$. With the profinite topology, $\mathbb{Z}_N$ and $\widehat{\mathbb{Z}}$ are compact topological rings. We have natural isomorphisms

$$\mathbb{Z}_N = \prod_{\ell | N} \mathbb{Z}_\ell \quad \text{and} \quad \widehat{\mathbb{Z}} = \mathbb{Z}_N \times \prod_{\ell \nmid N} \mathbb{Z}_\ell = \prod_{\ell} \mathbb{Z}_\ell,$$

where the product is over primes $\ell$. The symbol $\ell$ will always denote a rational prime.

The level of an open subgroup $G$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ is the smallest positive integer $n$ for which $G$ contains the kernel of the reduction modulo $n$ homomorphism $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. The level of an open subgroup $G$ of $\mathrm{GL}_2(\mathbb{Z}_N)$ is the smallest positive integer $n$ that divides some power of $N$ and for which $G$ contains the kernel of the reduction modulo $n$ homomorphism $\mathrm{GL}_2(\mathbb{Z}_N) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Similarly, we can define the level of open subgroups of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ and $\mathrm{SL}_2(\mathbb{Z}_N)$.

## 2. Cyclotomic constraints on the image of Galois

With a fixed non-CM elliptic curve $E$ defined over $\mathbb{Q}$, we consider the group $G_E := \rho_E^*(\mathrm{Gal}_{\mathbb{Q}})$ which from Serre we know is an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

2.1. **Kronecker–Weber constraint.** Let $\chi_{\mathrm{cyc}} \colon \mathrm{Gal}_{\mathbb{Q}} \to \widehat{\mathbb{Z}}^\times$ be the cyclotomic character, i.e., the continuous homomorphism such that for every integer $n \geq 1$ and every $n$-th root of unity $\zeta \in \overline{\mathbb{Q}}$ we have $\sigma(\zeta) = \zeta^{\chi_{\mathrm{cyc}}(\sigma) \bmod n}$ for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$. By considering the Weil pairing on the groups $E[n]$, we know that $\det \circ \rho_E = \chi_{\mathrm{cyc}}$ and hence $\det \circ \rho_E^* = \chi_{\mathrm{cyc}}^{-1}$. In particular, we have

$$\det(G_E) = \chi_{\mathrm{cyc}}(\mathrm{Gal}_{\mathbb{Q}}) = \widehat{\mathbb{Z}}^\times.$$

By Lemma 1.7, which makes use of the Kronecker–Weber theorem, we have

$$G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = [G_E, G_E]. \tag{2.1}$$

and $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E] = [\mathrm{SL}_2(\widehat{\mathbb{Z}}) : [G_E, G_E]]$. One consequence of (2.1) is that it is possible to compute the index of $G_E$ in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ using a group that is possibly larger than $G_E$.

**Lemma 2.1.** *Suppose $\mathcal{G} \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ is a group such that $G_E$ is a normal subgroup of $\mathcal{G}$ and $\mathcal{G}/G_E$ is abelian. Then $G_E$ and $\mathcal{G}$ have the same commutator subgroup. In particular, we have $G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = [\mathcal{G}, \mathcal{G}]$ and*

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E] = [\mathrm{SL}_2(\widehat{\mathbb{Z}}) : [\mathcal{G}, \mathcal{G}]].$$

*Proof.* We have $[\mathcal{G}, \mathcal{G}] \subseteq G_E$ since $\mathcal{G}/G_E$ is abelian. Therefore, $[\mathcal{G}, \mathcal{G}] \subseteq G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = [G_E, G_E]$, where the last equality uses Lemma 1.7. The opposite inclusion $[\mathcal{G}, \mathcal{G}] \supseteq [G_E, G_E]$ is clear since $\mathcal{G} \supseteq G_E$. Therefore, $[\mathcal{G}, \mathcal{G}] = [G_E, G_E]$. The final statement about $G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ and the index follows from Lemma 1.7. □

2.2. **Quadratic twists.** Fix a squarefree integer $d$ and let $E'/\mathbb{Q}$ be the quadratic twist of $E$ by $d$. In this section, we describe how the images of $\rho_E^*$ and $\rho_{E'}^*$ are related.

Let $\chi_d\colon \mathrm{Gal}_{\mathbb{Q}} \to \{\pm 1\}$ be the homomorphism that factors through $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \hookrightarrow \{\pm 1\}$. There is a unique homomorphism $\psi\colon \widehat{\mathbb{Z}}^\times \to \{\pm 1\}$ such that $\chi_d = \psi \circ \chi_{\mathrm{cyc}}^{-1}$. Define

$$\mathcal{H} := \{\psi(\det g) \cdot g : g \in G_E\};$$

it is an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

**Lemma 2.2.** *The groups $\rho_{E'}^*(\mathrm{Gal}_{\mathbb{Q}})$ and $\mathcal{H}$ are conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.*

*Proof.* After replacing $\rho_{E'}^*$ with an appropriate isomorphic representation, we may assume that $\rho_{E'}^* = \chi_d \cdot \rho_E^*$. For any $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$, we have

$$\rho_{E'}^*(\sigma) = \chi_d(\sigma) \cdot \rho_E^*(\sigma) = \psi(\chi_{\mathrm{cyc}}(\sigma)^{-1}) \cdot \rho_E^*(\sigma) = \psi(\det(\rho_E^*(\sigma)) \cdot \rho_E^*(\sigma),$$

where we have used that $\det \circ \rho_E^* = \chi_{\mathrm{cyc}}^{-1}$. Therefore, $\rho_{E'}^*(\mathrm{Gal}_{\mathbb{Q}}) = \{\psi(\det g) \cdot g : g \in \rho_E^*(\mathrm{Gal}_{\mathbb{Q}})\}$. □

Now suppose that we know the group $G_E$. More specifically, we have an integer $N \geq 1$ divisible by the level of $G_E$ and a set of generators of $G_E$ modulo $N$. The homomorphism $\psi$ is easy to find; it factors through a Dirichlet character $(\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}$, where $D$ is the discriminant of $\mathbb{Q}(\sqrt{d})$. Let $N'$ be the least common multiple of $N$ and $D$. Then the level of $\mathcal{H}$ divides $N'$ and we can find generators for the image of $\mathcal{H}$ modulo $N'$. By Lemma 2.2, we have thus computed the image of $\rho_{E'}^*$ up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

In particular, once we know the image of $\rho_E^*$, we can easily obtain the image for any quadratic twist of $E$ (equivalently, any elliptic curve over $\mathbb{Q}$ with the same $j$-invariant). In practice, when computing the image of $\rho_E^*$, we will first replace $E$ by a quadratic twist that has a minimal set of primes of bad reduction.

## 3. The modular curve $X_G$

The goal of this section is to give a quick definition of the modular curve $X_G$, where $G$ is either an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ with $\det(G) = \widehat{\mathbb{Z}}^\times$ or a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ with $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$. While we could define $X_G$ as a coarse moduli space, we will instead define it by explicitly giving its function field. Let $\zeta_N$ be the primitive $N$-th root of unity $e^{2\pi i/N}$ in $\mathbb{C}$.

3.1. **Modular functions.** The group $\mathrm{SL}_2(\mathbb{Z})$ acts by linear fractional transformations on the complex upper-half plane $\mathcal{H}$ and the extended upper-half plane $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$.

Let $\Gamma$ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. The quotient $\mathcal{X}_\Gamma := \Gamma\backslash\mathcal{H}^*$ is a smooth compact Riemann surface (away from the cusps and elliptic points use the analytic structure coming from $\mathcal{H}$ and extend to the full quotient). Denote by $\mathbb{C}(\mathcal{X}_\Gamma)$ the field of meromorphic functions on $\mathcal{X}_\Gamma$.

Fix a positive integer $N$. Every $f \in \mathbb{C}(\mathcal{X}_{\Gamma(N)})$ gives rise to a meromorphic function on $\mathcal{H}$ that satisfies

$$f(\tau) = \sum_{n \in \mathbb{Z}} c_n(f) q_N^n$$

for $\tau \in \mathcal{H}$, where $q_N := e^{2\pi i \tau/N}$ and the $c_n(f)$ are unique complex numbers that are nonzero for only finitely many $n < 0$. This Laurent series in $q_N$ is called the $q$-expansion of $f$ (at the cusp $\infty$).

Let $\mathcal{F}_N$ be the subfield of $\mathbb{C}(\mathcal{X}_{\Gamma(N)})$ consisting of all meromorphic functions $f$ such that $c_n(f)$ lies in $\mathbb{Q}(\zeta_N)$ for all $n \in \mathbb{Z}$. For example, $\mathcal{F}_1 = \mathbb{Q}(j)$, where $j$ is the modular $j$-invariant.

**Lemma 3.1.** *There is a unique right action $*$ of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on the field $\mathcal{F}_N$ such that the following hold for all $f \in \mathcal{F}_N$:*

- *For $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, we have $(f * A)(\tau) = f(\gamma\tau)$, where $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ is any matrix congruent to $A$ modulo $N$.*
- *For $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, the $q$-expansion of $f * A$ is $\sum_{n\in\mathbb{Z}} \sigma_d(c_n(f))q_N^n$, where $\sigma_d$ is the automorphism of the field $\mathbb{Q}(\zeta_N)$ that satisfies $\sigma_d(\zeta_N) = \zeta_N^d$.*

*Proof.* This follows from Theorem 6.6 and Proposition 6.9 of [Shi94]. □

For a subgroup $H$ of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, let $\mathcal{F}_N^H$ be the subfield of $\mathcal{F}_N$ fixed by $H$ under the action of Lemma 3.1.

**Lemma 3.2.**

(i) *The matrix $-I$ acts trivially on $\mathcal{F}_N$ and the right action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ on $\mathcal{F}_N$ is faithful.*
(ii) *We have $\mathcal{F}_N^{\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})} = \mathcal{F}_1 = \mathbb{Q}(j)$ and $\mathcal{F}_N^{\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})} = \mathbb{Q}(\zeta_N)(j)$.*
(iii) *The field $\mathbb{Q}(\zeta_N)$ is algebraically closed in $\mathcal{F}_N$.*

*Proof.* This also follows from Theorem 6.6 and Proposition 6.9 of [Shi94]. □

3.2. **Modular curves for finite groups.** Let $G$ be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that satisfies $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$. By Lemma 3.2 and our assumption $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$, the field $\mathcal{F}_N^G$ has transcendence degree 1 and $\mathbb{Q}$ is algebraically closed in $\mathcal{F}_N^G$.

**Definition 3.3.** The modular curve $X_G$ is the smooth, projective and geometrically irreducible curve over $\mathbb{Q}$ with function field $\mathcal{F}_N^G$.

3.3. **Modular curves for open groups.** Consider an open subgroup $G$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ that satisfies $\det(G) = \widehat{\mathbb{Z}}^\times$. We define the modular curve associated to $G$ to be the curve

$$X_G := X_{\overline{G}},$$

where $N$ is a positive integer that is divisible by the level of $G$ and $\overline{G} \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is the reduction of $G$ modulo $N$. Note that the function field $\mathbb{Q}(X_G) = \mathcal{F}_N^{\overline{G}}$, and hence also $X_G$, does not depend on the choice of $N$.

*Remark* 3.4. We will make use of both descriptions $X_G$ and $X_{\overline{G}}$ of a modular curve interchangeably. Working with open groups $G$ is more natural for our application and finite groups $\overline{G}$ is better when dealing with computational issues.

In the special case $G = \mathrm{GL}_2(\widehat{\mathbb{Z}})$ and using $\mathbb{Q}(X_G) = \mathbb{Q}(j)$, we make an identification $X_G = \mathbb{P}^1_{\mathbb{Q}}$ and call it the $j$-line.

Consider a larger group $G \subseteq G' \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$. The inclusion $\mathbb{Q}(X_G) \supseteq \mathbb{Q}(X_{G'})$ of fields induces a morphism $X_G \to X_{G'}$ of degree $[\pm G' : \pm G]$. In the special case $G' = \mathrm{GL}_2(\widehat{\mathbb{Z}})$, we denote the morphism by $\pi_G \colon X_G \to \mathbb{P}^1_{\mathbb{Q}}$ (or $\pi_{\overline{G}} \colon X_{\overline{G}} \to \mathbb{P}^1_{\mathbb{Q}}$).

Let $\Gamma_G$ be the congruence subgroup $\mathrm{SL}_2(\mathbb{Z}) \cap G$ of $\mathrm{SL}_2(\mathbb{Z})$; equivalently, the group of $A \in \mathrm{SL}_2(\mathbb{Z})$ for which $A$ modulo $N$ lies in the group $\overline{G}$ above. We have an inclusion $\mathbb{C} \cdot \mathbb{Q}(X_G) \subseteq \mathbb{C}(\mathcal{X}_{\Gamma_G})$ of fields that both have degree $[\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : \pm G] = [\mathrm{SL}_2(\mathbb{Z}) : \pm\Gamma_G]$ over $\mathbb{C}(j)$. Therefore, $\mathbb{C}(\mathcal{X}_{\Gamma_G}) = \mathbb{C}(X_G)$. Using this equality of function fields, we shall identify $X_G(\mathbb{C})$ with the Riemann surface $\mathcal{X}_{\Gamma_G}$. Taking complex points, $\pi_G$ gives rise to the morphism $\mathcal{X}_{\Gamma_G} \to \mathcal{X}_{\mathrm{SL}_2(\mathbb{Z})} \xrightarrow{\sim} \mathbb{P}^1(\mathbb{C})$ of Riemann surfaces obtained by composing the natural quotient map with the isomorphism given by $j$.

The following property of $X_G$ is fundamental to our application to elliptic curves; it follows from Proposition 6.4 which we will prove in §6.3.

**Proposition 3.5.** *Let $G$ be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ that satisfies $\det(G) = \widehat{\mathbb{Z}}^\times$ and $-I \in G$. Let $E$ be any elliptic curve defined over $\mathbb{Q}$ with $j_E \notin \{0, 1728\}$. Then $\rho_E^*(\mathrm{Gal}_\mathbb{Q})$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a subgroup of $G$ if and only if $j_E$ is an element of $\pi_G(X_G(\mathbb{Q})) \subseteq \mathbb{Q} \cup \{\infty\}$.*

*Remark* 3.6. As a warning we observe that in the literature, the notation $X_G$ sometimes denotes the modular curve that we call $X_{G^t}$, where $G^t$ is the group obtained by taking the transpose of the elements of $G$. The advantage of this alternate definition is that Proposition 3.5 could be stated with $\rho_E$ instead of the dual representation $\rho_E^*$. Our definition is more natural when working with the right actions of $G$ on spaces of modular forms.

## 4. Modular forms

In this section, we recall what we need concerning modular forms. For a modular form, we are particularly interested in computing arbitrarily many terms of the $q$-expansions at *every* cusp. For the basics on modular forms see [Shi94]. For an overview on computing modular forms see [BBB+21]; we will take our own approach using Eisenstein series that treats all the $q$-expansions at each cusp with equal importance.

For a subgroup $G$ of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ with $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$ and an even integer $k \geq 2$, we are especially interested in computing the space of modular forms $M_{k,G}$ from §4.6. We will see later that $M_{k,G}$ is the global sections of a line bundle on the modular curve $X_G$. For $k$ large enough, the line bundle will be very ample and $M_{k,G}$ will allow us to compute an explicit model of $X_G$ in $\mathbb{P}^n_\mathbb{Q}$ for some $n$.

Fix a congruence subgroup $\Gamma$ of $\mathrm{SL}_2(\mathbb{Z})$. For a positive integer $N$, define the primitive $N$-th root of unity $\zeta_N := e^{2\pi i/N}$ in $\mathbb{C}$.

4.1. **Setup and notation.** The group $\mathrm{SL}_2(\mathbb{Z})$ acts by linear fractional transformations on the complex upper-half plane $\mathcal{H}$ and the extended upper-half plane $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$. The quotient $\mathcal{X}_\Gamma := \Gamma\backslash\mathcal{H}^*$ is a smooth compact Riemann surface (away from the cusps and elliptic points use the analytic structure coming from $\mathcal{H}$ and extend to the full quotient).

Let $g$ be the genus of the Riemann surface $\mathcal{X}_\Gamma$. Let $P_1, \ldots, P_r$ be the cusps of $\mathcal{X}_\Gamma$, i.e., the $\Gamma$-orbits of $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$. Let $Q_1, \ldots, Q_s$ be the elliptic points of $\mathcal{X}_\Gamma$ and denote their orders by $e_1, \ldots, e_s$, respectively. Each $e_i$ is either 2 or 3. Let $v_2$ and $v_3$ be the number of elliptic points of $\mathcal{X}_\Gamma$ of order 2 and 3, respectively.

Consider an integer $k \geq 0$. For a meromorphic function $f$ on $\mathcal{H}$ and a matrix $\gamma \in \mathrm{GL}_2(\mathbb{R})$ with positive determinant, define the meromorphic function $f|_k\gamma$ on $\mathcal{H}$ by $(f|_k\gamma)(\tau) := \det(\gamma)^{k/2}(c\tau + d)^{-k} f(\gamma\tau)$; we call this the slash operator of weight $k$.

4.2. **Modular forms.** For an integer $k \geq 0$, we denote by $M_k(\Gamma)$ the set of modular forms of weight $k$ on $\Gamma$; it is a finite dimensional complex vector space. Recall that each $f \in M_k(\Gamma)$ is a holomorphic function of the upper-half plane $\mathcal{H}$ that satisfies $f|_k\gamma = f$ for all $\gamma \in \Gamma$ with the familiar growth condition at each cusp. For each modular form $f \in M_k(\Gamma)$, we have

$$f(\tau) = \sum_{n=0}^{\infty} a_n(f)\, q_w^n$$

for unique $a_n(f) \in \mathbb{C}$, where $w$ is the width of the cusp $\infty$ of $\Gamma$ and $q_w := e^{2\pi i\tau/w}$. We call this power series in $q_w$, the $q$-expansion of $f$ (at the cusp $\infty$). For a subring $R$ of $\mathbb{C}$, we denote by $M_k(\Gamma, R)$ the $R$-submodule of $M_k(\Gamma)$ consisting of modular forms whose $q$-expansion has coefficients in $R$.

Define the graded $\mathbb{C}$-algebra of modular forms on $\Gamma$ by

$$R_\Gamma := \bigoplus_{k\geq 0} M_k(\Gamma),$$

where $k$ varies over all nonnegative integers. The $\mathbb{C}$-algebra $R_\Gamma$ is finitely generated.

4.3. **$q$-expansion at cusps.** We now consider $q$-expansions at all the cusps $P_1, \ldots, P_r$ of $\mathcal{X}_\Gamma$. For each $1 \leq i \leq r$, choose a matrix $A_i \in \mathrm{SL}_2(\mathbb{Z})$ so that $A_i \cdot \infty \in \mathbb{Q} \cup \{\infty\}$ is a representative of the cusp $P_i$. Let $w_i$ and $h_i$ be the minimal positive integers $m$ for which $\left(\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right)$ lies in $A_i^{-1}\Gamma A_i$ and $A_i^{-1}(\pm\Gamma)A_i$, respectively. We say that $P_i$ is a regular cusp of $\Gamma$ if $w_i = h_i$; otherwise, it is an irregular cusp and we have $w_i = 2h_i$.

Consider a modular form $f \in M_k(\Gamma)$. For $1 \leq i \leq r$, we have

$$(f|_k A_i)(\tau) = \sum_{n=0}^{\infty} a_{n,i}(f)\, q_{w_i}^n \tag{4.1}$$

for unique $a_{n,i}(f) \in \mathbb{C}$, where $q_{w_i} = e^{2\pi i \tau/w_i}$. In particular, we can identify $f|_k A_i$ with a power series in $\mathbb{C}[\![q_{w_i}]\!]$. The ring $\mathbb{C}[\![q_{w_i}]\!]$ is a discrete valuation ring and we denote the corresponding valuation by $\mathrm{ord}_{q_{w_i}} \colon \mathbb{C}[\![q_{w_i}]\!] \twoheadrightarrow \mathbb{Z} \cup \{+\infty\}$. Define the value

$$v_{P_i}(f) := \frac{h_i}{w_i} \mathrm{ord}_{q_{w_i}}(f|_k A_i).$$

4.4. **Modular forms as global sections.** Fix an *even* integer $k \geq 0$. Take any modular form $f \in M_k(\Gamma)$. Using that $f|_k\gamma = f$ for all $\gamma \in \Gamma$, we find that the differential form

$$(2\pi i)^{k/2} f(\tau)\,(d\tau)^{k/2} = w^{k/2}\left(\sum_{n=0}^{\infty} a_n(f)\, q_w^n\right)\left(\frac{dq_w}{q_w}\right)^{k/2} \tag{4.2}$$

on $\mathcal{H}$ induces a meromorphic differential $k/2$-form $\omega_f$ on $\mathcal{X}_\Gamma$.

Let $\mathrm{div}(\omega_f) = \sum_{P\in\mathcal{X}_\Gamma} n_P \cdot P$ be the divisor of $\omega_f$. We now describe the integer $n_P$ in terms of $f$, cf. equations (2.4.4) and (2.4.5) of [Shi94]. If $P$ is a cusp, then $n_P = v_P(f) - k/2$ and hence $n_P + k/2 \geq 0$. Now suppose $P \in \mathcal{X}_\Gamma$ is not a cusp. Choose a $z \in \mathcal{H}$ that lies over $P$ and let $e$ be its order, i.e., the order of the cyclic group $\{\gamma \in \Gamma : \gamma \cdot z = z\}/(\Gamma \cap \{\pm I\})$. We have $n_P = v_z(f)/e - k/2 \cdot (1 - 1/e)$, where $v_z(f)$ is the order of vanishing of the meromorphic function $f$ at $z$. Since $f$ is holomorphic at $z$, we have $n_P + \lfloor k/2 \cdot (1-1/e)\rfloor \geq -k/2 \cdot (1-1/e) + \lfloor k/2 \cdot (1-1/e) > -1$. So $n_P + \lfloor k/2 \cdot (1 - 1/e)\rfloor \geq 0$ since $n_P$ is an integer. Therefore, $\mathrm{div}(\omega_f) + D_k \geq 0$ where $D_k$ is the divisor

$$\sum_{i=1}^{r} k/2 \cdot P_i + \sum_{i=1}^{s} \lfloor k/2 \cdot (1 - 1/e_i)\rfloor \cdot Q_i. \tag{4.3}$$

So we have an injective $\mathbb{C}$-linear map

$$\psi_k \colon M_k(\Gamma) \to H^0(\mathcal{X}_\Gamma, \mathcal{L}_k), \quad f \mapsto \omega_f,$$

where $\mathcal{L}_k$ is the invertible sheaf $\Omega_{\mathcal{X}_\Gamma}^{\otimes k/2}(D_k)$ on the Riemann surface $\mathcal{X}_\Gamma$.

Moreover, $\psi_k$ is an isomorphism. Indeed, given a differential form $\omega \in H^0(\mathcal{X}_\Gamma, \mathcal{L}_k)$, it lifts to a differential form (4.2) on $\mathcal{H}$, where $f$ is a meromorphic function on $\mathcal{H}$ that satisfies $f|_k\gamma = f$ for all $\gamma \in \Gamma$. That $f$ is holomorphic on $\mathcal{H}$ and has the desired conditions at the cusps follows from $\mathrm{div}(\omega) + D_k \geq 0$.

The invertible sheaf $\mathscr{L}_k$ has degree $B_{k,\Gamma} := k/2 \cdot (2g-2) + k/2 \cdot r + \lfloor k/4 \rfloor \cdot v_2 + \lfloor k/3 \rfloor \cdot v_3$. We have

$$B_{k,\Gamma} \leq k/12 \cdot [\mathrm{SL}_2(\mathbb{Z}) : \pm\Gamma] \tag{4.4}$$

since $g - 1 + v_2/4 + v_3/3 + r/2 = [\mathrm{SL}_2(\mathbb{Z}) : \pm\Gamma]/12$ by [Shi94, Proposition 1.40].

When $k \geq 2$, we have $\deg \mathscr{L}_k > 2g-2$, cf. [Shi94, §2.6] and use $r \geq 1$. So if $k \geq 2$, the Riemann–Roch theorem implies that

$$\dim_{\mathbb{C}} M_k(\Gamma) = \dim_{\mathbb{C}} \deg(\mathscr{L}_k) - g + 1 = (k-1)(g-1) + k/2 \cdot r + v_2 \cdot \lfloor k/4 \rfloor + v_3 \cdot \lfloor k/3 \rfloor. \tag{4.5}$$

In the excluded case $k = 0$, we have $M_0(\Gamma) = \mathbb{C}$. We now describe how many terms of the $q$-expansions of a modular form $f$ are required to determine it.

**Lemma 4.1** (Sturm bound)**.** *For any $f, f' \in M_k(\Gamma)$, we have $f = f'$ if and only if $\sum_{j=1}^{r} v_{P_j}(f - f') > B_{k,\Gamma}$.*

*Proof.* If $f = f'$, then $\sum_{j=1}^{r} v_{P_j}(f - f') = +\infty$. So take any distinct $f, f' \in M_k(\Gamma)$. It remains to show that $\sum_{j=1}^{r} v_{P_j}(f - f') \leq B_{k,\Gamma}$. Without loss of generality, we may assume that $f \neq 0$ and $f' = 0$.

The coefficient of the divisor $\mathrm{div}(\omega_f) + D_k$ at the cusp $P_i$ is $(v_{P_i}(f) - k/2) + k/2 = v_{P_i}(f)$. Since $\mathrm{div}(\omega_f) + D_k \geq 0$, we have $\sum_{i=1}^{r} v_{P_i}(f) \leq \deg(\mathrm{div}(\omega_f) + D_k) = k/2 \cdot (2g-2) + \deg D_k = B_{k,\Gamma}$. Therefore, $\sum_{i=1}^{r} v_{P_i}(f) \leq B_{k,\Gamma}$ as required. □

Now assume further that $-I \in \Gamma$ and hence $M_k(\Gamma) = 0$ for odd $k$. Using that $\mathscr{L}_k \otimes \mathscr{L}_{k'} \subseteq \mathscr{L}_{k+k'}$ for any even non-negative integers $k$ and $k'$, we find that the isomorphisms $\psi_k$ combine to give an isomorphism of graded $\mathbb{C}$-algebras:

$$\psi \colon R_\Gamma \xrightarrow{\sim} \bigoplus_{k \geq 0 \text{ even}} H^0(\mathscr{X}_\Gamma, \mathscr{L}_k).$$

4.5. **Actions.** Fix positive integers $k$ and $N$. Since $\Gamma(N)$ is normal in $\mathrm{SL}_2(\mathbb{Z})$, the slash operator of weight $k$ gives a right action of $\mathrm{SL}_2(\mathbb{Z})$ on $M_k(\Gamma(N))$. Take any modular form $f = \sum_{n=0}^{\infty} a_n(f) q_N^n$ in $M_k(\Gamma(N))$. For every field automorphism $\sigma$ of $\mathbb{C}$, there is a unique modular form $\sigma(f) \in M_k(\Gamma(N))$ whose $q$-expansion is $\sum_{n=0}^{\infty} \sigma(a_n(f))\, q_N^n$. This defines an action of $\mathrm{Aut}(\mathbb{C})$ on $M_k(\Gamma)$.

The following describes how these actions of $\mathrm{SL}_2(\mathbb{Z})$ and $\mathrm{Aut}(\mathbb{C})$ interact; it is [BN19, Theorem 3.3] (they give two proofs, one using Katz modular forms and another making use of a result of Khuri-Makdisi on Eisenstein series, cf. Theorem 4.9).

**Lemma 4.2.** *Take any modular form $f \in M_k(\Gamma(N))$. Take any $\sigma \in \mathrm{Aut}(\mathbb{C})$ and let $m$ be the unique element of $(\mathbb{Z}/N\mathbb{Z})^\times$ for which $\sigma(\zeta_N) = \zeta_N^m$. Take any $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and let $\gamma'$ be any element of $\mathrm{SL}_2(\mathbb{Z})$ congruent to $\left(\begin{smallmatrix} a & mb \\ m^{-1}c & d \end{smallmatrix}\right)$ modulo $N$. Then $\sigma(f|_k\gamma) = \sigma(f)|_k\gamma'$.*

Using Lemma 4.2 with $\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q}(\zeta_N))$ and $\gamma \in \Gamma(N)$, we find that the action of $\mathrm{SL}_2(\mathbb{Z})$ on $M_k(\Gamma(N))$ via the slash operator gives rise to a well-defined action on $M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$.

We have an isomorphism $(\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$, $d \mapsto \sigma_d$, where $\sigma_d(\zeta_N) = \zeta_N^d$. We now recall an action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$ viewed as a $\mathbb{Q}$-vector space.

**Lemma 4.3.** *There is a unique right action $*$ of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$ such that the following hold:*

- *if $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, then $f * A = f|_k\gamma$, where $\gamma$ is any matrix in $\mathrm{SL}_2(\mathbb{Z})$ that is congruent to $A$ modulo $N$,*
- *if $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$, then $f * A = \sigma_d(f)$.*

*Proof.* See [BN19, §3]; it is Lemma 4.2 that allows us to show that the actions in the two parts are compatible. □

*Remark* 4.4. We obtain a right action $*$ of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on the graded ring $\bigoplus_{k\geq 0} M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$ that respects multiplication. If $f$ and $f' \neq 0$ are modular forms in $M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$, then $f/f' \in \mathcal{F}_N$ and for $A \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, we have $(f/f') * A = (f * A)/(f' * A)$ with the action from §3.1.

Now suppose that $k \neq 1$. The natural map

$$M_k(\Gamma(N), \mathbb{Q}(\zeta_N)) \otimes_{\mathbb{Q}(\zeta_N)} \mathbb{C} \to M_k(\Gamma(N))$$

is an isomorphism of complex vector spaces, cf. [Kat73, §1.7]. For any congruence subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ whose level divides $N$, taking $\Gamma$-invariants shows that the natural map

$$M_k(\Gamma, \mathbb{Q}(\zeta_N)) \otimes_{\mathbb{Q}(\zeta_N)} \mathbb{C} \to M_k(\Gamma) \tag{4.6}$$

is an isomorphic of complex vector spaces.

4.6. **The spaces $M_{k,G}$.** Fix a positive integer $N$ and let $G$ be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that satisfies $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$. For each integer $k \geq 0$, we define the $\mathbb{Q}$-vector space

$$M_{k,G} := M_k(\Gamma(N), \mathbb{Q}(\zeta_N))^G,$$

where we are considering the subspace fixed by the $G$-action $*$ from Lemma 4.3. Let $\Gamma_G$ be the congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ consisting of matrices that are congruent modulo $N$ to an element of $H := G \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Note that $M_{k,G} \subseteq M_k(\Gamma(N), \mathbb{Q}(\zeta_N))^H = M_k(\Gamma_G, \mathbb{Q}(\zeta_N))$.

**Lemma 4.5.** *The natural homomorphisms*

$$M_{k,G} \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_N) \to M_k(\Gamma_G, \mathbb{Q}(\zeta_N)) \quad \text{and} \quad M_{k,G} \otimes_{\mathbb{Q}} \mathbb{C} \to M_k(\Gamma_G)$$

*are isomorphisms for $k \neq 1$.*

*Proof.* Since $H$ is normal in $G$, we have a right action of $G/H$ on $M_k(\Gamma(N), \mathbb{Q}(\zeta_N))^H = M_k(\Gamma_G, \mathbb{Q}(\zeta_N))$. Let $\varphi\colon G/H \to \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ be the homomorphism satisfying $\varphi(A)(\zeta_N) = \zeta_N^{\det A}$; it is an isomorphism since $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$. Since $G/H$ is abelian, the isomorphism $\varphi$ induces a (left) action $\bullet$ of $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ on $M_k(\Gamma_G, \mathbb{Q}(\zeta_N))$. We have $\sigma \bullet (cf) = \sigma(c)(\sigma \bullet f)$ for all $c \in \mathbb{Q}(\zeta_N)$, $f \in M_k(\Gamma_G, \mathbb{Q}(\zeta_N))$ and $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$. By Galois descent for vector spaces (see the corollary to Proposition 6 in Chapter V §10 of [Bou03]), the natural homomorphism

$$M_{k,G} \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_N) = M_k(\Gamma_G, \mathbb{Q}(\zeta_N))^{\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})} \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_N) \to M_k(\Gamma_G, \mathbb{Q}(\zeta_N))$$

is an isomorphism of $\mathbb{Q}(\zeta_N)$-vector spaces. The lemma follows by tensoring this isomorphism up to $\mathbb{C}$ and using (4.6). □

Later we will need the following which guarantees the existence of nonzero weight 3 modular forms whenever we have $-I \notin G$.

**Lemma 4.6.** *If $-I \notin G$, then $M_{3,G} \neq 0$.*

*Proof.* We need only verify that $M_3(\Gamma_G) \neq 0$ by Lemma 4.5. There is an explicit formula for the dimension $d$ of $M_3(\Gamma_G)$ over $\mathbb{C}$, cf. [Shi94, Theorem 2.25]. From this formula, we will clearly have $d \geq 1$ when $\Gamma_G$ has genus at least 1. In the genus 0 case, we verified that $d \geq 1$ by using the classification of genus 0 congruence subgroups from [CP03]. □

In §4.8, we will describe how to compute a basis of $M_{k,G}$ using Eisenstein series when $k \geq 2$.

4.7. **Eisenstein series.** We now describe some explicit modular forms. See [Kat04, §3] for the basics on Eisenstein series. For further information, we refer to §§2–3 of [BN19] where all the basic results below are summarized and referenced (except for the explicit constant $c_0$ in Lemma 4.7, see [Bru17, Lemma 3.1] instead).

Fix positive integers $k$ and $N$. Take any pair $\alpha \in (\mathbb{Z}/N\mathbb{Z})^2$ and choose $a, b \in \mathbb{Z}$ so that $\alpha \equiv (a, b) \pmod N$. With $\tau \in \mathcal{H}$, consider the series

$$E_\alpha^{(k)}(\tau, s) = \frac{(k-1)!}{(-2\pi i)^k} \sum_{\substack{\omega \in \mathbb{Z}+\mathbb{Z}\tau \\ \omega \neq -(a\tau+b)/N}} \left(\frac{a\tau+b}{N} + \omega\right)^{-k} \cdot \left|\frac{a\tau+b}{N} + \omega\right|^{-2s}. \tag{4.7}$$

The series (4.7) converges when the real part of $s \in \mathbb{C}$ is large enough. Hecke proved that $E_\alpha^{(k)}(\tau, s)$ can be analytically continued to all $s \in \mathbb{C}$. Using this analytic continuation, we define the Eisenstein series

$$E_\alpha^{(k)}(\tau) := E_\alpha^{(k)}(\tau, 0).$$

When $k \geq 3$, we can also obtain $E_\alpha^{(k)}(\tau)$ by simply setting $s = 0$ in the series (4.7).

For $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, we have

$$E_\alpha^{(k)}|_k \gamma = E_{\alpha\gamma}^{(k)},$$

where $\alpha\gamma \in (\mathbb{Z}/N\mathbb{Z})^2$ denotes matrix multiplication. In particular, $E_\alpha^{(k)}$ is fixed by $\Gamma(N)$.

**Lemma 4.7.** *Suppose that $k \geq 1$ and $k \neq 2$. Then $E_\alpha^{(k)}$ is a modular form of weight $k$ on $\Gamma(N)$ with $q$-expansion*

$$c_0 + \sum_{\substack{m,n \geq 1 \\ m \equiv a \bmod N}} n^{k-1} \zeta_N^{bn} q_N^{mn} + (-1)^k \sum_{\substack{m,n \geq 1 \\ m \equiv -a \bmod N}} n^{k-1} \zeta_N^{-bn} q_N^{mn},$$

*where $c_0$ is an element of $\mathbb{Q}(\zeta_N)$. When $k = 1$, we have*

$$c_0 = \begin{cases} 0 & \text{if } a \equiv b \equiv 0 \pmod N, \\ \frac{1}{2}\frac{1+\zeta_N^b}{1-\zeta_N^b} & \text{if } a \equiv 0 \pmod N \text{ and } b \not\equiv 0 \pmod N, \\ \frac{1}{2} - \frac{a_0}{N} & \text{if } a \not\equiv 0 \pmod N, \end{cases}$$

*where $0 \leq a_0 < N$ is the integer congruent to $a$ modulo $N$.*

*Remark* 4.8. For the excluded case $k = 2$, one should instead consider $E_\alpha^{(2)} - E_{(0,0)}^{(2)}$ which belongs to $M_2(\Gamma(N))$ and has a computable $q$-expansion.

Remarkably, we can recover all higher weight modular forms from the Eisenstein series of weight 1.

**Theorem 4.9** (Khuri-Makdisi)**.** *Suppose $N \geq 3$. Let $\mathcal{R}_N$ be the $\mathbb{C}$-subalgebra of $R_{\Gamma(N)} = \bigoplus_{k \geq 0} M_k(\Gamma(N))$ generated by the Eisenstein series $E_\alpha^{(1)}$ with $\alpha \in (\mathbb{Z}/N\mathbb{Z})^2$. Then $\mathcal{R}_N$ contains all modular forms of weight $k$ on $\Gamma(N)$ for all $k \geq 2$.*

*Proof.* This particular formulation of results of Khuri-Makdisi [KM12] is Theorem 3.1 of [BN19]. □

For our applications, the important part of this theorem is we have an explicit set of modular forms that span $M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$ and that we understand the action $*$ of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on these modular forms.

**Corollary 4.10.** *Fix integers $k \geq 2$ and $N \geq 3$.*

(i) *The $\mathbb{Q}(\zeta_N)$-vector space $M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$ is spanned by the set*

$$\left\{ E_{\alpha_1}^{(1)} \cdots E_{\alpha_k}^{(1)} : \alpha_1, \ldots, \alpha_k \in (\mathbb{Z}/N\mathbb{Z})^2 - \{0\} \right\}.$$

(ii) *For $\alpha_1, \ldots, \alpha_k \in (\mathbb{Z}/N\mathbb{Z})^2$ and $A \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, we have*

$$(E_{\alpha_1}^{(1)} \cdots E_{\alpha_k}^{(1)}) * A = E_{\alpha_1 A}^{(1)} \cdots E_{\alpha_k A}^{(1)}.$$

*Proof.* Let $S$ be the set of modular forms $E_{\alpha_1}^{(1)} \cdots E_{\alpha_k}^{(1)}$ with $\alpha_i \in (\mathbb{Z}/N\mathbb{Z})^2$. We have $S \subseteq M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$ by Lemma 4.7. As noted in §4.5, the natural map $M_k(\Gamma(N), \mathbb{Q}(\zeta_N)) \otimes_{\mathbb{Q}(\zeta_N)} \mathbb{C} \to M_k(\Gamma(N))$ is an isomorphism. Since $S$ spans $M_k(\Gamma(N))$ by Theorem 4.9, we deduce that $S$ spans the $\mathbb{Q}(\zeta_N)$-vector space $M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$. This proves part (i) after noting that $E_{(0,0)}^{(1)} = 0$.

We now prove (ii) for a fixed matrix $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Choose any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ for which $\gamma \equiv A \pmod{N}$. We have $E_{\alpha_i}^{(1)}|_1 \gamma = E_{\alpha_i \gamma}^{(1)} = E_{\alpha_i A}^{(1)}$ for $1 \le i \le k$ and hence

$$(E_{\alpha_1}^{(1)} \cdots E_{\alpha_k}^{(1)}) * A = (E_{\alpha_1}^{(1)} \cdots E_{\alpha_k}^{(1)})|_k \gamma = (E_{\alpha_1}^{(1)}|_1 \gamma) \cdots (E_{\alpha_k}^{(1)}|_1 \gamma) = E_{\alpha_1 A}^{(1)} \cdots E_{\alpha_k A}^{(1)}.$$

It thus suffices to prove (ii) for any matrix $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. If $\alpha_i = (a_i, b_i) \in (\mathbb{Z}/N\mathbb{Z})^2$, the explicit $q$-expansion of $E_{\alpha_i}^{(1)}$ in Lemma 4.7 gives us that $\sigma_d(E_{\alpha_i}^{(1)}) = E_{(a_i, b_i d)}^{(1)} = E_{\alpha_i A}^{(1)}$. Therefore, $(E_{\alpha_1}^{(1)} \cdots E_{\alpha_k}^{(1)}) * A = \sigma_d(E_{\alpha_1}^{(1)} \cdots E_{\alpha_k}^{(1)}) = E_{\alpha_1 A}^{(1)} \cdots E_{\alpha_k A}^{(1)}$. □

**Corollary 4.11.** *Fix integers $k \ge 2$ and $N \ge 3$. Let $G$ be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that satisfies $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$. Then the $\mathbb{Q}$-vector space $M_{k,G}$ is spanned by the set of modular forms of the form*

$$\sum_{g \in G} \zeta_N^{j \det g} E_{\alpha_1 g}^{(1)} \cdots E_{\alpha_k g}^{(1)} \tag{4.8}$$

*with $\alpha_i \in (\mathbb{Z}/N\mathbb{Z})^2 - \{0\}$ and $0 \le j < \phi(N) := |(\mathbb{Z}/N\mathbb{Z})^\times|$.*

*Proof.* Define the $\mathbb{Q}$-linear map $T\colon M_k(\Gamma(N), \mathbb{Q}(\zeta_N)) \to M_{k,G}$ by $f \mapsto \sum_{g \in G} f * g$. The map $T$ is surjective since it is multiplication by $|G|$ when restricted to $M_{k,G}$.

Let $S$ be the set of modular forms $\zeta_N^j E_{\alpha_1}^{(1)} \cdots E_{\alpha_k}^{(1)}$ with $\alpha_i \in (\mathbb{Z}/N\mathbb{Z})^2 - \{0\}$ and $0 \le j < \phi(N)$. By Corollary 4.10(i), we find that $S$ spans $M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$ as a $\mathbb{Q}$-vector space. Therefore, the $\mathbb{Q}$-vector space $M_{k,G}$ is spanned by the set $T(S)$.

The corollary follows by noting that $T(\zeta_N^j E_{\alpha_1}^{(1)} \cdots E_{\alpha_k}^{(1)})$ agrees with (4.8) by Corollary 4.10(ii). □

4.8. **Finding a basis for $M_{k,G}$.** Fix a positive integer $N$ and let $G$ be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that satisfies $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$ and $-I \in G$. Let $\Gamma_G$ be the congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ consisting of matrices whose image modulo $N$ lies in $G$. Fix notation as in §4.1 with $\Gamma := \Gamma_G$. In particular, let $P_1, \ldots, P_r \in \mathbb{Q} \cup \{\infty\}$ be representatives of the cusps of $\mathcal{X}_\Gamma$. The cusps are all regular since $-I \in \Gamma_G$.

Fix an integer $k \ge 0$. In this section, we describe how to compute a basis of $M_{k,G}$. A modular form in our basis will be explicitly given by its $q$-expansions at each cusp of $\mathcal{X}_{\Gamma_G}$ with enough terms computed to uniquely determine it. Moreover, we will be able to compute arbitrarily many terms of these $q$-expansions.

We may assume that $k$ is even since $-I \in G$ implies that $M_{k,G} = 0$ when $k$ is odd. We may assume that $k \ge 2$ since $M_{0,G} = \mathbb{Q}$. We can further assume that $N \ge 3$ (when $N \le 2$, we can replace $G$ by its inverse image under the reduction map $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$; this does not change $M_{k,G}$).

Let $d$ be the dimension of $M_{k,G}$ over $\mathbb{Q}$; it agrees with the dimension of the complex vector space $M_k(\Gamma_G)$ and hence is computable by (4.5). We may assume that $d \geq 1$ since otherwise $M_{k,G} = 0$. Set $B_{k,G} := B_{k,\Gamma_G}$ and let $b_{k,G}$ be the smallest integer satisfying

$$b_{k,G} > B_{k,G} \cdot N/[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_G]. \tag{4.9}$$

Define $m := \sum_{i=1}^{r} m_i$, where $m_i := \lceil w_i b_{k,G}/N \rceil$.

For each $1 \leq i \leq r$, we have chosen a matrix $A_i \in \mathrm{SL}_2(\mathbb{Z})$ satisfying $A_i \cdot \infty = P_i$ and this gives rise to $q$-expansions (4.1). Define the $\mathbb{Q}$-linear map

$$\begin{aligned}\varphi_k \colon M_{k,G} &\to \mathbb{Q}(\zeta_N)^m, \\ f &\mapsto \big(a_{0,1}(f), \ldots, a_{m_1-1,1}(f),\ a_{0,2}(f), \ldots, a_{m_2-1,2}(f),\ \ldots,\ a_{0,r}(f), \ldots, a_{m_r-1,r}(f)\big).\end{aligned}$$

**Lemma 4.12.** *The map $\varphi_k$ is injective.*

*Proof.* Take any $f \in \ker \varphi_k$. For each $1 \leq i \leq r$, we have

$$v_{P_i}(f) = \mathrm{ord}_{q_{w_i}}(f) \geq m_i \geq w_i b_{k,G}/N$$

and hence $\sum_{i=1}^{r} v_{P_i}(f) \geq \sum_{i=1}^{r} w_i \cdot b_{k,G}/N$. We have $\sum_{i=1}^{r} w_i = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_G]$; one way to see this is to add the ramification indices of the cusps with respect to the natural morphism $\mathcal{X}_{\Gamma_G} \to \mathcal{X}_{\mathrm{SL}_2(\mathbb{Z})}$ of degree $[\mathrm{SL}_2(\mathbb{Z}) : \pm\Gamma_G] = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_G]$. Therefore, $\sum_{i=1}^{r} v_{P_i}(f) \geq [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_G] \cdot b_{k,G}/N > B_{k,G}$. We have $f = 0$ by Lemma 4.1. □

*Remark* 4.13. Of course the map $\varphi$ remains injective if we replace $b_{k,G}$ by any larger integer $b$. In particular, any integer $b > kN/12$ will work by (4.4).

**Algorithm 4.14.** This algorithm computes a basis $\beta$ of the $\mathbb{Q}$-vector space $\varphi_k(M_{k,G})$.

(1) Compute the $q$-expansion $E_\alpha^{(1)} + O(q_N^b)$ for all $\alpha \in (\mathbb{Z}/N\mathbb{Z})^2 - \{0\}$ using the explicit expression from Lemma 4.7.

(2) Let $S$ be the set of all $k$-tuples $(\alpha_1, \ldots, \alpha_k)$ with $\alpha_i \in (\mathbb{Z}/N\mathbb{Z})^2 - \{0\}$. Set $\beta := \emptyset$.

(3) Choose a $k$-tuple $(\alpha_1, \ldots, \alpha_k) \in S$. For each integer $0 \leq j < \phi(N)$, define the modular form

$$f_j := \sum_{g \in G} \zeta_N^{j \det g}\, E^{(1)}_{\alpha_1 g} \cdots E^{(1)}_{\alpha_k g}; \tag{4.10}$$

it lies in $M_{k,G}$ by Corollary 4.11. Using our approximations of the $E_\alpha^{(1)}$ from Step 1, compute

$$f_j|_k A_i + O(q_N^b) = \sum_{g \in G} \zeta_N^{j \det g}\, E^{(1)}_{\alpha_1 g A_i} \cdots E^{(1)}_{\alpha_k g A_i} + O(q_N^b) \tag{4.11}$$

for all $1 \leq i \leq r$. Since $f_j|_k A_i \in \mathbb{Q}(\zeta_N)[\![q_{w_i}]\!]$, this gives us $f_j|_k A_i + O(q_{w_i}^{m_i})$ where $m_i = \lceil w_i b/N \rceil$. In particular, we can compute the vector $\varphi_k(f_j) \in \mathbb{Q}(\zeta_N)^m$.

Running over the integers $0 \leq j < \phi(N)$, if $\varphi_k(f_j)$ is not in the span of $\beta$ in $\mathbb{Q}(\zeta_N)^m$ as a $\mathbb{Q}$-vector space, then adjoin $\varphi_k(f_j)$ to the set $\beta$.

(4) Remove from the set $S$ all $k$-tuples of the form $(\alpha_{\sigma(1)} g, \ldots, \alpha_{\sigma(k)} g)$ for some $\sigma \in \mathfrak{S}_k$ and some $g \in G$. If $|\beta| < d$, then return to Step 3.

Since $\varphi_k$ is injective and $\dim_{\mathbb{Q}} M_{k,G} = d$, if the algorithm terminates, then it will produce a basis $\beta$ of the $\mathbb{Q}$-vector space $\varphi_k(M_{k,G})$. The modular form (4.10) does not change if we replace $(\alpha_1, \ldots, \alpha_k)$ with a $k$-tuple $(\alpha_{\sigma(1)} g, \ldots, \alpha_{\sigma(k)} g)$ with $\sigma \in \mathfrak{S}_k$ and $g \in G$; this justifies the elements removed from the set $S$ in Step 4 (they would not produce new modular forms). Corollary 4.11 ensures that we will eventually find enough modular forms so that the algorithm halts with a set $\beta$ of cardinality $d$.

This algorithm computes the basis of $M_{k,G}$ in the sense that there is a unique basis $F_1, \dots, F_d$ of $M_{k,G}$ as a $\mathbb{Q}$-vector space so that $\varphi_k(F_1), \dots, \varphi_k(F_d)$ is the ordered basis $\beta$. For each $1 \le e \le d$, the modular form $F_e$ will be of the form (4.10) for explicit $j$ and $(\alpha_1, \dots, \alpha_k)$. By computing the $q$-expansions of the relevant Eisenstein series to higher precision, one can compute an arbitrary number of terms in the $q$-expansion of $F_e$ at each cusp. By Lemma 4.5, $F_1, \dots, F_d$ is also a basis of the complex vector space $M_k(\Gamma_G)$.

*Remark* 4.15.

(i) Since our basis of $M_{k,G}$ is given by a $q$-expansion at each cusp, we can also compute subspaces obtained by forcing vanishing conditions at the cusps. For example, let $S_{k,G}$ be the $\mathbb{Q}$-subspace of $M_{k,G}$ consisting of modular forms $f \in M_{k,G}$ that satisfy $a_{0,i}(f) = 0$ for all $1 \le i \le r$. Alternatively, the group $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ acts on the cusps forms $S_k(\Gamma(N), \mathbb{Q}(\zeta_N))$ via $*$ and we have $S_{k,G} = S_k(\Gamma(N), \mathbb{Q}(\zeta_N))^G$. Thus $\varphi(S_{k,G})$ is an explicit subspace of $\varphi(M_{k,G})$ and a basis can be computed.

(ii) Once you have a basis of $M_{k,G}$, you can construct a "nicer" one. We have $(2N)^k \cdot \varphi_k(\beta) \subseteq \mathbb{Z}[\zeta_N]^m$ by considering the $q$-expansion in Lemma 4.7. Let

$$\iota \colon \mathbb{Z}[\zeta_N]^m \xrightarrow{\sim} (\mathbb{Z}^{\phi(N)})^m = \mathbb{Z}^{\phi(N)m}$$

be the isomorphism of $\mathbb{Z}$-modules obtained by applying to the coordinates the map $\mathbb{Z}[\zeta_N] \to \mathbb{Z}^{\phi(N)}$, $\sum_{i=1}^{\phi(N)} a_i \zeta_N^{i-1} \mapsto (a_1, \dots, a_{\phi(N)})$. Define $C := \iota((2N)^k \cdot \varphi_k(\beta)) \subseteq \mathbb{Z}^{\phi(N)m}$.

Let $L$ be the subgroup of $\mathbb{Z}^{\phi(N)m}$ generated by $C$ and let $L'$ be its *saturation*, i.e., the group of $a \in \mathbb{Z}^{\phi(N)m}$ such that $da \in L$ for some positive integer $d$. Let $C'$ be a basis of the free abelian group $L'$; applying the LLL algorithm [Coh93, §2.6] will produce basis elements with small entries. Define $\beta' := \iota^{-1}(C')$; it is also a basis of the $\mathbb{Q}$-vector space $\varphi_k(M_{k,G})$ but with integral (and in practice simpler) entries that the original basis $\beta$.

(iii) When some modular forms $f \in M_{k,G}$ are already known, we can adjoin the vectors $\varphi_k(f)$ to the set $\beta$ before beginning the algorithm (making sure the set $\beta$ is linearly independent over $\mathbb{Q}$). For example, some modular forms in $M_{k,G}$ can be obtained from modular forms of lower weight or from a larger group.

(iv) Set $H := G \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and let $R$ be a set of representatives of the cosets $G/H$. With notation as above, we have

$$f_j|_k A_i = \sum_{g \in R} \zeta_N^{j \det g} \Big( \sum_{h \in H} E^{(1)}_{\alpha_1 g h A_i} \cdots E^{(1)}_{\alpha_k g h A_i} \Big).$$

The inner sums of this expression can be computed first and used for all $j$.

Another observation that makes computing $f_j|_k A_i$ quicker is that its $q$-expansion is a power series in $q_{w_i} = q_N^{N/w_i}$. Let $U_i$ be the subgroup of $A_i^{-1} H A_i$ generated by $\left(\begin{smallmatrix} 1 & w_i \\ 0 & 1 \end{smallmatrix}\right)$ and let $R_i$ be a set of representatives of the cosets $(A_i^{-1} H A_i)/U_i$. We then have

$$\sum_{h \in H} E^{(1)}_{\alpha_1 g h A_i} \cdots E^{(1)}_{\alpha_k g h A_i} = \sum_{h \in A_i^{-1} H A_i} E^{(1)}_{\alpha_1 g A_i h} \cdots E^{(1)}_{\alpha_k g A_i h} = \sum_{u \in U_i} \Big( \sum_{h \in R_i} E^{(1)}_{\alpha_1 g A_i h} \cdots E^{(1)}_{\alpha_k g A_i h} \Big) * u.$$

An easy computation shows that for a modular form $f = \sum_{n=0}^{\infty} c_n q_N^n$ of weight $k$, we have

$$\sum_{u \in U_i} f * u = \frac{N}{w_i} \sum_{\substack{n=0 \\ n \equiv 0 \pmod{N/w_i}}}^{\infty} c_n q_N^n.$$

(v) Consider a subgroup $G \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that satisfies $-I \in G$. Let $L_G$ be the subfield of $\mathbb{Q}(\zeta_N)$ fixed by the group $\{\sigma_d : d \in \det(G)\}$. We have $L_G = \mathbb{Q}$ if and only if $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$. We can define $M_{k,G}$ as before. Now $M_{k,G}$ is an $L_G$-vector space of dimension $d$ and hence a

$\mathbb{Q}$-vector space of dimension $d \cdot [L_G : \mathbb{Q}] = d[(\mathbb{Z}/N\mathbb{Z})^\times : \det(G)]$. Some easy changes in the above algorithm can be made to compute a basis of $M_{k,G}$ over $\mathbb{Q}$ or $L_G$.

(vi) Much of this section can be easily generalized to deal with odd weights $k \geq 3$.

(vii) There are other methods for constructing a basis of $M_{k,G}$ whose $q$-expansions at each cusp we can compute arbitrarily many terms of.

In [Zyw20a], we explained how to compute an explicit basis of $M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$ and express the right action of $\mathrm{SL}_2(\mathbb{Z})$ with respect to this basis (we did numerical computations and then identified the algebraic numbers that arose). From this, we can then compute $M_{k,G}$. We did not take this approach since $M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$ is often significantly large than $M_{k,G}$. It should be possible to adapt the methods of [Zyw20a] to be more appropriate, but we instead have used Eisenstein series since they were more algebraic in flavour.

4.9. **Explicit slash action.** Fix a modular form $f \in M_{k,G}$ with assumptions as in §4.8. Now consider any matrix $B \in \mathrm{GL}_2(\mathbb{Q})$ with positive determinant. We shall explain how the $q$-expansion of $f$ at all the cusps allows us to find the Fourier expansion for $f|_k B$.

It is clear how scalar matrices act, so we may assume that $B$ is in $M_2(\mathbb{Z})$ and that the greatest common divisors of its entries is 1. There is a unique $1 \leq j \leq r$ and a matrix $\gamma \in \Gamma$ such that $B \cdot \infty = (\gamma A_j) \cdot \infty$. Therefore,

$$B = \varepsilon \gamma A_j \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$$

for some $\varepsilon \in \{\pm 1\}$ and integers $a, b, d \in \mathbb{Z}$ with $a$ and $d$ positive and relatively prime. Since $f|_k(-I) = (-1)^k f$ and $f|_k \gamma = f$, this implies that $f|_k B = \varepsilon^k (f|_k A_j)|_k \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$. Using (4.1), we deduce that

$$(f|_k B)(\tau) = \varepsilon^k \Big( \sum_{n=0}^{\infty} a_{n,j}(f) \cdot q_{w_j}^n \Big) \Big|_k \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) = \varepsilon^k (a/d)^{k/2} \sum_{n=0}^{\infty} a_{n,j}(f) \zeta_{dw_j}^{cb} \cdot q_{dw_j}^{an}.$$

## 5. Computing modular curves

Fix a positive integer $N$ and let $G$ be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that satisfies $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$ and $-I \in G$. In this section, using modular forms, we describe how to compute an explicit model of the curve $X_G$.

5.1. **Modular forms revisited.** The cusps of $\mathcal{X}_{\Gamma_G} = X_G(\mathbb{C})$ are precisely the points lying over $\infty$ via $\pi_G$. The elliptic points of $\mathcal{X}_{\Gamma_G}$ of order 2 and 3 are the points $P \in \mathcal{X}_\Gamma$ for which $\pi_G$ is unramified and $\pi_G(P)$ is 1728 and 0, respectively. In particular, the cusps, elliptic points of order 2, and elliptic points of order 3 define subschemes of $X_G$.

Fix an even integer $k \geq 0$. Let $D_k$ be the divisor of $\mathcal{X}_{\Gamma_G} = X_G(\mathbb{C})$ given by (4.3) with $\Gamma = \Gamma_G$. Note that $D_k$ is also a divisor of $X_G$ defined over $\mathbb{Q}$. Define the invertible sheaf $\mathscr{L}_k := \Omega_{X_G}^{\otimes k/2}(D_k)$ on $X_G$. Note that $\mathscr{L}_k$ gives rise to the invertible sheaf $\mathcal{L}_k$ on $X_G(\mathbb{C}) = \mathcal{X}_{\Gamma_G}$ with notation as in §4.4 with $\Gamma = \Gamma_G$. In particular, we have an inclusion $H^0(X_G, \mathscr{L}_k) \subseteq H^0(\mathcal{X}_{\Gamma_G}, \mathcal{L}_k)$ which induces an isomorphism $H^0(X_G, \mathscr{L}_k) \otimes_{\mathbb{Q}} \mathbb{C} \to H^0(\mathcal{X}_{\Gamma_G}, \mathcal{L}_k)$.

Recall from §4.4, we have an explicit isomorphism

$$\psi_k \colon M_k(\Gamma_G) \xrightarrow{\sim} H^0(\mathcal{X}_{\Gamma_G}, \mathcal{L}_k).$$

Under the isomorphism $\psi_k$, we now show that $H^0(X_G, \mathscr{L}_k)$ corresponds to the $\mathbb{Q}$-subspace $M_{k,G}$ of $M_k(\Gamma_G)$ from §4.6.

**Lemma 5.1.** *The map $\psi_k$ restricts to an isomorphism $M_{k,G} \xrightarrow{\sim} H^0(X_G, \mathscr{L}_k)$ of vector spaces over $\mathbb{Q}$.*

*Proof.* The isomorphism $\psi_k$ induces an isomorphism $M_{k,G} \otimes_{\mathbb{Q}} \mathbb{C} \xrightarrow{\sim} H^0(X_G, \mathscr{L}_k) \otimes_{\mathbb{Q}} \mathbb{C}$ of complex vector spaces. Therefore, the $\mathbb{Q}$-vector spaces $M_{k,G}$ and $H^0(X_G, \mathscr{L}_k)$ have the same dimension. Since $\psi_k$ is an isomorphism, it thus suffices to prove that $\psi_k^{-1}(H^0(X_G, \mathscr{L}_k)) \subseteq M_{k,G}$.

Take any differential form $\omega \in H^0(X_G, \mathscr{L}_k) \subseteq H^0(\mathscr{X}_{\Gamma_G}, \mathscr{L}_k)$. Choose an element $u \in \mathcal{F}_N^G - \mathbb{Q}$. Since $\mathbb{Q}(X_G) = \mathcal{F}_N^G$, there is a unique $v \in \mathcal{F}_N^G$ such that $\omega = v\,(du)^{k/2}$. Via the quotient map $\mathcal{H} \to \mathscr{X}_{\Gamma_G}$, $\omega = v(du)^{k/2}$ pulls back to the differential form $v(\tau)u'(\tau)^{k/2}(d\tau)^{k/2}$ on $\mathcal{H}$. So $f := \psi_k^{-1}(\omega) \in M_k(\Gamma_G)$ is given by $f(\tau) = (2\pi i)^{-k/2} v(\tau) u'(\tau)^{k/2}$.

Taking the derivative of the $q$-expansion $u = \sum_{n\in\mathbb{Z}} c_n(u) q_N^n$ gives $u'(\tau) = \sum_{n\in\mathbb{Z}} 2\pi i n/N\, c_n(u) q_N^n$. Therefore, $f(\tau) = \big(\sum_{n\in\mathbb{Z}} c_n(v) q_N^n\big) \cdot \big(\sum_{n\in\mathbb{Z}} n/N\, c_n(u) q_N^n\big)^{k/2}$. In particular, we find that $f$ is an element of $M_k(\Gamma_G, \mathbb{Q}(\zeta_N))$ since the $q$-expansions of both $u$ and $v$ have coefficients in $\mathbb{Q}(\zeta_N)$.

Now take any $A \in G$. Set $m := \det(A) \in (\mathbb{Z}/N\mathbb{Z})^\times$ and take any matrix $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ for which $A \equiv \gamma \left(\begin{smallmatrix} 1 & 0 \\ 0 & m \end{smallmatrix}\right) \pmod N$. We have $u|_0\gamma = \sigma_m^{-1}(u)$ and $v|_0\gamma = \sigma_m^{-1}(v)$ since $u * A = u$ and $v * A = v$. The equality $u|_0\gamma = \sigma_m^{-1}(u)$ is the same as $u(\gamma\tau) = \sum_{n\in\mathbb{Z}} \sigma_m^{-1}(c_n(u)) q_N^n$ and taking derivatives of both sides gives $u'(\gamma\tau)(c\tau + d)^{-2} = 2\pi i \sum_{n\in\mathbb{Z}} n/N\, \sigma_m^{-1}(c_n(u)) q_N^n$. Therefore,

$$\begin{aligned} f|_k\gamma &= (2\pi i)^{-k/2}\, v|_0\gamma\, (u'|_2\gamma)^{k/2} \\ &= (2\pi i)^{-k/2}\, \sigma_m^{-1}(v) \left(2\pi i \sum_{n\in\mathbb{Z}} \tfrac{n}{N}\, \sigma_m^{-1}(c_n(u)) q_N^n\right)^{k/2} \\ &= \sigma_m^{-1}\Big(\Big(\sum_{n\in\mathbb{Z}} c_n(v) q_N^n\Big)\Big(\sum_{n\in\mathbb{Z}} \tfrac{n}{N}\, c_n(u) q_N^n\Big)^{k/2}\Big) = \sigma_m^{-1}(f). \end{aligned}$$

Since $f|_k\gamma = \sigma_m^{-1}(f)$, we have $f * A = f$. Since $A$ was an arbitrary element of $G$, this implies that $f = \psi_k^{-1}(\omega)$ lies in $M_k(\Gamma_G, \mathbb{Q}(\zeta_N))^G = M_{k,G}$. We have $\psi_k^{-1}(H^0(X_G, \mathscr{L}_k)) \subseteq M_{k,G}$ since $\omega$ was an arbitrary element of $H^0(X_G, \mathscr{L}_k)$. □

Combining the $\psi_k$, we obtain an isomorphism

$$\bigoplus_k M_{k,G} \xrightarrow{\sim} \bigoplus_k H^0(X_G, \mathscr{L}_k)$$

of graded $\mathbb{Q}$-algebras, where the sums are over even integers $k \geq 0$.

5.2. **Galois action on the cusps.** Let $U$ be the group of upper triangular matrices in $\mathrm{SL}_2(\mathbb{Z})$; it is generated by $-I$ and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Let $U_N \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be the image of $U$ modulo $N$. Define the set of double cosets $\mathscr{C}_G := G\backslash \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/U_N$. In this section, we explain how to identify $\mathscr{C}_G$ with the set of cusps of $\mathscr{X}_{\Gamma_G} = X_G(\mathbb{C})$ and describe the Galois action on it.

The map $\mathrm{SL}_2(\mathbb{Z}) \to \mathbb{Q} \cup \{\infty\} = \mathbb{P}^1(\mathbb{Q})$, $A \mapsto A \cdot \infty$ is surjective and induces a bijection $\iota\colon \mathrm{SL}_2(\mathbb{Z})/U \to \mathbb{P}^1(\mathbb{Q})$. The map $\iota$ respects the natural $\mathrm{SL}_2(\mathbb{Z})$-actions and hence gives a bijection between the set of double cosets $\Gamma_G\backslash \mathrm{SL}_2(\mathbb{Z})/U$ and the set of $\Gamma_G$-orbits of $\mathbb{P}^1(\mathbb{Q})$, i.e., the set of cusps of $\mathscr{X}_{\Gamma_G}$. With notation as in §4.3, the matrices $A_1, \ldots, A_r$ are representatives of the double cosets $\Gamma_G\backslash \mathrm{SL}_2(\mathbb{Z})/U$. Using that the level of $\Gamma_G$ divides $N$ and $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$, we find that the map $\Gamma_G\backslash \mathrm{SL}_2(\mathbb{Z})/U \to \mathscr{C}_G$ obtained from reduction modulo $N$ is also a bijection. This allows us to identify $\mathscr{C}_G$ with the cusps of $\mathscr{X}_{\Gamma_G} = X_G(\mathbb{C})$.

For an $m \in (\mathbb{Z}/N\mathbb{Z})^\times$ and a cusp $P := G \cdot A \cdot U_N \in \mathscr{C}_G \subseteq X_G(\mathbb{C})$, define $m \cdot P := G \cdot A \left(\begin{smallmatrix} 1 & 0 \\ 0 & m \end{smallmatrix}\right) \cdot U_N$. This is well-defined and gives an action of $(\mathbb{Z}/N\mathbb{Z})^\times$ on $U_N$.

**Lemma 5.2.** *The cusps of $X_G$ are all defined over $\mathbb{Q}(\zeta_N)$. For a cusp $P \in X_G(\mathbb{Q}(\zeta_N))$ and an $m \in (\mathbb{Z}/N\mathbb{Z})^\times$, we have $\sigma_m(P) = m \cdot P$.*

*Proof.* Take any $m \in (\mathbb{Z}/N\mathbb{Z})^\times$ and choose any automorphism $\sigma$ of $\mathbb{C}$ for which $\sigma(\zeta_N) = \zeta_N^m$. Take any cusp $P \in \mathscr{C}_G \subseteq X_G(\mathbb{C})$. Fix matrices $A, A' \in \mathrm{SL}_2(\mathbb{Z})$ for which $A \cdot \infty$ and $A' \cdot \infty$ are representatives of the cusps $P$ and $m \cdot P$, respectively. There are $g \in G$ and $u \in U_N$ such that $A \left(\begin{smallmatrix} 1 & 0 \\ 0 & m \end{smallmatrix}\right) \equiv gA'u \pmod{N}$.

Consider a rational function $f \in \mathbb{Q}(X_G)$ that does not have a pole at any of the cusps. Consider the $q$-expansion $f|_0 A = \sum_{n\in\mathbb{Z}} c_n q_N^n$. We have $c_n = 0$ for all $n < 0$ since $f$ does not have a pole at $P$ and we have $c_0 = f(P)$. We have

$$(f|_0 A') * u = f * (gA'u) = f * \left(A \left(\begin{smallmatrix} 1 & 0 \\ 0 & m \end{smallmatrix}\right)\right) = (f|_0 A) * \left(\begin{smallmatrix} 1 & 0 \\ 0 & m \end{smallmatrix}\right) = \sum_{n\in\mathbb{Z}} \sigma_m(c_n) q_N^n$$

and hence $f(m \cdot P) = \sigma_m(c_0) = \sigma(f(P))$. So $f(m \cdot P) = f(\sigma(P))$ for all $f \in \mathbb{Q}(X_G)$ that do not have poles at any cusps. Therefore, $m \cdot P = \sigma(P)$. Since $\sigma|_{\mathbb{Q}(\zeta_N)} = \sigma_m$, it remains to show that $P$ lies in $X_G(\mathbb{Q}(\zeta_N))$.

Since $m \in (\mathbb{Z}/N\mathbb{Z})^\times$ is arbitrary, we have shown that for an automorphism $\sigma$ of $\mathbb{C}$, $\sigma(P)$ depends only on the restriction of $\sigma$ to $\mathbb{Q}(\zeta_N)$. Therefore, $P \in X_G(\mathbb{Q}(\zeta_N))$. □

5.3. **Constructing a model of $X_G$.** Fix notation as in §5.1 with an even integer $k \geq 2$. Let $P_1, \ldots, P_r$ be the cusps of $X_G(\mathbb{C}) = \mathcal{Y}_{\Gamma_G}$.

Take any divisor $E := \sum_{i=1}^r e_i P_i$ of $X_G$ with integers $e_i \geq 0$ that is defined over $\mathbb{Q}$. Note that the divisor $E$ is defined over $\mathbb{Q}$ if and only if the integer $e_i$ depends only on the Galois orbit of $P_i$ (such $E$ can be constructed using the explicit Galois action on cusps from Lemma 5.2). Define the $\mathbb{Q}$-vector space

$$V := \{f \in M_{k,G} : v_{P_i}(f) \geq e_i \text{ for all } 1 \leq i \leq r\}$$

From §4.8, there is an algorithm to compute a basis of $M_{k,G}$ with enough terms of the $q$-expansions known in order to find an explicit basis of $V$. Each modular form in the basis is given by its $q$-expansion at all the cusps of $X_G$ and we can compute arbitrarily many terms of each expansion.

We now assume that $\dim_{\mathbb{Q}} V \geq 2$. Set $d := \dim_{\mathbb{Q}} V - 1$ and denote our basis of $V$ by $f_0, \ldots, f_d$. For each $0 \leq i, j \leq d$, we have $f_j/f_i \in \mathcal{F}_N^G = \mathbb{Q}(X_G)$. Let

$$\varphi \colon X_G \to \mathbb{P}^d_{\mathbb{Q}}$$

be the morphism defined by $\varphi(P) = [f_0(P), \ldots, f_d(P)]$ for all but finitely many $P$. For a fixed $0 \leq i \leq d$ and all but finitely points $P$ of $X_G$, we have $\varphi(P) = [(f_0/f_i)(P), \ldots, (f_d/f_i)(P)]$. Up to composition with an automorphism of $\mathbb{P}^d_{\mathbb{Q}}$, $\varphi$ does not depend on the choice of basis of $V$.

Set $C := \varphi(X_G) \subseteq \mathbb{P}^d_{\mathbb{Q}}$; it is a curve since $d \geq 1$ and hence $f_0/f_1$ is non-constant. Let $I(C)$ be the homogeneous ideal of $\mathbb{Q}[x_0, \ldots, x_d]$ of $C \subseteq \mathbb{P}^d_{\mathbb{Q}}$. We have the usual grading $I(C) = \bigoplus_{n\geq 0} I(C)_n$, where $I(C)_n$ consist of homogeneous polynomials of degree $n$. Note that for a homogeneous polynomial $F \in \mathbb{Q}[x_0, \ldots, x_d]$, the polynomial $F$ lies in $I(C)$ if and only if $F(f_0, \ldots, f_d) = 0$.

For a fixed integer $n \geq 0$, let us now explain how to compute a basis of the $\mathbb{Q}$-vector space $I(C)_n$. Let $\mathscr{M}_n$ be the set of monic polynomials in $\mathbb{Q}[x_0, \ldots, x_d]$ of degree $n$. With notation as in §4.8, we have an injective $\mathbb{Q}$-linear map $\varphi_{nk} \colon M_{nk,G} \hookrightarrow \mathbb{Q}(\zeta_N)^h$ for an explicit integer $h \geq 1$. For each $m \in \mathscr{M}_n$, we can compute $v_m := \varphi_{nk}(m(f_0, \ldots, f_d)) \in \mathbb{Q}(\zeta_N)^h$ assuming we have have computed enough terms of the $q$-expansions of the $f_i$. We can then compute the $\mathbb{Q}$-vector space $W := \{(c_m) \in \mathbb{Q}^{\mathscr{M}_n} : \sum_{m\in\mathscr{M}_n} c_m v_m = 0\}$. The injectivity of $\varphi_{nk}$ implies that the map $W \to I(C)_n$, $(c_m) \mapsto \sum_{m\in\mathscr{M}_n} c_m m$ is an isomorphism of vector spaces over $\mathbb{Q}$ and we have found $I(C)_n$. In practice, to produce a "nice" basis of $W$, we apply the LLL algorithm to $W \cap \mathbb{Z}^{\mathscr{M}_n}$.

Define the invertible sheaf $\mathcal{F} := \mathscr{L}_k(-E)$ on $X_G$. The isomorphism $\psi_k$ restricts to an isomorphism $V \xrightarrow{\sim} H^0(X_G, \mathcal{F})$ of $\mathbb{Q}$-vector spaces; use Lemma 5.1 and the description of $\psi_k$ from §4.4. We have

$$\deg \mathcal{F} = \deg \mathscr{L}_k - \sum_{i=1}^{r} e_i = k/2 \cdot (2g-2) + k/2 \cdot r + \lfloor k/4 \rfloor \cdot v_2 + \lfloor k/3 \rfloor \cdot v_3 - \sum_{i=1}^{r} e_i. \tag{5.1}$$

Using the Riemann–Roch theorem, we have $d = \deg \mathcal{F} - g$ when $\deg \mathcal{F} > 2g-2$.

5.3.1. *Large degree case.* Assume that $\deg \mathcal{F} \geq 2g+1$. By the Riemann–Roch theorem, $\mathcal{F}$ is very ample and hence $\varphi$ is an embedding giving an isomorphism between $X_G$ and $C$. The homomomorphism

$$\mathbb{Q}[x_0, \ldots, x_d]/I(C) \to \bigoplus_{n \geq 0} H^0(X_G, \mathcal{F}^{\otimes n})$$

of graded $\mathbb{Q}$-algebras given by $x_i \mapsto \psi_k(f_i)$ is an isomorphism (the surjectivity follows from [Mum70, Theorem 6] and our assumption $\deg \mathcal{F} \geq 2g+1$). The ideal $I(C) \subseteq \mathbb{Q}[x_0, \ldots, x_d]$ is generated by $I(C)_2$ and $I(C)_3$, cf. [SD72]. If $\deg \mathcal{F} \geq 2g+2$, then the homogenous ideal $I(C)$ is generated by just $I(C)_2$, cf. [SD72].

Consider the special case where $\deg \mathcal{F} = 2g+1$. When $g = 0$, we have $C = \mathbb{P}^1_{\mathbb{Q}}$. When $g = 1$, the curve $C \subseteq \mathbb{P}^2_{\mathbb{Q}}$ is a plane cubic.

*Remark* 5.3. Suppose $\deg \mathcal{F} \geq 2g+2$. Consider a fixed positive integer $b$. Suppose we have computed the $q$-expansions $f_j|_k A_i + O(q_N^b)$ for all $0 \leq j \leq d$ and $1 \leq i \leq r$. From these expansions, we can find a basis of the $\mathbb{Q}$-vector space $W := \{F \in \mathbb{Q}[x_0, \ldots, x_d]_2 : F(f_0, \ldots, f_d) + O(q_N^b) = 0 + O(q_N^b)\}$. Let $C'$ be the subvariety of $\mathbb{P}^d_{\mathbb{Q}}$ defined by a basis of $W$. We have $C' \subseteq C$ since $I(C)_2 \subseteq W$ and $I(C)$ is generated by $I(C)_2$. So if $C'$ is not zero dimensional, we have $C' = C$ and $I(C)_2 = W$. Of course, we will have $I(C)_2 = W$ by taking $b$ sufficient large. The benefit of this approach is that we can often use a $b$ that is significantly smaller that the one arising from applying the Sturm bound.

5.3.2. *Canonical map.* Consider the special case where $g \geq 3$, $k = 2$, and $E = \sum_{i=1}^{r} P_i$. We have

$$\mathcal{F} := \mathscr{L}_2(-E) = \Omega_{X_G}(D_2 - E) = \Omega_{X_G}.$$

So $d = g-1$ and $\varphi \colon X_G \to \mathbb{P}^{g-1}_{\mathbb{Q}}$ is the canonical map. Define $C := \varphi(X_G) \subseteq \mathbb{P}^{g-1}_{\mathbb{Q}}$. We now recall some basic details, see [Zyw20a, §7] for further details and some computation details.

First suppose that $X_G$ is (geometrically) hyperelliptic. Then the curve $C$ has genus 0 and the morphism $\varphi \colon X_G \to C$ has degree 2. The ideal $I(C)$ is generated by $I_2(C)$ and $\dim_{\mathbb{Q}} I_2(C) = (g-1)(g-2)/2$.

Suppose that $X_G$ is not hyperelliptic. Then $\varphi$ is an embedding and in particular $C$ is isomorphic to $X_G$. The dimension of $I_2(C)$ and $I_3(C)$ over $\mathbb{Q}$ are $(g-2)(g-3)/2$ and $(g-3)(g^2+6g-10)/6$, respectively. If $g \geq 4$, the ideal $I(C)$ is generated by $I_2(C)$ and $I_3(C)$. If $g = 3$, then $I(C)$ is generated by $I_4(C)$ and $\dim_{\mathbb{Q}} I_4(C) = 1$.

We can compute $I_2(C)$ and its dimension over $\mathbb{Q}$ determines whether or not $X_G$ is hyperelliptic. Assume $X_G$ is not hyperelliptic. Then by computing $I_3(C)$, and $I_4(C)$ when $g = 3$, we can find equations for the curve $C \subseteq \mathbb{P}^1_{\mathbb{Q}}$.

5.3.3. *Computing a model for $X_G$.* If $g \geq 3$, we can first compute the image of the canonical map $\varphi \colon X_G \to \mathbb{P}^{g-1}_{\mathbb{Q}}$ and find equations defining the image $C := \varphi(X_G)$, cf. §5.3.2. If $C$ does not have genus 0, i.e., $C$ is not hyperelliptic, then $C$ is a model of $X_G$. If $C$ has genus 0 and $C(\mathbb{Q}) = \emptyset$, then $X_G(\mathbb{Q}) = \emptyset$ (which in our application means we do not need to compute a model of $X_G$).

Now consider the general case. Choose the smallest even integer $k \geq 2$ such that

$$k/2 \cdot (2g-2) + k/2 \cdot r + \lfloor k/4 \rfloor \cdot v_2 + \lfloor k/3 \rfloor \cdot v_3 \geq 2g+1.$$

Such an integer $k$ exists since $g - 1 + v_2/4 + v_3/3 + r/2 = [\mathrm{SL}_2(\mathbb{Z}) : \pm\Gamma_G]/12$ by [Shi94, Proposition 1.40]. Choose an effective divisor $E := \sum_{i=1}^{r} e_i P_i$ of $X_G$ defined over $\mathbb{Q}$ so that the right hand side of (5.1) is at least $2g+1$ and is as small as possible. By our choices, we have $\deg \mathcal{F} \geq 2g+1$. One can then compute a model as in §5.3.1.

5.3.4. *Cusps of our model.* With $f_0, \ldots, f_d \in M_{k,G}$ defining the morphism $\varphi\colon X_G \to C \subseteq \mathbb{P}^d_{\mathbb{Q}}$, we now describe the image of the cusps of $X_G$.

Take any $1 \leq j \leq r$. From Lemma 5.2, we know that $\varphi(P_j)$ will lie in $C(\mathbb{Q}(\zeta_N))$. There is an $0 \leq m \leq d$ such that for all $0 \leq i \leq d$, the $q$-expansion of $f_i/f_m$ at the cusp $P_j$ is a power series for all $0 \leq i \leq m$; denote its constant term by $c_i \in \mathbb{Q}(\zeta_N)$. Note that $f_i/f_m \in \mathbb{Q}(X_G)$ is regular at $P_j$ and $(f_i/f_m)(P_j) = c_i$. So we have $\varphi(P_i) = [c_0, \ldots, c_d] \in \mathbb{P}^d(\mathbb{Q}(\zeta_N))$.

5.4. **Curves of genus 0 and 1.** Assume that $X_G$ has genus at most 1. Such curves are important in our application since they potentially could have infinitely many rational points.

Assume that we have found an explicit smooth projective model $C \subseteq \mathbb{P}^n_{\mathbb{Q}}$ for the modular curve $X_G$ as in §5.3. In particular, we have modular forms $f_0, \ldots, f_d$ in $M_{k,G}$ for some even $k \geq 2$ such that $C$ is defined by the homogeneous polynomials $F \in \mathbb{Q}[x_0, \ldots, x_d]$ for which $F(f_0, \ldots, f_d) = 0$.

5.4.1. *Finding a simple model.* Suppose we have found a rational point $P \in C(\mathbb{Q})$. See §5.4.4 for details on how we check if there is a rational point.

If $X_G$ has genus 0, then using the point $P$, we can compute an isomorphism $\psi\colon C \xrightarrow{\sim} \mathbb{P}^1_{\mathbb{Q}}$. Using the modular forms $f_i$ and $\psi$, we can then compute a modular function $f$ for which $\mathbb{Q}(X_G) = \mathbb{Q}(f)$. Note that $f$ is given by its $q$-expansions at the cusps of $X_G$ and we can compute arbitrarily many terms of each expansion.

If $X_G$ has genus 1, then using the point $P$, we can compute an isomorphism $\psi\colon C \xrightarrow{\sim} E$, where $E$ is an elliptic curve over $\mathbb{Q}$ and $\psi(P) = 0$. Using the modular forms $f_i$ and $\psi$, we can compute modular functions $x$ and $y$ for which $\mathbb{Q}(X_G) = \mathbb{Q}(x, y)$ and for which $x$ and $y$ satisfy a Weierstrass equation with rational coefficients defining $E$. Note that $x$ and $y$ are given by their $q$-expansions at the cusps of $X_G$ and we can compute arbitrarily many terms of each expansion.

5.4.2. *Recognizing elements of the function field.* Assume we have found a model for $X_G$ as in §5.4.1. In particular, $\mathbb{Q}(X_G)$ is $\mathbb{Q}(f)$ or $\mathbb{Q}(x, y)$ if $X_G$ has genus 0 or 1, respectively.

Now suppose we have a function $h \in \mathbb{Q}(X_G)$ given by a $q$-expansion at each cusp of $X_G$ for which we can compute arbitrarily many terms. Also suppose we also have an upper bound on the number of poles, with multiplicity, of $h$. When $h$ is a quotient of two elements of $M_{k',G}$ for some even $k'$, then the number of poles of $h$ is bounded above by $k'/12 \cdot [\mathrm{SL}_2(\mathbb{Z}) : \pm\Gamma_G] = k'/12 \cdot [\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : G]$ (the divisor of a nonzero modular form in $M_{k',G}$, cf. [Shi94, §2.4], is effective and its degree can be computed using Propositions 2.16 and 1.40 of [Shi94]).

We want to express $h$ in terms of the generators of the field $\mathbb{Q}(f)$ or $\mathbb{Q}(x, y)$.

One approach is just to brute force search for an expression. Consider the genus 0 case. For a fixed integer $d \geq 0$, one can look for a relation $h = F_1(f)/F_2(f)$ where $F_1$ and $F_2$ are polynomials in $\mathbb{Q}[t]$ of degree at most $d$. For each cusp of $X_G$, substituting our $q$-expansions in the expression $F_2(f)h - F_1(f) = 0$, we obtain a homogeneous system of linear equations over $\mathbb{Q}(\zeta_N)$ whose unknowns are the coefficients of the polynomials $F_1$ and $F_2$. For the minimal $d$ for which such a relation exists, these linear equations will have a 1-dimension space of solutions over $\mathbb{Q}(\zeta_N)$ and scaling will produce a solution in rationals unique up to scaling by a nonzero rational. To rigorously verify that $F_2(f)h = F_1(f)$, with specific coefficients, is 0 it suffices to compute enough terms of the $q$-expansions at the cusps so that we have more zeros at the cusps, with multiplicity, than poles (we assumed we had a bound on the poles of $h$ and $f$ has a single simple pole). We can increase $d \geq 0$ until we find a relation.

In the special case where there is a degree 1 rational function $b \in \mathbb{Q}(\zeta_N)(t)$ such that $b(h) \in \mathbb{Q}(\zeta_N)(X_G)$ has all its poles at the cusps, we can take a more direct approach. Since we know the $q$-expansions of $f$ at the cusps, we can find a partial fractions decomposition of $b(h)$ in $\mathbb{Q}(\zeta_N)(f)$ and then find the desired expression for $h$ since $b$ has degree 1.

Similar remarks hold when $X_G$ has genus 1 except now we are looking for a relation $h = (F_1(x) + F_2(x)y)/F_3(x)$, where $F_1, F_3 \in \mathbb{Q}[t]$ have degree at most $d$ and $F_2 \in \mathbb{Q}[t]$ has degree at most $d-1$.

5.4.3. *Constructing the map to the $j$-line.* We want to describe the natural morphism $\pi_G$ from $X_G$ to the $j$-line. Since we are interested in rational points, we shall assume that $X_G$ has a rational point and that we have found a model for $X_G$ as in §5.4.1. In particular, $\mathbb{Q}(X_G)$ is $\mathbb{Q}(f)$ or $\mathbb{Q}(x,y)$ when $X_G$ has genus 0 or 1, respectively.

For simplicity, suppose that $X_G$ has genus 0 and hence $\mathbb{Q}(X_G) = \mathbb{Q}(f)$. Since the modular $j$-invariant $j$ lies in $\mathbb{Q}(X_G)$, the morphism $\pi_G$ is given by the unique $\pi(t) \in \mathbb{Q}(t)$ for which $\pi(f) = j$. We can find $\pi(t)$ using the methods from §5.4.2 and use that $\pi(t)$ has degree $[\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : G]$.

In practice, it is more efficient to make use of intermediate fields lying between $\mathbb{Q}(j)$ and $\mathbb{Q}(f)$. We can assume that $G \neq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ since otherwise $X_G$ is the $j$-line. Choose a group $G \subsetneq G_0 \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ for which $[G_0 : G]$ is minimal. Then $\mathbb{Q}(X_{G_0}) = \mathbb{Q}(f')$ and hence $f' = \varphi(f)$ for a unique rational function $\varphi(t) \in \mathbb{Q}(t)$ of degree $[G_0 : G]$. We can then find $\varphi$ using the methods from §5.4.2. This reduces the computation to the curve $X_{G_0}$ and we can continue in this manner until we get to the $j$-line. The advantage in working with intermediate subfields is that in the method of §5.4.2 we require less terms of the $q$-expansions.

Similar remarks hold when $X_G$ has genus 1 except now $X_{G_0}$ will have genus 0 or 1.

5.4.4. *Determining whether there is a rational point.* We are interested in determining whether $X_G$, equivalently $C$, has a rational point. We first check whether $X_G$ has a local obstruction to rational points.

For real points this can be done without the model since we know that $X_G(\mathbb{R}) \neq \emptyset$ if and only if $G$ contains an element that is conjugate in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ to $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right)$, cf. [Zyw15a, Proposition 3.5].

Using our explicit model, we can verify whether $C(\mathbb{Q}_p)$ is empty for any given prime $p$. If $X_G(\mathbb{R}) = \emptyset$ or $C(\mathbb{Q}_p) = \emptyset$ for some prime $p$, then we of course have $X_G(\mathbb{Q}) = \emptyset$.

When $X_G$ has genus 0 and $X_G(\mathbb{R})$ is nonempty, we know that we will either be able to find a rational point on $C$ or we will be able to find a prime $p$ such that $C(\mathbb{Q}_p) = \emptyset$.

*Remark* 5.4. There is a more general definition of $X_G$ as a coarse moduli space that would realize it as a smooth scheme over $\mathbb{Z}[1/N]$. For a prime $p \nmid N$, the reduction $(X_G)_{\mathbb{F}_p}$ would then be a smooth projective and geometrically irreducible curve of genus at most 1 over $\mathbb{F}_p$ and hence have an $\mathbb{F}_p$-point. Hensel's lemma would then implies that $X_G(\mathbb{Q}_p) \neq \emptyset$. So when looking for local obstructions, we limit ourselves to primes $p$ dividing $N$.

Now suppose that $X_G$ is genus 1 for which we have not found a rational point and we have found no local obstructions. The Jacobian of $C$ is an elliptic curve $E$ over $\mathbb{Q}$. Using our embedding $C \subseteq \mathbb{P}^d_{\mathbb{Q}}$, we find that $C$ is a principal homogeneous space of $E$ that has order $n := d+1$ in the Weil–Châtelet group of $E$.

When $n \leq 5$, there are explicit equations for $E$ and for a covering map $\varphi\colon C \to E$ of degree $n^2$ (when base extended to a field where $C$ and $E$ are isomorphic, it corresponds to multiplication by $n$ on $E$). When $n \leq 4$ or $n = 5$, see [AKM+01] and [Fis08], respectively. Note that these constructions have been implemented in `Magma`. If $C$ has a rational point, then we find that $\varphi(C(\mathbb{Q}))$ is a coset of $nE(\mathbb{Q})$ in $E(\mathbb{Q})$. We can compute the weak Mordell–Weil group $E(\mathbb{Q})/nE(\mathbb{Q})$. For points $P \in E(\mathbb{Q})$ that represent the elements of the finite group $E(\mathbb{Q})/nE(\mathbb{Q})$, we can check

whether the fiber $\varphi^{-1}(P) \subseteq C$ has any rational points. If not, then we have verified that $C(\mathbb{Q})$ is empty (otherwise, we have found a point).

In our application, the above determines whether $X_G$ has a rational point for all but a few cases we consider. In the cases where this does not apply (i.e., $n > 5$), there was always a group $G \subseteq G_0 \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ for which $[G_0 : G] = 2$ and $X_{G_0} \cong \mathbb{P}^1_{\mathbb{Q}}$. In these cases, we could find an alternate model $C'$ of $X_G$ given as a hyperelliptic curve over $\mathbb{Q}$. The above reasoning then applies to check whether there are rational points; the relevant morphism $\varphi\colon C' \to E$ now has degree $2^2$.

5.5. **Some alternate models for curves.** Assume that $X_G$ has genus at least 2 and choose a group $G \subsetneq G_0 \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ for which $X_{G_0}$ has genus at most 1. In practice, one chooses $G_0$ with $[G_0 : G]$ minimal. We shall assume that $X_{G_0}$ has a rational point; we are interested in knowing the rational points of $X_G$ and there are none if $X_{G_0}(\mathbb{Q}) = \emptyset$. Assume we have found a model as in §5.4.1 with $\mathbb{Q}(X_{G_0})$ of the form $\mathbb{Q}(f)$ or $\mathbb{Q}(x, y)$.

5.5.1. *Minimal polynomial.* Let $S$ be a set of matrices in $\mathrm{SL}_2(\mathbb{Z})$ whose reductions modulo $N$ represent the cosets $G\backslash G_0$.

Consider a modular function $h \in \mathbb{Q}(X_G)$ for which we have compute arbitrarily many terms of the $q$-expansion at each the cusps of $X_G$. Using these expansions and §4.9, we can compute the $q$-expansions of $h|_k A$ for all $A \in S$. Assume that $h|_k A \neq h$ for all $A \in S$ and hence $\mathbb{Q}(X_{G_0})(h) = \mathbb{Q}(X_G)$. To construct a suitable element $h \in \mathbb{Q}(X_G)$, we can look at the quotient of nonzero elements in $M_{k,G}$ for even $k \geq 2$; there will be such modular forms for $k$ large enough by §5.3.3.

Define the polynomial

$$P(t) := \prod_{A \in S} (t - h|_k A).$$

By our choice of $S$, $P(t)$ is a polynomial of degree $[G_0 : G]$ with coefficients in $\mathbb{Q}(X_{G_0})$ that satisfies $P(h) = 0$. The coefficients of $P(t)$ line in $\mathbb{Q}(X_{G_0})$ and can be given explicitly in $\mathbb{Q}(f)$ or $\mathbb{Q}(x, y)$ by the method described in §5.4.2 (the methods of §4.9 can be used to take the $q$-expansions, which are in terms of the cusps of $X_G$, to those at cusps of $X_{G_0}$).

Since $\mathbb{Q}(X_{G_0})(h) = \mathbb{Q}(X_G)$, the polynomial $P(t)$ gives rise to a possibly singular model of the curve $X_G$ in $\mathbb{P}^2_{\mathbb{Q}}$ or $\mathbb{P}^3_{\mathbb{Q}}$ with a rational map to $X_{G_0}$ corresponding to the natural morphism $X_G \to X_{G_0}$. In many situations, a singular model of $X_G$ will be preferably to a model that lies in some large dimensional ambient space. An important special case is when $[G_0 : G] = 2$ and $X_{G_0} \cong \mathbb{P}^1_{\mathbb{Q}}$ since then we can use the singular model to find a smooth model of $X_G$ as a hyperelliptic curve.

5.5.2. *Serre type.* Now suppose that $N = N_1 N_2$ with $N_1 > 1$ a power of 2 and $N_2$ odd. Set $G_1 = \mathrm{GL}_2(\mathbb{Z}/N_1\mathbb{Z})$. Suppose further that there is a subgroup $G_2$ of $\mathrm{GL}_2(\mathbb{Z}/N_2\mathbb{Z})$ such that $G$ is an index 2 subgroup of $G_0 := G_1 \times G_2 \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ so that the projective map $G \to G_i$ is surjective for $i \in \{1, 2\}$.

The kernel of the projection maps $G \to G_1$ and $G \to G_2$ are of the form $\{I\} \times H_2$ and $H_1 \times \{I\}$, where $H_i$ is an index 2 subgroup of $G_i$. Note that $H_1 \times H_2 \subseteq G \subseteq G_1 \times G_2$.

Take any $i \in \{1, 2\}$ and suppose that $\det(H_i) = (\mathbb{Z}/N_i\mathbb{Z})^\times$. As in §5.5.1, we can find a $h \in \mathbb{Q}(X_{H_i})$ such that $\mathbb{Q}(X_{H_i}) = \mathbb{Q}(X_{G_0})(h)$ and compute an irreducible polynomial of degree 2 in $\mathbb{Q}(X_{G_0})[x]$ with root $h$. By taking the discriminant of the polynomial, we obtain an element $c_i \in \mathbb{Q}(X_{G_0})$ that is a square in $\mathbb{Q}(X_{H_i})$ but not in $\mathbb{Q}(X_{G_0})$. Note that $c_i$ is unique up to multiplication by a nonzero square in $\mathbb{Q}(X_{G_0})$.

Take any $i \in \{1, 2\}$ and suppose that $\det(H_i) \neq (\mathbb{Z}/N_i\mathbb{Z})^\times$. The group $\det(H_i)$ is an index 2 subgroup of $(\mathbb{Z}/N_i\mathbb{Z})^\times$. Let $K_i \subseteq \overline{\mathbb{Q}}$ be the corresponding quadratic extension of $\mathbb{Q}$, i.e., the

quadratic extension for which the image of $\chi_{\mathrm{cyc}}(\mathrm{Gal}_{K_i}) \subseteq \widehat{\mathbb{Z}}^\times$ modulo $N_i$ is the group $\det(H_i)$. Let $c_i$ be the unique squarefree integer for which $K_i = \mathbb{Q}(\sqrt{c_i})$.

When $i = 1$, a computation shows that $c_i$ can always be chosen to lie in the set $\{-1, \pm 2, \pm(j - 1728), \pm 2(j - 1728)\}$.

Putting everything together, we find that there is a $y \in \mathbb{Q}(X_G)$ such that $y^2 = c_1c_2$ and $\mathbb{Q}(X_G) = \mathbb{Q}(X_{G_0})(y)$. Therefore, $y^2 = c_1c_2$ defines a singular model of $X_G$. In the special case where $X_{G_0} \cong \mathbb{P}^1_{\mathbb{Q}}$, this gives rise to a hyperelliptic model.

*Remark* 5.5. Though this might seem like a very niche case, groups with the above conditions arise frequently in our application to Serre's open image theorem and are often the slowest to deal with using the strategy from §5.5.1.

## 6. A generic family and modular functions

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

$$y^2 = x^3 - 27 \cdot j(j - 1728) \cdot x + 54 \cdot j(j - 1728)^2, \tag{6.1}$$

where $j$ is the modular $j$-invariant. The elliptic curve $\mathcal{E}$ has $j$-invariant $j$.

Fix an integer $N \geq 3$ and a nonzero modular form $f_0 \in M_3(\Gamma(N), \mathbb{Q}(\zeta_N))$. Let $\mathcal{F}_N$ be the field of modular functions of level $N$ whose $q$-expansions have coefficients in $\mathbb{Q}(\zeta_N)$, cf. §3.1. We have $f_0^2/E_6 \in \mathcal{F}_N$, where $E_6$ is the usual Eisenstein series of weight 6 as given by (6.2). In a field extension of $\mathcal{F}_N$, choose a $\beta$ satisfying

$$\beta^2 = j \cdot f_0^2/E_6.$$

Note that $\beta$ need not be a modular function.

In §6.1, we will show that $\mathcal{F}_N(\beta)$ is a minimal field extension of $\mathbb{Q}(j)$ for which all of the $N$-torsion points of $\mathcal{E}$ are defined. Let $\mathrm{Gal}_{\mathbb{Q}(j)}$ be the absolute Galois group of $\mathbb{Q}(j)$ for which the implicit algebraic closure contains $\mathcal{F}_N(\beta)$. With respect to a suitable basis of $\mathcal{E}[N]$, we will show that there is a surjective Galois representation

$$\rho^*_{\mathcal{E},N} \colon \mathrm{Gal}_{\mathbb{Q}(j)} \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

that satisfies

$$\sigma(f) = f * \rho^*_{\mathcal{E},N}(\sigma)^{-1}$$

for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}(j)}$ and $f \in \mathcal{F}_N$, where the $*$ action is described in §3.1. For details, see §6.2. In particular, $\rho^*_{\mathcal{E},N}$ induces isomorphisms $\mathrm{Gal}(\mathcal{F}_N(\beta)/\mathbb{Q}(j)) \xrightarrow{\sim} \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and $\mathrm{Gal}(\mathcal{F}_N/\mathbb{Q}(j)) \xrightarrow{\sim} \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$.

### 6.1. $N$-torsion points of $\mathcal{E}$.

Define the usual Eisenstein series

$$E_4(\tau) = 1 + 240\sum_{n=1}^{\infty} n^3q^n/(1 - q^n) \quad \text{and} \quad E_6(\tau) = 1 - 504\sum_{n=1}^{\infty} n^5q^n/(1 - q^n); \tag{6.2}$$

they are modular forms on $\mathrm{SL}_2(\mathbb{Z})$ of weight 4 and 6, respectively. Define the weight 12 modular form $\Delta(\tau) = q\prod_{n=1}^{\infty}(1 - q^n)^{24}$ on $\mathrm{SL}_2(\mathbb{Z})$. We have relations $E_4^3 - E_6^2 = 1728\Delta$, $j = E_4^3/\Delta$ and $j - 1728 = E_6^2/\Delta$. For $\tau \in \mathcal{H}$, let $\wp(z;\tau)$ be the Weierstrass elliptic function for the lattice $\mathbb{Z}\tau + \mathbb{Z} \subseteq \mathbb{C}$. Let $\wp'(z;\tau)$ be the derivative of $\wp(z;\tau)$ with respect to $z$.

Take any nonzero $\alpha \in (\mathbb{Z}/N\mathbb{Z})^2$ and choose integers $r$ and $s$ such that $\alpha$ is congruent to $(r, s)$ modulo $N$. Let $x_\alpha$ and $u_\alpha$ be the function of the upper-half plane defined by

$$x_\alpha(\tau) := 36\,\frac{E_4(\tau)E_6(\tau)}{\Delta(\tau)} \cdot (2\pi i)^{-2}\wp(\tfrac{r}{N}\tau + \tfrac{s}{N}; \tau)$$
$$u_\alpha(\tau) := 108\,\frac{E_6(\tau)^2}{f_0(\tau)\Delta(\tau)} \cdot (2\pi i)^{-3}\wp'(\tfrac{r}{N} \cdot \tau + \tfrac{s}{N}; \tau).$$

These definitions do not depend on the choice of $r$ and $s$ since $\wp(z;\tau)$ and $\wp'(z;\tau)$ are unchanged if we replace $z$ by $z + \omega$ with $\omega \in \mathbb{Z}\tau + \mathbb{Z}$.

**Lemma 6.1.**

(i) *For any nonzero $\alpha \in (\mathbb{Z}/N\mathbb{Z})^2$, $x_\alpha$ and $u_\alpha$ are elements of $\mathcal{F}_N$.*
(ii) *The field $\mathcal{F}_N$ is the extension of $\mathbb{Q}(j)$ generated by $x_\alpha$ with nonzero $\alpha \in (\mathbb{Z}/N\mathbb{Z})^2$.*
(iii) *Take any nonzero $\alpha \in (\mathbb{Z}/N\mathbb{Z})^2$ and $A \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. We have*

$$x_\alpha * A = x_{\alpha A} \quad \text{and} \quad u_\alpha * A = \tfrac{f_0}{f_0 * A}\, u_{\alpha A}.$$

*In particular, $u_\alpha * A = u_{\alpha A}$ if $f_0 * A = f_0$.*

*Proof.* Take any nonzero $\alpha \in (\mathbb{Z}/N\mathbb{Z})^2$. Fix integers $0 \le r < N$ and $s$ so that $(r, s)$ is congruent to $\alpha$ modulo $N$. Our function $x_\alpha$ agrees with the function $f_{(r/N,s/N)}$ from §6.1 of [Shi94] up to multiplication by a nonzero rational number. Part (ii) follows from Proposition 6.9(1) of [Shi94]; this implies (i) for the function $x_\alpha$.

Let $h_\alpha$ be the function of the upper-half plane defined by $(2\pi i)^{-3}\wp'(\frac{r}{N} \cdot \tau + \frac{s}{N}; \tau)$. We now explain why $h_\alpha$ lies in $M_3(\Gamma(N), \mathbb{Q}(\zeta_N))$. Recall that for $\tau \in \mathcal{H}$, we have the notation $q = e^{2\pi i\tau}$ and $q_N = e^{2\pi i\tau/N}$. We have

$$(2\pi i)^{-2}\wp(u;\tau) = \frac{1}{12} - 2\sum_{m=1}^{\infty}\sum_{n=1}^{\infty} nq^{mn} + \sum_{n=1}^{\infty} ne^{2\pi inu} + \sum_{m=1}^{\infty}\sum_{n=1}^{\infty} n\Big(e^{2\pi inu}q^{mn} + e^{-2\pi inu}q^{mn}\Big);$$

see the proof of Proposition 6.9 on p. 140 in [Shi94] (with $\omega_1 = \tau$, $\omega_2 = 1$, and $v$ in loc. cit. should be defined as $u/\omega_2$). Therefore,

$$(2\pi i)^{-3}\wp'(u;\tau) = \sum_{n=1}^{\infty} n^2e^{2\pi inu} + \sum_{m=1}^{\infty}\sum_{n=1}^{\infty} n^2\Big(e^{2\pi inu}q^{mn} - e^{-2\pi inu}q^{mn}\Big).$$

With $u = r/N \cdot \tau + s/N$, we have $e^{2\pi iu} = \zeta_N^s q_N^r$ and hence

$$h_\alpha(\tau) = \sum_{n=1}^{\infty} n^2\zeta_N^{sn}q_N^{rn} + \sum_{m=1}^{\infty}\sum_{n=1}^{\infty} n^2\Big(\zeta_N^{sn}q_N^{rn}q^{mn} - \zeta_N^{-sn}q_N^{-rn}q^{mn}\Big). \tag{6.3}$$

Since $0 \le r < N$, this shows that $h_\alpha$ has a $q$-expansion that is a power series in $q_N$ with coefficients in $\mathbb{Q}(\zeta_N)$.

Take any matrix $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Since $\wp'(u;\tau) = \sum_{\lambda\in\mathbb{Z}\tau+\mathbb{Z}} -2/(u+\lambda)^3$, we have

$$\begin{aligned}(h_\alpha|_3\gamma)(\tau) &= (c\tau + d)^{-3} \cdot (2\pi i)^{-3} \sum_{\lambda\in\mathbb{Z}\gamma\tau+\mathbb{Z}} \frac{-2}{(\frac{r}{N} \cdot \gamma\tau + \frac{s}{N} + \lambda)^3} \\ &= (2\pi i)^{-3} \sum_{\lambda\in\mathbb{Z}(a\tau+b)+\mathbb{Z}(c\tau+d)} \frac{-2}{(\frac{r}{N} \cdot (a\tau + b) + \frac{s}{N}(c\tau + d) + \lambda)^3} \\ &= (2\pi i)^{-3} \sum_{\lambda\in\mathbb{Z}\tau+\mathbb{Z}} \frac{-2}{(\frac{ra+sc}{N} + \frac{rb+sd}{N} + \lambda)^3}.\end{aligned}$$

So $h_\alpha|_3\gamma = h_{\alpha\gamma}$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. In particular, $h_\alpha|_3\gamma = h_\alpha$ for all $\gamma \in \Gamma(N)$. We conclude that $h_\alpha$ is an element of $M_3(\Gamma(N), \mathbb{Q}(\zeta_N))$ since the $q$-expansions of $h_\alpha|_3\gamma = h_{\alpha\gamma}$ is a power series in $q_N$ with coefficients in $\mathbb{Q}(\zeta_N)$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

For any $A \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, we claim that $h_\alpha * A = h_{\alpha A}$. From our above proof, this holds when $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, so we need only prove the claim in the case where $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$. Applying $\sigma_d$ to the coefficients of the expansion (6.3) gives the expansion where we replace $s$ by $ds$. Therefore, $h_\alpha * A = h_{\alpha A}$ as expected.

That $u_\alpha$ lies in $\mathcal{F}_N$ is clear since it is the quotient of modular forms on $\Gamma(N)$ with coefficients in $\mathbb{Q}(\zeta_N)$ and it has weight $2 \cdot 6 - 3 - 12 + 3 = 0$. Take any $A \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Since $E_4$ and $E_6$ are modular forms on $\mathrm{SL}_2(\mathbb{Z})$ with coefficients in $\mathbb{Q}$, we find that

$$u_\alpha * A = 108\,\frac{E_6^2}{f_0 * A \cdot \Delta} \cdot h_\alpha * A = \frac{f_0}{f_0 * A} \cdot 108\,\frac{E_6^2}{f_0\Delta} \cdot h_{\alpha A} = \frac{f_0}{f_0 * A} \cdot u_{\alpha A}.$$

We have proved the parts of the lemma concerning the functions $u_\alpha$.

Now take any nonzero $\alpha \in (\mathbb{Z}/N\mathbb{Z})^2$. It remains to prove that $x_\alpha * A = x_{\alpha A}$ for all $A \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. For $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, this follows from equation (6.1.3) of [Shi94]. It remains to prove it for $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$; this follows from the $q$-expansion of $x_\alpha$, see equation (6.2.1) of [Shi94]. □

Recall that we fixed a nonzero modular form $f_0$ in $M_3(\Gamma(N), \mathbb{Q}(\zeta_N))$ and chose a $\beta$ satisfying $\beta^2 = j \cdot f_0^2/E_6 \in \mathcal{F}_N$. For each nonzero $\alpha \in (\mathbb{Z}/N\mathbb{Z})^2$, define $y_\alpha := \beta \cdot u_\alpha \in \mathcal{F}_N(\beta)$ and the pair $P_\alpha := (x_\alpha, y_\alpha)$.

**Lemma 6.2.**

(i) *For every nonzero $\alpha \in (\mathbb{Z}/N\mathbb{Z})^2$, $P_\alpha$ is a $N$-torsion point in $\mathcal{E}(\mathcal{F}_N(\beta))$.*

(ii) *We have a group isomorphism*

$$\iota_N \colon (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} \mathcal{E}[N], \quad \alpha \mapsto P_\alpha,$$

*where $P_{(0,0)}$ is defined as the identity of $\mathcal{E}$.*

*Proof.* Fix any $\tau \in \mathcal{H}$ satisfying $j(\tau) \notin \{0, 1728\}$ and $f_0(\tau) \neq 0$. Let $\mathscr{E}_\tau$ be the elliptic curve over $\mathbb{C}$ defined by the Weierstrass equation $y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$, where $g_2$ and $g_3$ are modular invariants. Note that $g_2/(2\pi i)^4 = E_4/12$ and $g_3/(2\pi i)^6 = -E_6/216$. Let $\mathscr{E}'_\tau$ be the elliptic curve over $\mathbb{C}$ defined by the equation

$$j(\tau)f_0(\tau)^2/E_6(\tau) \cdot y^2 = x^3 - 27 \cdot j(\tau)(j(\tau) - 1728) \cdot x + 54 \cdot j(\tau)(j(\tau) - 1728)^2. \tag{6.4}$$

Define $c := 36(2\pi i)^{-2}E_4(\tau)E_6(\tau)/\Delta(\tau)$ and $d := 108(2\pi i)^{-3}E_6(\tau)/(\Delta(\tau)f_0(\tau))$. By using $j = E_4^3/\Delta$ and $j - 1728 = E_6^2/\Delta$, and dividing (6.4) by $c^3/4$, we find that

$$\begin{aligned} \frac{4}{c^3} \cdot \frac{j(\tau)f_0(\tau)^2}{E_6(\tau)} \cdot y^2 &= 4(x/c)^3 - 27\frac{4E_4(\tau)^3E_6(\tau)^2}{c^2\Delta(\tau)^2}(x/c) + 54\frac{4E_4(\tau)^3E_6(\tau)^4}{c^3\Delta(\tau)^3} \\ &= 4(x/c)^3 - (2\pi i)^4E_4(\tau)/12 \cdot (x/c) + (2\pi i)^6E_6(\tau)/216 \\ &= 4(x/c)^3 - g_2(\tau) \cdot (x/c) - g_3(\tau). \end{aligned}$$

Observing that

$$\frac{4}{c^3} \cdot \frac{j(\tau)f_0(\tau)^2}{E_6(\tau)} = \frac{4}{c^3} \cdot \frac{E_4(\tau)^3f_0(\tau)^2}{\Delta(\tau)E_6(\tau)} = \left(\frac{(2\pi i)^3\Delta(\tau)f_0(\tau)}{108E_6(\tau)}\right)^2 = \frac{1}{d}^2,$$

we deduce that the map $(x, y) \mapsto (x/c, y/d)$ defines an isomorphism $\mathscr{E}'_\tau \to \mathscr{E}_\tau$ of elliptic curves over $\mathbb{C}$. Using this isomorphism and properties of the Weierstrass function, we obtain an isomorphism $\mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z}) \xrightarrow{\sim} \mathscr{E}'_\tau(\mathbb{C})$ of complex Lie groups which maps a nonidentity element $z + (\mathbb{Z}\tau + \mathbb{Z})$ to

$(c\wp(z;\tau), d\wp'(z;\tau))$. In particular, we have a group isomorphism $\mathbb{Z}^2/N\mathbb{Z}^2 \xrightarrow{\sim} \mathscr{E}'_\tau[N]$ which away from the identity is defined by

$$(r,s) + N^2\mathbb{Z} \mapsto \left(c\wp(\tfrac{r}{N}\tau + \tfrac{s}{N};\tau), d\wp'(\tfrac{r}{N}\tau + \tfrac{s}{N};\tau)\right) = (x_\alpha(\tau), u_\alpha(t)), \tag{6.5}$$

where $\alpha$ is the image of $(r,s)$ modulo $N$.

We now view $\tau$ as a variable again. Letting $\mathscr{E}'$ be the elliptic curve defined by (6.4), say over the field of meromorphic functions of $\mathcal{H}$, we find that (6.5) also defines an isomorphism $\mathbb{Z}^2/N\mathbb{Z}^2 \to \mathscr{E}'[N]$ (the points are torsion and satisfy the expected property since they hold for all but finitely many specializations of $\tau$).

Now by our choice of $\beta$, we deduce that the points $P_\alpha = (x_\alpha, y_\alpha)$ lie in $\mathcal{E}(\mathcal{F}_N(\beta))$ and that $(\mathbb{Z}/N\mathbb{Z})^2 \to \mathcal{E}[N]$, $\alpha \mapsto P_\alpha$ is an isomorphism. Note that $\beta$ is not a function of the upper-half plane, so we avoided using it when we fixed specific values of $\tau$. □

6.2. **Galois representations of $\mathcal{E}$.** Fix an integer $N \geq 3$. Fix notation as in §6.1; in particular, we have a basis $P_{(1,0)}$ and $P_{(0,1)}$ of the $\mathbb{Z}/N\mathbb{Z}$-module $\mathcal{E}[N] \subseteq \mathcal{E}(\mathcal{F}_N(\beta))$. With respect to the basis $\{P_{(1,0)}, P_{(0,1)}\}$, let

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

be the associated Galois representation, where the implicit algebraic closure of $\mathbb{Q}(j)$ used for the absolute Galois group contains $\mathcal{F}_N(\beta)$. So for $\alpha \in (\mathbb{Z}/N\mathbb{Z})^2$ and $\sigma \in \mathrm{Gal}_{\mathbb{Q}(j)}$, we have $\sigma(P_\alpha) = P_{\alpha A}$ where $A := \rho_{\mathcal{E},N}(\sigma)^t = \rho^*_{\mathcal{E},N}(\sigma)^{-1}$.

**Lemma 6.3.**

(i) *We have* $\mathbb{Q}(j)(\mathcal{E}[N]) = \mathcal{F}_N(\beta)$.

(ii) *We have* $\rho^*_{\mathcal{E},N}(\mathrm{Gal}_{\mathbb{Q}(j)}) = \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ *and* $\rho^*_{\mathcal{E},N}(\mathrm{Gal}_{\overline{\mathbb{Q}}(j)}) = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

(iii) *For* $\sigma \in \mathrm{Gal}_{\mathbb{Q}(j)}$ *and* $f \in \mathcal{F}_N$, *we have*

$$\sigma(f) = f * \rho^*_{\mathcal{E},N}(\sigma)^{-1}.$$

(iv) *Composing* $\rho^*_{\mathcal{E},N}$ *with the quotient map to* $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ *induces an isomorphism*

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

(v) *Let* $G$ *be a subgroup of* $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ *that satisfies* $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$ *and* $-I \in G$. *Then* $\rho^*_{\mathcal{E},N}(\mathrm{Gal}_{\mathbb{Q}(X_G)}) = G$.

(vi) *For* $\sigma \in \mathrm{Gal}_{\mathbb{Q}(j)}$, *we have* $\sigma(\beta) = \frac{f_0 * A}{f_0} \cdot \beta$, *where* $A := \rho^*_{\mathcal{E},N}(\sigma)^{-1}$.

*Proof.* Part (i) follows from Lemma 6.1 and the definition of our points $P_\alpha$. Take any nonzero $\alpha \in (\mathbb{Z}/N\mathbb{Z})^2$ and $\sigma \in \mathrm{Gal}_{\mathbb{Q}(j)}$. Define $A := \rho^*_{\mathcal{E},N}(\sigma)^{-1} = \rho_{\mathcal{E},N}(\sigma)^t$. By our choice of basis in defining $\rho_{\mathcal{E},N}$, we have $\sigma(P_\alpha) = P_{\alpha A}$. We then have $\sigma(x_\alpha) = x_{\alpha A}$ by considering $x$-coordinates. By Lemma 6.1(iii), we have $\sigma(x_\alpha) = x_\alpha * A$. Since $\alpha$ was an arbitrary nonzero element of $(\mathbb{Z}/N\mathbb{Z})^2$, Lemma 6.1(ii) implies that $\sigma(f) = f * A$ for all $f \in \mathcal{F}_N$. We have thus proved (iii).

Using $\sigma(P_\alpha) = P_{\alpha A}$ and taking $y$-coordinates, gives $\sigma(\beta)\sigma(u_\alpha) = \beta u_{\alpha A}$. Therefore, we have

$$\sigma(\beta) \cdot u_\alpha * A = \sigma(\beta)\sigma(u_\alpha) = \beta u_{\alpha A} = \beta \cdot \tfrac{f_0 * A}{f} \cdot u_\alpha * A,$$

where we have used part (iii) and Lemma 6.1(iii). Part (vi) follows by cancelling $u_\alpha * A$ from both sides.

By (iii), composing $\rho^*_{\mathcal{E},N}$ with the obvious quotient map gives an injective homomorphism $\mathrm{Gal}(\mathcal{F}_N/\mathbb{Q}(j)) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$; it is an isomorphism since we know the degree of the extension $\mathcal{F}_N/\mathbb{Q}(j)$, cf. Lemma 3.2(i). Therefore, $\pm\rho^*_{\mathcal{E},N}(\mathrm{Gal}_{\mathbb{Q}(j)}) = \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and $\pm\rho^*_{\mathcal{E},N}(\mathrm{Gal}_{\overline{\mathbb{Q}}(j)}) = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ by Lemma 3.2. We have $\rho^*_{\mathcal{E},N}(\mathrm{Gal}_{\overline{\mathbb{Q}}(j)}) = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ since there is no proper subgroup $H$ of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ for which $\pm H = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, cf. Lemma 7.8. Part (ii) now follows.

Finally take $G$ as in (v). From parts (i) and (iii) and $-I \in G$, the subfield of $\mathcal{F}_N(\beta)$ fixed by $(\rho^*_{\mathcal{E},N})^{-1}(G)$ is $\mathcal{F}_N^G$. Part (v) is now immediate since $\mathcal{F}_N^G = \mathbb{Q}(X_G)$. □

6.3. **Specializations.** Define $U := \mathbb{A}^1_{\mathbb{Q}} - \{0, 1728\} = \operatorname{Spec} \mathbb{Q}[j, j^{-1}, (j-1728)^{-1}]$ and view it as an open subvariety of the $j$-line. Let $\pi_1(U, \overline{\eta})$ be the étale fundamental group of $U$, where $\overline{\eta}$ is the geometric generic point of $U$ corresponding to our choice of algebraic closure of $\mathbb{Q}(j)$. The Weierstrass equation (6.1) has discriminant $2^{12}3^{12}j^2(j-1728)^3$ and hence defines an elliptic scheme $\mathscr{E} \to U$ whose generic fiber is the elliptic curve $\mathcal{E}$ over $\mathbb{Q}(j)$.

Let $\mathscr{E}[N]$ be the $N$-torsion subscheme of $\mathscr{E}$. We can identify the fiber of $\mathscr{E}[N] \to U$ at $\overline{\eta}$ with $\mathcal{E}[N]$. We can view $\mathscr{E}[N]$ as a rank 2 lisse sheaf of $\mathbb{Z}/N\mathbb{Z}$-modules over $U$ and it thus corresponds to a representation

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

By making an appropriate choice of basis, we may assume that the specialization of

$$\varrho^*_{\mathscr{E},N} \colon \pi_1(U, \overline{\eta}) \to \operatorname{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

at the generic fiber of $U$ gives our representation $\rho^*_{\mathcal{E},N} \colon \operatorname{Gal}_{\mathbb{Q}(j)} \to \operatorname{GL}_2(\mathbb{Z}/N\mathbb{Z})$. The representation $\varrho^*_{\mathscr{E},N}$ is surjective by Lemma 6.3(ii).

Take any subgroup $G$ of $\operatorname{GL}_2(\mathbb{Z}/N\mathbb{Z})$ satisfying $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$ and $-I \in G$. Let $\pi_G \colon U_G \to U$ be the étale cover corresponding to the subgroup $(\varrho^*_{\mathscr{E},N})^{-1}(G)$ of $\pi_1(U, \overline{\eta})$. The function field of $U_G$ is $\mathcal{F}_N^G = \mathbb{Q}(X_G)$ by Lemma 6.3(v). So we can identify $U_G$ with an open subvariety of the modular curve $X_G$ and the morphism $\pi_G$ extends to the morphism from $X_G$ to the $j$-line that we had also denoted by $\pi_G$. In particular, $U_G$ is the open subvariety of $X_G$ that is the complement of $\pi_G^{-1}(\{0, 1728, \infty\})$. (When $-I \notin G$, we will simply define $U_G$ to be $X_G - \pi_G^{-1}(\{0, 1728, \infty\})$.)

**Proposition 6.4.** *Let $G$ be a subgroup of $\operatorname{GL}_2(\mathbb{Z}/N\mathbb{Z})$ satisfying $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$ and $-I \in G$. Let $E$ be an elliptic curve defined over a number field $K$ with $j_E \notin \{0, 1728\}$. Then $\rho^*_{E,N}(\operatorname{Gal}_K)$ is conjugate in $\operatorname{GL}_2(\mathbb{Z}/N\mathbb{Z})$ to a subgroup of $G$ if and only if $j_E = \pi_G(u)$ for some $u \in U_G(K)$.*

*Proof.* We may assume $K \subseteq \overline{\mathbb{Q}}$. Define the surjective homomorphism $\varrho := \varrho^*_{\mathscr{E},N} \colon \pi_1(U, \overline{\eta}) \to \operatorname{GL}_2(\mathbb{Z}/N\mathbb{Z})$. For each $u \in U(K) = K - \{0, 1728\}$, let $\varrho_u \colon \operatorname{Gal}_K \to \operatorname{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be the specialization of $\varrho$ at $u$; it is uniquely determined up to conjugation by an element of $\operatorname{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

We claim that $\varrho_u(\operatorname{Gal}_K)$ is conjugate in $\operatorname{GL}_2(\mathbb{Z}/N\mathbb{Z})$ to a subgroup of $G$ if and only if $u = \pi_G(P)$ for some $P \in U_G(K)$. Let $\varphi \colon Y \to U$ be the étale cover corresponding to $\varrho$; the curve $Y$ is defined over $\mathbb{Q}$ but need not be geometrically irreducible. The group $\operatorname{GL}_2(\mathbb{Z}/N\mathbb{Z})$ acts on $Y$ and acts simply faithful on the fiber $\varphi^{-1}(u) := \{P \in Y(\overline{\mathbb{Q}}) : \varphi(P) = u\}$. The group $\operatorname{Gal}_K$ acts on $\varphi^{-1}(u)$ since $\varphi$ and $u$ are defined over $K$. There is a point $P_0 \in \varphi^{-1}(u)$ such that $\sigma(P_0) = \varrho_u(\sigma) \cdot P_0$ for all $\sigma \in \operatorname{Gal}_K$ (a different choice of $P_0$ results in a conjugate of $\varrho_u$). The $G$-orbits of $\varphi^{-1}(u)$ correspond with the points $P \in U_G(\overline{\mathbb{Q}})$ that satisfy $\pi_G(P) = u$ via the natural morphism $Y \to U_G$. Since $\varphi$ and $u$ are defined over $K$, those $G$-orbits of $\varphi^{-1}(u)$ that are stable under the $\operatorname{Gal}_K$-action correspond with the points $P \in U_G(K)$ that satisfy $\pi_G(P) = u$. Therefore, there is a point $P \in U_G(K)$ with $\pi_G(P) = u$ if and only if there is a point $P_0 \in \varphi^{-1}(u)$ such that for each $\sigma \in \operatorname{Gal}_K$, we have $\sigma(P_0) = g \cdot P_0$ for some $g \in G$; equivalently, $\varrho_u(\operatorname{Gal}_K)$ is conjugate to a subgroup of $G$. This proves the claim.

The specialization $\varrho_u \colon \operatorname{Gal}_K \to \operatorname{GL}_2(\mathbb{Z}/N\mathbb{Z})$ of $\varrho$ at $u$ is isomorphic to the representation $\rho^*_{\mathcal{E}_u,N} \colon \operatorname{Gal}_K \to \operatorname{GL}_2(\mathbb{Z}/N\mathbb{Z})$, where $\mathcal{E}_u$ is the elliptic curve over $K$ defined by the Weierstrass equation (6.1) with $j$ replaced by $u$. Since $\mathcal{E}_u$ has $j$-invariant $u$, the above claim proves the lemma in the case where $E = \mathcal{E}_u$.

Since $-I \in G$, it now suffices to show that $\pm\rho^*_E(\operatorname{Gal}_K)$ and $\pm\rho^*_{\mathcal{E}_u}(\operatorname{Gal}_K)$ are conjugate in $\operatorname{GL}_2(\mathbb{Z}/N\mathbb{Z})$ where $u := j_E \in K - \{0, 1728\} = U(K)$. The curve $E$ and $\mathcal{E}_u$ are quadratic twists of each other

since they have the same $j$-invariant which is neither 0 or 1728. So after choosing compatible bases, there is a quadratic character $\chi\colon \mathrm{Gal}_K \to \{\pm 1\}$ such that $\rho^*_{\mathscr{E}_u,N} = \chi \cdot \rho^*_{E,N}$. In particular, $\pm\rho^*_{\mathscr{E}_u,N}(\mathrm{Gal}_K) = \pm\rho^*_{E,N}(\mathrm{Gal}_K)$. □

6.3.1. *Elliptic scheme for the group $G$.* Let $G$ be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ satisfying $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$ and $-I \in G$. Let $\mathscr{E}_G \to U_G$ be the elliptic scheme obtained by base extending $\mathscr{E} \to U$ by the étale morphism $\pi_G\colon U_G \to U$. Then we can construct a representation $\varrho^*_{\mathscr{E}_G,N}\colon \pi_1(U_G, \overline{\eta}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ as before, where now $\overline{\eta}$ denotes the geometric generic point of $U_G$ corresponding to our choice of algebraic closure of $\mathbb{Q}(j)$ (which contains $\mathbb{Q}(X_G)$). The morphism $\pi_G$ allows us to view $\pi_1(U_G, \overline{\eta})$ as a subgroup of $\pi_1(U, \overline{\eta})$; we may assume that our representation was chosen so that the restriction of $\varrho^*_{\mathscr{E},N}$ to $\pi_1(U_G, \overline{\eta})$ agrees with $\varrho^*_{\mathscr{E}_G,N}$. In particular, we have a surjective homomorphism

$$\varrho^*_{\mathscr{E}_G,N}\colon \pi_1(U_G, \overline{\eta}) \to G.$$

Take any number field $K \subseteq \overline{\mathbb{Q}}$ and point $u \in U_G(K)$. Let $(\mathscr{E}_G)_u$ be the elliptic curve over $K$ that is the fiber of $\mathscr{E}_G \to U_G$ over $u$; it is isomorphic to the elliptic curve over $K$ defined by (6.1) with $j$ replaced by $\pi_G(u)$. The specialization of $\varrho^*_{\mathscr{E}_G,N}$ at $u$ is a representation $\mathrm{Gal}_{\mathbb{Q}} \to G \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that is isomorphic to $\rho^*_{(\mathscr{E}_G)_u,N}$.

## 7. Some basic group theory

We now collect some basic group theoretic results that we will use. Most of it concerns the groups $\mathrm{SL}_2(\mathbb{Z}_\ell)$ and $\mathrm{GL}_2(\mathbb{Z}_\ell)$, with $\ell$ prime, and the groups $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ and $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

7.1. **Goursat's lemma.** We will make frequent use of the following in §8.

**Lemma 7.1** (Goursat's lemma, [Rib76, Lemma 5.2.1])**.** *Let $G_1$ and $G_2$ be two groups and let $H$ be a subgroup of $G_1 \times G_2$ so that the projection maps $p_1\colon H \to G_1$ and $p_2\colon H \to G_2$ are surjective. Let $N_1$ and $N_2$ be the normal subgroups of $G_1$ and $G_2$, respectively, for which $\ker(p_2) = N_1 \times \{1\}$ and $\ker(p_1) = \{1\} \times N_2$. Then the image of $H$ in $(G_1 \times G_2)/(N_1 \times N_2) = G_1/N_1 \times G_2/N_2$ is the graph of an isomorphism $G_1/N_1 \xrightarrow{\sim} G_2/N_2$.*

7.2. **Determining closed subgroups by their reductions.**

**Lemma 7.2.** *Fix an integer $N = \prod_p p^{e_p} > 1$ with $e_2 \neq 1$. For each prime $\ell$ dividing $N$, define the integer*

$$N_\ell := \ell^{e_\ell} \prod_{p \mid N,\, p^2 \equiv 1 \bmod \ell} p;$$

*it is a divisor of $N$. Let $G$ be a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_N)$. For each prime $\ell$ dividing $N$, assume that the image of $G$ in $\mathrm{GL}_2(\mathbb{Z}/N_\ell\ell\mathbb{Z})$ contains all matrices that are congruent to $I$ modulo $N_\ell$. Then $G$ is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_N)$ with level dividing $N$.*

*Proof.* We first consider the special case where $N = \ell^{e_\ell} > 1$ is a prime power (with $e_\ell \geq 2$ if $\ell = 2$). For $i \geq 1$, define the group $H_i := G \cap (I + \ell^i M_2(\mathbb{Z}_\ell))$. We have an injective homomorphism

$$\phi_i\colon H_i/H_{i+1} \hookrightarrow \mathfrak{g}, \quad 1 + \ell^i A \mapsto A \bmod \ell,$$

where $\mathfrak{g} := M_2(\mathbb{F}_\ell)$.

We claim that $\phi_i$ is surjective for all $i \geq e_\ell$. We shall prove this by induction on $i$. We have $N_\ell = \ell^{e_\ell}$ and the homomorphism $\phi_{e_\ell}$ is surjective by our assumption that the image of $G$ in $\mathrm{GL}_2(\mathbb{Z}/N_\ell\ell\mathbb{Z}) = \mathrm{GL}_2(\mathbb{Z}/\ell^{e_\ell+1}\mathbb{Z})$ contains all matrices that are congruent to $I$ modulo $\ell^{e_\ell}$. Now consider any $i \geq e_\ell$ for which $\phi_i$ is surjective. Take any $B \in \mathfrak{g}$. Since $\phi_i$ is surjective, there is a matrix $A \in M_2(\mathbb{Z}_\ell)$ such that $I + \ell^i A \in G$ and $A \equiv B \pmod{\ell}$. Raising to the $\ell$-th power, we find that $g := (I + \ell^i A)^\ell$ is an element of $G$ with $g \equiv I + \ell^{i+1} A \pmod{\ell^{i+2}}$ (this uses that $\binom{\ell}{j} \equiv 0 \pmod{\ell}$

when $0 < j < \ell$ and that $i \geq 2$ when $\ell = 2$). So $g \in H_{i+1}$ and $\phi_{i+1}(g \cdot H_{i+2}) \equiv A \equiv B \pmod{\ell}$. Since $B \in \mathfrak{g}$ was arbitrary, this proves that $\phi_{i+1}$ is surjective. The claim follows by induction.

For any $i \geq e_\ell$, the above claim implies that the image of $G$ in $\mathrm{GL}_2(\mathbb{Z}/\ell^i\mathbb{Z})$ contains all matrices $A \in \mathrm{GL}_2(\mathbb{Z}/\ell^i\mathbb{Z})$ with $A \equiv I \pmod{\ell^{e_\ell}}$. Since $G$ is a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, we deduce that $G$ is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ whose level divides $\ell^{e_\ell}$. This completes the proof in the special case where $N$ is a prime power.

We now consider the general case. Take any prime $\ell | N$ and let

$$\varphi \colon G \to \prod_{p|N,\, p \neq \ell} \mathrm{GL}_2(\mathbb{Z}_p)$$

be the projection homomorphism. We have $\ker(\varphi) = H_\ell \times \{I\}$, where $H_\ell$ is a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$.

Take any $B \in \mathfrak{g}$. By assumption, the image of $G$ in $\mathrm{GL}_2(\mathbb{Z}/N_\ell \ell \mathbb{Z})$ contains all matrices that are congruent to $I$ modulo $N_\ell$. So there is a $g_0 \in G$ such that $g_0 \equiv I + \ell^{e_\ell} B \pmod{\ell^{e_\ell+1}}$ and $g_0 \equiv I \pmod{p}$ for all $p|N$ with $p^2 \equiv 1 \pmod{\ell}$. Observe that if $\ell$ divides $|\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})| = (p-1)^2(p+1)p$ for a prime $p \neq \ell$, then $p^2 \equiv 1 \pmod{\ell}$. So for any $m \geq 1$, there is a positive integer $f \equiv 1 \pmod{\ell}$ for which $g_0^f \equiv \varphi(g_0)^f \equiv I \pmod{\prod_{p|N, p\neq\ell} p^m}$. We have $g_0^f \equiv I + \ell^{e_\ell} B \pmod{\ell^{e_\ell+1}}$. By taking $m$ larger and larger and using that $G$ is a closed, and hence compact, subgroup of $\mathrm{GL}_2(\mathbb{Z}_N)$, we deduce that there is a $g \in \ker(\varphi)$ for which $g \equiv I + \ell^{e_\ell} B \pmod{\ell^{e_\ell+1}}$. Since $B \in \mathfrak{g}$ was arbitrary, we deduce that the image of $H_\ell$ in $\mathrm{GL}_2(\mathbb{Z}/\ell^{e_\ell+1}\mathbb{Z})$ contains all matrices that are congruent to $I$ modulo $\ell^{e_\ell}$.

By the prime power case of the lemma, which we have already proved, $H_\ell$ is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ whose level divides $\ell^{e_\ell}$. Since $\ell$ was an arbitrary prime divisor of $N$, we deduce that $\prod_{\ell|N} H_\ell$ is a subgroup of $G$ and hence $G$ is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_N)$ whose level divides $\prod_{\ell|N} \ell^{e_\ell} = N$. □

For an open subgroup $G$ of $\mathrm{GL}_2(\mathbb{Z}_N)$, the following lemma is useful for finding its maximal subgroups; the issue being that these maximal subgroups may have strictly larger level.

**Lemma 7.3.** *Fix an integer $N = \prod_p p^{e_p} > 1$ with $e_2 \neq 1$. Let $G$ be an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_N)$ whose level divides $N$. If $M$ is a maximal open subgroup of $G$, then the level of $M$ divides $N\ell$ for some $\ell | N$.*

*Proof.* Let $M$ be a maximal open subgroup of $G$. Take any prime $\ell | N$. If the image of $M$ and $G$ modulo $N\ell$ give different subgroups of $\mathrm{GL}_2(\mathbb{Z}/N\ell\mathbb{Z})$, then the level of $M$ divides $N\ell$ (using that $M$ is maximal, it agrees with the group of $g \in G$ whose image modulo $N\ell$ lies in the image of $M$ modulo $N\ell$).

So we can assume that $M$ and $G$ have the same image modulo $N\ell$ for all primes $\ell | N$. Since $G$ has level $N$, we deduce that for each $\ell | N$, the image of $M$ modulo $N\ell$ contains all matrices $A \in \mathrm{GL}_2(\mathbb{Z}/N\ell\mathbb{Z})$ satisfying $A \equiv I \pmod{N}$. Applying Lemma 7.2 to the group $M$, we deduce that the level of $M$ divides $N$. □

The following is an analogous version of Lemma 7.4.

**Lemma 7.4.** *Fix an integer $N = \prod_p p^{e_p} > 1$ with $e_2 \neq 1$. For each prime $\ell$ dividing $N$, define the integer*

$$N_\ell := \ell^{e_\ell} \prod_{p|N,\, p^2 \equiv 1 \bmod \ell} p;$$

*it is a divisor of $N$. Let $G$ be a closed subgroup of $\mathrm{SL}_2(\mathbb{Z}_N)$. For each prime $\ell$ dividing $N$, assume that the image of $G$ in $\mathrm{SL}_2(\mathbb{Z}/N_\ell\ell\mathbb{Z})$ has level which divides $N_\ell$. Then $G$ is an open subgroup of $\mathrm{SL}_2(\mathbb{Z}_N)$ with level dividing $N$.*

*Proof.* This can be proved in the exact same way as Lemma 7.4 with $\mathrm{GL}_2$ replaced by $\mathrm{SL}_2$ and with $\mathfrak{g} = \{A \in M_2(\mathbb{F}_\ell) : \mathrm{tr}(A) = 0\}$. □

**Lemma 7.5.** *Fix a prime $\ell$. Let $G$ be a closed subgroup of $\mathrm{SL}_2(\mathbb{Z}_\ell)$ whose image modulo $\ell^e$ is $\mathrm{SL}_2(\mathbb{Z}/\ell^e\mathbb{Z})$, where $e$ is 3, 2 or 1 when $\ell$ is 2, 3 or at least 5, respectively. Then $G = \mathrm{SL}_2(\mathbb{Z}_\ell)$.*

*Proof.* For $\ell \geq 5$, the lemma follows from [Ser98, IV, Lemma 3]. For $\ell \in \{2, 3\}$, this follows from Lemma 7.4. □

Many of the open subgroups $G$ of $\mathrm{GL}_2(\mathbb{Z}_N)$ contai

**Lemma 7.6.** *Fix an integer $N > 1$. Let $H$ be a subgroup of $\mathrm{GL}_2(\mathbb{Z}_N)$ for which $H \cap \mathrm{SL}_2(\mathbb{Z}_N)$ is an open subgroup of $\mathrm{SL}_2(\mathbb{Z}_N)$ whose level divides $N_0$. Assume that $N_0 \equiv 0 \pmod 4$ if $N_0$ is even. Define $N_1 := N_0$ if $N_0$ is odd and $N_1 := 2N_0$ if $N_0$ is even. Then $\mathbb{Z}_N^\times \cdot H$ is an open subgroups of $\mathrm{GL}_2(\mathbb{Z}_N)$ whose level divides $N_1$.*

*Proof.* By considering the $\ell$-adic projections, we reduce to the case where $N$ is a power of a prime $\ell$ and $N_0 = \ell^e$ (with $e \geq 2$ if $\ell = 2$). Let $f = e$ if $\ell$ is odd and $f = e + 1$ if $\ell = 2$. One can check that $(1 + \ell^e\mathbb{Z}_\ell)^2 = 1 + \ell^f\mathbb{Z}_\ell$; this uses that $e \geq 2$ when $\ell = 2$.

Take any matrix $A \in I + \ell^f M_2(\mathbb{Z}_\ell)$. We have $\det(A) \in 1 + \ell^f\mathbb{Z}_\ell = (1 + \ell^e\mathbb{Z}_\ell)^2$, so $\det(A) = d^2$ for some $d \in 1 + \ell^e\mathbb{Z}_\ell$. The matrix $d^{-1}A \in \mathrm{GL}_2(\mathbb{Z}_\ell)$ has determinant 1 and is congruent to $I$ modulo $\ell^e$. Since the level of $H \cap \mathrm{SL}_2(\mathbb{Z}_N)$ in $\mathrm{SL}_2(\mathbb{Z}_N)$ divides $N_0 = \ell^e$, we must have $d^{-1}A \in H$. Therefore, $A = d \cdot d^{-1}A$ is an element of $\widehat{\mathbb{Z}}^\times H$. The level of $\widehat{\mathbb{Z}}^\times H$ divides $\ell^f = N_1$ since $A$ was an arbitrary element of $I + \ell^f M_2(\mathbb{Z}_\ell)$. □

7.3. **Commutator subgroups.** We first consider some basic results about commutator subgroups.

**Lemma 7.7.**

(i) *If $\ell \geq 5$, the group $\mathrm{SL}_2(\mathbb{Z}_\ell)$ is perfect, i.e., it is equal to its commutator subgroup.*
(ii) *The commutator subgroup of $\mathrm{SL}_2(\mathbb{Z}_3)$ has level 3 and index 3.*
(iii) *The commutator subgroup of $\mathrm{SL}_2(\mathbb{Z}_2)$ has level 4 and index 4, and the quotient is a cyclic group of order 4.*
(iv) *If $\ell \geq 3$, the commutator subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ is $\mathrm{SL}_2(\mathbb{Z}_\ell)$.*
(v) *The commutator subgroup of $\mathrm{GL}_2(\mathbb{Z}_2)$ is a subgroup of $\mathrm{SL}_2(\mathbb{Z}_2)$ of level 2 and index 2.*
(vi) *The commutator subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ is an open subgroup of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ of level 2 and index 2.*

*Proof.* Parts (i)–(iii) follow immediately from [Zyw10, Lemma A.1]. Now take any prime $\ell$. We have

$$[\mathrm{SL}_2(\mathbb{Z}_\ell), \mathrm{SL}_2(\mathbb{Z}_\ell)] \subseteq [\mathrm{GL}_2(\mathbb{Z}_\ell), \mathrm{GL}_2(\mathbb{Z}_\ell)] \subseteq \mathrm{SL}_2(\mathbb{Z}_\ell).$$

Part (iv) with $\ell \geq 5$ is now a consequence of (i).

When $\ell = 3$, we deduce from (ii) that $[\mathrm{GL}_2(\mathbb{Z}_3), \mathrm{GL}_2(\mathbb{Z}_3)]$ has level 1 or 3 in $\mathrm{SL}_2(\mathbb{Z}_3)$. Part (iv) with $\ell = 3$ follows by verifying that $[\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})] = \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$.

When $\ell = 2$, we deduce from (iii) that the level of $[\mathrm{GL}_2(\mathbb{Z}_2), \mathrm{GL}_2(\mathbb{Z}_2)]$ in $\mathrm{SL}_2(\mathbb{Z}_2)$ divides 4. Part (v) with $\ell = 2$ follows by verifying that $[\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})]$ is a subgroup of $\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$ of index 2 that contains all the matrices $A \in \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$ with $A \equiv I \pmod 2$.

For the group $\mathrm{GL}_2(\widehat{\mathbb{Z}}) = \prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell)$, part (vi) follows from (iv) and (v). □

**Lemma 7.8.** *Take any integer $N > 1$. There are no proper subgroups $H$ of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ that satisfy $\pm H = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.*

*Proof.* Suppose that $H$ is a proper subgroup of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ that satisfies $\pm H = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. The group $H$ has index 2 in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and contains the commutator subgroup of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Using the description of commutator subgroups of $\mathrm{SL}_2(\mathbb{Z}_\ell)$ with $\ell|N$ from Lemma 7.7, we find that $N$ is even and $H$ is the unique index 2 subgroup of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ containing all matrices $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ for which $A \equiv I \pmod 2$. In particular, we have $-I \in H$ since $-I \equiv I \pmod 2$. This contradicts that $H$ is a proper subgroup of $\pm H$. □

**Lemma 7.9.** *For a prime $\ell \geq 5$, let $G$ be a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ for which $\det(G) = \mathbb{Z}_\ell^\times$ and $G$ modulo $\ell$ is equal to $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Then $G = \mathrm{GL}_2(\mathbb{Z}_\ell)$.*

*Proof.* The commutator subgroup $[G, G]$ is a closed subgroup of $\mathrm{SL}_2(\mathbb{Z}_\ell)$ whose image modulo $\ell$ is $[\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})] = \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$, where we have used our assumption on the image of $G$ modulo $\ell$ and Lemma 7.7(i). By Lemma 7.5, we have $[G, G] = \mathrm{SL}_2(\mathbb{Z}_\ell)$. We conclude that $G = \mathrm{GL}_2(\mathbb{Z}_\ell)$ since $G \supseteq [G, G] = \mathrm{SL}_2(\mathbb{Z}_\ell)$ and $\det(G) = \mathbb{Z}_\ell^\times$. □

**Lemma 7.10.** *Let $G$ be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ or $\mathrm{SL}_2(\widehat{\mathbb{Z}})$. Then the commutator subgroup $[G, G]$ is an open subgroup of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$.*

*Proof.* We obviously have $[G, G] \subseteq \mathrm{SL}_2(\widehat{\mathbb{Z}})$. We can always replace $G$ by a smaller group since this the will make $[G, G]$ smaller as well. So without loss of generality, we may assume that $G$ is an open subgroup of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ and that $G = \prod_\ell G_\ell$ with $G_\ell$ an open subgroup of $\mathrm{SL}_2(\mathbb{Z}_\ell)$. For $\ell \geq 5$ large enough, we have $G_\ell = \mathrm{SL}_2(\mathbb{Z}_\ell)$ and $[G_\ell, G_\ell] = \mathrm{SL}_2(\mathbb{Z}_\ell)$ by Lemma 7.7(i). So for any fixed prime $\ell$, we need only show that $[G_\ell, G_\ell]$ is an open subgroup of $\mathrm{SL}_2(\mathbb{Z}_\ell)$.

Take any prime $\ell$. By Lemma 7.6, there is an integer $e \geq 1$ such that $W := \mathbb{Z}_\ell^\times \cdot G_\ell \supseteq 1 + \ell^e M_2(\mathbb{Z}_\ell)$. By Lemma 1 of [LT76, p.163], we have $[G_\ell, G_\ell] = [W, W] \supseteq (1 + \ell^{2e} M_2(\mathbb{Z}_\ell)) \cap \mathrm{SL}_2(\mathbb{Z}_\ell)$ and hence $[G_\ell, G_\ell]$ is an open subgroup of $\mathrm{SL}_2(\mathbb{Z}_\ell)$. □

7.3.1. *Computing commutator subgroups.* Now let $G$ be an open subgroup of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ or $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. Assume $G$ is given explicitly, i.e., we have generators for the image of $G$ modulo $m$ for some positive integer $m$ divisible by the level of $G$.

We will need to be able to compute the commutator subgroup $[G, G]$; note the level of $[G, G]$ in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ may be strictly larger than $m$.

By Lemma 7.10, $[G, G]$ is an open subgroup of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$. By Lemma 7.7(i), we find that the level of $[G, G]$ is not divisible by any prime $\ell \geq 5$ for which $\ell \nmid m$. For any positive integer $n$, we can compute the image of $[G, G]$ modulo $n$; it equals $[\overline{G}, \overline{G}] \subseteq \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$, where $\overline{G}$ is the image of $G$ modulo $n$. By computing $[G, G]$ modulo $n$ for suitable $n$ that are not divisible by any prime $\ell \geq 5$ satisfying $\ell \nmid m$, we can use the criterion of Lemma 7.4 to find a positive integer $N$ that is divisible by the level of $[G, G]$ in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$. Once we have such a $N$, we have explicitly found $[G, G]$ since it is determined by $N$ and its image modulo $N$.

7.4. **Full $\ell$-adic images.** The next lemma shows that if $G$ is a proper closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ with full determinant, then it is prosolvable.

**Lemma 7.11.** *Take any prime $\ell$ and let $G$ be a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ with $\det(G) = \mathbb{Z}_\ell^\times$. If $S$ is a nonabelian simple group that occurs as the quotient of some closed normal subgroup of $G$, then $\ell \geq 5$, $G = \mathrm{GL}_2(\mathbb{Z}_\ell)$ and $S \cong \mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm I\}$.*

*Proof.* The kernel of the reduction modulo $\ell$ homomorphism $G \to \mathrm{GL}_2(\mathbb{F}_\ell)$ is prosolvable. So the image $\overline{G}$ of $G$ in $\mathrm{GL}_2(\mathbb{F}_\ell)$ satisfies $\det(\overline{G}) = \mathbb{F}_\ell^\times$ and contains the nonabelian simple group $S$ as a factor in its composition series. Since $\mathrm{GL}_2(\mathbb{F}_2)$ and $\mathrm{GL}_2(\mathbb{F}_3)$ are solvable, we have $\ell \geq 5$.

First suppose that the cardinality of $\overline{G}$ is not divisible by $\ell$. Since $\overline{G}$ is nonsolvable, we find from §2.6 of [Ser72] that the image of $\overline{G}$ in $\mathrm{PGL}_2(\mathbb{F}_\ell) := \mathrm{GL}_2(\mathbb{F}_\ell)/(\mathbb{F}_\ell^\times \cdot I)$ is isomorphic to the

alternating group $\mathfrak{A}_5$. Since $\mathfrak{A}_5$ is nonabelian and simple, we must have $\det(\overline{G}) \subseteq (\mathbb{F}_\ell^\times)^2$ which is a contradiction.

So the prime $\ell$ must divide the cardinality of $\overline{G}$. Since $\overline{G}$ is nonsolvable, [Ser72, Proposition 15] shows that $\overline{G} \supseteq \mathrm{SL}_2(\mathbb{F}_\ell)$. The group $\mathrm{SL}_2(\mathbb{F}_\ell)$ is perfect since $\ell \geq 5$ and hence $[G, G]$ is a closed subgroup of $\mathrm{SL}_2(\mathbb{Z}_\ell)$ whose image modulo $\ell$ is $\mathrm{SL}_2(\mathbb{F}_\ell)$. We have $[G, G] = \mathrm{SL}_2(\mathbb{Z}_\ell)$ by Lemma 7.5. We thus have $G = \mathrm{GL}_2(\mathbb{Z}_\ell)$ since $\det(G) = \mathbb{Z}_\ell^\times$. Finally $S$ must be isomorphic to $\mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm I\}$ since it is the only nonabelian simple group that occurs as a factor in a composition series of $\overline{G} = \mathrm{GL}_2(\mathbb{F}_\ell)$. □

**Lemma 7.12.** *Let $G$ be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ satisfying $\det(G) = \widehat{\mathbb{Z}}^\times$. Take any prime $\ell \geq 5$ and let $G_\ell$ be the image of $G$ under the projection map $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$. Then the following are equivalent:*

(a) *$G_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$,*
(b) *$\ell$ does not divide the level of $[G, G]$ in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$,*
(c) *$\ell$ does not divide the level of $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$.*

*Proof.* First suppose that $G_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$. Let $H$ be one of the groups $[G, G]$ or $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$; it is an open subgroup of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$. Since $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) \supseteq [G, G]$, we have $\mathrm{SL}_2(\mathbb{Z}_\ell) \supseteq H_\ell \supseteq [G, G]_\ell = [G_\ell, G_\ell]$, where $H_\ell$ and $[G, G]_\ell$ are the images of $H$ and $[G, G]$, respectively, under the projection map $\mathrm{SL}_2(\widehat{\mathbb{Z}}) \to \mathrm{SL}_2(\mathbb{Z}_\ell)$. By Lemma 7.7(iv), we deduce that $H_\ell = \mathrm{SL}_2(\mathbb{Z}_\ell)$. Let $H'$ be the image of $H$ under the projection $\mathrm{SL}_2(\widehat{\mathbb{Z}}) \to \prod_{p \neq \ell} \mathrm{SL}_2(\mathbb{Z}_p)$. So we may identify $H$ with a closed subgroup of $H_\ell \times H'$. Let $B$ and $B'$ be the normal subgroups of $H_\ell$ and $H'$, respectively, such that $B \times \{I\}$ is the kernel of the projection $H \to H'$ and $\{I\} \times B'$ is the kernel of the projection $H \to H_\ell$. Since $H$ is open in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$, the groups $B$ and $B'$ are open in $H_\ell$ and $H'$, respectively. By Goursat's lemma, we have an isomorphism of (finite) groups $H_\ell/B \cong H'/B'$.

Suppose that $H_\ell/B \neq 1$. There is a simple group $S$ that is the quotient of both $H_\ell$ and $H_p$ for some prime $p \neq \ell$. The groups $H_\ell$ and $H_p$ are normal subgroups of $G_\ell$ and $G_p$, respectively, since $H$ is a normal subgroup of $G$. Since the groups $\mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm I\}$ and $\mathrm{SL}_2(\mathbb{F}_p)/\{\pm I\}$ have different cardinalities and $G_\ell$ and $G_p$ have full determinants, Lemma 7.11 implies that $S$ is abelian. However, $H_\ell = \mathrm{SL}_2(\mathbb{Z}_\ell)$ has no nontrivial abelian quotients by Lemma 7.7(i). Therefore, $H_\ell/B = 1$.

The groups $H_\ell/B$ and $H'/B'$ are trivial. Therefore, $H \supseteq B \times B' = H_\ell \times H'$ and hence $H = H_\ell \times H' = \mathrm{SL}_2(\mathbb{Z}_\ell) \times H'$. This description of $H$ shows that $\ell$ does not divide its level. This shows that (a) implies (b) and (c).

Now suppose that (b) or (c) holds. In either case, we have $G_\ell \supseteq \mathrm{SL}_2(\mathbb{Z}_\ell)$. Since $G$ has full determinant, this implies (a). □

7.5. **Some 3-adic computations.** To study the prime $\ell = 3$, we define a surjective homomorphism

$$\varphi_3 \colon \mathrm{GL}_2(\mathbb{Z}_3) \to \mathrm{GL}_2(\mathbb{F}_3) \to \mathrm{GL}_2(\mathbb{F}_3)/[\mathrm{SL}_2(\mathbb{F}_3), \mathrm{SL}_2(\mathbb{F}_3)] \xrightarrow{\sim} \mathfrak{S}_3,$$

where we compose reduction modulo 3, the natural quotient map, and a choice of isomorphism with the symmetric group $\mathfrak{S}_3$. Note that $\varphi_3(\mathrm{SL}_2(\mathbb{Z}_3))$ is the alternating group $\mathfrak{A}_3$.

**Lemma 7.13.** *If $H$ is a closed normal subgroup of $\mathrm{GL}_2(\mathbb{Z}_3)$, then either $\varphi_3(H) = 1$ or $H \supseteq \mathrm{SL}_2(\mathbb{Z}_3)$.*

*Proof.* If $H \supseteq \mathrm{SL}_2(\mathbb{Z}_3)$, then $\varphi_3(H) \supseteq \varphi_3(\mathrm{SL}_2(\mathbb{Z}_3)) = \mathfrak{A}_3 \neq 1$. So we may now assume that $\varphi_3(H) \neq 1$. We need to show that $H \supseteq \mathrm{SL}_2(\mathbb{Z}_3)$.

We have $\varphi_3(H) \supseteq \mathfrak{A}_3$ since $\varphi_3(H)$ is a nontrivial normal subgroup of $\mathfrak{S}_3$. So there is an $a \in H$ such that $\varphi_3(a) \in \mathfrak{A}_3 - \{1\}$. The two elements of $\mathfrak{A}_3 - \{1\}$ are conjugate in $\mathfrak{S}_3$, so there is a $g \in \mathrm{GL}_2(\mathbb{Z}_3)$ such that $\varphi_3(ga^{-1}g^{-1}) = \varphi_3(g)\varphi_3(a)^{-1}\varphi_3(g)^{-1}$ equals $\varphi_3(a)$. Therefore, $\varphi_3(ga^{-1}g^{-1}a) = \varphi_3(a)^2$ has order 3. Since $H$ is normal in $\mathrm{GL}_2(\mathbb{Z}_3)$, we deduce that $\varphi_3(ga^{-1}g^{-1}a)$

is an element of $\varphi_3(H \cap \mathrm{SL}_2(\mathbb{Z}_3))$ of order 3. So after replacing $H$ by $H \cap \mathrm{SL}_2(\mathbb{Z}_3)$, we may assume that $H \subseteq \mathrm{SL}_2(\mathbb{Z}_3)$.

The image $\overline{H}$ of $H$ modulo 3 is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ that contains an element of order 3. We have $\overline{H} = \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ since the only maximal normal subgroup of $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ is its commutator subgroup which has order 8. A direct computation shows that there are no normal subgroup of $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ whose image modulo 3 is the group $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ (however, there are such subgroups if we exclude the normal condition). So $H$ is a closed subgroup of $\mathrm{SL}_2(\mathbb{Z}_3)$ whose image modulo 9 equals $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$. By Lemma 7.5, we have $H = \mathrm{SL}_2(\mathbb{Z}_3)$. □

## 8. Agreeable groups

We say that subgroup $\mathcal{G}$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ is agreeable if it is open in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, satisfies $\det(\mathcal{G}) = \widehat{\mathbb{Z}}^\times$, contains the scalar matrices $\widehat{\mathbb{Z}}^\times \cdot I$, and the levels of $\mathcal{G} \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ and $\mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) \subseteq \mathrm{SL}_2(\widehat{\mathbb{Z}})$ have the same odd prime divisors.

The following proposition, which we will prove in §8.3, shows that every open subgroup $G$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ with full determinant lies in a unique minimal agreeable group $\mathcal{G} \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$. We call $\mathcal{G}$ the agreeable closure of $G$.

**Proposition 8.1.** *Let $G$ be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ with $\det(G) = \widehat{\mathbb{Z}}^\times$. Then there is a unique minimal agreeable subgroup $\mathcal{G}$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, with respect to inclusion, that satisfies $G \subseteq \mathcal{G}$. We have $[G, G] = [\mathcal{G}, \mathcal{G}]$ and hence $G$ is a normal subgroup of $\mathcal{G}$ with $\mathcal{G}/G$ finite and abelian.*

Recall that for our application to Serre's open image theorem, we will study the agreeable closure $\mathcal{G}_E$ of $\rho_E^*(\mathrm{Gal}_{\mathbb{Q}})$ for non-CM elliptic curves $E/\mathbb{Q}$. Since $\rho_E^*$ is defined up to isomorphism, the group $\mathcal{G}_E \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ is uniquely determined up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

8.1. **Projection notation.** We now introduce notation that we will use through §8.

Let $G$ be a subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. For each positive integer $n$, we let $G_n$ be the image of $G$ under the homomorphism $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}_n)$ arising from the natural ring homomorphism $\widehat{\mathbb{Z}} = \mathbb{Z}_n \times \prod_{\ell \nmid n} \mathbb{Z}_\ell \to \mathbb{Z}_n$. For example, the *level* of an open subgroup $G$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ is the smallest positive integer $n$ for which we have a natural identification $G = G_n \times \prod_{\ell \nmid n} \mathrm{GL}_2(\mathbb{Z}_\ell)$.

Let $G$ be a subgroup of $\mathrm{GL}_2(\mathbb{Z}_N)$ for an integer $N > 1$. For a positive integer $n$ that divides some power of $N$, we denote by $G_n$ the image of $G$ under the homomorphism $\mathrm{GL}_2(\mathbb{Z}_N) \to \mathrm{GL}_2(\mathbb{Z}_n)$ arising from the projection ring homomorphism $\mathbb{Z}_N = \mathbb{Z}_n \times \prod_{\ell \mid N,\, \ell \nmid n} \mathbb{Z}_\ell \to \mathbb{Z}_n$.

Suppose $N = n_1 n_2$ with $n_1$ and $n_2$ positive integers that are relatively prime. Then any subgroup $G$ of $\mathrm{GL}_2(\mathbb{Z}_N)$ can be identified with a subgroup of $G_{n_1} \times G_{n_2}$; the projections of $G$ onto the first and second coordinate are surjective. Note that we are now in a setting where we can apply Goursat's lemma (Lemma 7.1).

8.2. **Finiteness of agreeable groups with given projections.** An advantage of working with agreeable groups is that there are only finitely many with given $\ell$-adic projections.

**Lemma 8.2.** *For each prime $\ell$, fix an open subgroup $H_\ell$ of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ satisfying $\det(H_\ell) = \mathbb{Z}_\ell^\times$ and $\mathbb{Z}_\ell^\times \cdot I \subseteq H_\ell$. Then there are only finite many agreeable subgroups $G$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ such that $G_\ell = H_\ell$ for all $\ell$.*

*Proof.* Take any agreeable subgroup $G$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ such that $G_\ell = H_\ell$ for all $\ell$. We may assume that there are only finite many primes $\ell$ with $H_\ell \neq \mathrm{GL}_2(\mathbb{Z}_\ell)$ since otherwise it would contradict that $G$ is open in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. Let $N$ be the product of primes $\ell$ for which $\ell \leq 3$ or $H_\ell \neq \mathrm{GL}_2(\mathbb{Z}_\ell)$.

For a group $H$ and an integer $n \geq 0$, let $H^{(n)}$ be the group obtained from $H$ by taking commutator subgroups $n$ times, i.e., $H^{(0)} := H$ and $H^{(n)} := [H^{(n-1)}, H^{(n-1)}]$ for $n \geq 1$. Define

$B := G^{(4)}$; it is an open subgroup of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ since $G$ is open in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, cf. Lemma 7.10. We have a natural inclusion

$$B \subseteq \prod_\ell H_\ell^{(4)}$$

so that the projection map $B \to B_\ell = (G_\ell)^{(4)} = H_\ell^{(4)}$ is surjective for all $\ell$.

Suppose that $B = \prod_\ell H_\ell^{(4)}$. The primes dividing the level of $B \subseteq \mathrm{SL}_2(\widehat{\mathbb{Z}})$ divide $N$ since $H_\ell^{(4)} = \mathrm{SL}_2(\mathbb{Z}_\ell)^{(4)} = \mathrm{SL}_2(\mathbb{Z}_\ell)$ for $\ell \nmid N$, where we have used Lemma 7.7(i). Since $B \subseteq [G, G]$ and $G$ is agreeable, we find that the primes dividing the level of $G$ divide $N$ as well. Therefore, we have an inclusion

$$W := \prod_{\ell \mid N} (\mathbb{Z}_\ell^\times \cdot H_\ell^{(4)}) \times \prod_{\ell \nmid N} \mathrm{GL}_2(\mathbb{Z}_\ell) \subseteq G.$$

Since $W$ is an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, $G$ is one of the finitely many groups that lies between $W$ and $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

Now suppose that $B \neq \prod_\ell H_\ell^{(4)}$. To finish the proof, it suffices to obtain a contradiction. By Goursat's lemma, we find that there is a finite simple group that is isomorphic to the quotient of $H_\ell^{(4)}$ for two distinct primes $\ell$. For $\ell \nmid N$, we have $H_\ell^{(4)} = \mathrm{SL}_2(\mathbb{Z}_\ell)$ by Lemma 7.7(i) and its only simple quotient is isomorphic to $\mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm I\}$.

For $\ell \mid N$, we claim that $H_\ell^{(4)}$ is pro-$\ell$ and hence every simple quotient is isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$. By Lemma 7.11, the group $H_\ell \subseteq \mathrm{GL}_2(\mathbb{Z}_\ell)$ is prosolvable. So to verify the claim, it suffices to prove that $M^{(4)} = 1$ for any solvable subgroup $M \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. For $\ell \in \{2, 3\}$ this holds since a direct computation shows that $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})^{(4)} = 1$. Now assume $\ell \geq 5$. For a description of the subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, see §2 of [Ser72]. If $M$ is contained in the normalizer of a Cartan subgroup or a Borel subgroups, we have $M^{(2)} = 1$. The remaining possibility is that the image of $M$ in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})/((\mathbb{Z}/\ell\mathbb{Z})^\times \cdot I)$ is isomorphic to a subgroup of $\mathfrak{S}_4$. So $M^{(4)} = 1$ since $\mathfrak{S}_4^{(3)} = 1$. So we have proved that there is no simple group that is isomorphic to quotients of $H_\ell^{(4)}$ for two distinct primes $\ell$; this is the desired contradiction. □

8.3. **Agreeable closure.** Fix an open subgroup $G$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ that satisfies $\det(G) = \widehat{\mathbb{Z}}^\times$. Let $N$ be the product of primes that divide the level of $[G, G] \subseteq \mathrm{SL}_2(\widehat{\mathbb{Z}})$. Define the subgroup

$$\mathcal{G} := (\mathbb{Z}_N^\times \cdot G_N) \times \prod_{\ell \nmid N} \mathrm{GL}_2(\mathbb{Z}_\ell) \tag{8.1}$$

of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. The rest of this section is devoted to showing that $\mathcal{G}$ is the agreeable group satisfying the properties in Proposition 8.1.

We clearly have $G \subseteq \mathcal{G}$ and $\widehat{\mathbb{Z}}^\times \cdot I \subseteq \mathcal{G}$. The group $\mathcal{G}$ is open in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ with full determinant since $G$ has these properties. The integer $N$ is even since the commutator subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ has level 2 in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ by Lemma 7.7(vi). The commutator subgroups of $\mathbb{Z}_N^\times \cdot G_N$ and $G_N$ agree, and $\mathrm{GL}_2(\mathbb{Z}_\ell)$ has commutator subgroup $\mathrm{SL}_2(\mathbb{Z}_\ell)$ for all $\ell \nmid N$ by Lemma 7.7(iv). Therefore,

$$[\mathcal{G}, \mathcal{G}] = [G_N, G_N] \times \prod_{\ell \nmid N} \mathrm{SL}_2(\mathbb{Z}_\ell) = [G, G],$$

where the last equality uses that $N$ is the product of primes that divide the level of $[G, G]$. In particular, $G$ is a normal subgroup of $\mathcal{G}$ with $\mathcal{G}/G$ abelian.

**Lemma 8.3.**

(i) *For an odd prime $\ell$, we have $G_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$ if and only if $\mathcal{G}_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$.*

(ii) *Suppose that* 3 *divides* $N$ *and* $\mathcal{G}_3 = \mathrm{GL}_2(\mathbb{Z}_3)$. *Then there is a surjective homomorphism* $\psi\colon \mathcal{G}_{N/3} \to \mathfrak{S}_3$ *such that*

$$\mathcal{G}_N \subseteq \{(a,b) \in \mathrm{GL}_2(\mathbb{Z}_3) \times \mathcal{G}_{N/3} : \varphi_3(a) = \psi(b)\},$$

*with* $\varphi_3$ *as in §7.5.*

(iii) *The levels of* $[\mathcal{G},\mathcal{G}]$ *and* $\mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ *in* $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ *and the level of* $\mathcal{G}$ *in* $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ *have the same odd prime divisors as* $N$.

*Proof.* We first prove (i). If $G_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$, then we have $\mathcal{G}_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$ by the inclusion $G_\ell \subseteq \mathcal{G}_\ell$. We now may assume that $\mathcal{G}_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$. Since $\mathbb{Z}_\ell^\times \cdot G_\ell \supseteq \mathcal{G}_\ell$, we have $G_\ell \supseteq [G_\ell, G_\ell] \supseteq [\mathcal{G}_\ell, \mathcal{G}_\ell] = [\mathrm{GL}_2(\mathbb{Z}_\ell), \mathrm{GL}_2(\mathbb{Z}_\ell)]$. Since $\ell$ is odd, we have $G_\ell \supseteq \mathrm{SL}_2(\mathbb{Z}_\ell)$ by Lemma 7.7(iv) and hence $G_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$ since $G$ has full determinant.

We now prove (ii). Assume that 3 divides $N$ and $\mathcal{G}_3 = \mathrm{GL}_2(\mathbb{Z}_3)$. Set $m := N/3$. We can identify $\mathcal{G}_N$ with a proper subgroup of $\mathrm{GL}_2(\mathbb{Z}_3) \times \mathcal{G}_m$ so that the projection maps $\mathcal{G}_N \to \mathrm{GL}_2(\mathbb{Z}_3)$ and $\mathcal{G}_N \to \mathcal{G}_m$ are surjective. Let $B$ be the subgroup of $\mathrm{GL}_2(\mathbb{Z}_3)$ for which $B \times \{I\}$ is the kernel of $\mathcal{G} \to \mathcal{G}_m$. The group $B$ is open and normal in $\mathrm{GL}_2(\mathbb{Z}_3)$. By Goursat's lemma, there is a surjective homomorphism $\psi'\colon \mathcal{G}_m \to \mathrm{GL}_2(\mathbb{Z}_3)/B$ such that

$$\mathcal{G}_N = \{(a,b) \in \mathrm{GL}_2(\mathbb{Z}_3) \times \mathcal{G}_m : aB = \psi'(b)\}.$$

Suppose that $B \supseteq \mathrm{SL}_2(\mathbb{Z}_3)$. Since $B$ contains the scalar matrices $\mathbb{Z}_3^\times \cdot I$, we deduce that $B \supseteq \mathbb{Z}_3^\times \cdot \mathrm{SL}_2(\mathbb{Z}_3) := W$. The group $W$ is the index 2 subgroup of $\mathrm{GL}_2(\mathbb{Z}_3)$ consisting of matrices whose determinant is a square in $\mathbb{Z}_3^\times$. Therefore, $\mathcal{G}_3/B$ is cyclic of order 1 or 2. Fix an element $c \in \mathcal{G}_m$ that generates $\mathcal{G}_m/\ker(\psi')$. Take any $a, b \in \mathcal{G}_3 = \mathrm{GL}_2(\mathbb{Z}_3)$. There are integers $i, j \in \{0,1\}$ such that $(a, c^i)$ and $(b, c^j)$ lie in $\mathcal{G}_N \subseteq \mathcal{G}_3 \times \mathcal{G}_m$. Taking the commutator of these two elements, we find that $(aba^{-1}b^{-1}, I) \in [\mathcal{G}_N, \mathcal{G}_N] = [G_N, G_N]$. Since the commutator subgroup of $\mathrm{GL}_2(\mathbb{Z}_3)$ is $\mathrm{SL}_2(\mathbb{Z}_3)$ by Lemma 7.7(iv), we deduce that $[G_N, G_N]$ equals $\mathrm{SL}_2(\mathbb{Z}_3) \times [G_m, G_m]$. However, this contradicts that 3 divides $N$. Therefore, $B \not\supseteq \mathrm{SL}_2(\mathbb{Z}_3)$.

Since $B \not\supseteq \mathrm{SL}_2(\mathbb{Z}_3)$, Lemma 7.13 implies that $\varphi_3(B) = 1$ and we thus have a surjective homomorphism $\varphi_3\colon \mathrm{GL}_2(\mathbb{Z}_3)/B \to \mathfrak{S}_3$. Let $\psi\colon \mathcal{G}_m \to \mathfrak{S}_3$ be the surjective homomorphism obtained by composing $\psi'$ and $\varphi_3$. We have

$$\mathcal{G}_N \subseteq \{(a,b) \in \mathrm{GL}_2(\mathbb{Z}_3) \times \mathcal{G}_m : \varphi_3(a) = \psi(b)\}.$$

This completes the proof of (ii).

Since $[G,G] = [\mathcal{G},\mathcal{G}]$, part (iii) is immediate for the group $[\mathcal{G},\mathcal{G}]$ from the definition of $N$. From its construction, the level of $\mathcal{G}$ cannot be divisible by primes $\ell \nmid N$. Since the level of $\mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ divides the level of $\mathcal{G}$, it suffices to prove (iii) for the group $\mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$.

For a prime $\ell \geq 5$, Lemmas 7.12 and 8.3(i) imply that $\ell$ divides $N$ if and only if $\mathcal{G}_\ell \neq \mathrm{GL}_2(\mathbb{Z}_\ell)$. So the integer $N$ and the level of $\mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ have the same prime divisors $\ell \geq 5$ by Lemma 7.12. It thus remains to prove (iii) for the group $\mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ and the prime $\ell = 3$.

If $3 \nmid N$, then from the definition of $\mathcal{G}$ we find that the level of $\mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ is not divisible by 3. So we may assume that 3 divides $N$; we need to prove that 3 also divides the level of $\mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$.

Suppose that $\mathcal{G}_3 \neq \mathrm{GL}_2(\mathbb{Z}_3)$. We have $(\mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}))_3 \subseteq \mathcal{G}_3 \cap \mathrm{SL}_2(\mathbb{Z}_3) \subsetneq \mathrm{SL}_2(\mathbb{Z}_3)$ since $\mathcal{G}_3$ has full determinant. This shows that $\mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ has level divisible by 3.

Finally suppose that 3 divides $N$ and $\mathcal{G}_3 = \mathrm{GL}_2(\mathbb{Z}_3)$. So there is a surjective homomorphism $\psi\colon \mathcal{G}_{N/3} \to \mathfrak{S}_3$ as in (ii). We thus have

$$(\mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}))_N = \mathcal{G}_N \cap \mathrm{SL}_2(\mathbb{Z}_N) \subseteq \{(a,b) \in \mathrm{SL}_2(\mathbb{Z}_3) \times (\mathcal{G}_{N/3} \cap \mathrm{SL}_2(\mathbb{Z}_{N/3})) : \varphi_3(a) = \psi(b)\}.$$

Since $\varphi_3(\mathrm{SL}_2(\mathbb{Z}_3)) = \mathfrak{A}_3$, we deduce that $\mathcal{G}_N \cap \mathrm{SL}_2(\mathbb{Z}_N)$ is a proper subgroup of $\mathrm{SL}_2(\mathbb{Z}_N)$ whose level is divisible by 3. Therefore, 3 divides the level of $\mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. □

*Proof of Proposition 8.1.* We have already show that the group $\mathcal{G}$ defined by (8.1) contains $G$ and has the same commutator subgroup. We have already observed that $\mathcal{G}$ is open in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, contains the scalars $\widehat{\mathbb{Z}}^\times \cdot I$ and satisfies $\det(\mathcal{G}) = \widehat{\mathbb{Z}}^\times$. Lemma 8.3(iii) says that the levels of $\mathcal{G}$ and $[\mathcal{G}, \mathcal{G}]$ have the same odd prime divisors. Therefore, $\mathcal{G}$ is agreeable.

Now take any agreeable group $H \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ that satisfies $G \subseteq H$. We have $[G, G] \subseteq [H, H]$, so the primes that divide the level of $[H, H]$ must also divide $N$. Since $N$ is even and $H$ is agreeable, the primes dividing the level of $H$ all divide $N$. Therefore, $H = H_N \times \prod_{\ell \nmid N} \mathrm{GL}_2(\mathbb{Z}_\ell)$. Since $G$ and $\widehat{\mathbb{Z}}^\times \cdot I$ are subgroups of $H$, we have $\mathbb{Z}_N^\times \cdot G_N \subseteq H_N$. Therefore, $\mathcal{G} \subseteq H$ from our definition of $\mathcal{G}$. This proves that $\mathcal{G}$ is the minimal agreeable group, with respect to inclusion, that contains $G$. □

8.4. **Maximal agreeable subgroups.** Fix an agreeable subgroup $\mathcal{G}$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. Amongst the proper agreeable subgroups $G$ of $\mathcal{G}$ that satisfy $G_\ell = \mathcal{G}_\ell$ for all primes $\ell$, we define $\mathscr{M}(\mathcal{G})$ to be the set of those that are maximal with respect to inclusion. The set $\mathscr{M}(\mathcal{G})$ is finite by Lemma 8.2.

In this section, we give information about the groups in $\mathscr{M}(\mathcal{G})$ and explain how they can be computed. The results are straightforward but a little tedious due to the annoying nature of the primes 2 and 3. Let $\varphi_3 \colon \mathrm{GL}_2(\mathbb{Z}_3) \to \mathfrak{S}_3$ be the surjective homomorphism from §7.5.

**Lemma 8.4.** *Take any group $G \in \mathscr{M}(\mathcal{G})$. Let $M$ and $N$ be the product of the primes that divide the level of $G$ and $\mathcal{G}$, respectively.*

(i) *The integers $M$ and $N$ have the same prime divisors $\ell \geq 5$ and $M$ is divisible by $N$. In particular, we have $M \in \{N, 2N, 3N, 6N\}$.*

(ii) *Suppose $M = 2N$. Then there are surjective homomorphisms $\alpha \colon \mathrm{GL}_2(\mathbb{Z}_2) \to \{\pm 1\}$ and $\beta \colon \mathcal{G}_N \to \{\pm 1\}$ such that*

$$G_M = \{(a, b) \in \mathrm{GL}_2(\mathbb{Z}_2) \times \mathcal{G}_N : \alpha(a) = \beta(b)\}.$$

*The level of $G$ is 2, 4 or 8 times the level of $\mathcal{G}$.*

(iii) *Suppose $M = 3N$. Then there is a surjective homomorphism $\psi \colon \mathcal{G}_N \to \mathfrak{S}_3$ such that*

$$G_M = \{(a, b) \in \mathrm{GL}_2(\mathbb{Z}_3) \times \mathcal{G}_N : \varphi_3(a) = \psi(b)\}.$$

*The level of $G$ is 3 times the level of $\mathcal{G}$.*

(iv) *Suppose $M = 6N$. Then there is a surjective homomorphism $\psi \colon \mathrm{GL}_2(\mathbb{Z}_2) \to \mathfrak{S}_3$ such that*

$$G_M = \{(a, b) \in \mathrm{GL}_2(\mathbb{Z}_2) \times \mathrm{GL}_2(\mathbb{Z}_3) : \psi(a) = \varphi_3(b)\} \times \mathcal{G}_N.$$

*The level of $G$ is 6 times the level of $\mathcal{G}$.*

*Proof.* Since $G_\ell = \mathcal{G}_\ell$ for all primes $\ell$, Lemma 7.12 implies that the levels of $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ and $\mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ have the same prime divisors $\ell \geq 5$. Since $G$ and $\mathcal{G}$ are both agreeable, we deduce that the levels of $G$ and $\mathcal{G}$ have the same prime divisors $\ell \geq 5$. The inclusion $G \subseteq \mathcal{G}$ implies that $N | M$. We have $M \in \{N, 2N, 3N, 6N\}$ since $M$ and $N$ are squarefree. This proves (i).

Now suppose that $M = 2N$ and hence $N$ is odd.

We claim that $G_N = \mathcal{G}_N$. Define $W := G_N \times \prod_{\ell \nmid N} \mathrm{GL}_2(\mathbb{Z}_\ell)$. We have inclusions $G \subseteq W \subseteq \mathcal{G}$ since $G \subseteq \mathcal{G}$ and $N | M$. The group $W$ is open in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and satisfies $\det(W) = \widehat{\mathbb{Z}}^\times$ and $\widehat{\mathbb{Z}}^\times \cdot I \subseteq W$ since $G$ has these properties as well. Intersecting with $\mathrm{SL}_2(\widehat{\mathbb{Z}})$, we obtain inclusions $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) \subseteq W \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) \subseteq \mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. Since $G$ and $\mathcal{G}$ are agreeable group whose levels have the same odd primes divisors, these inclusions imply that $W$ is also agreeable. For each prime $\ell$, we have $G_\ell = \mathcal{G}_\ell$ since $G \in \mathscr{M}(\mathcal{G})$ and hence $W_\ell = \mathcal{G}_\ell$. Since $G \subseteq W \subseteq \mathcal{G}$ and $G \in \mathscr{M}(\mathcal{G})$, we have $W = G$

or $W = \mathcal{G}$. We have $W = \mathcal{G}$ since 2 divides the level of $G$ but not the level of $W$. Therefore, $G_N = W_N = \mathcal{G}_N$ as claimed.

We have $G_N = \mathcal{G}_N$ and $G_2 = \mathcal{G}_2 = \mathrm{GL}_2(\mathbb{Z}_2)$, where the last equality uses that $2 \nmid N$. So we can identify $G_M$ with a proper subgroup of $\mathrm{GL}_2(\mathbb{Z}_2) \times \mathcal{G}_N$ so that the projection maps $G \to \mathrm{GL}_2(\mathbb{Z}_2)$ and $G \to \mathcal{G}_N$ are surjective. Let $B$ be the subgroup of $\mathrm{GL}_2(\mathbb{Z}_2)$ for which $B \times \{I\}$ is the kernel of $G \to \mathcal{G}_N$. The group $B$ is open and normal in $\mathrm{GL}_2(\mathbb{Z}_2)$. By Goursat's lemma, there is a surjective homomorphism $\psi' \colon \mathcal{G}_N \to \mathrm{GL}_2(\mathbb{Z}_2)/B$ such that

$$G_M = \{(a, b) \in \mathrm{GL}_2(\mathbb{Z}_2) \times \mathcal{G}_N : aB = \psi'(b)\}.$$

We have $\mathrm{GL}_2(\mathbb{Z}_2)/B \neq 1$ since 2 divides the level of $G$. The maximal abelian quotient of $\mathrm{GL}_2(\mathbb{Z}_2)$ is pro-2 by Lemma 7.7(v), so $\mathrm{GL}_2(\mathbb{Z}_2)/B$ has a quotient isomorphic to $\{\pm 1\}$. So there are surjective homomorphisms $\alpha \colon \mathrm{GL}_2(\mathbb{Z}_2) \to \{\pm 1\}$ and $\beta \colon \mathcal{G}_N \to \{\pm 1\}$ such that

$$G_M \subseteq \{(a, b) \in \mathrm{GL}_2(\mathbb{Z}_2) \times \mathcal{G}_N : \alpha(a) = \beta(b)\} =: W_M.$$

Define $W := W_M \times \prod_{\ell \nmid M} \mathrm{GL}_2(\mathbb{Z}_\ell) \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$. We have inclusions $G \subseteq W \subsetneq \mathcal{G}$, where $W \neq \mathcal{G}$ since the level of $\mathcal{G}$ is not divisible by 2. Since $G$ and $\mathcal{G}$ are agreeable and $M = 2N$, we find that $W$ is also agreeable. We have $G = W$ since $G$ is in $\mathscr{M}(\mathcal{G})$ and hence $G_M = W_M$.

From our description of $G_M$, we find that the level of $G$ is equal to the product of the levels of $\ker \alpha$ and $\ker \beta$. The level of $\ker \beta$ is the same as the level of $\mathcal{G}_N$, and hence also $\mathcal{G}$, since $N$ is odd. So to complete the proof of (ii), it suffices to show that $\ker \alpha$ has level 2, 4 or 8. We have $\mathbb{Z}_2^\times \cdot I \subseteq \ker \alpha$ since $G$ is agreeable. Therefore, $\ker \alpha \supseteq \mathbb{Z}_2^\times \cdot [\mathrm{GL}_2(\mathbb{Z}_2), \mathrm{GL}_2(\mathbb{Z}_2)]$ and this second group has level dividing 8 by Lemmas 7.7(v) and 7.6. Since $\ker \alpha \neq 1$, it must has level 2, 4 or 8.

Now suppose that $M$ is $3N$ or $6N$, and hence $3 \nmid N$. Define $N_0 := M/3 \in \{N, 2N\}$.

We claim that $G_{N_0} = \mathcal{G}_{N_0}$. Define $W := G_{N_0} \times \prod_{\ell \nmid N_0} \mathrm{GL}_2(\mathbb{Z}_\ell)$. We have $G \subseteq W$ since $N_0 | M$. The group $W$ is open in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and satisfies $\det(W) = \widehat{\mathbb{Z}}^\times$ and $\widehat{\mathbb{Z}}^\times \cdot I \subseteq W$ since $G$ has these properties as well. Since $G \subseteq \mathcal{G}$ and $N | N_0$, we have inclusions $G \subseteq W \subseteq \mathcal{G}$ and hence also $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) \subseteq W \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. Since $G$ and $\mathcal{G}$ are agreeable, we deduce that the levels of $W$ and $W \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ have the same prime divisors $\ell \geq 5$, i.e., the odd prime that divide $N$. Since $3 \nmid N_0$, the levels of $W$ and $W \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ are not divisible by 3 and hence they have the same odd prime divisors. Therefore, $W$ is agreeable. For each prime $\ell$, we have $G_\ell = \mathcal{G}_\ell$ since $G \in \mathscr{M}(\mathcal{G})$ and hence $W_\ell = \mathcal{G}_\ell$. Since $G \subseteq W \subseteq \mathcal{G}$ and $G \in \mathscr{M}(\mathcal{G})$, we have $W = G$ or $W = \mathcal{G}$. We have $W = \mathcal{G}$ since 3 divides the level of $G$ but not the level of $W$. So $G_{N_0} = W_{N_0} = \mathcal{G}_{N_0}$ as claimed.

We have $G_3 = \mathcal{G}_3 = \mathrm{GL}_2(\mathbb{Z}_3)$ and $G_{N_0} = \mathcal{G}_{N_0}$. So we can identify $G_M$ with a proper subgroup of $\mathrm{GL}_2(\mathbb{Z}_3) \times \mathcal{G}_{N_0}$ so that the projection maps $G \to \mathrm{GL}_2(\mathbb{Z}_3)$ and $G \to \mathcal{G}_{N_0}$ are surjective. Let $B$ be the subgroup of $\mathrm{GL}_2(\mathbb{Z}_3)$ for which $B \times \{I\}$ is the kernel of $G \to \mathcal{G}_{N_0}$. The group $B$ is open and normal in $\mathrm{GL}_2(\mathbb{Z}_3)$. By Goursat's lemma, there is a surjective homomorphism $\psi' \colon \mathcal{G}_{N_0} \to \mathrm{GL}_2(\mathbb{Z}_3)/B$ such that

$$G_M = \{(a, b) \in \mathrm{GL}_2(\mathbb{Z}_3) \times \mathcal{G}_{N_0} : aB = \psi'(b)\}.$$

If $B \supseteq \mathrm{SL}_2(\mathbb{Z}_3)$, then 3 does not divide the level of $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. Since $3 | M$ and $G$ is agreeable, the level of $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ must be divisible by 3. Therefore, $B \not\supseteq \mathrm{SL}_2(\mathbb{Z}_3)$. By Lemma 7.13, we have $\varphi_3(B) = 1$. Let $\psi \colon \mathcal{G}_{N_0} \to \mathfrak{S}_3$ be the composition of $\psi'$ with $\varphi_3$. Using that $\varphi_3(B) = 1$, we deduce that

$$G_M \subseteq \{(a, b) \in \mathrm{GL}_2(\mathbb{Z}_3) \times \mathcal{G}_{N_0} : \varphi_3(a) = \psi(b)\} =: W_M.$$

Define the subgroup $W := W_M \times \prod_{\ell \nmid M} \mathrm{GL}_2(\mathbb{Z}_\ell)$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. We have inclusions $G \subseteq W \subseteq \mathcal{G}$ and hence also $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) \subseteq W \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) \subseteq \mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. Since $G$ and $\mathcal{G}$ are agreeable and their levels have the same prime divisors $\ell \geq 5$, the inclusions imply that $W$ and $W \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ have the same

prime divisors $\ell \geq 5$. Since the levels of $W$ and $W \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ are both divisible by 3, we deduce that $W$ is agreeable. Since $G \subseteq W \subseteq \mathcal{G}$ and $G \in \mathscr{M}(\mathcal{G})$, we have $W = G$ or $W = \mathcal{G}$. We have $W = G$ since 3 divides the level of $W$ but not the level of $\mathcal{G}$. So

$$G_M = W_M = \{(a, b) \in \mathrm{GL}_2(\mathbb{Z}_3) \times \mathcal{G}_{N_0} : \varphi_3(a) = \psi(b)\}.$$

Consider the special case $M = 3N$, equivalently $N_0 = N$. To prove part (iii), it remains to show that the level of $G$ is 3 times the level of $\mathcal{G}$. From our description of $G_M$, it suffices to show that the level of $\ker \psi$ is equal to the level of $\mathcal{G}_N$ (and hence also the level of $\mathcal{G}$). Let $B$ be the subgroup of $\mathcal{G}_N$ consisting of matrices that are congruent modulo the level of $\mathcal{G}$ to the identity matrix. Since $B$ is a normal subgroup of $\mathcal{G}_N$ that is the product of $p$-groups, $\psi(B)$ is a normal subgroup of $\mathfrak{S}_3$ whose $p$-Sylow subgroups are all normal. Therefore, $\psi(B) = 1$ and hence the level of $\ker \psi$ equals the level $\mathcal{G}_N$.

Finally, we are left with the special case $M = 6N$; equivalently, $N_0 = 2N$. Since 2 does not divide the level of $\mathcal{G}$, we have $\mathcal{G}_{N_0} = \mathrm{GL}_2(\mathbb{Z}_2) \times \mathcal{G}_N$. Since $\psi$ is surjective, $\psi(\mathrm{GL}_2(\mathbb{Z}_2) \times \{I\})$ and $\psi(\{I\} \times \mathcal{G}_N))$ are normal subgroup of $\mathfrak{S}_3$ that commute with each other and generate $\mathfrak{S}_3$; this can only happen if one of these groups is trivial and the other is $\mathfrak{S}_3$. From our description of $G_M$, if $\psi$ is trivial on $\mathrm{GL}_2(\mathbb{Z}_2) \times \{I\}$, then the level of $G_M$ (and also $G$) is not divisible by 2. Since $2|M$, we deduce that $\psi$ is trivial on $\{I\} \times \mathcal{G}_N$. So there is a surjective homomorphism $\psi\colon \mathrm{GL}_2(\mathbb{Z}_2) \to \mathfrak{S}_3$ such that

$$G_6 = \{(a, b) \in \mathrm{GL}_2(\mathbb{Z}_3) \times \mathrm{GL}_2(\mathbb{Z}_2) : \varphi_3(a) = \psi(b)\}$$

and $G_M = G_6 \times \mathcal{G}_N$. From this description of $G_M$, the level of $G$ is clearly 6 times the level of $\mathcal{G}$. This completes the proof of (iv). □

Lemma 8.4 gives a description of the groups $G \in \mathscr{M}(\mathcal{G})$ for which the levels of $G$ and $\mathcal{G}$ have different prime divisors (actually it gives a finite number of candidates for $G$ for which one can check directly if they are agreeable). We now want to say something about the case where the prime divisors are the *same*. Let $N$ be the product the primes that divide the level of $\mathcal{G}$.

Take any proper divisor $1 < d_1 \leq \sqrt{N}$ of $N$. Set $d_2 = N/d_1$; it is relatively prime to $d_1$ and $d_1 < d_2$. We may identify $\mathcal{G}_N$ with a subgroup of $\mathcal{G}_{d_1} \times \mathcal{G}_{d_2}$. The kernel of the projection maps $\mathcal{G}_N \to \mathcal{G}_{d_2}$ and $\mathcal{G}_N \to \mathcal{G}_{d_1}$ are of the form $B_1 \times \{I\}$ and $\{I\} \times B_2$, respectively.

Let $\mathscr{C}_{d_1}$ be the set of pairs $(C_1, C_2)$ with open subgroups $C_1 \subsetneq B_1$ and $C_2 \subsetneq B_2$ that satisfy the following conditions:

- $C_i$ is a normal subgroup of $\mathcal{G}_{d_i}$,
- $C_i$ is maximal amongst the closed normal subgroup $H$ of $\mathcal{G}_{d_i}$ that satisfy $H \subsetneq B_i$,
- $C_i$ contains the scalar matrices $\mathbb{Z}_{d_i}^{\times} \cdot I$,
- $B_1/C_1$ and $B_2/C_2$ are isomorphic abelian groups,
- $\mathcal{G}_{d_1}/C_1$ and $\mathcal{G}_{d_2}/C_2$ are isomorphic groups.

For a pair $(C_1, C_2) \in \mathscr{C}_{d_1}$, let $\mathscr{A}(C_1, C_2)$ denote an abelian group isomorphic to $B_1/C_1$ and $B_2/C_2$.

**Lemma 8.5.** *Take any group $G$ in $\mathscr{M}(\mathcal{G})$ and suppose that $N$ and the level of $G$ have the same prime divisors. Then there is a proper divisor $1 < d_1 \leq \sqrt{N}$ of $N$ and a pair $(C_1, C_2) \in \mathscr{C}_{d_1}$ such that*

$$C_1 \times C_2 \subseteq G_N \subsetneq \mathcal{G}_N$$

*and $[\mathcal{G} : G] = |\mathscr{A}(C_1, C_2)|$.*

*Proof.* We have $G = G_N \times \prod_{\ell \nmid N} \mathrm{GL}_2(\mathbb{Z}_\ell)$ and $\mathcal{G} = \mathcal{G}_N \times \prod_{\ell \nmid N} \mathrm{GL}_2(\mathbb{Z}_\ell)$ by our assumption on the level of $G$. Therefore, $G_N \subsetneq \mathcal{G}_N$ since $G \subsetneq \mathcal{G}$ . In particular, $[\mathcal{G} : G] = [\mathcal{G}_N : G_N]$.

Let $n \geq 1$ be the smallest divisor of $N$ for which $G_n \subsetneq \mathcal{G}_n$. The integer $n$ is composite since $G_\ell = \mathcal{G}_\ell$ for all primes $\ell | N$. Choose a proper divisor $1 < d_1 \leq \sqrt{n}$ of $n$ and set $d_2 = N/d_1$. By

the minimality of $n$, we have $G_{d_1} = \mathcal{G}_{d_1}$ and $G_{n/d_1} = \mathcal{G}_{n/d_1}$. Let $G'$ be the inverse image of $G_n$ under the projection map $\mathcal{G} \to \mathcal{G}_n$. For any prime $\ell$, we have $G_\ell \subseteq G'_\ell \subseteq \mathcal{G}_\ell$ and hence $G'_\ell = \mathcal{G}_\ell$. We have $G \subseteq G' \subsetneq \mathcal{G}$ and hence the level of $G'$ has the same prime divisors as $N$. Since $G$ and $\mathcal{G}$ are agreeable, the inclusions $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) \subseteq G' \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) \subseteq \mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ imply that the odd primes dividing the level of $G' \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ are the same as those that divide $N$. Therefore, $G'$ is agreeable. We must have $G' = G$ since $G \in \mathscr{M}(\mathcal{G})$. Therefore, $G_{d_1} = \mathcal{G}_{d_1}$ and $G_{d_2} = \mathcal{G}_{d_2}$ where $N = d_1 d_2$ with $1 < d_1 \leq \sqrt{n} \leq \sqrt{N}$.

We may identify $G_N$ and $\mathcal{G}_N$ with subgroups of $\mathcal{G}_{d_1} \times \mathcal{G}_{d_2}$. The kernel of the projection maps $G_N \to G_{d_2} = \mathcal{G}_{d_2}$ and $G_N \to G_{d_1} = \mathcal{G}_{d_1}$ are of the form $C_1 \times \{I\}$ and $\{I\} \times C_2$, respectively, where $C_i$ is a normal subgroup of $\mathcal{G}_{d_i}$. By Goursat's lemma, the image of the natural homomorphism

$$G_N/(C_1 \times C_2) \hookrightarrow (\mathcal{G}_{d_1} \times \mathcal{G}_{d_2})/(C_1 \times C_2) = \mathcal{G}_{d_1}/C_1 \times \mathcal{G}_{d_2}/C_2$$

is the graph of an isomorphism $f \colon \mathcal{G}_{d_1}/C_1 \xrightarrow{\sim} \mathcal{G}_{d_2}/C_2$.

The kernel of the projection maps $\mathcal{G}_N \to \mathcal{G}_{d_2}$ and $\mathcal{G}_N \to \mathcal{G}_{d_1}$ are of the form $B_1 \times \{I\}$ and $\{I\} \times B_2$, respectively, where $B_i$ is a normal subgroup of $\mathcal{G}_{d_i}$. By Goursat's lemma, the image of the natural homomorphism

$$\mathcal{G}_N/(B_1 \times B_2) \hookrightarrow (\mathcal{G}_{d_1} \times \mathcal{G}_{d_2})/(B_1 \times B_2) = \mathcal{G}_{d_1}/B_1 \times \mathcal{G}_{d_2}/B_2$$

is the graph of an isomorphism $\overline{f} \colon \mathcal{G}_{d_1}/B_1 \xrightarrow{\sim} \mathcal{G}_{d_2}/B_2$. Using that $G_N \subseteq \mathcal{G}_N$, we find that $C_i \subseteq B_i$ and that $f$ induces $\overline{f}$, i.e, composing $f$ with the quotient map $\mathcal{G}_{d_2}/C_2 \to \mathcal{G}_{d_2}/B_2$ gives a homomorphism that factors through $\overline{f}$. In particular, $B_1/C_1$ and $B_2/C_2$ are isomorphic.

For a fixed $i \in \{1,2\}$, take any normal subgroup $D_i$ of $\mathcal{G}_{d_i}$ satisfying $C_i \subseteq D_i \subseteq B_i$. Using the isomorphism $f$, we may assume that such a group $D_i$ exists for each $i \in \{1,2\}$ and that $f$ induces an isomorphism $D_1/C_1 \xrightarrow{\sim} D_2/C_2$. Then $W := \{(g_1, g_2) \in \mathcal{G}_{d_1} \times \mathcal{G}_{d_2} : f(g_1 D_1) = g_2 D_2\}$ satisfies $G_N \subseteq W \subseteq \mathcal{G}_N$ and $[\mathcal{G}_N : W] = [B_i : D_i]$ and $[W : G_N] = [D_i : C_i]$. The subgroup $G_N$ of $\mathcal{G}_N$ is maximal since $G$ is a maximal agreeable subgroup of $\mathcal{G}$ and $G_N \neq \mathcal{G}_N$, so $D_i = B_i$ or $D_i = C_i$. Therefore, there are no normal subgroups $D_i$ of $\mathcal{G}_{d_i}$ that satisfy $C_i \subsetneq D_i \subsetneq B_i$. By considering the special case where $D_i = C_i$, we find that $[\mathcal{G} : G] = [B_i : C_i]$. We have $C_i \neq B_i$ since $G \neq \mathcal{G}$.

Now suppose that the groups $B_i/C_i$ are nonabelian. The group $[B_i, B_i] \cdot C_i$ is a normal subgroup of $\mathcal{G}_{d_i}$ that lies between $C_i$ and $B_i$, so it is either $C_i$ or $B_i$. Since $B_i/C_i$ is nonabelian by assumption, we deduce that $[B_i, B_i] \cdot C_i = B_i$ and hence $B_i/C_i$ is a nonabelian perfect group. So there is a nonabelian simple group $S$ that is isomorphic to the quotient of an open normal subgroup of $\mathcal{G}_{p_1}$ and $\mathcal{G}_{p_2}$ for some prime $p_1 | d_1$ and $p_2 | d_2$. Since $p_1 \neq p_2$, Lemma 7.11 implies that $\mathrm{SL}_2(\mathbb{F}_{p_1})/\{\pm I\}$ and $\mathrm{SL}_2(\mathbb{F}_{p_2})/\{\pm I\}$ are isomorphic which is impossible since they have different cardinalities. So the groups $B_1/C_1$ and $B_2/C_2$ are both abelian

We have now verified that $(C_1, C_2)$ is in $\mathscr{C}_{d_1}$, $G_N \supseteq C_1 \times C_2$, and $[\mathcal{G} : G] = [\mathcal{G}_N : G_N] = [B_i : C_i] = |\mathcal{A}(C_1, C_2)|$. □

8.4.1. *Computing $\mathscr{M}(\mathcal{G})$.* Fix an agreeable subgroup $\mathcal{G}$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. We now explain how to compute the groups in the set $\mathscr{M}(\mathcal{G})$. We assume that $\mathcal{G}$ is given explicitly by its level and generators of its image modulo its level. Let $N$ be the product of the primes that divide the level of $\mathcal{G}$.

Take any proper divisor $1 < d_1 \leq \sqrt{N}$ of $N$ and set $d_2 = N/d_1$. From $\mathcal{G}$, we can compute the corresponding subgroups $B_1 \subseteq \mathcal{G}_{d_1}$ and $B_2 \subseteq \mathcal{G}_{d_2}$. The group $\mathbb{Z}_{d_i}^\times \cdot [B_i, B_i]$ is open in $\mathrm{GL}_2(\mathbb{Z}_{d_i})$, normal in $\mathcal{G}_{d_i}$ and is computable using §7.3.1 and Lemma 7.6. For any pair $(C_1, C_2) \in \mathscr{C}_{d_1}$, we have

$$\mathbb{Z}_{d_i}^\times \cdot [B_i, B_i] \subseteq C_i \subsetneq B_i \tag{8.2}$$

for $i \in \{1,2\}$ since $B_i/C_i$ is abelian and $C_i$ contains the scalar matrices.

We can compute the finite number of pairs of groups $(C_1, C_2)$ that satisfy (8.2). The group $C_i$ contains the scalars $\mathbb{Z}_{d_i}^\times$. The group $C_i$ is normal in $B_i$ and $B_i/C_i$ is abelian since $[B_i, B_i] \subseteq C_i$. For each pair, we can determine whether $(C_1, C_2)$ lies in $\mathscr{C}_{d_i}$. So we can thus compute the set $\mathscr{C}_{d_i}$. For each pair $(C_1, C_2) \in \mathscr{C}_{d_i}$, we can compute the groups $G$ satisfying $\mathcal{G} \supseteq G \supseteq C_1 \times C_2$ and $[\mathcal{G} : G] = |\mathcal{A}(C_1, C_2)|$, and determine which lie in $\mathscr{M}(\mathcal{G})$.

By varying over all proper divisors $1 < d_1 \leq \sqrt{N}$ of $N$, Lemma 8.5 says that the above method will find all the groups $G$ in $\mathscr{M}(\mathcal{G})$ for which the levels of $G$ and $\mathcal{G}$ have the same prime divisors.

To compute the $G \in \mathscr{M}(\mathcal{G})$ for which the levels of $G$ and $\mathcal{G}$ have different prime divisors, we can check the finite number of possible groups $G$ arising from parts (ii), (iii) and (iv) of Lemma 8.4.

## 9. Constructing agreeable groups

The goal of this section is to prove Theorem 1.9 and to explain how to construct all the relevant groups and modular curves. Set $\mathcal{L} := \{2, 3, 5, 7, 11, 13, 17, 37\}$.

9.1. **$\ell$-adic case.** Fix any prime $\ell \in \mathcal{L}$. We want to construct an analogue of the set $\mathscr{A}$ in Theorem 1.9 when we restrict to groups whose level is a power of $\ell$. More precisely, we want a finite set $\mathscr{S}_\ell$ of agreeable subgroups that are pairwise non-conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and satisfy the following conditions:

- For any group $\mathcal{G} \in \mathscr{S}_\ell$, the level of $\mathcal{G}$ is a power of $\ell$.
- Let $G$ be any agreeable group whose level is a power of $\ell$ and $X_G(\mathbb{Q})$ has a non-CM point.
  - If $X_G(\mathbb{Q})$ is infinite, then $G$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to some group $\mathcal{G} \in \mathscr{S}_\ell$.
  - If $X_G(\mathbb{Q})$ is finite, then $G$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a subgroup of some $\mathcal{G} \in \mathscr{S}_\ell$ with $X_{\mathcal{G}}(\mathbb{Q})$ finite.
- If $\mathcal{G} \in \mathscr{S}_\ell$ is a group for which $X_{\mathcal{G}}(\mathbb{Q})$ is finite, then $X_G(\mathbb{Q})$ is infinite for all agreeable groups $\mathcal{G} \subsetneq G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$.
- If $\mathcal{G} \in \mathscr{S}_\ell$ is a group for which $X_{\mathcal{G}}(\mathbb{Q})$ has genus at most 1, then $X_{\mathcal{G}}(\mathbb{Q})$ has a non-CM point.

In [SZ17], there is a classification of the open subgroups $\mathcal{G}$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ for which the level of $\mathcal{G}$ is a power of $\ell$, $\det(\mathcal{G}) = \widehat{\mathbb{Z}}^\times$, $-I \in \mathcal{G}$, and $X_{\mathcal{G}}(\mathbb{Q})$ is infinite. In the recent work of Rouse, Sutherland and Zureick-Brown [RSZB22], they consider the more general problem of describing the $\ell$-adic images of elliptic curves over $\mathbb{Q}$ and they give a complete description up to a few modular curves of high genus whose rational points they cannot determine.

By combining the results from [SZ17] and [RSZB22], it is easy to produce a finite set $\mathscr{S}_\ell$ of agreeable groups that satisfy the desired properties. Note that our groups need to be open in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ with $\ell$-power level, have full determinant, and contain the scalars $\widehat{\mathbb{Z}}^\times$; the agreeable property is then immediate.

For the groups $\mathcal{G} \in \mathscr{S}_\ell$ of genus at most 1, we computed a model for $X_{\mathcal{G}}$ and the morphism $\pi_{\mathcal{G}} \colon X_{\mathcal{G}} \to \mathbb{P}^1_{\mathbb{Q}}$ to the $j$-line using the methods outlined in §5.4. For these groups $\mathcal{G}$ and a rational number $j \in \mathbb{Q}$, it is a direct computation to check whether $j = \pi_{\mathcal{G}}(P)$ for some $P \in X_{\mathcal{G}}$ (it will reduce to finding roots of polynomials in $\mathbb{Q}[x]$).

Now consider a group $\mathcal{G} \in \mathscr{S}_\ell$ with $X_{\mathcal{G}}$ having genus at least 2. In the cases where $X_{\mathcal{G}}(\mathbb{Q})$ is known in [RSZB22], they have computed the finite number of $j$-invariants of the non-CM points (if there are no non-CM points, then $\mathcal{G}$ can be removed from the set $\mathscr{A}$). In the few cases, where $X_{\mathcal{G}}(\mathbb{Q})$ is not known, we can follow the method of §11 in [RSZB22] to use Frobenius matrices to rule out rational points lying above any particular $j$-invariant $j \in \mathbb{Q}$ of a non-CM elliptic curve (or in an incredibly unlikely case, you will find an unexpected rational point on their modular curves).

9.2. **Constructions of $\mathscr{A}$.** For each prime $\ell \in \mathcal{L}$, let $\mathscr{S}_\ell$ be a set of agreeable groups as in §9.1. Let $\mathscr{S}$ be the (finite) set of subgroups of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ that are of the form $\bigcap_{\ell\in\mathcal{L}} H_\ell$ with $H_\ell \in \mathscr{S}_\ell$. Every group $G \in \mathscr{S}$ is of the form $\prod_\ell G_\ell$ where $G_\ell$ is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ that satisfies $\det(G_\ell) = \mathbb{Z}_\ell^\times$ and $\mathbb{Z}_\ell^\times \cdot I \subseteq G_\ell$ for all $\ell$, and $G_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$ for $\ell \notin \mathcal{L}$. So each group $G \in \mathscr{S}$ is agreeable and its level is not divisible by any prime $\ell \notin \mathcal{L}$.

The groups in $\mathscr{S}$ are pairwise non-conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. We define a partial ordering on the set $\mathscr{S}$ by saying that $G \preceq \mathcal{G}$ if $G$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a subgroup of $\mathcal{G}$. We now construct a subset $\mathscr{B} \subseteq \mathscr{S}$ by applying the following algorithm.

- Set $\mathscr{B} := \emptyset$ and $\mathcal{S} := \mathscr{S}$.
- Choose a maximal element $G$ of $\mathcal{S}$ with respect to $\preceq$ and remove it from the set $\mathcal{S}$.
  When $X_G$ has genus at most 1, we can determine whether the set $X_G(\mathbb{Q})$ is infinite and whether it has a non-CM point. As in §5.4, we can compute an explicit model of $X_G$ and compute its rational points. When $X_G$ has a rational point, we can also compute the morphism $\pi_G$ down to the $j$-line and then determine if $X_G(\mathbb{Q})$ has a non-CM point.
  When $X_G$ has genus at least 2, then $X_G(\mathbb{Q})$ is finite by Faltings.
- If $X_G$ has genus at least 2 or $X_G(\mathbb{Q})$ has a non-CM point, then adjoin $G$ to the set $\mathscr{B}$.
- If $X_G(\mathbb{Q})$ is finite, then remove from $\mathcal{S}$ all the elements $\mathcal{G}$ for which $\mathcal{G} \preceq G$.
- If $\mathcal{S}$ is nonempty, we go back to the second step where we chose another maximal element of $\mathcal{S}$.

The above process eventually halts since $\mathscr{S}$ is finite and when it ends we will have our desired set $\mathscr{B}$.

**Lemma 9.1.** *Let $G$ be an agreeable subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ such that $X_G(\mathbb{Q})$ has a non-CM point. Assume further that $G = \prod_\ell G_\ell$, where $G_\ell$ is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ satisfying $G_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$ for all primes $\ell \notin \mathcal{L}$.*

(i) *If $X_G(\mathbb{Q})$ is infinite, then $G$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to some group $\mathcal{G} \in \mathscr{B}$.*
(ii) *If $X_G(\mathbb{Q})$ is finite, then $G$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a subgroup of some $\mathcal{G} \in \mathscr{B}$ with $X_{\mathcal{G}}(\mathbb{Q})$ finite.*

*Proof.* For each $\ell \in \mathcal{L}$, define $H_\ell := G_\ell \times \prod_{p\neq\ell} \mathrm{GL}_2(\mathbb{Z}_p)$. The group $H_\ell$ is agreeable and $X_{H_\ell}(\mathbb{Q})$ has a non-CM point since $G \subseteq H_\ell$ and $X_G(\mathbb{Q})$ has a non-CM point.

First suppose that $X_{H_\ell}(\mathbb{Q})$ is finite for some $\ell \in \mathcal{L}$ and hence $X_G(\mathbb{Q})$ is finite. By the properties of $\mathscr{S}_\ell$, there is a group $\mathcal{G} \in \mathscr{S}_\ell$ such that $H_\ell$ is conjugate to a subgroup of $\mathcal{G}$, $X_{\mathcal{G}}(\mathbb{Q})$ is finite, and $X_{G'}(\mathbb{Q})$ is infinite for all $\mathcal{G} \subsetneq G' \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$. We have $\mathcal{G} \in \mathscr{S}$. Since $X_{G'}(\mathbb{Q})$ is infinite for all $\mathcal{G} \subsetneq G' \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$, we find that $\mathcal{G}$ is in the set $\mathscr{B}$. Therefore, $G$ is conjugate to a subgroup of $\mathcal{G} \in \mathscr{B}$ and $X_{\mathcal{G}}(\mathbb{Q})$ is finite.

For the rest of the proof, we may assume that $X_{H_\ell}(\mathbb{Q})$ is infinite for all $\ell \in \mathcal{L}$. After replacing $G$ by a conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, we may assume by the properties of the sets $\mathscr{S}_\ell$ that $H_\ell \in \mathscr{S}_\ell$ for all $\ell \in \mathcal{L}$. Therefore, $G = \cap_{\ell\in\mathcal{L}} H_\ell$ is an element of $\mathscr{S}$.

Suppose $X_G(\mathbb{Q})$ is infinite and hence $X_{\mathcal{G}}(\mathbb{Q})$ is infinite for all groups $\mathcal{G} \in \mathscr{S}$ with $G \preceq \mathcal{G}$. From our construction of $\mathscr{B}$ and $G \in \mathscr{S}$, we deduce that $G$ is an element of $\mathscr{B}$. This completes the proof of part (i).

Finally suppose that $X_G(\mathbb{Q})$ is finite. Let $\mathcal{G} \in \mathscr{S}$ be a group that is maximal, with respect to $\preceq$, amongst the groups for which $X_{\mathcal{G}}(\mathbb{Q})$ is finite and $G \preceq \mathcal{G}$ (such a group exists since $G \in \mathscr{S}$ and $X_G(\mathbb{Q})$ is finite). For every group $G' \in \mathscr{S}$ with $\mathcal{G} \preceq G'$ and $\mathcal{G} \neq G'$, $X_{G'}(\mathbb{Q})$ is infinite by the maximality of $\mathcal{G}$. From our construction of $\mathscr{B}$, we deduce that $\mathcal{G}$ is an element of $\mathscr{B}$. This completes the proof of part (ii). □

Take any group $H \in \mathscr{B}$; it is agreeable and satisfies $H = \prod_\ell H_\ell$. From $H$, we now construct a finite set $\mathscr{A}_H$ of agreeable groups by applying the following algorithm.

- Set $\mathscr{A}_H := \{H\}$ and $\mathcal{S} := \{H\}$.
- Choose a group $\mathcal{G}$ in $\mathcal{S}$ with minimal index $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathcal{G}]$ and remove it from the set $\mathcal{S}$.
- We compute the set $\mathscr{M}(\mathcal{G})$, with notation as in §8.4, using the method outlined in §8.4.1.
- We now let $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ vary over the elements of $\mathscr{M}(\mathcal{G})$.

  If $X_G$ has genus at least 2 and $G$ is not conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a group in $\mathscr{A}_H$, then we adjoin $G$ to the set $\mathscr{A}_H$.

  Now suppose that $X_G$ has genus at most 1 and $G$ is not conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a group in $\mathscr{A}_H$. As in §5.4, we can compute an explicit model of $X_G$ and compute its rational points. When $X_G$ has a rational point, we can also compute the morphism from $X_G$ to $X_H$ and then down to the $j$-line. We can then determine if $X_G(\mathbb{Q})$ has a non-CM point. If $X_G(\mathbb{Q})$ has infinitely many points, then we adjoin $G$ to the sets $\mathscr{A}_H$ and $\mathcal{S}$. If $X_G(\mathbb{Q})$ has finitely many points and a non-CM point, then we adjoin $G$ to the set $\mathscr{A}_H$.
- If $\mathcal{S}$ is nonempty, we go back to the second step where we chose another group $\mathcal{G}$ in $\mathcal{S}$.

For each $\mathcal{G} \in \mathscr{A}_H$, we will have $\mathcal{G}_\ell = H_\ell$ for all primes $\ell$. The above process halts by Lemma 8.2. Finally, define the (finite) set

$$\mathscr{A} := \bigcup_{H \in \mathscr{B}} \mathscr{A}_H$$

of agreeable subgroups of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. From our descriptions of the sets $\mathscr{B}$ and $\mathscr{A}_H$, we have explained how the set $\mathscr{A}$ is computable.

For any group $\mathcal{G} \in \mathscr{A}$, the level of $\mathcal{G}$ is divisible only by primes in $\mathcal{L}$. For each $\mathcal{G} \in \mathscr{A}$ with $X_\mathcal{G}$ having genus at most 1, $X_\mathcal{G}(\mathbb{Q})$ has a non-CM point by construction; moreover, we will have found a model of $X_\mathcal{G}$ and the morphism from $X_\mathcal{G}$ to the $j$-line.

**Lemma 9.2.** *Take any agreeable group $G$ for which $X_G(\mathbb{Q})$ has a non-CM point. Assume that the level of $G$ is not divisible by any prime $\ell \notin \mathcal{L}$.*

(i) *If $X_G(\mathbb{Q})$ is infinite, then $G$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a group $\mathcal{G} \in \mathscr{A}$.*
(ii) *If $X_G(\mathbb{Q})$ is finite, then $G$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a subgroup of some group $\mathcal{G} \in \mathscr{A}$ with $X_\mathcal{G}(\mathbb{Q})$ finite.*

*Proof.* Define $H := \prod_\ell G_\ell$, where $G_\ell \subseteq \mathrm{GL}_2(\mathbb{Z}_\ell)$ is the $\ell$-adic projection of $G$; it is an agreeable group whose level is only divisible by primes in $\mathcal{L}$. Since $G \subseteq H$, we deduce that $X_H(\mathbb{Q})$ has a non-CM point.

Suppose that $X_H(\mathbb{Q})$ is finite. By Lemma 9.1(ii), $H$ is conjugate to a subgroup of some group $\mathcal{G} \in \mathscr{B}$ with $X_\mathcal{G}(\mathbb{Q})$ finite. In particular, $X_G(\mathbb{Q})$ is finite and $G$ is conjugate to a subgroup of $\mathcal{G}$. Part (ii) in this case follows since $\mathcal{G} \in \mathscr{B}$ and hence $\mathcal{G} \in \mathscr{A}_\mathcal{G} \subseteq \mathscr{A}$.

We may now assume that $X_H(\mathbb{Q})$ is infinite. After first replacing $G$ by a conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, we may assume by Lemma 9.1(i) that $H \in \mathscr{B}$. Let $\mathcal{G} \in \mathscr{A}_H$ be a group with maximal index in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ for which $G$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a subgroup of $\mathcal{G}$ (it exists since $G \subseteq H$ and $H \in \mathscr{A}_H$). If $G$ is conjugate to $\mathcal{G}$ in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, then the lemma is immediate since $\mathcal{G} \in \mathscr{A}_H \subseteq \mathscr{A}$. If $X_\mathcal{G}(\mathbb{Q})$ is finite, and hence $X_G(\mathbb{Q})$ is finite as well, then the lemma also holds.

Finally, after replacing $G$ by a conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, we are left to consider the case where $G$ is a proper subgroup of $\mathcal{G}$ and $X_\mathcal{G}(\mathbb{Q})$ is infinite. Choose an agreeable group $M$ that is maximal amongst those that satisfy $G \subseteq M \subsetneq \mathcal{G}$. Since $\mathcal{G} \in \mathscr{A}_H$, we have $G_\ell = \mathcal{G}_\ell$ and hence $M_\ell = \mathcal{G}_\ell$ for all primes $\ell$, where $\mathcal{G}_\ell$ and $M_\ell$ are the $\ell$-adic projections of $\mathcal{G}$ and $M$, respectively. Since $M$ is a maximal agreeable subgroup of $\mathcal{G}$, we have $M \in \mathscr{M}(\mathcal{G})$. Since $\mathcal{G} \in \mathscr{A}_H$ and $X_\mathcal{G}(\mathbb{Q})$ is infinite,

we have $M \in \mathscr{A}_H \subseteq \mathscr{A}$. Since $G \subseteq M \subsetneq \mathcal{G}$, this contradicts the maximality in our choice of $\mathcal{G}$. Therefore, this final case does not occur. □

9.3. **Proof of Theorem 1.9.** Let $\mathscr{A}$ be the finite set of agreeable groups constructed in §9.2.

By construction, our set $\mathscr{A}$ satisfies (a). The set $\mathscr{A}$ satisfies (b) by Lemma 9.2. The set $\mathscr{A}$ satisfies (d) and (e) since in our construction we computed a model of any modular curve of genus at most 1 that occurred and ignored those with no non-CM points.

For each group $\mathcal{G} \in \mathscr{A}$ for which $X_{\mathcal{G}}$ has genus at least 2, we can check whether there is a group $G \in \mathscr{A}$ that is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a proper subgroup of $\mathcal{G}$. If any such group $G$ exists, we can remove it from the set $\mathscr{A}$. Since condition (b) holds, our possibly smaller set $\mathscr{A}$ will satisfy condition (c).

The set $\mathscr{A}$ we constructed may contain distinct subgroups of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ that are conjugate. To obtain our final set, we replace $\mathscr{A}$ by a maximal subset of groups that are non-conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. This does not affect the validity of conditions (a)–(e).

It remains to explain how to implement (f). Take any group $\mathcal{G} \in \mathscr{A}$. If $X_{\mathcal{G}}$ has genus at most 1, then from (e) we have an explicit model of $X_{\mathcal{G}}$ and we have computed the map to the $j$-line. So (f) can be done directly when $X_{\mathcal{G}}$ has genus at most 1. We may now assume that $X_{\mathcal{G}}$ has genus at least 2.

As mentioned in §9.1, [RSZB22] explains how to check whether a given $j \in \mathbb{Q} - \{0, 1728\}$ is in $\pi_G(X_G(\mathbb{Q}))$ for an open subgroup $G$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ with $\det(G) = \widehat{\mathbb{Z}}^\times$ and prime power level. So we may further assume that the level of $\mathcal{G}$ is not a prime power.

For each prime $\ell$, let $\mathcal{G}_\ell$ be the $\ell$-adic projection of $\mathcal{G}$. Define $H := \prod_\ell \mathcal{G}_\ell \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$; it is agreeable and $\mathcal{G} \subseteq H$. Suppose that $\mathcal{G} = H$, i.e., $\mathcal{G}$ has no "entanglements". Take any $j \in \mathbb{Q} - \{0, 1728\}$. Using Proposition 6.4 and $\mathcal{G} = H$, we have $j \in \pi_{\mathcal{G}}(X_{\mathcal{G}}(\mathbb{Q}))$ if and only if $j \in \pi_{\mathcal{G}'}(X_{\mathcal{G}'}(\mathbb{Q}))$ with $\mathcal{G}' := \mathcal{G}_\ell \times \prod_{p \neq \ell} \mathrm{GL}_2(\mathbb{Z}_p)$ for all $\ell$ dividing the level of $\mathcal{G}$. So in this case, (f) reduces to the prime power case covered in [RSZB22].

We are left to consider the case where also $\mathcal{G}$ is a proper subgroup of $H = \prod_\ell \mathcal{G}_\ell$. Choose an agreeable group $\mathcal{G} \subsetneq G \subseteq H$ with $[G : \mathcal{G}]$ minimal. Since $X_{\mathcal{G}}$ has genus at least 2, and hence $X_{\mathcal{G}}(\mathbb{Q})$ is finite by Faltings, (c) implies that $X_G(\mathbb{Q})$ is infinite. By (b), $G$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a group in $\mathscr{A}$. After replacing $\mathcal{G}$ with a conjugate, we may assume without loss of generality that $G \in \mathscr{A}$.

We are now in the setting of §5.5. So we can compute a singular model of $X_{\mathcal{G}}$ and, with respect to this model, we have the natural morphism $\pi\colon X_{\mathcal{G}} \to X_G$. Now take any $j \in \mathbb{Q} - \{0, 1728\}$. By (e), we have a model of $X_G$ and can compute the morphism $\pi_G\colon X_G \to \mathbb{P}^1_{\mathbb{Q}}$. So we can compute the finite set of $Q \in X_G(\mathbb{Q})$ with $\pi_G(Q) = j$. For each such $Q$, we can then compute if there are any $P \in X_{\mathcal{G}}(\mathbb{Q})$ with $\pi(P) = Q$. This gives (f) since $\pi_G \circ \pi = \pi_{\mathcal{G}}$. (To deal with any singularities we can either resolve them or compute another model of the curve with different choices.)

*Remark* 9.3. In practice, one wants to conjugate the groups in $\mathscr{A}$ so that for each $\mathcal{G} \in \mathscr{A} - \{\mathrm{GL}_2(\widehat{\mathbb{Z}})\}$, there is another group $G \in \mathscr{A}$ with $\mathcal{G} \subsetneq G$ and $[G : \mathcal{G}]$ as small as possible. We have $\pi_{\mathcal{G}} = \pi_G \circ \pi$, where $\pi\colon X_{\mathcal{G}} \to X_G$ is the natural morphism of degree $[G : \mathcal{G}]$. Repeating, we can hope to express $\pi_{\mathcal{G}}$ as the composition of morphisms of relatively small degree. Having such an expression makes it easier to compute the set of $P \in X_{\mathcal{G}}(\mathbb{Q})$ with $\pi_{\mathcal{G}}(P)$ equal to a fixed $j \in \mathbb{Q} - \{0, 1728\}$.

## 10. Finding the agreeable closure of the image of Galois

Fix a non-CM elliptic curve $E$ defined over $\mathbb{Q}$. We have defined a representation

$$\rho_E^*\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_2(\widehat{\mathbb{Z}}).$$

From Serre (Theorem 1.1), we known that the image $G_E$ of $\rho_E^*$ is an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. We have $\det(G_E) = \widehat{\mathbb{Z}}^\times$. By Proposition 8.1, there is a minimal agreeable subgroup $\mathcal{G}_E$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ for which $G_E \subseteq \mathcal{G}_E$, i.e., the agreeable closure of $G_E$. The group $G_E$, and hence also $\mathcal{G}_E$, is uniquely determined up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. In this section, we describe how to compute the group $\mathcal{G}_E$.

The hardest steps have already been completed by the proof of Theorem 1.9 in §9. Let $\mathscr{A}$ be a finite set of agreeable subgroups of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ as in Theorem 1.9. Note that the set $\mathscr{A}$ can be computed once and does not depend on the curve $E/\mathbb{Q}$.

For our algorithm, we want as input an elliptic curve $E/\mathbb{Q}$ given by a Weierstrass model with output the level $N$ of $\mathcal{G}_E$ along with a set of generators of the image of $\mathcal{G}_E$ modulo $N$. This algorithm has been implemented [Zyw22] assuming that Conjecture 1.2 holds for $E$ and that $E$ does not give rise to unknown rational points on a few explicit high genus modular curves (these conditions are verified during the algorithm). For any remaining cases, which involve only a finite number of $j$-invariants or a counterexample to Conjecture 1.2, we can compute the group $\mathcal{G}_E$ using ad hoc techniques like those in §10.2.

Once we know $\mathcal{G}_E$, we can compute the commutator subgroup $[\mathcal{G}_E, \mathcal{G}_E]$, cf. §7.3.1, which is an open subgroup of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$. By Proposition 8.1 and Lemma 2.1, we have $G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = [\mathcal{G}_E, \mathcal{G}_E]$ and

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E] = [\mathrm{SL}_2(\widehat{\mathbb{Z}}) : [\mathcal{G}_E, \mathcal{G}_E]].$$

In particular, we have an algorithm to compute the group $G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$, up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, and to compute the index $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E] = [\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(\mathrm{Gal}_{\mathbb{Q}})]$ occurring in Serre's open image theorem.

**Lemma 10.1.** *Let $E/\mathbb{Q}$ be a non-CM elliptic curve over $\mathbb{Q}$ for which Conjecture 1.2 holds. Then the level of $\mathcal{G}_E$ in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ is not divisible by any prime $\ell \notin \mathcal{L} := \{2, 3, 5, 7, 11, 13, 17, 37\}$.*

*Proof.* By hypothesis on $E/\mathbb{Q}$, we have $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all primes $\ell \notin \mathcal{L}$. By Lemma 7.9, we have $\rho_{E,\ell^\infty}(\mathrm{Gal}_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{Z}_\ell)$ for all primes $\ell \notin \mathcal{L}$. So for each prime $\ell \notin \mathcal{L}$, we have $\mathrm{GL}_2(\mathbb{Z}_\ell) = (G_E)_\ell \subseteq (\mathcal{G}_E)_\ell$ and hence $(\mathcal{G}_E)_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$, where $(G_E)_\ell$ and $(\mathcal{G}_E)_\ell$ are the $\ell$-adic projections of $G_E$ and $\mathcal{G}_E$, respectively. Since $\mathcal{G}_E$ is agreeable, its level is not divisible by any prime $\ell \notin \mathcal{L}$ by Lemma 7.12. □

10.1. **Finding the agreeable closure in most cases.** Throughout §10.1, we assume that $j_E \notin \pi_{\mathcal{G}}(X_{\mathcal{G}}(\mathbb{Q}))$ for all groups $\mathcal{G} \in \mathscr{A}$ for which $X_{\mathcal{G}}$ is finite. This can be verified for the given $j_E$ using Theorem 1.9(f). This excludes a finite number of $j$-invariants from consideration that we will describe how to deal with in §10.2.

We can apply the algorithm in [Zyw20b] to compute the finite set of primes $\ell > 13$ for which $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}}) \neq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. For the rest of §10.1, we shall further assume that Conjecture 1.2 holds for $E$, i.e., $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all primes $\ell > 13$ with

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

Any potential counterexample to Conjecture 1.2 can be dealt with using the methods from §10.2.

By Lemma 10.1, the level of $\mathcal{G}_E$ is not divisible by any primes $\ell \notin \mathcal{L} := \{2, 3, 5, 7, 11, 13, 17, 37\}$. Since $G_E \subseteq \mathcal{G}_E$, we know that $X_{\mathcal{G}_E}$ has a rational non-CM point; in particular, there is a $P \in X_{\mathcal{G}_E}(\mathbb{Q})$ such that $\pi_{\mathcal{G}_E}(P) = j_E$.

If $X_{\mathcal{G}_E}(\mathbb{Q})$ is finite, then $\mathcal{G}_E$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a subgroup of some $\mathcal{G} \in \mathscr{A}$ for which $X_{\mathcal{G}}(\mathbb{Q})$ is finite by Theorem 1.9(b). Therefore, $X_{\mathcal{G}_E}(\mathbb{Q})$ is infinite by our assumption on $E$. By Theorem 1.9(b), $\mathcal{G}_E$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a unique group $\mathcal{G} \in \mathscr{A}$. Since $\mathcal{G}_E$ is the agreeable

closure of $G_E$, we can characterize $\mathcal{G}$ as the group in $\mathscr{A}$ with maximal index in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ for which $j_E \in \pi_{\mathcal{G}}(X_{\mathcal{G}}(\mathbb{Q}))$. So by making use of Theorem 1.9(f), we can find $\mathcal{G}$ which gives the group $\mathcal{G}_E$ up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

10.2. **Finding the agreeable closure in exceptional cases.** Now suppose that $j_E \in \pi_{\mathcal{G}}(X_{\mathcal{G}}(\mathbb{Q}))$ for some group $\mathcal{G} \in \mathscr{A}$ with $X_{\mathcal{G}}(\mathbb{Q})$ finite. There are only finitely many $j$-invariants $j_E$ that can arise in this way but they are difficult to determine since finding rational points on high genus curves can be very challenging. In §10.2, we shall make use of the notation from §8.1.

However, we can compute the agreeable closure $\mathcal{G}_E$ for any such $E/\mathbb{Q}$ that arises. The group $\mathcal{G}_E$, up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, depends only on $j_E$. So far, we have found 81 exceptional $j$-invariants that needed to be considered specially. Any others that may arise can be dealt with in a similar manner. For simplicity, let us assume that Conjecture 1.2 holds for $E/\mathbb{Q}$; we can handle any counterexamples that occur by similar techniques.

By assumption, there is an agreeable group $\mathcal{G} \in \mathscr{A}$ such that $j_E \in \pi_{\mathcal{G}}(X_{\mathcal{G}}(\mathbb{Q}))$ and $X_{\mathcal{G}}$ has only finite many rational points. After conjugating $\rho_E^*$, we may assume that $\mathcal{G}_E \subseteq \mathcal{G}$.

We claim that we can compute the $\ell$-adic projection $(\mathcal{G}_E)_\ell$, up to conjugacy in $\mathrm{GL}_2(\mathbb{Z}_\ell)$, for all primes $\ell$. Using the explicit definition (8.1) of the agreeable closure, this is equivalent to computing $\mathbb{Z}_\ell^\times \cdot \rho_{E,\ell^\infty}^*(\mathrm{Gal}_{\mathbb{Q}})$ for all primes $\ell$. When $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ and $\ell \geq 5$, we have $\rho_{E,\ell^\infty}^*(\mathrm{Gal}_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{Z}_\ell)$ by Lemma 7.9, and hence $(\mathcal{G}_E)_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$. For the finite number of $\ell$ with $\ell \leq 3$ or $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}}) \neq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, we can compute $\rho_{E,\ell^\infty}(\mathrm{Gal}_{\mathbb{Q}})$, and hence also $(\mathcal{G}_E)_\ell$, by using the results from [RSZB22].

Using $\mathcal{G}_E \subseteq \mathcal{G}$, we can then check whether or not $(\mathcal{G}_E)_\ell = \mathcal{G}_\ell$ for all primes $\ell$. Suppose that $(\mathcal{G}_E)_\ell \subsetneq \mathcal{G}_\ell$ for some prime $\ell$. This will produce an explicit proper agreeable group $\mathcal{G}' \subsetneq \mathcal{G}$ for which $j_E \in \pi_{\mathcal{G}'}(X_{\mathcal{G}'}(\mathbb{Q}))$. We can replace $\mathcal{G}$ by $\mathcal{G}'$ and then repeat the above process. We will eventually end up with an explicit agreeable subgroup $\mathcal{G}$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ with $X_{\mathcal{G}}(\mathbb{Q})$ finite, $j_E \in \pi_{\mathcal{G}}(X_{\mathcal{G}}(\mathbb{Q}))$, and $\mathcal{G}_\ell$ and $(\mathcal{G}_E)_\ell$ conjugate in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ for all primes $\ell$.

As in §8.4, we can define $\mathscr{M}(\mathcal{G})$ to be the set of maximal proper agreeable subgroups $G$ of $\mathcal{G}$ that satisfy $G_\ell = \mathcal{G}_\ell$ for all primes $\ell$. The set $\mathscr{M}(\mathcal{G})$ is finite and computable, cf. 8.4.1.

Take any of the groups $G \in \mathscr{M}(\mathcal{G})$ up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. We want to know whether or not $j_E \in \pi_G(X_G(\mathbb{Q}))$. The direct approach is to check after first computing a model for the curve $X_G$ and the morphism $\pi_G$ to the $j$-line; this is doable using the techniques from §5. However, these computations seem excessive to deal with a single $j$-invariant $j_E$. We now explain our ad hoc computations with traces of Frobenius, which can be found in [Zyw22], that allows to verify if $j_E \in \pi_G(X_G(\mathbb{Q}))$ holds without computing any further modular curves.

Let $N$ be the level of $G$ and let $M$ be the product of $N$ with the bad primes of $E/\mathbb{Q}$. Take any prime $p \nmid M$ and let $a_p(E)$ be the trace of Frobenius of the reduction of $E$ mod $p$, i.e., $a_p(E) = p + 1 - |E(\mathbb{F}_p)|$, where we are using a model of $E$ with good reduction at $p$. The representation $\rho_{E,N}^*$ has good reduction at $p$ and $\rho_{E,N}^*(\mathrm{Frob}_p)^{-1} \in \rho_{E,N}^*(\mathrm{Gal}_{\mathbb{Q}}) \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ has trace $a_p(E)$ and determinant $p$ modulo $N$. Let $\mathcal{E}_p$ be the pair $(a_p(E), p)$ modulo $N$. Now suppose we found a prime $p \nmid M$ such that $(\mathrm{tr}(g), \det(g)) \neq \mathcal{E}_p$ for all $g$ in the image of $G$ modulo $N$. In particular, the group $\rho_{E,N}^*(\mathrm{Gal}_{\mathbb{Q}})$ contains an element that is not conjugate in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ to any element of the image of $G$ modulo $N$. Therefore, $\rho_E^*(\mathrm{Gal}_{\mathbb{Q}})$ is not conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a subgroup of $G$ and thus $j_E \notin \pi_G(X_G(\mathbb{Q}))$. So by computing $\mathcal{E}_p$ for many primes $p \nmid M$, we hope to be able to prove that $j_E \notin \pi_G(X_G(\mathbb{Q}))$.

Now suppose that after computing $\xi_p$ for many primes $p \nmid M$, we are unable to conclude that $j_E \notin \pi_G(X_G(\mathbb{Q}))$. In all the exceptional cases we considered, we then had $[\mathcal{G} : G] = 2$. The group $G$ is normal in $\mathcal{G}$ and we obtain a quadratic character

$$\chi\colon \mathrm{Gal}_{\mathbb{Q}} \xrightarrow{\rho_E^*} \mathcal{G}_E \hookrightarrow \mathcal{G} \to \mathcal{G}/G \cong \{\pm 1\}.$$

For $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$, $\chi(\sigma)$ depends only on $\rho_{E,N}^*(\sigma)$ since $G$ has level $N$. Therefore, $\chi$ is unramified at all primes $p \nmid M$. In particular, there are only finite many possible quadratic characters that could arise as $\chi$. Take any prime $p \nmid M$. If $(\mathrm{tr}(g), \det(g)) \neq \xi_p$ for all $g$ in the image of $\mathcal{G} - G$ modulo $N$, then $\chi(\mathrm{Frob}_p) = 1$.

Suppose that we are able to show that $\chi(\mathrm{Frob}_p) = 1$ for enough primes $p \nmid M$, to rule out all possibilities for the characters $\chi$ except $\chi = 1$. Since $\chi = 1$, we deduce that $\rho_E^*(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to subgroup $G$. Therefore, $j_E \in \pi_G(X_G(\mathbb{Q}))$ and we can replace $\mathcal{G}$ by $G$ and repeat the above process.

In the remaining cases, which occurred for three of our $j$-invariants, we are left with a unique $G \in \mathscr{M}(\mathcal{G})$, up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, for which we were not yet able to determine whether or not $j_E$ lies in $\pi_G(X_G(\mathbb{Q}))$. In these remaining cases, we found that for some prime $p \in \{3, 5\}$, we have $\mathcal{G}_{2p} = \mathcal{G}_2 \times \mathcal{G}_p$ and $G_{2p} \subsetneq G_2 \times G_p = \mathcal{G}_{2p}$. We computed the division polynomials for $E$ at 2 and $p$, factored them into irreducible polynomials over $\mathbb{Q}$, and computing the discriminants of these polynomials. From this information, we found a quadratic extension $K/\mathbb{Q}$ with $K \subseteq \mathbb{Q}(E[2])$, $K \subseteq \mathbb{Q}(E[p])$ and $K$ not equal to $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$. Since $\mathcal{G}_{2p} = \mathcal{G}_2 \times \mathcal{G}_p$, this proves that $\mathcal{G}$ is not the agreeable closure of $\rho_E^*(\mathrm{Gal}_{\mathbb{Q}})$. Therefore, $j_E \in \pi_G(X_G(\mathbb{Q}))$ and we can replace $\mathcal{G}$ by $G$ and repeat the above process.

In all our cases, the above arguments eventually lead to an explicit minimal agreeable group $\mathcal{G}$ with $j_E \in \pi_{\mathcal{G}}(X_{\mathcal{G}}(\mathbb{Q}))$ and hence we can take $\mathcal{G}_E = \mathcal{G}$.

## 11. Abelian quotients

Let $\mathcal{G}$ be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ satisfying $\det(\mathcal{G}) = \widehat{\mathbb{Z}}^\times$ and $-I \in \mathcal{G}$. Fix an open subgroup $G$ of $\mathcal{G}$ satisfying $\det(G) = \widehat{\mathbb{Z}}^\times$ such that $G$ is a normal subgroup of $\mathcal{G}$ with $\mathcal{G}/G$ abelian. From the openness, the abelian group $\mathcal{G}/G$ is also finite. Fix an integer $N \geq 3$ divisible by the level of $G$ and let $\overline{G}$ and $\overline{\mathcal{G}}$ be the images of $G$ and $\mathcal{G}$, respectively, in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Reduction modulo $N$ induces an isomorphism $\mathcal{G}/G \xrightarrow{\sim} \overline{\mathcal{G}}/\overline{G}$ that we will use as an identification.

### 11.1. Setup.

11.1.1. *Some representations.* With notation as in §6.3, we have a surjective homomorphism

$$\varrho := \varrho_{\mathscr{E}_{\mathcal{G}},N}^*\colon \pi_1(U_{\mathcal{G}}, \overline{\eta}) \to \overline{\mathcal{G}}$$

Recall that $\varrho$ depends on a choice of a nonzero modular form $f_0$ in $M_3(\Gamma(N), \mathbb{Q}(\zeta_N))$ and a choice of $\beta$ in a field extension of $\mathcal{F}_N$ that satisfies $\beta^2 = j \cdot f_0^2/E_6$. When $-I \notin G$, we shall further assume that $f_0$ is chosen to be a nonzero element of $M_{3,\overline{G}}$; the existence of such an $f_0$ is a consequence of Lemma 4.6. By composing $\varrho$ with the quotient map $\overline{\mathcal{G}} \to \overline{\mathcal{G}}/\overline{G} = \mathcal{G}/G$, we obtain a surjective homomorphism

$$\alpha\colon \pi_1(U_{\mathcal{G}}, \overline{\eta}) \to \mathcal{G}/G.$$

Let $\phi\colon Y \to U_{\mathcal{G}}$ be the étale cover corresponding to $\alpha$. The cover $\phi$ is Galois with Galois group $\mathcal{G}/G$. When $-I \in G$, we will have $Y = U_G$ and $\phi$ will be the natural morphism.

Now consider the representation $\rho_{\mathscr{E},N}^*\colon \mathrm{Gal}_{\mathbb{Q}(j)} \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ as in §6.2. By Lemma 6.3, $\rho_{\mathscr{E},N}^*$ is surjective and factors through an isomorphism $\mathrm{Gal}(\mathcal{F}_N(\beta)/\mathbb{Q}(j)) \xrightarrow{\sim} \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. We let $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$

act on the right of $\mathcal{F}_N(\beta)$ via $f * \rho^*_{\mathscr{E},N}(\sigma)^{-1} := \sigma(f)$ for all $f \in \mathcal{F}_N(\beta)$. By Lemma 6.3(iii), this extends our earlier right action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $\mathcal{F}_N$. Since $\beta \notin \mathcal{F}_N$, we have $\beta * (-I) = -\beta$ by Lemma 6.3(vi). Define the subfield $L := \mathcal{F}_N(\beta)^{\overline{G}}$ of $\mathcal{F}_N(\beta)$. The representations $\rho^*_{\mathscr{E},N}$ induces an isomorphism $\mathrm{Gal}(L/\mathbb{Q}(X_{\mathcal{G}})) \xrightarrow{\sim} \overline{\mathcal{G}}/\overline{G} = \mathcal{G}/G$.

Moreover, the representation $\varrho$ in §6.3 is constructed so that the specialization at the generic point of $U_G$ gives the representation $\mathrm{Gal}_{\mathbb{Q}(X_G)} \to \overline{\mathcal{G}} \subseteq \overline{\mathcal{G}} \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that is the restriction of the representation $\rho^*_{\mathscr{E},N}$. We can thus identify $L$ with the function field of $Y$ and the field extension $L/\mathbb{Q}(X_{\mathcal{G}})$ corresponds to the morphism $\phi\colon Y \to U_{\mathcal{G}}$. Note that the curve $Y$ is geometrically irreducible since $\mathbb{Q}$ is algebraically closed in $L$ by Lemma 6.3(ii) and our assumption $\det(G) = \widehat{\mathbb{Z}}^\times$.

11.1.2. *Specializations.* Take any point $u \in U_{\mathcal{G}}(\mathbb{Q})$. Specializing $\varrho$ at $u$ gives a homomorphism $\varrho_u\colon \mathrm{Gal}_{\mathbb{Q}} \to \overline{\mathcal{G}}$. The representations $\mathrm{Gal}_{\mathbb{Q}} \xrightarrow{\varrho_u} \overline{\mathcal{G}} \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and $\rho^*_{(\mathscr{E}_{\mathcal{G}})_u,N}\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ are isomorphic, where $(\mathscr{E}_{\mathcal{G}})_u$ is the elliptic curve over $\mathbb{Q}$ defined by the Weierstrass equation $y^2 = x^3 - 27j(j-1728)\cdot x + 54j(j-1728)^2$ with $j := \pi_{\mathcal{G}}(u)$. Let

$$\alpha_u\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathcal{G}/G$$

be the homomorphism that is the specialization of $\alpha$ at $u$. Equivalently, $\alpha_u$ is the composition of $\varrho_u$ with the quotient map $\overline{\mathcal{G}} \to \overline{\mathcal{G}}/\overline{G} = \mathcal{G}/G$. Since $\mathcal{G}/G$ is abelian, $\alpha_u$ is uniquely determined (while the specialization $\varrho_u$ is only uniquely determined up to conjugation by an element in $\overline{\mathcal{G}}$).

Let $\phi^{-1}(u) \subseteq Y$ be the fiber of $\phi$ over $u$. The action of $\mathcal{G}/G$ on the $\overline{\mathbb{Q}}$-points of $\phi^{-1}(u)$ is simply transitive since $\phi$ is étale. The group $\mathrm{Gal}_{\mathbb{Q}}$ acts on the $\overline{\mathbb{Q}}$-points of $\phi^{-1}(u)$ since $\phi$ and $u$ are defined over $\mathbb{Q}$. These actions of $\mathcal{G}/G$ and $\mathrm{Gal}_{\mathbb{Q}}$ commute. For a fixed $y_0 \in Y(\overline{\mathbb{Q}})$ with $\phi(y_0) = u$, we have

$$\sigma(y_0) = \alpha_u(\sigma) \cdot y_0 \tag{11.1}$$

for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$; note that this does not depend on the choice of $y_0$ since $\mathcal{G}/G$ is abelian and it commutes with the Galois action. In particular, the expression (11.1) determines $\alpha_u(\sigma)$.

11.2. **Defining $\alpha_E$ using modular curves.** Consider a non-CM elliptic curve $E/\mathbb{Q}$ for which $G_E = \rho^*_E(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a subgroup of $\mathcal{G}$. By Proposition 3.5, there is a point $u \in U_{\mathcal{G}}(\mathbb{Q})$ such that $\pi_{\mathcal{G}}(u) = j_E$.

Since any two non-CM elliptic curves with the same $j$-invariant are quadratic twists of each other, there is a unique squarefree integer $d$ such that $E/\mathbb{Q}$ is isomorphic to the quadratic twist of $E' := (\mathscr{E}_{\mathcal{G}})_u$ by $d$, where $(\mathscr{E}_{\mathcal{G}})_u$ is the elliptic curve over $\mathbb{Q}$ defined as in §11.1.2. Let $\chi_d\colon \mathrm{Gal}_{\mathbb{Q}} \to \{\pm 1\}$ be the homomorphism that factors through $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \hookrightarrow \{\pm 1\}$. Define the homomorphism

$$\alpha_E\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathcal{G}/G$$

by $\alpha_E = \chi_d \cdot \alpha_u$ with $\alpha_u$ as in §11.1.2. The following lemma shows that this definition of $\alpha_E$ is consistent with our earlier definition in §1.5.

**Lemma 11.1.** *After replacing $\rho^*_E$ by an isomorphic representation, we will have $\rho^*_E(\mathrm{Gal}_{\mathbb{Q}}) \subseteq \mathcal{G}$ and the composition of $\rho^*_E\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathcal{G}$ with the quotient map $\mathcal{G} \to \mathcal{G}/G$ is $\alpha_E$.*

*Proof.* Since $E$ is a quadratic twist of $E'$ by $d$, we can choose bases so that $\rho^*_{E',N} = \varrho_u$ and $\rho^*_E = \chi_d \cdot \rho^*_{E'}$. In particular, $\rho^*_{E,N}(\mathrm{Gal}_{\mathbb{Q}}) \subseteq \pm\varrho_u(\mathrm{Gal}_{\mathbb{Q}}) \subseteq \overline{\mathcal{G}}$ and hence $\rho^*_E(\mathrm{Gal}_{\mathbb{Q}}) \subseteq \mathcal{G}$ since the level of $\mathcal{G}$ divides $N$. Take any $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$. We have $\rho^*_{E,N}(\sigma) \cdot \overline{G} = \chi_d(\sigma) \cdot \varrho_u(\sigma) \cdot \overline{G}$ and hence $\rho^*_E(\sigma) \cdot G = \chi_d(\sigma) \cdot \alpha_u(\sigma) = \alpha_E(\sigma)$. □

**Lemma 11.2.** *The homomorphism $\alpha_E$ is unramified at all primes $p \nmid N$ for which $E$ has good reduction.*

*Proof.* Using our isomorphism $\mathcal{G}/G = \overline{\mathcal{G}}/\overline{G}$, we could also view $\alpha_E$ as the composition of $\rho^*_{E,N}$ with the quotient map $\overline{\mathcal{G}} \to \overline{\mathcal{G}}/\overline{G} = \mathcal{G}/G$. The lemma is immediate since $\rho^*_{E,N}$ is unramified at all primes $p \nmid N$ for which $E$ has good reduction. □

Take any prime $p \nmid 2Nd$ for which $E$ has good reduction. The character $\chi_d$ is unramified at $p$ and $\chi_d(\mathrm{Frob}_p) = 1$ if and only if $d$ is a square modulo $p$. By Lemma 11.2, we deduce that $\alpha_u$ is unramified at $p$ and that $\alpha_E(\mathrm{Frob}_p) = \chi_d(\mathrm{Frob}_p) \cdot \alpha_u(\mathrm{Frob}_p)$.

In §11.3.1, we will describe how to compute $\alpha_u(\mathrm{Frob}_p) \in \mathcal{G}/G$ for all sufficiently large primes $p$ under the additional assumptions that $\mathcal{G}/G$ is cyclic of prime power order, $X_{\mathcal{G}}(\mathbb{Q})$ is infinite, and $u$ lies outside some explicit finite subset of $X_{\mathcal{G}}(\mathbb{Q})$.

11.3. **The function field $L$ in a special case.** We shall now assume further that $\mathcal{G}/G$ is a cyclic group of prime power order $p_0^e > 1$. In this section, we will describe a set of generators of the extension $L$ of $\mathbb{Q}(X_{\mathcal{G}})$ with a simple and explicit action of $\mathcal{G}/G$ on them.

Fix a matrix $g_0 \in \overline{\mathcal{G}} \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ so that $g_0\overline{G}$ generates the cyclic group $\overline{\mathcal{G}}/\overline{G} = \mathcal{G}/G$. For an integer $k \geq 2$, $M_{k,\overline{G}}$ has a right action by the group $\mathcal{G}/G$. We can compute a basis of $M_{k,\overline{G}}$ using the methods of §4.6 and we can compute the action of $g_0$ with respect to this basis by using §4.9. We can choose $k \geq 2$ so that the action of $\mathcal{G}/G$ on $M_{k,\overline{G}}$ is faithful. When $-I \in G$, we further assume that $k$ is chosen to be even and large enough so that there is a nonzero $h \in M_{k,\overline{\mathcal{G}}}$.

Suppose $-I \notin G$. By Lemma 4.6, there is a nonzero $f_1 \in M_{3,\overline{G}}$. We claim that $\mathcal{G}/G$ acts faithfully on $M_{3,\overline{G}}$. Since $\mathcal{G}/G$ is cyclic of order $p_0^e > 1$, it suffices to show that the minimal nontrivial subgroup of $\mathcal{G}/G$ acts faithfully. Since $-I \notin G$, this group is $(\pm G)/G$ and it acts faithfully on $M_{3,\overline{G}}$ because this space is nonzero and $-I$ acts as multiplication by $-1$. So when $-I \notin G$, we may always take $k = 3$.

Since $\mathcal{G}/G$ is cyclic of prime power order, there is a $\mathbb{Q}$-subspace $V \subseteq M_{k,\overline{G}}$ for which the right action of $\mathcal{G}/G$ is faithful and irreducible. Moreover, we can find an explicit basis $f_1, \ldots, f_m$ of $V$ such that

$$f_j * g_0 = \sum_{i=1}^{m} f_i \cdot C_{i,j}$$

for all $1 \leq j \leq m$, where $m = \phi(p_0^e) = p_0^{e-1}(p_0 - 1)$ and $C \in \mathrm{GL}_m(\mathbb{Q})$ is the companion matrix of the cyclotomic polynomial $\Phi_{p_0^e}(x)$. Note that the matrix $C$ has order $p_0^e$ in $\mathrm{GL}_m(\mathbb{Q})$.

Let $\mathcal{R}$ be the $\mathbb{Q}$-subalgebra of $\mathbb{Q}[x_1, \ldots, x_m]$ consisting of polynomials $F$ for which $F(x_1, \ldots, x_m) = F((x_1, \ldots, x_m)C)$. Take any homogeneous polynomial $F \in \mathcal{R}$ and denote its degree by $d$. When $-I \notin G$, a power of $C$ is $-I$ and hence $d$ is even. The modular form $F(f_1, \ldots, f_m)$ has weight $dk$ and is fixed by $\overline{G}$ and $g_0$. Therefore, $F(f_1, \ldots, f_m)$ is an element of $M_{dk,\overline{\mathcal{G}}}$. Define

$$c_F := \begin{cases} \dfrac{F(f_1, \ldots, f_m)}{h^d} & \text{if } -I \in \overline{G}, \\ \dfrac{F(f_1, \ldots, f_m)\, j^{d/2}}{E_6^{d/2}} & \text{if } -I \notin \overline{G}. \end{cases}$$

Note that $c_F$ is in $\mathcal{F}_N^{\overline{\mathcal{G}}} = \mathbb{Q}(X_{\mathcal{G}})$. The following lemma describes the extension $L/\mathbb{Q}(X_{\mathcal{G}})$ in terms of the $c_F$.

**Lemma 11.3.** *We have $L = \mathbb{Q}(X_{\mathcal{G}})(y_1, \ldots, y_m)$, where the $y_j$ can be chosen such that:*

- *$y_j * g_0 = \sum_{i=1}^{m} y_i \cdot C_{i,j}$ for all $1 \leq m$,*

- $F(y_1,\dots,y_m) = c_F$ *for all homogeneous polynomials* $F \in \mathcal{R}$.

*Proof.* First suppose that $-I \in G$. We define $y_j := f_j/h$ for $1 \le j \le m$. For a homogeneous $F \in \mathcal{R}$ of degree $d$, we have $F(y_1,\dots,y_m) = F(f_1,\dots,f_m)/h^d = c_F$. Take any $\sigma \in \mathrm{Gal}_{\mathbb{Q}(X_{\mathcal{G}})}$ and set $A := \rho^*_{\mathcal{E},N}(\sigma)^{-1} \in \overline{\mathcal{G}}$. We have $\sigma(y_j) = y_j * A = (f_j * A)/(h * A) = (f_j * A)/h$, where the last equality uses our choice of $h$. We have $y_j \in L$ since $\sigma(y_j) = y_j$ when $A \in \overline{G}$. Now suppose $\sigma$ is chosen such that $A = g_0$. Then $y_j * g_0 = (f_j * g_0)/h = (\sum_{i=1}^m f_i \cdot C_{i,j})/h = \sum_{i=1}^m y_i \cdot C_{i,j}$.

Now suppose that $-I \notin G$ and hence $k = 3$. Define $y_i := \beta \cdot f_i/f_0$ for $1 \le i \le m$. Take any homogeneous $F \in \mathcal{R}$ of (even) degree $d$. Since $\beta^2 = j \cdot f_0^2/E_6$, we have

$$F(y_1,\dots,y_m) = \left(\frac{\beta^2}{f_0^2}\right)^{d/2} F(f_1,\dots,f_m) = \left(\frac{j}{E_6}\right)^{d/2} F(f_1,\dots,f_m) = c_F.$$

Take any $\sigma \in \mathrm{Gal}_{\mathbb{Q}(X_{\mathcal{G}})}$ and set $A := \rho^*_{\mathcal{E},N}(\sigma)^{-1}$. By Lemma 6.3(vi), we have $\sigma(\beta) = \frac{f_0 * A}{f_0}\beta$. Since $f_j/f_0 \in \mathcal{F}_N$, we have

$$\sigma(y_j) = \sigma(\beta)\cdot\sigma(\tfrac{f_j}{f_0}) = \tfrac{f_0*A}{f_0}\beta \cdot (\tfrac{f_j}{f_0}) * A = \tfrac{f_0*A}{f_0}\beta \cdot \tfrac{f_j*A}{f_0*A} = \beta \cdot \tfrac{f_j*A}{f_0}.$$

If $A \in \overline{G}$, then $\sigma(y_j) = \beta \cdot f_j/f_0 = y_j$. Therefore, $y_1,\dots,y_m$ all lie in $L$. Now suppose $\sigma$ is chosen such that $A = g_0$. Therefore,

$$y_j * g_0 = \sigma(y_j) = \beta \cdot \tfrac{f_j*A}{f_0} = \beta\tfrac{f_j*g_0}{f_0} = \beta(\sum_{i=1}^m f_i \cdot C_{i,j})/f_0 = \sum_{i=1}^m y_i \cdot C_{i,j}.$$

In both cases, we have proved that $\mathbb{Q}(X_{\mathcal{G}})(y_1,\dots,y_m) \subseteq L$ and that $y_1,\dots,y_m$ have the desired properties. In both constructions, we have shown that there is a $\sigma \in \mathrm{Gal}_{\mathbb{Q}(X_{\mathcal{G}})}$ whose action on $\oplus_{j=1}^m \mathbb{Q}y_j \subseteq L$ is given by the matrix $C$. Since the order of $C \in \mathrm{GL}_m(\mathbb{Q})$ is equal to $|\overline{\mathcal{G}}/\overline{G}| = [L : \mathbb{Q}(X_{\mathcal{G}})]$, we deduce that $L = \mathbb{Q}(X_{\mathcal{G}})(y_1,\dots,y_m)$. □

11.3.1. *Low genus setting.* We now further assume that the curve $X_{\mathcal{G}}$ has infinitely many rational points; in particular, $X_{\mathcal{G}}$ has genus at most 1 and a rational point. As outlined in §5.4, we can compute an explicit model for $X_{\mathcal{G}}$. In particular, the function field $\mathbb{Q}(X_{\mathcal{G}})$ will be of the form $\mathbb{Q}(f)$ or $\mathbb{Q}(x,y)$ with $x$ and $y$ satisfying a Weierstrass equation of an elliptic curve over $\mathbb{Q}$.

For any given homogeneous polynomial $F \in \mathcal{R}$, we can express $c_F \in \mathbb{Q}(X_{\mathcal{G}})$ in terms of the explicit generators of our function field $\mathbb{Q}(X_{\mathcal{G}})$ using the methods from §5.4.2.

We now apply Lemma 11.3 to describe all but finite many fibers of $\phi$. Since $\mathcal{R}$ is a finitely generated $\mathbb{Q}$-algebra, there are only finite many $u \in U_{\mathcal{G}}(\mathbb{Q})$ for which $c_F$ has a pole at $u$ for some homogeneous $F \in \mathcal{R}$. For a point $u \in U_{\mathcal{G}}(\mathbb{Q})$ for which $c_F$ never has a pole at $u$, we let $Z_u \subseteq \mathbb{A}^m_{\mathbb{Q}}$ be the subscheme defined by the equations

$$F(x_1,\dots,x_m) = c_F(u)$$

with $F \in \mathcal{R}$ homogeneous. The group $\overline{\mathcal{G}}/\overline{G} = \mathcal{G}/G$ acts on $Z_u(\overline{\mathbb{Q}})$ by $g_0\overline{G} \cdot (a_1,\dots,a_m) := (a_1,\dots,a_m)\cdot C$. For all but finitely many $u$, $Z_u$ is a reduced finite $\mathbb{Q}$-scheme of degree $|\mathcal{G}/G| = p_0^e$ with $\mathcal{G}/G$ acting transitively on $Z_u(\overline{\mathbb{Q}})$; for such $u$, we have an isomorphism $\phi^{-1}(u) \xrightarrow{\sim} Z_u$ with compatible $\mathcal{G}/G$-actions.

Choose homogeneous polynomials $F_1,\dots,F_r \in \mathcal{R}$ such that there is a point $u \in U_{\mathcal{G}}(\mathbb{Q})$ for which the equations

$$F_1(x_1,\dots,x_m) = c_{F_1}(u), \quad \dots, \quad F_r(x_1,\dots,x_m) = c_{F_r}(u) \tag{11.2}$$

define $Z_u$ as a variety (so it is finite of degree $p_0^e$ with a transitive $\mathcal{G}/G$-action on its $\overline{\mathbb{Q}}$-points). Recall that we can compute the functions $c_{F_j} \in \mathbb{Q}(X_{\mathcal{G}})$. The equations (11.2) will also define $Z_u$

for $u \in U_{\mathcal{G}}(\mathbb{Q}) - \mathcal{S}$, where $\mathcal{S}$ is a finite set that can be computed. So for any point $u \in U_{\mathcal{G}}(\mathbb{Q}) - \mathcal{S}$, (11.2) gives an explicit model for the fiber $\phi^{-1}(u)$ with the action of $\mathcal{G}/G$ upon it. So from (11.1), we have

$$\sigma(z_0) = \alpha_u(\sigma) \cdot z_0$$

for any fixed point $z_0 \in Z_u(\overline{\mathbb{Q}})$ and $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$.

Fix a point $u \in U_{\mathcal{G}}(\mathbb{Q}) - \mathcal{S}$. For all primes $p \nmid N p_0$ large enough, we can reduce the equations (11.2) modulo $p$ to obtain a variety $Z_{u,p} \subseteq \mathbb{A}^m_{\mathbb{F}_p}$ with an action of $\mathcal{G}/G$ so that the action of $\mathcal{G}/G$ on $Z_{u,p}(\overline{\mathbb{F}}_p)$ is simply transitive. For such a prime $p$, $\alpha_u$ is unramified at $p$ and we have $(z_1^p, \ldots, z_m^p) = \alpha_u(\mathrm{Frob}_p) \cdot (z_1, \ldots, z_m)$ for any $(z_1, \ldots, z_m) \in Z_{u,p}(\overline{\mathbb{F}}_p)$. In particular, for any large enough prime $p$, we can use this to compute $\alpha_u(\mathrm{Frob}_p) \in \mathcal{G}/G$.

*Remark* 11.4. There are a finite number of excluded points $u \in \mathcal{S} \subseteq U_{\mathcal{G}}(\mathbb{Q})$. By changing variables, adding more equations of the form $F_i(x_1, \ldots, x_m) = c_{F_i}(u)$, or making a different choice of $h$ if relevant, we can often find a model for the fiber $\phi^{-1}(u)$ that allows us to compute $\alpha_u(\mathrm{Frob}_p)$ for any sufficiently large prime $p$.

For our application to Serre's open image theorem, we work with a *single* choice of $u \in U_{\mathcal{G}}(\mathbb{Q})$ satisfying $\pi_{\mathcal{G}}(u) = j$ for some fixed $j \in \mathbb{Q} - \{0, 1728\}$. So for our application we can exclude from consideration any $u \in \mathcal{S}$ for which there is another point $u' \in U_{\mathcal{G}}(\mathbb{Q}) - \mathcal{S}$ satisfying $\pi_{\mathcal{G}}(u) = \pi_{\mathcal{G}}(u')$.

11.4. **Precomputations.** We now describe some one-time computations that will be required for our algorithm for computing the image of $\rho_E^*$, up to conjugacy, for any non-CM elliptic curve $E/\mathbb{Q}$.

Consider any of the finite number of groups $\mathcal{G} \in \mathscr{A}$, with $\mathscr{A}$ from Theorem 1.9, that satisfy the following properties:

(a) $X_{\mathcal{G}}(\mathbb{Q})$ is infinite,
(b) if $\mathcal{G}$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a proper subgroup of some $\mathcal{G}' \in \mathscr{A}$, then $[\mathcal{G}, \mathcal{G}]$ and $[\mathcal{G}', \mathcal{G}']$ are not conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

From Theorem 1.9, we will already have computed a model for $X_{\mathcal{G}}$ and the morphism $\pi_{\mathcal{G}}$ to the $j$-line. In particular, we have a model for $U_{\mathcal{G}}$.

Choose an open subgroup $G_0$ of $\mathcal{G}$ satisfying $\det(G_0) = \widehat{\mathbb{Z}}^\times$ and $G_0 \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = [\mathcal{G}, \mathcal{G}]$. In our cases, we choose $G_0$ with minimal level; the levels of the groups $G_0$ and $\mathcal{G}$ turn out to have the same odd prime divisors. Note that $G_0$ is a normal subgroup of $\mathcal{G}$ and that $\mathcal{G}/G_0$ is finite and abelian. So we can chose proper normal subgroups $G_1, \ldots, G_s$ of $\mathcal{G}$ containing $G_0$ such that the quotient maps $\mathcal{G} \to \mathcal{G}/G_i$ induce an isomorphism

$$\mathcal{G}/G_0 \xrightarrow{\sim} \mathcal{G}/G_1 \times \cdots \times \mathcal{G}/G_s, \tag{11.3}$$

where the groups $\mathcal{G}/G_i$ are all nontrivial and cyclic of prime power order. Moreover, we choose our groups $G_i$, with $1 \le i \le s$, so that at most one does not contain $-I$ and so that the levels of the groups are as small as possible. Since $G_0 \subseteq G_i \subseteq \mathcal{G}$, the group $G_i$ is open in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, $\det(G_i) = \widehat{\mathbb{Z}}^\times$ and $-I \in G_i$.

With notation as in §11.1 and $G := G_0$, we have a homomorphism

$$\alpha \colon \pi_1(U_{\mathcal{G}}, \overline{\eta}) \to \mathcal{G}/G_0$$

with specializations $\alpha_u \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathcal{G}/G_0$ for $u \in U_{\mathcal{G}}(\mathbb{Q})$. Taking instead $G := G_i$ with $1 \le i \le s$, we obtain a homomorphism

$$\alpha_i \colon \pi_1(U_{\mathcal{G}}, \overline{\eta}) \to \mathcal{G}/G_i$$

with specializations $\alpha_{i,u} \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathcal{G}/G_i$. Note that $\alpha_i$ can also be obtained by composing $\alpha$ with the isomorphism (11.3) and then projecting to the factor $\mathcal{G}/G_i$.

Now take any $1 \le i \le s$ and consider the setting of §11.3 with $G := G_i$. With notation as in §11.3 and §11.3.1, we compute homogeneous polynomials $F_1, \dots, F_r$ and rational functions $c_{F_1}, \dots, c_{F_r} \in \mathbb{Q}(X_{\mathcal{G}})$ such that for all $u \in U_{\mathcal{G}}(\mathbb{Q})$ away from an explicit finite set $\mathcal{S}_i$, the equations (11.2) define a $\mathbb{Q}$-scheme $Z_u$ with a transitive $\mathcal{G}/G$-action on $Z_u(\overline{\mathbb{Q}})$ such that

$$\sigma(z) = \alpha_{i,u}(\sigma) \cdot z$$

for all $z \in Z_u(\overline{\mathbb{Q}})$ and $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$. As explained in §11.3.1, we can compute $\alpha_{i,u}(\mathrm{Frob}_p) \in \mathcal{G}/G = \mathcal{G}/G_i$ for any sufficiently large primes $p$ by considering the reduction modulo $p$.

*Remark* 11.5. For $p$ large enough, the point $u$ modulo $p$ will be enough to determine $\alpha_{i,u}(\mathrm{Frob}_p)$. So that we can reuse computations when dealing with many elliptic curves over $\mathbb{Q}$, we have precomputed these values for several primes $p$ and $\mathbb{F}_p$-points on a model of $U_{\mathcal{G}}$.

Define $\mathcal{S} := \mathcal{S}_1 \cup \cdots \cup \mathcal{S}_s$; it is an explicit finite set. Consider any $u \in U_{\mathcal{G}}(\mathbb{Q}) - \mathcal{S}$. For each $1 \le i \le s$, we noted that one can compute $\alpha_{i,u}(\mathrm{Frob}_p)$ for all sufficiently large primes $p$. By making use of the isomorphism (11.3), we can verify that $\alpha_u$ is unramified at $p$ and compute $\alpha_u(\mathrm{Frob}_p) \in \mathcal{G}/G_0$ for any sufficient large primes.

## 12. Computing the image of $\rho_E$

Take any non-CM elliptic curve $E/\mathbb{Q}$. We now combine the previous sections to explain how to compute the image of $\rho_E$ up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. We assume that $E$ is given explicitly as a Weierstrass model. Let $j_E \in \mathbb{Q}$ be the $j$-invariant of $E$.

12.1. **Agreeable closure.** As outlined in §10, we can compute the agreeable closure $\mathcal{G}_E$ of $G_E := \rho_E^*(\mathrm{Gal}_{\mathbb{Q}})$, up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, and determine whether $X_{\mathcal{G}_E}(\mathbb{Q})$ is infinite or not. If $X_{\mathcal{G}_E}(\mathbb{Q})$ is infinite, we may choose $\mathcal{G}_E$ so that it lies in our finite set $\mathscr{A}$ from Theorem 1.9.

As noted in §10, from $\mathcal{G}_E$ we can already compute the index $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E]$ and the open subgroup $G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = [\mathcal{G}_E, \mathcal{G}_E]$ of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

12.2. **Computing the image of Galois in most cases.** Fix a group $\mathcal{G} \in \mathscr{A}$ with $X_{\mathcal{G}}(\mathbb{Q})$ infinite for which $\mathcal{G}_E$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a subgroup of $\mathcal{G}$. If $X_{\mathcal{G}_E}(\mathbb{Q})$ is infinite, we shall further assume that $\mathcal{G}$ is chosen so that $[\mathcal{G}_E, \mathcal{G}_E]$ and $[\mathcal{G}, \mathcal{G}]$ are conjugate in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ (such a group exists in this case since $\mathcal{G}_E$ is conjugate to an element of $\mathscr{A}$). After possibly replacing $\mathcal{G}$ by a different group in $\mathscr{A}$, we may further assume that condition (b) of §11.4 holds; it already satisfies condition (a).

In §11.4, we chose (independent of $E$) an open subgroup $G := G_0$ of $\mathcal{G}$ such that $\det(G) = \widehat{\mathbb{Z}}^\times$ and $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = [\mathcal{G}, \mathcal{G}]$. In particular, $G$ is a normal subgroup of $\mathcal{G}$ with $\mathcal{G}/G$ finite and abelian.

Let $\mathcal{S} \subseteq X_{\mathcal{G}}(\mathbb{Q})$ be finite set from §11.4. We now make the additional assumption on $E/\mathbb{Q}$ that there is a rational point $u \in U_{\mathcal{G}}(\mathbb{Q}) - \mathcal{S}$ for which $j_E = \pi_{\mathcal{G}}(u)$. For the models from our computations, this assumption always holds; if not, it could be treated separately as we do in §12.3. As in §11.4, we have a homomorphism

$$\alpha_u \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathcal{G}/G$$

and for all sufficiently large primes $p$, we can verify that $\alpha_u$ is unramified at $p$ and actually compute $\alpha_u(\mathrm{Frob}_p) \in \mathcal{G}/G$.

Let $d$ be the unique squarefree integer for which $E$ is isomorphic to the quadratic twist of $E'$ by $d$, where $E'/\mathbb{Q}$ is the elliptic curve defined by the Weierstrass equation $y^2 = x^3 - 27j_E(j_E - 1728) \cdot x + 54j_E(j_E - 1728)^2$. As in §11.2, we can define a homomorphism

$$\alpha_E \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathcal{G}/G, \quad \sigma \mapsto \chi_d(\sigma) \cdot \alpha_u(\sigma),$$

where $\chi_d\colon \mathrm{Gal}_{\mathbb{Q}} \to \{\pm 1\}$ is the character that factors through $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \hookrightarrow \{\pm 1\}$. For $p \nmid 2d$, $\chi_d$ is unramified at $p$ and $\chi_d(\mathrm{Frob}_p) = 1$ if and only if $d$ is a square modulo $p$. Let $M$ be the product of those primes that divide $N$ or for which $E$ has bad reduction. The homomorphism $\alpha_E$ is unramified at all $p \nmid M$ by Lemma 11.2. We can thus compute $\alpha_E(\mathrm{Frob}_p) \in \mathcal{G}/G$ for any sufficiently large primes $p \nmid M$.

By Lemma 11.1, we may assume that, after possibly replacing $\rho_E^*$ by an isomorphic representation, that $\rho_E^*(\mathrm{Gal}_{\mathbb{Q}}) \subseteq \mathcal{G}$ and that $\alpha_E$ is the composition of $\rho_E^*$ with the quotient map $\mathcal{G}/G$. Let

$$\gamma_E\colon \widehat{\mathbb{Z}}^\times \to \mathcal{G}/G$$

be the unique homomorphism for which $\gamma_E(\chi_{\mathrm{cyc}}(\sigma)^{-1}) = \alpha_E(\sigma)$ for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$. Since $\alpha_E$ is unramified at all primes $p \nmid M$, we find that $\gamma_E$ factors through a homomorphism

$$\overline{\gamma}_E\colon \mathbb{Z}_M^\times/(\mathbb{Z}_M^\times)^e \to \mathcal{G}/G,$$

where $e$ is the exponent of the group $\mathcal{G}/G$, and $\overline{\gamma}_E(p\cdot(\mathbb{Z}_M^\times)^e) = \alpha_E(\mathrm{Frob}_p)^{-1} \in \mathcal{G}/G$ for all primes $p \nmid M$. So we can find $\gamma_E$ by computing $\alpha_E(\mathrm{Frob}_p)$ for a finite set of primes $p \nmid M$ that generate the finite group $\mathbb{Z}_M^\times/(\mathbb{Z}_M^\times)^e$.

*Remark* 12.1. We have used the larger group $\mathcal{G}$ instead of $\mathcal{G}_E$ since it leads to fewer cases to consider in §11.4. There are 454 groups $H \in \mathscr{A}$ for which $X_H(\mathbb{Q})$ is infinite, but only 138 of these groups $H$ will arise as a group $\mathcal{G}$ like above.

Define the explicit subgroup

$$\mathcal{H}_E := \{g \in \mathcal{G} : g \cdot G = \gamma_E(\det g)\}$$

of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. In particular, note that $\mathcal{H}_E$ is computable, cf. Remark 1.12. The group $G_E := \rho_E^*(\mathrm{Gal}_{\mathbb{Q}})$ is a subgroup of $\mathcal{H}_E$ since $\rho_E^*(\sigma)\cdot G = \alpha_E(\sigma) = \gamma_E(\chi_{\mathrm{cyc}}(\sigma)^{-1}) = \gamma_E(\det(\rho_E^*(\sigma)))$ for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$.

Now consider the case where $[\mathcal{G}_E, \mathcal{G}_E]$ and $[\mathcal{G}, \mathcal{G}]$ are conjugate subgroups of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$; this condition is automatic when $X_{\mathcal{G}_E}(\mathbb{Q})$ is infinite by our choice of $\mathcal{G}$. We have $\mathcal{G}_E \subseteq \mathcal{G}$ so $[\mathcal{G}_E, \mathcal{G}_E] \subseteq [\mathcal{G}, \mathcal{G}]$ and hence $[\mathcal{G}_E, \mathcal{G}_E] = [\mathcal{G}, \mathcal{G}]$ since they are conjugate open subgroups of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$. In particular, $G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = [\mathcal{G}, \mathcal{G}]$ by Lemma 1.7 and Proposition 8.1. Therefore,

$$\mathcal{H}_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = [\mathcal{G}, \mathcal{G}] = G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}).$$

Since $G_E$ is a subgroup of $\mathcal{H}_E$ with $G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = \mathcal{H}_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ and $\det(G_E) = \widehat{\mathbb{Z}}^\times$, we deduce that $G_E = \mathcal{H}_E$.

12.3. **Computing the image of Galois in the remaining cases.** We have already computed $\mathcal{G}_E$, up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, and we know if $X_{\mathcal{G}_E}(\mathbb{Q})$ is infinite or not. If $X_{\mathcal{G}_E}(\mathbb{Q})$ is infinite, then §12.2 shows how to compute the group $\rho_E^*(\mathrm{Gal}_{\mathbb{Q}})$ up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

We now restrict our attention to the case when $X_{\mathcal{G}_E}(\mathbb{Q})$ is finite. If $E/\mathbb{Q}$ is not a counterexample to Conjecture 1.2, then the $j$-invariant $j_E$ lies in the finite set

$$\mathcal{J} := \bigcup_{\mathcal{G}\in\mathscr{A},\, X_{\mathcal{G}}(\mathbb{Q}) \text{ finite}} \pi_{\mathcal{G}}(U_{\mathcal{G}}(\mathbb{Q})) \subseteq \mathbb{Q}$$

with $\mathscr{A}$ as in Theorem 1.9. We are aware of 81 rational numbers $j \in \mathcal{J}$ for which $j$ is the $j$-invariant of a non-CM elliptic curve. We will explain how to compute $G_E := \rho_E^*(\mathrm{Gal}_{\mathbb{Q}})$, up to conjugacy, in these cases. Any other non-CM $j$-invariants in $\mathcal{J}$, or counterexamples to Conjecture 1.2, can be dealt with in a similar direct manner.

For the finite number of $j$-invariants under consideration, we need only consider a single elliptic curve with that $j$-invariant (from Lemma 2.2, replacing $E$ by a quadratic twist changes $G_E$ in an explicit way).

12.3.1. *Case 1: the previous approach works.* For our 81 exceptional $j$-invariants, the group $G_E$ can be computed for 28 of them using the method of §12.2. In particular, we can find an agreeable groups $\mathcal{G} \in \mathscr{A}$ so that $\mathcal{G}_E$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a subgroup of $\mathcal{G}$, $X_{\mathcal{G}}(\mathbb{Q})$ is infinite, and $[\mathcal{G}_E, \mathcal{G}_E]$ is conjugate to a subgroup of $[\mathcal{G}, \mathcal{G}]$ in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$.

12.3.2. *Case 2: intersections with relatively prime levels.* Suppose that there are distinct primes $2 = \ell_1 < \ell_2 < \cdots < \ell_s$ and agreeable subgroups $\mathcal{G}_1, \ldots, \mathcal{G}_s \in \mathscr{A}$ so that all the following hold:

- $\mathcal{G}_E$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a subgroup of $\mathcal{G}_i$ for all $1 \le i \le s$,
- the level of $\mathcal{G}_i$ divides a power of $\ell_i$ for all $1 \le i \le s$,
- $X_{\mathcal{G}_i}(\mathbb{Q})$ has infinitely many points for all $1 \le i \le s$,
- $[\mathcal{G}_E, \mathcal{G}_E]$ and $\bigcap_{i=1}^s [\mathcal{G}_i, \mathcal{G}_i]$ are open subgroups of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ that are conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

Since the levels of the groups $\mathcal{G}_i$ are pairwise relatively prime, we find that the group $\bigcap_{i=1}^s [\mathcal{G}_i, \mathcal{G}_i]$, up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, does not change if we replace any $\mathcal{G}_i$ by a conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. Thus we may assume further that the $\mathcal{G}_i$ are chosen so that they satisfy condition (b) of §11.4.

For each $1 \le i \le s$, we choose an open subgroup $G_i$ of $\mathcal{G}_i$ with $\det(G_i) = \widehat{\mathbb{Z}}^\times$ such that the level of $G_i$ is a power of $\ell_i$ and $G_i \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = [\mathcal{G}_i, \mathcal{G}_i]$. We have $j_E \in \pi_{\mathcal{G}_i}(X_{\mathcal{G}_i}(\mathbb{Q}))$ since $\mathcal{G}_E$ is conjugate to a subgroup of $\mathcal{G}_i$. As in §11.4 and §12.2, we can compute an explicit homomorphism $\gamma_{E,i} \colon \widehat{\mathbb{Z}}^\times \to \mathcal{G}_i/G_i$ so that $\rho_E^*(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a subgroup of

$$\mathcal{H}_i := \{g \in \mathcal{G}_i : g \cdot G_i = \gamma_{E,i}(\det(g))\}.$$

This previous step uses that $X_{\mathcal{G}_i}(\mathbb{Q})$ is infinite.

Since the group $G_1, \ldots, G_s$ have pairwise relatively prime levels, we find that after replacing $\rho_E^*$ by an isomorphic representation we have $G_E := \rho_E^*(\mathrm{Gal}_{\mathbb{Q}}) \subseteq \mathcal{H}_i$ for all $1 \le i \le s$. In particular, $G_E \subseteq \mathcal{H} := \bigcap_{i=1}^s \mathcal{H}_i$.

We claim that $G_E = \mathcal{H}$; since $\mathcal{H}$ has an explicit description this will conclude our description of how to compute $G_E$ up to conjugacy. We have

$$G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) \subseteq \mathcal{H} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) \subseteq \bigcap_{i=1}^s (\mathcal{H}_i \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})) = \bigcap_{i=1}^s (G_i \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})) = \bigcap_{i=1}^s [\mathcal{G}_i, \mathcal{G}_i]. \tag{12.1}$$

We have $G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = [\mathcal{G}_E, \mathcal{G}_E]$ by Lemma 1.7 and Proposition 8.1. So by assumption, $G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ and $\bigcap_{i=1}^s [\mathcal{G}_i, \mathcal{G}_i]$ are open subgroups of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ that are conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. From the inclusions (12.1), we deduce that $G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = \mathcal{H} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. Since $G_E$ is a subgroup of $\mathcal{H}$ with full determinant, we conclude that $G_E = \mathcal{H}$.

Of the 53 exceptional $j$-invariants not handled by Case 1, we use the method above to compute $G_E$, up to conjugacy, for an additional 24 $j$-invariants. Of the 29 remaining exceptional $j$-invariants, 20 of them arise in [RSZB22].

12.3.3. *Case 3: check directly.* We already know the agreeable closure $\mathcal{G}_E$ of $G_E = \rho_E^*(\mathrm{Gal}_{\mathbb{Q}})$. We can choose an open subgroup $G$ of $\mathcal{G}_E$ with minimal level that satisfies $\det(G) = \widehat{\mathbb{Z}}^\times$ and $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = [\mathcal{G}_E, \mathcal{G}_E]$. Let $M$ be the product of the primes $p$ so that $p$ divides the level of $G$ or $E$ has bad reduction at $p$; this is an integer we can compute. The homomorphism $\alpha_E \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathcal{G}_E/G$ obtained by composing $\rho_E^*$ with the obvious quotient map will be unramified at all primes $p \nmid M$. Using Lemma 1.10, we deduce that the every prime that divides the level of $G_E$ must also divide $M$.

After replacing $\mathcal{G}_E$ by a conjugate, we can find a group $\mathcal{G} \in \mathscr{A}$ so that $X_{\mathcal{G}}(\mathbb{Q})$ is infinite and $\mathcal{G}_E \subseteq \mathcal{G}$. We choose $\mathcal{G}$ so that $[\mathcal{G} : \mathcal{G}_E]$ is minimal. Using §12.2, we can construct a computable

open subgroup $\mathcal{H}$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ for which $\mathcal{H} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = [\mathcal{G}, \mathcal{G}]$, $\det \mathcal{H} = \widehat{\mathbb{Z}}^\times$ and $G_E$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a subgroup of $\mathcal{H}$.

So after possibly replacing $\rho_E^*$ by an isomorphic representation, we find that $G_E = \rho_E^*(\mathrm{Gal}_{\mathbb{Q}})$ is an open subgroup of $\mathcal{H}$ with

$$[\mathcal{H} : G_E] = [\mathcal{H} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) : G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})] = [[\mathcal{G}, \mathcal{G}], [\mathcal{G}_E, \mathcal{G}_E]] =: m$$

So $G_E$ is an index $m$ open subgroup of $\mathcal{H}$ whose level in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ divides some power of $M$. However, there are are only finitely many such groups, so we can compute them all up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. It remains to check which of these explicit candidates is actually conjugate to $G_E$. Looking at traces of Frobenius can be useful to rule out some possibilities and hope that one case remains. In any remaining cases, one can directly compute division polynomials for the curve $E$ and study their Galois groups to determine $G_E$. For example, §1.7 gives one of the exceptional elliptic curves we dealt with directly using division polynomials.

12.4. **Finding the image.** From §12.2 or §12.3, we have found the following:

- an agreeable group $\mathcal{G}$ and an open and normal subgroup $G$ of $\mathcal{G}$ satisfying $\det(G) = \widehat{\mathbb{Z}}$ and $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = [\mathcal{G}, \mathcal{G}]$,
- a homomorphism $\gamma_E \colon \widehat{\mathbb{Z}}^\times \to \mathcal{G}/G$ such that, after replacing $\rho_E^*$ by an isomorphic representation, we have $\rho_E^*(\mathrm{Gal}_{\mathbb{Q}}) \subseteq \mathcal{G}$ and the homomorphism

  $$\alpha_E \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathcal{G}/G$$

  obtained by composing $\rho_E^*$ with the quotient map $\mathcal{G} \to \mathcal{G}/G$ satisfies $\gamma_E(\chi_{\mathrm{cyc}}(\sigma)^{-1}) = \alpha_E(\sigma)$ for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$.
- the commutator subgroups of the two groups $\rho_E^*(\mathrm{Gal}_{\mathbb{Q}})$ and $\mathcal{G}$ are conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

We have $G_E := \rho_E^*(\mathrm{Gal}_{\mathbb{Q}}) \subseteq \mathcal{G}$ and hence $[G_E, G_E] \subseteq [\mathcal{G}, \mathcal{G}]$. We have $[G_E, G_E] = [\mathcal{G}, \mathcal{G}]$ since they are open subgroups of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ that are conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. In particular, $G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = [\mathcal{G}, \mathcal{G}]$ by Lemma 1.7. By Lemma 1.10, $\rho_E^*(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to the explicit group

$$\mathcal{H}_E := \{g \in \mathcal{G} : g \cdot G = \gamma_E(\det g)\}$$

which is computable, cf. Remark 1.12.

Let $\mathcal{H}_E^t \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ be the group obtained by taking the transpose of all elements in $\mathcal{H}_E$. The groups $\rho_E(\mathrm{Gal}_{\mathbb{Q}})$ and $\mathcal{H}_E^t$ are then conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

## 13. Universal elliptic curves

Consider an open subgroup $G$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ that satisfies $\det(G) = \widehat{\mathbb{Z}}^\times$ and $-I \notin G$. Define the group $\mathcal{G} := \pm G$. From our definition in §3, we have $X_{\mathcal{G}} = X_G$. Recall that $U_G = U_{\mathcal{G}}$ is the open subvariety $X_G - \pi_G^{-1}(\{0, 1728, \infty\})$ of $X_G$.

We will say that an elliptic scheme $E \to U_G$ is a universal elliptic curve over $U_G$ if the following hold for any number field $K$:

- for any point $u \in U_G(K)$, the $j$-invariant of $E_u/K$ is $\pi_G(u)$, where the elliptic curve $E_u$ is the fiber of $E \to U_G$ over $u$,
- for all $u \in U_G(K)$, $\rho_{E_u}^*(\mathrm{Gal}_K)$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a subgroup of $G$.

In this section, we sketch some methods for computing such a universal elliptic curve. This will follows directly from other parts of the paper, but we state it here for convenient reference. We will not use this elsewhere.

*Remark* 13.1. In this paper, we have not taken a moduli point of view for modular curves. However, such a viewpoint makes the existence of a universal elliptic curve obvious; the underlying moduli space is fine since $-I \notin G$ (note that we are excluding elliptic curves with extra automorphisms by focusing on $U_G$). Moreover, using the moduli approach, one can also show that if $E'$ is an elliptic curve over a number field $K$ with $j_{E'} \in K - \{0, 1728\}$, then $\rho_{E'}^*(\mathrm{Gal}_K)$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a subgroup of $G$ if and only if $E'/K$ is isomorphic to $E_u$ for some $u \in U_G(K)$.

Let $N$ be the level of $G$. We have $N \geq 3$ since $-I \notin G$. Let $\overline{G}$ and $\overline{\mathcal{G}} = \pm\overline{G}$ be the images of $G$ and $\mathcal{G}$, respectively, in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. By Lemma 4.6, there is a nonzero modular form $f_0 \in M_{3,\overline{G}}$; we can construct such an $f_0$ by using Corollary 4.11. Define

$$\delta := j \cdot f_0^2/E_6;$$

it is a nonzero element of $\mathcal{F}_N^{\overline{G}} = \mathbb{Q}(X_G)$. All poles of $\delta$ lie above the points 0, 1 and $\infty$ on the $j$-line; recall that $E_6^2 = (j - 1728)\Delta$. In particular, we can view $\delta$ and $j$ as morphisms $U_G \to \mathbb{A}^1_{\mathbb{Q}}$.

Consider the Weierstrass equation:

$$\delta \cdot y^2 = x^3 - 27 \cdot j(j - 1728) \cdot x + 54 \cdot j(j - 1728)^2. \tag{13.1}$$

Let $U'$ be the maximal open subvariety of $U_G$ such that the valuation of $\delta$ at $P$ is even for all closed points $P$ of $U_G$. The equation (13.1) defines an elliptic scheme $E \to U'$. This is clear if we instead restrict to the smaller open subvariety of $U_G$ for which $\delta$ is nonzero. For excluded points of $U'$, we can scale $y$ appropriately and change coordinates, using our assumption on valuations, to extend the model.

**Proposition 13.2.** *We have $U' = U_G$ and $E \to U' = U_G$ defined by (13.1) is a universal elliptic curve over $U_G$.*

*Proof.* With notation as in §6.3, we have an elliptic scheme $\mathscr{E}_{\mathcal{G}} \to U_{\mathcal{G}}$ and a surjective homomorphism

$$\varrho_{\mathscr{E}_{\mathcal{G}},N}^*\colon \pi_1(U_{\mathcal{G}}, \overline{\eta}) \to \overline{\mathcal{G}}.$$

Recall that $\varrho_{\mathscr{E}_{\mathcal{G}},N}^*$ depends on a choice of a nonzero modular form $f_0$ in $M_3(\Gamma(N), \mathbb{Q}(\zeta_N))$ and a choice of $\beta$ in a field extension of $\mathcal{F}_N$ that satisfies $\beta^2 = j \cdot f_0^2/E_6$. By Lemma 4.6, we can assume that $f_0 \in M_{3,\overline{G}}$ since $-I \notin \overline{G}$. Let $\alpha\colon \pi_1(U_{\mathcal{G}}, \overline{\eta}) \to \overline{\mathcal{G}}/\overline{G}$ be the homomorphism obtained by composing $\varrho_{\mathscr{E}_{\mathcal{G}},N}^*$ with the quotient map $\overline{\mathcal{G}} \to \overline{\mathcal{G}}/\overline{G}$. Let $\chi\colon \pi_1(U_{\mathcal{G}}, \overline{\eta}) \to \{\pm 1\}$ be the character obtained by composing $\alpha$ with the isomorphism $\overline{\mathcal{G}}/\overline{G} \cong \{\pm 1\}$.

Take any number field $K \subseteq \overline{\mathbb{Q}}$ and point $u \in U_{\mathcal{G}}(K)$. The fiber $(\mathscr{E}_{\mathcal{G}})_u$ above $u$ is an elliptic curve over $K$ that is isomorphic to the curve given defined by (6.1) with $j = \pi_{\mathcal{G}}(u) \in K - \{0, 1728\}$. In particular, $(\mathscr{E}_{\mathcal{G}})_u$ has $j$-invariant $\pi_{\mathcal{G}}(u)$. The specialization of $\varrho_{\mathscr{E}_{\mathcal{G}},N}^*$ at $u$ is a representation $\mathrm{Gal}_K \to \overline{\mathcal{G}} \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that is isomorphic to $\rho_{(\mathscr{E}_{\mathcal{G}})_u,N}^*$. In particular, if $E'/K$ is the quadratic twist of $(\mathscr{E}_{\mathcal{G}})_u$ by the specialization $\chi_u\colon \mathrm{Gal}_K \to \{\pm 1\}$ of $\chi$ at $u$, then $E'$ has $j$-invariant $\pi_{\mathcal{G}}(u)$ and $\rho_{E',N}^*(\mathrm{Gal}_K)$ is conjugate in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ to a subgroup of $\overline{G}$.

Since $N$ is the level of $G$, we deduce that the elliptic scheme $E \to U_{\mathcal{G}} = U_G$ obtained by taking the quadratic twist of the elliptic scheme $\mathscr{E}_{\mathcal{G}} \to U_{\mathcal{G}}$ by $\chi$.

The homomorphisms $\alpha$ and $\chi$ correspond to an étale cover $\phi\colon Y \to U_{\mathcal{G}}$ of degree 2. With notation as in §11.1.1, $\phi$ corresponds to a quadratic extension $L/\mathbb{Q}(X_G)$ with $L \subseteq \mathcal{F}_N(\beta)$. Since $\beta^2 = \delta \in \mathbb{Q}(X_{\mathcal{G}})$, it suffices to prove that $L = \mathbb{Q}(X_{\mathcal{G}})(\beta)$. That $U' = U_{\mathcal{G}} = U_G$ is a consequence of $L/\mathbb{Q}(X_{\mathcal{G}})$ arising from an étale cover of $U_{\mathcal{G}}$.

The group $\overline{\mathcal{G}}/\overline{G}$ is cyclic of order 2 and $-I \notin \overline{G}$. With notation and definitions as in §11.3, we can assume that $m = 1$, $C = (-1)$, $g_0 = -I$, $k = 3$ and $f_1 := f_0$. Moreover, with $F(x_1) := x_1^2$ we

have $c_F = j \cdot f_0^2/E_6 = \delta$. By Lemma 11.3, we find that $L = \mathbb{Q}(X_{\mathcal{G}})(y_1)$ where $y_1^2 = \delta$. Since $\beta^2 = \delta$, we conclude that $L = \mathbb{Q}(X_{\mathcal{G}})(\beta)$. □

## 14. Families of modular curves

We now discuss a point of view that may be of use for further study of modular curves and Mazur's Program B; these remarks will not be used elsewhere in the paper.

Let $\mathcal{G}$ be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ satisfying $\det(\mathcal{G}) = \widehat{\mathbb{Z}}^\times$ and $-I \in \mathcal{G}$. Fix an closed subgroup $B$ of $\mathcal{G}$ satisfying $[\mathcal{G}, \mathcal{G}] \subseteq B$.

**Definition 14.1.** The family of groups associated to the pair $(\mathcal{G}, B)$ is the set $\mathscr{F}(\mathcal{G}, B)$ of subgroups $H$ of $\mathcal{G}$ that satisfy $\det(H) = \widehat{\mathbb{Z}}^\times$ and $H \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = B \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$.

Suppose that $\mathscr{F}(\mathcal{G}, B) \neq \emptyset$. Fix a group $G \in \mathscr{F}(\mathcal{G}, B)$. Note that $\mathscr{F}(\mathcal{G}, B) = \mathscr{F}(\mathcal{G}, G)$. Since $G \supseteq [\mathcal{G}, \mathcal{G}]$ and $G$ is open, we find that $G$ is a normal subgroup of $\mathcal{G}$ and that the group $\mathcal{G}/G$ is finite and abelian. For each homomorphism $\gamma\colon \widehat{\mathbb{Z}}^\times \to \mathcal{G}/G$, define the subgroup

$$G_\gamma := \{g \in \mathcal{G} : g \cdot G = \gamma(\det g)\}$$

of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

**Lemma 14.2.** *With notation as above, the set $\mathscr{F}(\mathcal{G}, B)$ consists of the groups $G_\gamma$ with $\gamma\colon \widehat{\mathbb{Z}}^\times \to \mathcal{G}/G$ a homomorphism.*

*Proof.* First take any $\gamma$. We have $G_\gamma \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = B$. The natural map $(\mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}))/B \to \mathcal{G}/G$ is an isomorphism since $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = B$ and $\det(G) = \widehat{\mathbb{Z}}^\times$. Using this isomorphism, we find that $\det(G_\gamma) = \widehat{\mathbb{Z}}^\times$. Therefore, $G_\gamma \in \mathscr{F}(\mathcal{G}, B)$.

Conversely, take any $H \in \mathscr{F}(\mathcal{G}, B)$. The quotient map $H \to \mathcal{G}/G$ induces a homomorphism $f\colon H/(H \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})) \to \mathcal{G}/G$ since $H \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = B = G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. Let $\gamma\colon \mathbb{Z}^\times \to \mathcal{G}/G$ be the homomorphism obtained by composing the inverse of the determinant map $H/(H \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})) \xrightarrow{\sim} \widehat{\mathbb{Z}}^\times$ with $f$. For each $h \in H$, we have $h \cdot G = \gamma(\det h)$. Therefore, $H \subseteq G_\gamma$. Since $H$ and $G_\gamma$ both have full determinant and have the same intersection with $\mathrm{SL}_2(\widehat{\mathbb{Z}})$, we conclude that $H = G_\gamma$. □

*Remark* 14.3. . We saw a family of groups in §1.6 when discussing Serre curves. In fact, one can show that $E/\mathbb{Q}$ is a Serre curve if and only if $\rho_E(\mathrm{Gal}_\mathbb{Q})$ is an element of $\mathscr{F}(\mathrm{GL}_2(\widehat{\mathbb{Z}}), [\mathrm{GL}_2(\widehat{\mathbb{Z}}), \mathrm{GL}_2(\widehat{\mathbb{Z}})])$. With terminology from [Jon15], $E/\mathbb{Q}$ is a "$\mathcal{G}$-Serre curve" if and only if $\rho_E(\mathrm{Gal}_\mathbb{Q})$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to some group in $\mathscr{F}(\mathcal{G}, [\mathcal{G}, \mathcal{G}])$.

Let us loosely reinterpret some our results from §1.4 and §1.5 in terms of families.

We have proved that there are finitely many pairs $\mathcal{G}_1, \ldots, \mathcal{G}_m$ such that for any non-CM elliptic curve $E/\mathbb{Q}$ for which Conjecture 1.2 holds, $\rho_E^*(\mathrm{Gal}_\mathbb{Q})$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a group in the family $\mathscr{F}(\mathcal{G}_i, [\mathcal{G}_i, \mathcal{G}_i])$ for some $1 \leq i \leq m$. The agreeable closure of $\rho_E^*(\mathrm{Gal}_\mathbb{Q})$, computed as in §1.4, determines which of our explicit families $\mathscr{F}(\mathcal{G}_i, [\mathcal{G}_i, \mathcal{G}_i])$ our group lies in. Once we know the specific family of groups, the results from §1.5 allow us to identify $\rho_E^*(\mathrm{Gal}_\mathbb{Q})$ in the family by constructing the appropriate homomorphism $\gamma_E\colon \widehat{\mathbb{Z}}^\times \to \mathcal{G}_i/G_i$, where $G_i$ is a fixed group in $\mathscr{F}(\mathcal{G}_i, [\mathcal{G}_i, \mathcal{G}_i])$.

So that we can talk about modular curves and groups interchangeably, let us now consider the case a nonempty family $\mathscr{F}(\mathcal{G}, B)$ for which $-I \in B$. As before, fix $G \in \mathscr{F}(\mathcal{G}, B)$; we have $-I \in G$.

Let $\pi\colon X_G \to X_{\mathcal{G}}$ be the morphism of modular curves induced by the inclusion $G \subseteq \mathcal{G}$. Since $G$ is a normal subgroup of $\mathcal{G}$, the group $\mathcal{G}$ acts on the modular curve $X_G$ with $G$ acting trivially. This induces an isomorphism $\mathcal{G}/G \xrightarrow{\sim} \mathrm{Aut}(X_G/X_{\mathcal{G}})$, where $\mathrm{Aut}(X_G/X_{\mathcal{G}})$ is the group of automorphisms $f$ of the curve $X_G$ that satisfy $\pi \circ f = \pi$.

For a fixed homomorphism $\gamma\colon \widehat{\mathbb{Z}}^\times \to \mathcal{G}/G$, we obtain a homomorphism

$$\xi := \gamma \circ \chi_{\mathrm{cyc}}^{-1}\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathcal{G}/G \cong \mathrm{Aut}(X_G/X_{\mathcal{G}}).$$

In particular, we can view $\xi$ as a 1-cocycle of $X_G$. Twisting $X_G$ by $\xi$ gives a curve $(X_G)_\xi$ and a morphism $\pi_\xi\colon (X_G)_\xi \to X_{\mathcal{G}}$ that are both defined over $\mathbb{Q}$. A straightforward computation shows that we can in fact take $(X_G)_\xi = X_{G_\gamma}$ with $\pi_\xi\colon X_{G_\gamma} \to X_{\mathcal{G}}$ being the morphism induced by the inclusion $G_\gamma \subseteq \mathcal{G}$. So our family of groups $\mathscr{F}(\mathcal{G}, B) = \mathscr{F}(\mathcal{G}, G)$ corresponds to a family of twists $\{(X_G)_\xi\}_\xi$ as we vary over 1-cocycles $\xi\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{Aut}(X_G/X_{\mathcal{G}})$.

Note that the modular curve $X_{G_\gamma}$ need not have a rational non-CM point for every $\gamma$ (moreover, there are families where $X_{G_\gamma}(\mathbb{Q}) = \emptyset$ for all $\gamma$).

Consider two pairs $(C_1, \pi_1)$ and $(C_2, \pi_2)$, where $C_i$ is a curve over $\mathbb{Q}$ and $\pi_i\colon C_i \to \mathbb{P}^1_{\mathbb{Q}}$ is a morphism. We say that the pairs $(C_1, \pi_1)$ and $(C_2, \pi_2)$ are isomorphic if there is an isomorphism $f\colon C_1 \to C_2$ defined over $\mathbb{Q}$ so that $\pi_2 \circ f = \pi_1$. Rakvi [Rak21] has recently classified the pairs $(X_G, \pi_G)$, up to isomorphism, for which $G$ is an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ satisfying $\det(G) = \widehat{\mathbb{Z}}^\times$, $-I \in G$, and $X_G \cong \mathbb{P}^1_{\mathbb{Q}}$. She accomplishes this by showing that all such group $G$ lie in a finite number of families and then identifying which curves arising from these families are isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$.

## References


[AKM+01] Sang Yook An, Seog Young Kim, David C. Marshall, Susan H. Marshall, William G. McCallum, and Alexander R. Perlis, *Jacobians of genus one curves*, J. Number Theory **90** (2001), no. 2, 304–315, DOI 10.1006/jnth.2000.2632. MR1858080 ↑5.4.4

[BDM+19] Jennifer Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk, *Explicit Chabauty-Kim for the split Cartan modular curve of level 13*, Ann. of Math. (2) **189** (2019), no. 3, 885–944, DOI 10.4007/annals.2019.189.3.6. MR3961086 ↑1.9

[BDM+21] ———, *Quadratic Chabauty for modular curves: Algorithms and examples* (2021). arXiv:2101.01862 [math.NT]. ↑1.9

[BBB+21] Alex Best, Jonathan Bober, Andrew Booker, Edgar Costa, John Cremona, Maarten Derickx, Min Lee, David Lowry-Duda, David Roe, Andrew Sutherland, and John Voight, *Computing classical modular forms*, Arithmetic Geometry, Number Theory, and Computation, 2021, pp. 131–213. ↑4

[BPR13] Yuri Bilu, Pierre Parent, and Marusia Rebolledo, *Rational points on $X_0^+(p^r)$*, Ann. Inst. Fourier (Grenoble) **63** (2013), no. 3, 957–984, DOI 10.5802/aif.2781 (English, with English and French summaries). MR3137477 ↑1.9

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Computational algebra and number theory (London, 1993). ↑1.1, 1.11

[Bou03] Nicolas Bourbaki, *Algebra II. Chapters 4–7*, Elements of Mathematics (Berlin), Springer-Verlag, Berlin, 2003. Translated from the 1981 French edition by P. M. Cohn and J. Howie; Reprint of the 1990 English edition [Springer, Berlin; MR1080964 (91h:00003)]. ↑4.6

[BJ16] Julio Brau and Nathan Jones, *Elliptic curves with 2-torsion contained in the 3-torsion field*, Proc. Amer. Math. Soc. **144** (2016), no. 3, 925–936. ↑1.9

[BA15] Julio Brau Avilo, *Galois representations of elliptic curves and abelian entanglements*, Doctoral Thesis, Leiden University, 2015. ↑1.9

[Bru17] François Brunault, *Régulateurs modulaires explicites via la méthode de Rogers-Zudilin*, Compos. Math. **153** (2017), no. 6, 1119–1152, DOI 10.1112/S0010437X17007023 (French, with English and French summaries). MR3705252 ↑4.7

[BN19] François Brunault and Michael Neururer, *Fourier expansions at cusps*, The Ramanujan Journal (2019). ↑4.5, 4.5, 4.7, 4.7

[Coh93] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993. MR1228206 ↑ii

[CP03] C. J. Cummins and S. Pauli, *Congruence subgroups of* $\mathrm{PSL}(2,\mathbb{Z})$ *of genus less than or equal to 24*, Experiment. Math. **12** (2003), no. 2, 243–255. ↑4.6

[DLRM21] Harris Daniels, Álvaro Lozano-Robledo, and Jackson Morrow, *A group theoretic perspective on entanglements of division fields* (2021). arXiv:2105.02060 [math.NT]. ↑1.9

[DM22] Harris Daniels and Jackson Morrow, *A group theoretic perspective on entanglements of division fields* (2022). arXiv:2008.09886 [math.NT]. ↑1.9

[Fis08] Tom Fisher, *The invariants of a genus one curve*, Proc. Lond. Math. Soc. (3) **97** (2008), no. 3, 753–782, DOI 10.1112/plms/pdn021. MR2448246 ↑5.4.4

[Jon09] Nathan Jones, *A bound for the torsion conductor of a non-CM elliptic curve*, Proc. Amer. Math. Soc. **137** (2009), no. 1, 37–43, DOI 10.1090/S0002-9939-08-09436-7. MR2439422 ↑1.9

[Jon10] ———, *Almost all elliptic curves are Serre curves*, Trans. Amer. Math. Soc. **362** (2010), no. 3, 1547–1570. ↑ii

[Jon15] ———, $\mathrm{GL}_2$*-representations with maximal image*, Math. Res. Lett. **22** (2015), no. 3, 803–839, DOI 10.4310/MRL.2015.v22.n3.a10. MR3350106 ↑1.9, 14.3

[Jon20] ———, *A bound for the conductor of an open subgroup of* $\mathrm{GL}_2$ *associated to an elliptic curve*, Pacific J. Math. **308** (2020), no. 2, 307–331, DOI 10.2140/pjm.2020.308.307. MR4190460 ↑1.9

[JM22] Nathan Jones and Ken McMurdy, *Elliptic curves with non-abelian entanglements*, New York J. Math. **28** (2022), 182–229. ↑1.9

[Kat04] Kazuya Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque **295** (2004), ix, 117–290 (English, with English and French summaries). Cohomologies p-adiques et applications arithmétiques. III. MR2104361 ↑4.7

[Kat73] Nicholas M. Katz, *p-adic properties of modular schemes and modular forms*, Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 69–190. Lecture Notes in Mathematics, Vol. 350. ↑4.5

[KM12] Kamal Khuri-Makdisi, *Moduli interpretation of Eisenstein series*, Int. J. Number Theory **8** (2012), no. 3, 715–748, DOI 10.1142/S1793042112500418. MR2904927 ↑4.7

[LT76] Serge Lang and Hale Trotter, *Frobenius distributions in* $\mathrm{GL}_2$*-extensions*, Lecture Notes in Mathematics, Vol. 504, Springer-Verlag, Berlin, 1976. Distribution of Frobenius automorphisms in $GL_2$-extensions of the rational numbers. MR0568299 (58 #27900) ↑1.6, 7.3

[Maz77a] B. Mazur, *Rational points on modular curves*, Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), Springer, Berlin, 1977, pp. 107–148. Lecture Notes in Math., Vol. 601. MR0450283 ↑1.9

[Maz77b] ———, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186 (1978). With an appendix by Mazur and M. Rapoport. MR488287 ↑1.9

[Maz78] ———, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162, DOI 10.1007/BF01390348. MR482230 ↑1.9

[Mor19] Jackson S. Morrow, *Composite images of Galois for elliptic curves over* $\mathbf{Q}$ *and entanglement fields*, Math. Comp. **88** (2019), no. 319, 2389–2421, DOI 10.1090/mcom/3426. MR3957898 ↑1.9

[Mum70] David Mumford, *Varieties defined by quadratic equations*, Questions on Algebraic Varieties (C.I.M.E., III Ciclo, Varenna, 1969), Edizioni Cremonese, Rome, 1970, pp. 29–100. MR0282975 ↑5.3.1

[Rak21] Rakvi, *A Classification of Genus* 0 *Modular Curves with Rational Points* (2021). arXiv:2105.14623 [math.NT]. ↑1.9, 14

[Rib76] K. A. Ribet, *Galois action on division points of abelian varieties with real multiplications*, Amer. J. Math. **98** (1976), no. 3, 751–804. ↑7.1

[RSZB22] Jeremy Rouse, Andrew Sutherland, and David Zureick-Brown, *$\ell$-adic images of Galois for elliptic curves over* $\mathbb{Q}$ (2022). arXiv:2 106.11141 [math.NT]. ↑1.9, 9.1, 9.3, 10.2, 12.3.2

[RZB15] Jeremy Rouse and David Zureick-Brown, *Elliptic curves over* $\mathbb{Q}$ *and 2-adic images of Galois*, Res. Number Theory **1** (2015), Paper No. 12, 34, DOI 10.1007/s40993-015-0013-7. MR3500996 ↑1.9

[SD72] Bernard Saint-Donat, *Sur les équations définissant une courbe algébrique*, C. R. Acad. Sci. Paris Sér. A-B **274** (1972), A324–A327 (French). MR289516 ↑5.3.1

[Ser72] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331. ↑1.1, 1.1, 1.8, 1.6, 1.9, 7.4, 8.2

[Ser81] ———, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. **54** (1981), 323–401. ↑1.1

[Ser98] ———, *Abelian l-adic representations and elliptic curves*, Research Notes in Mathematics, vol. 7, A K Peters Ltd., Wellesley, MA, 1998. With the collaboration of Willem Kuyk and John Labute; Revised reprint of the 1968 original. ↑7.2

[Shi94] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original; Kanô Memorial Lectures, 1. ↑3.1, 3.1, 4, 4.4, 4.4, 4.6, 5.3.3, 5.4.2, 6.1, 6.1

[Sut16] Andrew V. Sutherland, *Computing images of Galois representations attached to elliptic curves*, Forum Math. Sigma **4** (2016), Paper No. e4, 79. MR3482279 ↑1.1, 1.9

[SZ17] Andrew V. Sutherland and David Zywina, *Modular curves of prime-power level with infinitely many rational points*, Algebra Number Theory **11** (2017), no. 5, 1199–1229, DOI 10.2140/ant.2017.11.1199. MR3671434 ↑1.9, 9.1

[Zyw10] David Zywina, *Elliptic curves with maximal Galois action on their torsion points*, Bull. Lond. Math. Soc. **42** (2010), no. 5, 811–826. ↑iii, 7.3

[Zyw15a] _____, *Possible indices for the Galois image of elliptic curves over* $\mathbb{Q}$ (2015). arXiv:1508.07663 [math.NT]. ↑1.1, 1.9, 5.4.4

[Zyw15b] _____, *On the possible images of the mod* $\ell$ *representations associated to elliptic curves over* $\mathbb{Q}$ (2015). arXiv:1508.07660 [math.NT]. ↑1.1, 1.9

[Zyw20a] _____, *Computing actions on cusp forms* (2020). arXiv:2001.07270 [math.NT]. ↑vii, 5.3.2

[Zyw20b] _____, *On the surjectivity of mod* $\ell$ *representations associated to elliptic curves* (2020). arXiv:1508.07661 [math.NT] (To appear: Bulletin of the London Mathematical Society). ↑1.4, 1.9, 10.1

[Zyw22] _____, GitHub repository related to *Explicit open images for elliptic curves over* $\mathbb{Q}$, 2022. `https://github.com/davidzywina/OpenImage`. ↑1.1, 1.11, 10, 10.2

Department of Mathematics, Cornell University, Ithaca, NY 14853, USA
*Email address*: `zywina@math.cornell.edu`