OPEN IMAGE COMPUTATIONS FOR ELLIPTIC CURVES OVER NUMBER FIELDS

DAVID ZYWINA

Abstract. For a non-CM elliptic curve E defined over a number field K, the Galois action on its torsion points gives rise to a Galois representation $\rho_E\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$ that is unique up to isomorphism. A renowned theorem of Serre says that the image of ρ_E is an open, and hence finite index, subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. In an earlier work of the author, an algorithm was given, and implemented, that computed the image of ρ_E up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ in the special case $K = \mathbb{Q}$. A fundamental ingredient of this earlier work was the Kronecker–Weber theorem whose conclusion fails for number fields $K \neq \mathbb{Q}$. We shall give an overview of an analogous algorithm for a general number field and work out the required group theory. We also give some bounds on the index in Serre's theorem for a typical elliptic curve over a fixed number field.

1. Introduction

1.1. **Serre's open image theorem.** Let E be an elliptic curve defined over a number field K. We denote its j-invariant by j_E. For each integer $N > 1$, let $E[N]$ be the N-torsion subgroup of $E(\overline{K})$, where $\overline{K}$ is a fixed algebraic closure of K. The group $E[N]$ is a free $\mathbb{Z}/N\mathbb{Z}$-module of rank 2. The absolute Galois group $\mathrm{Gal}_K := \mathrm{Gal}(\overline{K}/K)$ acts on $E[N]$ and respects the group structure. We may express this Galois action in terms of a representation $\rho_{E,N}\colon \mathrm{Gal}_K \to \mathrm{Aut}(E[N]) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. By choosing compatible bases and taking the inverse limit, these representations combine into a single Galois representation

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

where $\widehat{\mathbb{Z}}$ is the profinite completion of $\mathbb{Z}$. The representation ρ_E is uniquely determined up to isomorphism and hence the image $\rho_E(\mathrm{Gal}_K)$ is uniquely determined up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. With respect to the profinite topologies, we find that ρ_E is continuous and hence $\rho_E(\mathrm{Gal}_K)$ 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 ρ_E is as large as possible when E is non-CM.

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

Consider a non-CM elliptic curve E over a number field K. We will find it convenient to instead work with the dual representation

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

2020 *Mathematics Subject Classification.* Primary 11G05; Secondary 11F80.

of ρ_E, i.e., $\rho_E^*(\sigma)$ is the transpose of $\rho_E(\sigma^{-1})$. Similarly, we can define $\rho_{E,N}^*$. Define the group $G_E := \rho_E^*(\mathrm{Gal}_K)$. The group G_E is uniquely determined up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and is open in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ by Theorem 1.1. Of course, computing G_E is equivalent to computing the image of ρ_E since $\rho_E(\mathrm{Gal}_K) = \{A^t : A \in G_E\}$. The group G_E, 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 $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

Serre's proof is ineffective in general. In the special case $K = \mathbb{Q}$, the author has recently given, and fully implemented, an algorithm to compute G_E up to conjugacy, see [Zyw22b]. The images for all non-CM elliptic curves over $\mathbb{Q}$ of conductor at most 500000 are easily accessible via the LMFDB [LMFDB].

The goal of this article is to begin the study of how to compute the groups G_E for a general number K. A vital ingredient in the arguments of [Zyw22b] is that the commutator subgroup of G_E agrees with $G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ when $K = \mathbb{Q}$; this makes use of the Kronecker–Weber theorem, cf. §2.1. When $K \neq \mathbb{Q}$, the commutator subgroup of G_E is usually strictly smaller than $G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. Much of this paper is dedicated to dealing with the new group theoretic complications that arise for this reason.

Fix a number field K. We shall give an algorithm which defines a finite set $J_K \subseteq K$ and computes the group G_E, up to conjugacy, for all non-CM elliptic curves E over K whose j-invariant does not lie in J_K and for which $\rho_{E,\ell}(\mathrm{Gal}_K) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ holds for all primes $\ell > 19$.

Our set J_K and our algorithm depend only on a *finite* number of modular curves and morphisms which do not depend on K (these curves and morphisms can thus be precomputed). Given any number in K, we will be able to determine whether or not it lies in J_K (explicitly giving the set is much harder since its finiteness uses Faltings theorem). The group theoretic aspects of the algorithm have been fully implemented. The modular curve computations have not been performed yet. In fact, one of the main goals of this work was to confirm there were not too many cases as to make the modular curve computations infeasible.

From our group theory computations, we are able to prove the following theorem which bounds the index $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E]$ for most non-CM elliptic curves E over a fixed number field K. We have

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E] = [\widehat{\mathbb{Z}}^\times : \det(G_E)] \cdot [\mathrm{SL}_2(\widehat{\mathbb{Z}}) : G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})].$$

Since the group $\det(G_E)$ depends only on K, see §2.1, we will focus on the index $[\mathrm{SL}_2(\widehat{\mathbb{Z}}) : G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})]$.

Theorem 1.2. *Let K be a number field. There is a finite set $J_K \subseteq K$ such that for any non-CM elliptic curve E over K with $j_E \notin J_K$ and $\rho_{E,\ell}(\mathrm{Gal}_K) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all primes $\ell > 19$, we have*

$$[\mathrm{SL}_2(\widehat{\mathbb{Z}}) : G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})] \leq \begin{cases} 1382400, & \\ 677376 & \text{if } K \not\supseteq \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \sqrt{5}), \\ 172800 & \text{if } K \cap \mathbb{Q}(\sqrt{-1}) = \mathbb{Q}, \\ 30000 & \text{if } K \cap \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}) = \mathbb{Q}, \\ 7200 & \text{if } K \cap \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}) = \mathbb{Q}, \\ 1536 & \text{if } K = \mathbb{Q}. \end{cases}$$

We will prove Theorem 1.2 in §2.3 where we reduce it to a direct computation involving a finite number of open subgroups of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

Remark 1.3.

(i) A well-known uniformity conjecture (Conjecture 2.11) would imply that Theorem 1.2 still holds after removing the assumption on the images of the $\rho_{E,\ell}$.

(ii) The index $[\mathrm{SL}_2(\widehat{\mathbb{Z}}) : G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})]$ can of course become arbitrarily large as we vary over all number fields K and all non-CM elliptic curves E/K. For example, consider a fixed non-CM elliptic curve $E/\mathbb{Q}$ base extended by $K := \mathbb{Q}(E[2^i])$ with integers $i \geq 0$. Theorem 1.2, along with Conjecture 2.11, shows that large indices are rare when the number field K is fixed.

1.2. **Notation.** We now give 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 closed 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 ordered by divisibility. With the profinite topology, $\mathbb{Z}_N$ and $\widehat{\mathbb{Z}}$ are compact topological rings. We have natural isomorphisms

$$\mathbb{Z}_N = \prod\nolimits_{\ell \mid N} \mathbb{Z}_\ell \quad \text{and} \quad \widehat{\mathbb{Z}} = \mathbb{Z}_N \times \prod\nolimits_{\ell \nmid N} \mathbb{Z}_\ell = \prod\nolimits_{\ell} \mathbb{Z}_\ell,$$

where the products are over primes ℓ. The symbol ℓ will always denote a rational prime. Fix a positive integer n dividing a power of N. For a subgroup G of $\mathrm{GL}_2(\mathbb{Z}_N)$ or $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, let $G_n \subseteq \mathrm{GL}_2(\mathbb{Z}_n)$ be the group that is the image of G under the n-adic projection map. From context it should be clear when we have G_i with an index i instead.

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 $\mathrm{SL}_2(\mathbb{Z}_N)$.

We shall view $\overline{\mathbb{Q}}$ and any other algebraic field extension of $\mathbb{Q}$ that arise as subfields of $\mathbb{C}$ (this is mainly to ensure easy comparison with the analytic theory when working with modular curves).

1.3. **Acknowledgements.** The computations in this paper were performed using the Magma computer algebra system [BCP97].

2. Overview of ideas and group theoretic results

2.1. **Cyclotomic 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 $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$.

Fix a number field K and a non-CM elliptic curve E over K. We can identify K with a subfield of $\overline{\mathbb{Q}}$ and take $\overline{K}=\overline{\mathbb{Q}}$. Using the Weil pairing on $E[n]$ for $n\geq 1$, one can show that $\det\circ\rho_E^* = \chi_{\mathrm{cyc}}^{-1}|_{\mathrm{Gal}_K}$. In particular, $\det(G_E)=\chi_{\mathrm{cyc}}(\mathrm{Gal}_K)$ is an open subgroup of $\widehat{\mathbb{Z}}^\times$ that depends only on K.

Let K^{cyc} be the cyclotomic extension of K in $\overline{K}$. We have an inclusion $K^{\mathrm{cyc}}\subseteq K^{\mathrm{ab}}$, where K^{ab} is the maximal abelian extension of K. The *Kronecker–Weber theorem* says that $\mathbb{Q}^{\mathrm{cyc}}=\mathbb{Q}^{\mathrm{ab}}$. We have $K^{\mathrm{cyc}}\subsetneq K^{\mathrm{ab}}$ when $K\neq\mathbb{Q}$.

Lemma 2.1.

(i) *We have* $\rho_E^*(\mathrm{Gal}_{K^{\mathrm{cyc}}}) = G_E\cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ *and* $\rho_E^*(\mathrm{Gal}_{K^{\mathrm{ab}}})=[G_E,G_E]$.

(ii) *We have an inclusion* $[G_E,G_E]\subseteq G_E\cap\mathrm{SL}_2(\widehat{\mathbb{Z}})$.

(iii) *If* $K=\mathbb{Q}$, *then* $[G_E,G_E]=G_E\cap\mathrm{SL}_2(\widehat{\mathbb{Z}})$.

Proof. We have $\rho_E^*(\mathrm{Gal}(\overline{K}/K^{\mathrm{ab}}))=[G_E,G_E]$ since $\mathrm{Gal}(\overline{K}/K^{\mathrm{ab}})$ is the commutator subgroup of Gal_K. Since $\chi_{\mathrm{cyc}}^{-1}=\det\circ\rho_E^*$, we have $\rho_E^*(\mathrm{Gal}(\overline{K}/K^{\mathrm{cyc}}))=G_E\cap\mathrm{SL}_2(\widehat{\mathbb{Z}})$. The inclusion $[G_E,G_E]\subseteq G_E\cap\mathrm{SL}_2(\widehat{\mathbb{Z}})$ thus follows from $K^{\mathrm{cyc}}\subseteq K^{\mathrm{ab}}$. We have equality when $K=\mathbb{Q}$ since $\mathbb{Q}^{\mathrm{cyc}}=\mathbb{Q}^{\mathrm{ab}}$. □

Example 2.2. Consider any number field $K\neq\mathbb{Q}$. The main result of [Zyw10] implies that for a "random" elliptic curve E/K, we have $G_E\supseteq\mathrm{SL}_2(\widehat{\mathbb{Z}})$. For such an elliptic curve E/K, we have

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

where $[G_E,G_E]\neq\mathrm{SL}_2(\widehat{\mathbb{Z}})$ can be shown by noting that the commutator subgroup of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ is a proper subgroup of $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$.

Now suppose that $K=\mathbb{Q}$. Since $[G_E,G_E]=G_E\cap\mathrm{SL}_2(\widehat{\mathbb{Z}})$ by Lemma 2.1(iii) and $[G_E,G_E]\subsetneq\mathrm{SL}_2(\widehat{\mathbb{Z}})$, we find that $G_E\not\supseteq\mathrm{SL}_2(\widehat{\mathbb{Z}})$. That $\rho_E\colon\mathrm{Gal}_{\mathbb{Q}}\to\mathrm{GL}_2(\widehat{\mathbb{Z}})$ is never surjective was first observed by Serre, cf. Proposition 22 of [Ser72].

2.2. **Modular curves.** Let G be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ that contains $-I$. We define K_G to be the unique subfield of $\mathbb{Q}^{\mathrm{cyc}}$ for which $\chi_{\mathrm{cyc}}(\mathrm{Gal}(\overline{\mathbb{Q}}/K_G))=\det(G)$; it is a number field.

Associated to G, there is a modular curve X_G; it is a smooth projective and geometrically irreducible curve defined over K_G that comes with a morphism

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

We define the genus of the group G to be the genus of the curve X_G. For our applications, the following property of these curves is key.

Proposition 2.3. *For any number field* $K\subseteq\overline{\mathbb{Q}}$ *and non-CM elliptic curve* E/K, $\rho_E^*(\mathrm{Gal}_K)$ *is conjugate in* $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ *to a subgroup of* G *if and only if* $K\supseteq K_G$ *and* $j_E\in\pi_G(X_G(K))$.

Remark 2.4. Modular curves are fully discussed in §3 of [Zyw22b] with the additional assumption $\det(G)=\widehat{\mathbb{Z}}^\times$ (equivalently, $K_G=\mathbb{Q}$). We now make some remarks indicating that everything in §3 of [Zyw22b] carries over straightforwardly to the general setting. Let N be a positive integer divisible by the level of G and let $\overline{G}\subseteq\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be the image of G modulo N. With notation as in [Zyw22b, §3], we define X_G to be smooth, projective and geometrically irreducible curve over K_G whose function field $\mathcal{F}_N^{\overline{G}}$; this field indeed has transcendence degree 1 over $\mathbb{Q}$ and the

number field K_G is the algebraically closure of $\mathbb{Q}$ in $\mathcal{F}_N^{\overline{G}}$. The field $K_G(X_G) = \mathcal{F}_N^{\overline{G}}$ consists of modular functions of level N and contains the modular j-invariant j. The inclusion of function fields $K_G(X_G) \supseteq K_G(j)$ induces a dominant morphism $\pi_G\colon X_G \to \mathbb{P}^1_{K_G} = \operatorname{Spec} K_G[j] \cup \{\infty\} = \mathbb{A}^1_{K_G} \cup \{\infty\}$ of curves over K_G. Since $\det(G_E) = \chi_{\mathrm{cyc}}(\mathrm{Gal}_K)$, we have $\det(G_E) \subseteq \det(G)$ if and only if $K \supseteq K_G$. Proposition 2.3 is proved in the same manner as [Zyw22b, Proposition 6.4] by working over K_G instead of $\mathbb{Q}$.

Let Γ_G be the congruence subgroup consisting of matrices in $\mathrm{SL}_2(\mathbb{Z})$ whose image modulo N lies in $\overline{G}$. With our implicit embedding $K_G \subseteq \mathbb{C}$, there is an isomorphism of smooth compact Riemann surface between $X_G(\mathbb{C})$ and $\mathcal{X}_{\Gamma_G} := \Gamma_G \backslash \mathcal{H}^*$, where $\mathcal{H}^*$ is the extended complex upper half-plane and Γ_G acts on it by linear fractional transformations (as noted in §3.3 of [Zyw22b], they have the same function field). In particular, the genus of Γ_G, i.e., the genus of $\mathcal{X}_{\Gamma_G}$, agrees with the genus of G.

There are many approaches to computing models of X_G. In §5 of [Zyw22b], we give an algorithm for computing a model of X_G using modular forms under the assumption $\det(G) = \widehat{\mathbb{Z}}^\times$. This assumption is not needed with the only change being that the spaces of modular forms $M_{k,G}$ that arise in [Zyw22b] are now vector spaces over K_G instead of $\mathbb{Q}$. For our exposition below, we will take it for granted that one can always compute a model of X_G in terms of modular forms/functions. With respect to this model, one can also compute the morphism π_G.

2.3. **The agreeable closure.** Our initial strategy in computing the group G_E is to instead compute a larger group that has the same commutator subgroup. We first define the class of groups we will consider.

We say that a subgroup $\mathcal{G}$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ is agreeable if it is open, contains all the scalar matrices in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, and each prime dividing the level of $\mathcal{G}$ also divides the level of $[\mathcal{G},\mathcal{G}] \subseteq \mathrm{SL}_2(\widehat{\mathbb{Z}})$. This definition uses that $[\mathcal{G},\mathcal{G}]$ is open in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$, cf. Lemma 3.3. For any open subgroup G of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, there is a unique minimal agreeable subgroup $\mathcal{G}$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ that satisfies $G \subseteq \mathcal{G}$, cf. §4.1. We call $\mathcal{G}$ the agreeable closure of G. We have $[G,G] = [\mathcal{G},\mathcal{G}]$, cf. Lemma 4.1.

Let $\mathcal{A}_1'$ be the set of subgroups of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ that are agreeable and have genus at most 1. The set $\mathcal{A}_1'$ is stable under conjugation by $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. Let $\mathcal{A}_1$ be a set of representatives of the $\mathrm{GL}_2(\widehat{\mathbb{Z}})$-conjugacy classes of $\mathcal{A}_1'$.

Theorem 2.5. *The set $\mathcal{A}_1$ is finite and computable. For all $G \in \mathcal{A}_1$, the level of $[G,G] \subseteq \mathrm{SL}_2(\widehat{\mathbb{Z}})$ is not divisible by any prime $\ell > 19$.*

Theorem 2.5, along with the other theorems in §2.3, will be proved in §5. The groups in $\mathcal{A}_1$, up to conjugacy, can be found it the repository [Zyw24]. The set $\mathcal{A}_1$ has cardinality 11972. The number of groups $G \in \mathcal{A}_1$ in terms of genus and the index $[\widehat{\mathbb{Z}}^\times : \det(G)]$ is given in Table 1. The largest level of a group in $\mathcal{A}_1$ is 1176.

	1	2	2^2	2^3	2^4
genus 0	418	1490	1319	417	38
genus 1	1078	3383	2897	868	64

TABLE 1. Number of groups G in $\mathcal{A}_1$ broken up by the genus and the index of $\det(G)$ in $\widehat{\mathbb{Z}}^\times$.

Let $\mathcal{A}_2'$ be the set of agreeable subgroups $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ such that the following hold:

- G has genus at least 2 and every agreeable group $G \subsetneq G' \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ has genus at most 1,
- the level of G is not divisible by any prime $\ell > 19$.

The set $\mathcal{A}_2'$ is stable under conjugation by $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. Let $\mathcal{A}_2$ be a set of representatives of the $\mathrm{GL}_2(\widehat{\mathbb{Z}})$-conjugacy classes of $\mathcal{A}_2'$.

Theorem 2.6.

(i) *The set $\mathcal{A}_2$ is finite and computable.*

(ii) *Take any agreeable subgroup G of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ with genus at least 2 that satisfies $G_\ell \supseteq \mathrm{SL}_2(\mathbb{Z}_\ell)$ for all $\ell > 19$. Then G is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a subgroup of some group in $\mathcal{A}_2$.*

For each number field K, let J_K be the intersection of K with the subset

$$\bigcup_{G \in \mathcal{A}_2,\, K_G \subseteq K} \pi_G(X_G(K))$$

of $K \cup \{\infty\}$. The set J_K is finite by Theorem 2.6(i) and Faltings theorem.

Theorem 2.7. *Let K be a number field and let E/K be a non-CM elliptic curve with $j_E \notin J_K$ that satisfies $\rho_{E,\ell}(\mathrm{Gal}_K) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all primes $\ell > 19$. Take a group $G \in \mathcal{A}_1$ with maximal index $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G]$ for which $K_G \subseteq K$ and $j_E \in \pi_G(X_G(K))$. Then G and the agreeable closure of G_E are conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.*

Since the sets $\mathcal{A}_1$ and $\mathcal{A}_2$ are both finite, we can compute a model for the curve X_G and compute the morphism π_G, with respect to this model, for each group $G \in \mathcal{A}_1 \cup \mathcal{A}_2$.

We can effectively determine whether a number in K lies in the set J_K by using explicit models of the curves X_G for $G \in \mathcal{A}_2$. Using explicit models of X_G, with $G \in \mathcal{A}_1$, Theorem 2.7 lets us compute the agreeable closure of G_E, up to conjugacy, for all elliptic curves E/K satisfying the assumptions of the theorem.

Proof of Theorem 1.2. Consider a number field K. Take any non-CM elliptic curve E/K with $j_E \notin J_K$ and $\rho_{E,\ell}(\mathrm{Gal}_K) \supseteq \mathrm{SL}_2(\mathbb{Z}_\ell)$ for $\ell > 19$. By Thereom 2.7, there is a group $\mathcal{G} \in \mathcal{A}_1$ that is conjugate to the agreeable closure of G_E. There is no harm in conjugating G_E so that $G_E \subseteq \mathcal{G}$. We have $[\mathcal{G}, \mathcal{G}] = [G_E, G_E]$ since $\mathcal{G}$ is the agreeable closure of G_E. Therefore, $[\mathcal{G}, \mathcal{G}] \subseteq G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ by Lemma 2.1(ii). In particular, we have

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

The group $\widehat{\mathbb{Z}}^\times / \det(\mathcal{G})$ is an elementary 2-group since $\widehat{\mathbb{Z}}^\times I \subseteq \mathcal{G}$. Therefore, the number field $K_{\mathcal{G}}$ is the compositum of quadratic extensions of $\mathbb{Q}$. We have $K_{\mathcal{G}} \subseteq K$ since $\chi_{\mathrm{cyc}}(\mathrm{Gal}_K) = \det(G_E) \subseteq \det(\mathcal{G})$.

For the finite number of groups $\mathcal{G} \in \mathcal{A}_1$, one can compute the index $[\mathrm{SL}_2(\widehat{\mathbb{Z}}) : [\mathcal{G}, \mathcal{G}]]$ and the number field $K_{\mathcal{G}}$; this data can be found in [Zyw24]. All but the last inequality in Theorem 1.2 follow from a direct inspection of this data.

Suppose $K = \mathbb{Q}$. Only groups $\mathcal{G} \in \mathcal{A}_1$ with $\det(\mathcal{G}) = \widehat{\mathbb{Z}}^\times$ will arise. After possibly increasing the finite set J_K, we need only consider those groups $\mathcal{G}$ for which $X_{\mathcal{G}}(\mathbb{Q})$ is infinite. This was worked out in [Zyw22b]. □

2.4. **Some abelian quotients.** Fix an agreeable subgroup $\mathcal{G}$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. Consider any non-CM elliptic curve E over a number field K for which the agreeable closure of G_E is $\mathcal{G}$. We have $[G_E, G_E] = [\mathcal{G}, \mathcal{G}]$ so G_E is a normal subgroup of $\mathcal{G}$ and $\mathcal{G}/G_E$ is abelian. Moreover, $\mathcal{G}/G_E$ is a finite abelian groups since G_E is open in $\mathcal{G}$ by Theorem 1.1.

There may be infinitely many open subgroups G of $\mathcal{G}$ with $[\mathcal{G}, \mathcal{G}] \subseteq G$. The following theorem, which we prove in §4.4, promises a finite collection of nice subgroups $G \subseteq \mathcal{G}$ that will be suitable for our applications; we want the level of G and the index $[\widehat{\mathbb{Z}}^\times : \det(G)]$ to both be small in order to make future computations easier.

Theorem 2.8. *Let N be the least common multiple of the levels of $\mathcal{G}$ and $[\mathcal{G}, \mathcal{G}]$. Then there is a computable finite set $\mathcal{S}_\mathcal{G}$ of open subgroups of $\mathcal{G}$ such that:*

- *For every group $G \in \mathcal{S}_\mathcal{G}$, we have $[\mathcal{G}, \mathcal{G}] \subseteq G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) \subseteq \mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$.*
- *For every group $G \in \mathcal{S}_\mathcal{G}$, the level of G divides some power of 2 times N.*
- *For every group $G \in \mathcal{S}_\mathcal{G}$, $[\widehat{\mathbb{Z}}^\times : \det(G)]$ is a power of 2.*
- *For every group $[\mathcal{G}, \mathcal{G}] \subseteq W \subseteq \mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$, we have $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = W$ for a unique $G \in \mathcal{S}_\mathcal{G}$.*

2.5. **Some abelian representations.** Throughout this section we fix an agreeable subgroup $\mathcal{G}$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and a finite set of open subgroups $\mathcal{S}_\mathcal{G}$ of $\mathcal{G}$ as in Theorem 2.8. Fix an integer $N \geq 3$ that is divisible by the level of $[\mathcal{G}, \mathcal{G}]$, the level of $\mathcal{G}$, and the level of each $G \in \mathcal{S}_\mathcal{G}$.

Define the open subvariety $U_\mathcal{G} := \pi_\mathcal{G}^{-1}(\mathbb{P}^1_{K_\mathcal{G}} - \{0, 1728, \infty\})$ of $X_\mathcal{G}$. The Weierstrass equation

$$y^2 = x^3 - 27 \cdot j(j - 1728) \cdot x + 54 \cdot j(j - 1728)^2, \tag{2.1}$$

with $j = \pi_\mathcal{G}$, defines an elliptic scheme $\mathscr{E}_\mathcal{G}$ over $U_\mathcal{G}$. For a number field $K \supseteq K_\mathcal{G}$ and point $u \in U_\mathcal{G}(K)$, the fiber of $\mathscr{E}_\mathcal{G}$ over u is the elliptic curve $\mathscr{E}_{\mathcal{G},u}$ over K given by (2.1) with j replaced by $\pi_\mathcal{G}(u) \in K - \{0, 1728\}$; it has j-invariant $\pi_\mathcal{G}(u)$.

Let $\overline{\mathcal{G}}$ be the image of $\mathcal{G}$ modulo N. As in [Zyw22b, §6.3.1], we have a surjective and continuous representation

$$\varrho^*_{\mathscr{E}_\mathcal{G},N} \colon \pi_1(U_\mathcal{G}, \overline{\eta}) \to \overline{\mathcal{G}} \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}),$$

where $\overline{\eta}$ is a particular geometric generic point of $U_\mathcal{G}$ and π_1 denotes the étale fundamental group (the only difference being to base extend by K_G first). The representation $\varrho^*_{\mathscr{E}}$ can be constructed in a similar fashion to our adelic representations for elliptic curves; the N-torsion subscheme $\mathscr{E}_\mathcal{G}[N]$ can be viewed as lisse sheaf on $U_\mathcal{G}$ that gives rise to the representation. For any number field $K \supseteq K_G$ and point $u \in U_\mathcal{G}(K)$, the specialization of $\varrho^*_{\mathscr{E}_\mathcal{G},N}$ at u defines a representation $\mathrm{Gal}_K \to \overline{\mathcal{G}} \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ that is isomorphic to $\rho^*_{(\mathscr{E}_\mathcal{G})_u,N}$.

Now take any group $G \in \mathcal{S}_\mathcal{G}$ and let $\overline{G}$ be the image of G modulo N. Since the level of G divides N, reduction modulo N induces an isomorphism $\mathcal{G}/G \xrightarrow{\sim} \overline{\mathcal{G}}/\overline{G}$ that we will view as an equality. Define the homomorphism

$$\alpha_G \colon \pi_1(U_\mathcal{G}) \to \mathcal{G}/G$$

by composing $\varrho^*_{\mathscr{E}_\mathcal{G},N}$ with the quotient map $\mathcal{G} \to \overline{\mathcal{G}}/\overline{G} = \mathcal{G}/G$; we may suppress the point $\overline{\eta}$ since $\mathcal{G}/G$ is abelian.

Proposition 2.9. *The homomorphism α_G is computable, i.e., one can compute a model of $U_{\mathcal{G}}$ and an étale cover $Y \to U_{\mathcal{G}}$ corresponding to α_G along with the action of $\mathcal{G}/G$ on Y. In particular, for any number field $K \supseteq K_{\mathcal{G}}$ and point $u \in U_{\mathcal{G}}(K)$, one can compute the specialization $\mathrm{Gal}_K \to \mathcal{G}/G$ of α_G at u.*

Proof. This follows from the same argument as in [Zyw22b, §11] except working over K_G. A slight difference to keep in mind is that the field of constants $K_{\mathcal{G}}$ in $K_{\mathcal{G}}(U_{\mathcal{G}})$ will not be algebraically closed in the function field of Y when $\det(G)$ is a proper subgroup of $\det(\mathcal{G})$ (in [Zyw22b], we only considered cases where $\det(G) = \det(\mathcal{G})$). □

2.5.1. *A description of G_E.* Now consider any non-CM elliptic curve E defined over a number field K for which the agreeable closure is conjugate to $\mathcal{G}$ in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

By Proposition 2.3, we have $j_E = \pi_{\mathcal{G}}(u)$ for some point $u \in U_{\mathcal{G}}(K)$. The elliptic curve E is a quadratic twist of $E' := (\mathscr{E}_{\mathcal{G}})_u$ by a character $\chi\colon \mathrm{Gal}_K \to \{\pm 1\}$ since E is non-CM and the two elliptic curves have the same j-invariant. For each group $G \in \mathcal{S}_{\mathcal{G}}$, let

$$\alpha_{G,E}\colon \mathrm{Gal}_K \to \mathcal{G}/G$$

be the homomorphism that is the product of χ and the specialization of α_G at u.

Proposition 2.10.

(i) *There is a unique group $G \in \mathcal{S}_{\mathcal{G}}$ such that $\alpha_{G,E}(\mathrm{Gal}_{K^{\mathrm{cyc}}}) = 1$ and $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ is minimal with respect to inclusion.*

(ii) *Take $G \in \mathcal{S}_{\mathcal{G}}$ as in (i). The groups G_E and*

$$\mathcal{H}_E := \{g \in \mathcal{G} : \det g \in \chi_{\mathrm{cyc}}(\mathrm{Gal}_K),\ gG = \gamma_E(\det g)\}$$

are conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, where $\gamma_E\colon \chi_{\mathrm{cyc}}(\mathrm{Gal}_K) \to \mathcal{G}/G$ is the unique homomorphism satisfying $\alpha_{G,E}(\sigma) = \gamma_E(\chi_{\mathrm{cyc}}(\sigma)^{-1})$ for all $\sigma \in \mathrm{Gal}_K$.

Proof. The specialization of $\varrho^*_{\mathscr{E}_{\mathcal{G}},N}$ at u is a representation $\mathrm{Gal}_K \to \overline{\mathcal{G}} \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ isomorphic to $\rho^*_{(\mathscr{E}_{\mathcal{G}})_u,N} = \rho^*_{E',N}$. So by replacing $\rho^*_{E',N}$ with an isomorphic representation, we may assume that it is the specialization of $\varrho^*_{\mathscr{E}_{\mathcal{G}},N}$ at u. In particular, we have $\rho^*_{E',N}(\mathrm{Gal}_K) \subseteq \overline{\mathcal{G}}$. We also have $\rho^*_{E'}(\mathrm{Gal}_K) \subseteq \mathcal{G}$ since the level of $\mathcal{G}$ divides N. Since E is the quadratic twist of E' by χ, we may assume that $\rho^*_E = \chi \cdot \rho^*_{E'}$ and hence also $\rho^*_{E,N} = \chi \cdot \rho^*_{E',N}$. In particular, $\rho^*_{E,N}(\mathrm{Gal}_K) \subseteq \overline{\mathcal{G}}$ and $G_E = \rho^*_E(\mathrm{Gal}_K) \subseteq \mathcal{G}$ since $-I \in \mathcal{G}$.

Now take any $G \in \mathcal{S}_{\mathcal{G}}$. The homomorphism $\alpha_{G,E}$ agrees with the composition of $\rho^*_{E,N}\colon \mathrm{Gal}_K \to \overline{\mathcal{G}}$ with the quotient map $\overline{\mathcal{G}} \to \overline{\mathcal{G}}/\overline{G} = \mathcal{G}/G$. Therefore, $\alpha_{G,E}(\mathrm{Gal}_{K^{\mathrm{cyc}}})$ is equal to the image of $\rho^*_E(\mathrm{Gal}_{K^{\mathrm{cyc}}}) = G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ in $\mathcal{G}/G$, where we have used Lemma 2.1(i). So $\alpha_{G,E}(\mathrm{Gal}_{K^{\mathrm{cyc}}}) = 1$ if and only if $G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) \subseteq G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. Thus to prove (i), it suffices to show that $[\mathcal{G},\mathcal{G}] \subseteq G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) \subseteq \mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ since any such group is of the form $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ for a unique $G \in \mathcal{S}_{\mathcal{G}}$. The group $\mathcal{G}$ is the agreeable closure of G_E since it is conjugate to the agreeable closure and $G_E \subseteq \mathcal{G}$. Therefore, $[G_E, G_E] = [\mathcal{G},\mathcal{G}]$ and hence $[\mathcal{G},\mathcal{G}] \subseteq G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) \subseteq \mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ by Lemma 2.1(ii).

We may now suppose that G is chosen as in (i). We have just shown that $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. We have already made choices so that $G_E \subseteq \mathcal{G}$. For each $g \in G_E$, we have $\det g \in \det(G_E) = \chi_{\mathrm{cyc}}(\mathrm{Gal}_K)$. Note that the existence

and uniqueness of γ_E is clear since χ_{cyc} induces an isomorphism $\mathrm{Gal}(K^{\mathrm{cyc}}/K) \xrightarrow{\sim} \chi_{\mathrm{cyc}}(\mathrm{Gal}_K)$.

We claim that $gG = \gamma_E(\det g)$ for all $g \in G_E$. Take any $\sigma \in \mathrm{Gal}_K$. From our identification $\overline{\mathcal{G}}/\overline{G} = \mathcal{G}/G$, $\rho^*_{E,N}(\sigma) \cdot \overline{G}$ and $\rho^*_E(\sigma) \cdot G$ represent the same coset. Therefore, $\rho^*_E(\sigma) \cdot G = \alpha_{G,E}(\sigma) = \gamma_E(\chi_{\mathrm{cyc}}(\sigma)^{-1})$. Since $\det \circ \rho^*_E = \chi_{\mathrm{cyc}}^{-1}|_{\mathrm{Gal}_K}$, we have $\rho^*_E(\sigma) \cdot G = \gamma_E(\det \rho^*_E(\sigma))$. The claim follows since σ was an arbitrary element of Gal_K.

Using the claim, we have now shown that $G_E \subseteq \mathcal{H}_E$. Taking determinants gives $\chi_{\mathrm{cyc}}(\mathrm{Gal}_K) = \det(G_E) \subseteq \det(\mathcal{H}_E) \subseteq \chi_{\mathrm{cyc}}(\mathrm{Gal}_K)$ and hence $\det(G_E) = \det(\mathcal{H}_E)$. We also have

$$\mathcal{H}_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = \{g \in \mathcal{G} : g \in \mathrm{SL}_2(\widehat{\mathbb{Z}}),\, gG = G\} = G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}).$$

Therefore, $G_E = \mathcal{H}_E$ since G_E is a subgroup of $\mathcal{H}_E$ with the same determinant and the same intersection with $\mathrm{SL}_2(\widehat{\mathbb{Z}})$. □

2.6. **Computing the Galois image for most elliptic curves.** For our algorithm, we first shall perform some one-time precomputations. For each group $\mathcal{G} \in \mathcal{A}_1 \cup \mathcal{A}_2$, we can compute a model for the curve $X_{\mathcal{G}}$ and, with respect to this model, compute the morphism $\pi_{\mathcal{G}}$. For each $\mathcal{G} \in \mathcal{A}_1$, we can compute a set $\mathcal{S}_{\mathcal{G}}$ as in Theorem 2.8. For each $\mathcal{G} \in \mathcal{A}_1$ and $G \in \mathcal{S}_{\mathcal{G}}$, we can compute α_G as in Proposition 2.9.

Fix an explicit non-CM elliptic curve E defined over a number field K for which $j_E \notin J_K$ and $\rho_{E,\ell}(\mathrm{Gal}_K) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all primes $\ell > 19$. Note that the condition $j_E \notin J_K$ can be checked since the morphisms $\pi_{\mathcal{G}}$ with $\mathcal{G} \in \mathcal{A}_2$ are computed already. We will discuss the conditions on the $\rho_{E,\ell}$ in §2.7. We can also compute the open group $\chi_{\mathrm{cyc}}(\mathrm{Gal}_K) \subseteq \widehat{\mathbb{Z}}^\times$.

Using Theorem 2.7 and our precomputed modular curves, we can find a group $\mathcal{G} \in \mathcal{A}_1$ that is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to the agreeable closure of $G_E = \rho^*_E(\mathrm{Gal}_K)$. Choose a point $u \in U_{\mathcal{G}}(K)$ for which $\pi_{\mathcal{G}}(u) = j_E$. Let E' be the elliptic curve over K defined by the equation (2.1) with j replaced by j_E. The curve E is a quadratic twist of E' by a computable character $\chi\colon \mathrm{Gal}_K \to \{\pm 1\}$ since E is non-CM and $j_{E'} = j_E$.

Take any group $G \in \mathcal{S}_{\mathcal{G}}$. We define $\alpha_{E,G}\colon \mathrm{Gal}_K \to \mathcal{G}/G$ to be product of χ and the specialization of α_G at u; this is computable by using our precomputed α_G. We can find the group $G \in \mathcal{S}_{\mathcal{G}}$ that satisfies Proposition 2.10(i); for the rest of the section, we work with this fixed group G. There is a unique computable homomorphism $\gamma_E\colon \chi_{\mathrm{cyc}}(\mathrm{Gal}_K) \to \mathcal{G}/G$ satisfying $\alpha_{G,E}(\sigma) = \gamma_E(\chi_{\mathrm{cyc}}(\sigma)^{-1})$ for all $\sigma \in \mathrm{Gal}_K$.

From $\mathcal{G}$, G, $\chi_{\mathrm{cyc}}(\mathrm{Gal}_K)$ and γ_E, Proposition 2.10(i) gives an explicit subgroup $\mathcal{H}_E$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ that is conjugate to G_E. This is the desired explicit computation of G_E up to conjugacy.

2.7. **Loose ends 1: images modulo ℓ and uniformity.** Consider a non-CM elliptic curve E over a number field K. A consequence of Theorem 1.1, and also one of the ingredients of its proof, is that $\rho_{E,\ell}(\mathrm{Gal}_K) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all primes $\ell > c_{E,K}$, where $c_{E,K}$ is a positive integer which we take to be minimal. In the case $K = \mathbb{Q}$, Serre asked whether $c_{E,\mathbb{Q}}$ can be bounded independent of E, see [Ser72, §4.3] and the final remarks of [Ser81] where he asks if $c_{E,\mathbb{Q}} \leq 37$. We formulate this as a conjecture over a general number field.

Conjecture 2.11 (Serre uniformity problem)**.** *For any number field K, the following equivalent conditions hold:*

(a) *There is a constant c_K such that for any prime $\ell > c_K$ and any non-CM elliptic curves E/K, we have $\rho_{E,\ell}(\mathrm{Gal}_K) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$.*

(b) *There is a finite set $\mathcal{J}_K \subseteq K$ such that for any prime $\ell > 19$ and any non-CM elliptic curve E/K with $j_E \notin \mathcal{J}_K$, we have $\rho_{E,\ell}(\mathrm{Gal}_K) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$.*

It is an important problem to determine the finite set of primes $\ell > 19$ for which $\rho_{E,\ell}(\mathrm{Gal}_K) \not\supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$. For a fixed prime $\ell > 19$, there are fast probabilistic methods of Sutherland [Sut16] to identify the image of $\rho_{E,\ell}$ up to a notion of local conjugacy. Note that whenever the algorithm of [Sut16] predicts $\rho_{E,\ell}(\mathrm{Gal}_K) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$, the result is guaranteed to be correct.

There are various bounds for $c_{E,K}$ in the literature. For example, in [Kaw03] one finds an explicit upper bound for $c_{E,K}$; however, it is too large for use in practice. Bounds for $c_{E,K}$ assuming GRH, like suggested in [LV14], should do better.

In the case $K = \mathbb{Q}$, [Zyw22a] gives an efficient algorithm that computes a relatively small finite set of primes S for which $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}}) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all $\ell > 19$ with $\ell \notin S$ (one can then quickly address any primes in S). An analogous algorithm over a general number field should be worked out.

Proof of the equivalence in Conjecture 2.11. Take any prime $\ell > 19$ and any non-CM elliptic curve E/K. Since $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is equal to its own commutator subgroup, see Lemma 3.2(i), we have $\rho_{E,\ell}(\mathrm{Gal}_K) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ if and only if $\pm\rho_{E,\ell}(\mathrm{Gal}_K) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Since $\pm\rho_{E,\ell}(\mathrm{Gal}_K)$, up to conjugacy, does not change if we replace E/K by an quadratic twist and E is non-CM, we find that the condition $\rho_{E,\ell}(\mathrm{Gal}_K) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ depends only on j_E, K and ℓ. Therefore, condition (b) implies (a) since for each $j \in \mathcal{J}_K$ that is the j-invariant of a non-CM elliptic curve E/K, we can applying Theorem 1.1.

We now assume that (a) holds for some constant c_K. Suppose that we have $\rho_{E,\ell}(\mathrm{Gal}_K) \not\supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for some non-CM elliptic curve E/K and prime $\ell > 19$. We have $19 < \ell < c_K$. Let $\mathcal{G}$ be the open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ of level ℓ whose image modulo ℓ is the transpose of $\pm\rho_{E,\ell}(\mathrm{Gal}_K)$ (and hence does not contain $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$). Using the classification in [CP03] and $\ell > 19$, the genus of $X_{\mathcal{G}}$ is at least 2. We have $j_E \in \pi_{\mathcal{G}}(X_{\mathcal{G}}(K))$ by Proposition 2.3. Therefore, (b) holds since only finitely many group $\mathcal{G}$ arise and $X_{\mathcal{G}}(K)$ is finite by Faltings theorem. □

2.8. **Loose ends 2: sporadic images.** In general, computing G_E for an arbitrary non-CM elliptic curve E over a number field is still an extremely difficult problem. The fundamental reason being that *every* open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ will occur as such an image (to prove this one need only show that $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ occurs, see [Zyw10]).

For a fixed number field K, and assuming Conjecture 2.11 for simplicity, we have shown how to compute G_E for all non-CM elliptic curves E/K whose j-invariant lies away from some finite subset of K. What makes this proposed algorithm especially practical is that one need only compute a finite number of modular curves and this can be done ahead of time.

For non-CM elliptic curves over K with one of the excluded j-invariants, a similar approach works but requires more modular curves computations or ad hoc computations. For how we dealt with this in the $K = \mathbb{Q}$ case, see §10.2 and §12.3 of [Zyw22b].

3. Basic group theory

In this section, we collect some basic group theory facts that will be used in our arguments.

3.1. Goursat's lemma.

Lemma 3.1 (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 B_1 and B_2 be the normal subgroups of G_1 and G_2, respectively, for which $\ker(p_2) = B_1 \times \{1\}$ and $\ker(p_1) = \{1\} \times B_2$. Then the image of H in $(G_1 \times G_2)/(B_1 \times B_2) = G_1/B_1 \times G_2/B_2$ is the graph of an isomorphism $G_1/B_1 \xrightarrow{\sim} G_2/B_2$.*

3.2. Commutator subgroups.

Lemma 3.2. [Zyw22b, Lemma 7.7]

(i) *The commutator subgroups of $\mathrm{SL}_2(\mathbb{Z}_\ell)$ is equal to $\mathrm{SL}_2(\mathbb{Z}_\ell)$ for all $\ell > 3$.*
(ii) *The commutator subgroups of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ is equal to $\mathrm{SL}_2(\mathbb{Z}_\ell)$ for all $\ell \geq 3$.*
(iii) *The commutator subgroup of $\mathrm{SL}_2(\mathbb{Z}_3)$ has level 3 and index 3.*

Lemma 3.3. [Zyw22b, 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 $\mathrm{SL}_2(\widehat{\mathbb{Z}})$.*

Lemma 3.4. *Take any prime $\ell \geq 3$.*

(i) *There is a unique closed normal subgroup W_ℓ of $\mathrm{SL}_2(\mathbb{Z}_\ell)$ for which $\mathrm{SL}_2(\mathbb{Z}_\ell)/W_\ell$ is a simple group.*
(ii) *Suppose $\ell > 3$. Then the group W_ℓ consists of the matrices in $\mathrm{SL}_2(\mathbb{Z}_\ell)$ whose image modulo ℓ are $\pm I$. We have $\mathrm{SL}_2(\mathbb{Z}_\ell)/W_\ell \cong \mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm I\}$.*
(iii) *The group W_3 is the commutator subgroup of $\mathrm{SL}_2(\mathbb{Z}_3)$ and $\mathrm{SL}_2(\mathbb{Z}_3)/W_3$ is cyclic of order 3.*

Proof. Let Q be a finite simple group that is a quotient of $\mathrm{SL}_2(\mathbb{Z}_\ell)$ by a closed normal subgroup.

Suppose $\ell > 3$. The simple group Q is non-abelian by Lemma 3.2(i). Since pro-ℓ groups are prosolvable and Q is simple and nonabelian, we find that any continuous surjective homomorphism $\mathrm{SL}_2(\mathbb{Z}_\ell) \twoheadrightarrow Q$ factors through $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})/\{\pm I\} \twoheadrightarrow Q$. The lemma is immediate in this case since $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})/\{\pm I\}$ is simple.

The group $\mathrm{SL}_2(\mathbb{Z}_3)$ is prosolvable since pro-3 groups are prosolvable and $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ is solvable. Therefore, Q is a cyclic group of prime order. The lemma for $\ell = 3$ follows since $\mathrm{SL}_2(\mathbb{Z}_3)/[\mathrm{SL}_2(\mathbb{Z}_3), \mathrm{SL}_2(\mathbb{Z}_3)] \cong \mathbb{Z}/3\mathbb{Z}$ by Lemma 3.2(iii). □

Lemma 3.5. *Let G be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ or $\mathrm{SL}_2(\widehat{\mathbb{Z}})$. Take any prime $\ell > 5$. Then $G_\ell \supseteq \mathrm{SL}_2(\mathbb{Z}_\ell)$ if and only if ℓ does not divides the level of $[G, G]$.*

Proof. First suppose that ℓ does not divides the level of $[G, G] \subseteq \mathrm{SL}_2(\widehat{\mathbb{Z}})$. Then $G_\ell \supseteq [G, G]_\ell \supseteq \mathrm{SL}_2(\mathbb{Z}_\ell)$.

Now suppose that $G_\ell \supseteq \mathrm{SL}_2(\mathbb{Z}_\ell)$. Define $G' = [G, G]$; it is an open subgroup of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ by Lemma 3.3. We have $G'_\ell = [G_\ell, G_\ell] \supseteq \mathrm{SL}_2(\mathbb{Z}_\ell)$ by Lemma 3.2(i). The level of $[G', G']$ divides the level of the larger group $[G, G]$. So after replacing G by G', we may assume that $G \subseteq \mathrm{SL}_2(\widehat{\mathbb{Z}})$ and that $G_\ell = \mathrm{SL}_2(\mathbb{Z}_\ell)$. Let H be the image of G under the projection map to $\prod_{p \neq \ell} \mathrm{SL}_2(\mathbb{Z}_p)$. We may view G as a subgroup of $H \times \mathrm{SL}_2(\mathbb{Z}_\ell)$ for which the projections to the factors H and $\mathrm{SL}_2(\mathbb{Z}_\ell)$ are surjective.

By Goursat's lemma (Lemma 3.1), we have $B_1 \times B_2 \subseteq G$ and $H/B_1 \cong \mathrm{SL}_2(\mathbb{Z}_\ell)/B_2$, where B_1 and B_2 are certain normal subgroup of H and $\mathrm{SL}_2(\mathbb{Z}_\ell)$, respectively. In our case, the groups B_1 and B_2 are also closed.

Suppose that $B_2 \neq \mathrm{SL}_2(\mathbb{Z}_\ell)$. By Lemma 3.4, the simple group $Q := \mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm I\}$ is isomorphic to a quotient of $\mathrm{SL}_2(\mathbb{Z}_\ell)/B_2 \cong H/B_1$. Therefore, Q is a quotient of H_p for some prime $p \neq \ell$, where H_p is a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$. The group Q is not isomorphic to either of the groups $\mathrm{SL}_2(\mathbb{F}_p)/\{\pm I\}$ or A_5 by cardinality considerations. However, this contradicts the computation of the sets "$\mathrm{Occ}(\mathrm{GL}_2(\mathbb{Z}_\ell))$" in [Ser98, IV §3.4].

Therefore, $B_2 = \mathrm{SL}_2(\mathbb{Z}_\ell)$ and hence also $B_1 = H$. From the inclusions $H \times \mathrm{SL}_2(\mathbb{Z}_\ell) \supseteq G \supseteq B_1 \times B_2$, we deduce that $G = H \times \mathrm{SL}_2(\mathbb{Z}_\ell)$. Therefore, $[G,G] = [H,H] \times \mathrm{SL}_2(\mathbb{Z}_\ell)$ by Lemma 3.2(i) and hence ℓ does not divide the level of $[G,G]$. □

Lemma 3.6. *Fix a prime $\ell \geq 5$ and let G be a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Then $G \supseteq \mathrm{SL}_2(\mathbb{Z}_\ell)$ if and only if the image of G modulo ℓ contains $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$.*

Proof. After replacing G by $[G,G]$, and using Lemma 3.2(i), we may assume that $G \subseteq \mathrm{SL}_2(\mathbb{Z}_\ell)$. The lemma now follows from [Ser98, IV §3.4 Lemma 3]. □

3.3. **Determining the level of groups.** The following lemmas give cases where we can show that a subgroup of $\mathrm{GL}_2(\mathbb{Z}_N)$ is open and also give a bound on its level.

Lemma 3.7. [Zyw22b, Lemma 7.6] *Fix an integer $N > 1$ with $N \not\equiv 2 \pmod 4$. Let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}_N)$ for which $G \cap \mathrm{SL}_2(\mathbb{Z}_N)$ is an open subgroup of $\mathrm{SL}_2(\mathbb{Z}_N)$ whose level divides N. Define $N_1 := N$ if N is odd and $N_1 := 2N$ if N is even. Then $\mathbb{Z}_N^\times \cdot G$ is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_N)$ whose level divides N_1.*

Lemma 3.8. *Fix an integer $N > 1$ with $N \not\equiv 2 \pmod 4$. For each prime ℓ dividing N, define the integer*

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

where ℓ^{e_ℓ} is the largest power of ℓ dividing N. Note that N_ℓ is a divisor of N.

Let $\mathcal{G}$ be an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_N)$ whose level divides N. Let G be a maximal open subgroup of $\mathcal{G}$ whose level does not divide N. Then for some prime $\ell \mid N$, the images of $\mathcal{G}$ and G modulo $N_\ell \ell$ are distinct subgroups of $\mathrm{GL}_2(\mathbb{Z}/N_\ell\ell\mathbb{Z})$.

Proof. Suppose that G is a maximal open subgroup of $\mathcal{G}$ such that G and $\mathcal{G}$ have the same image in $\mathrm{GL}_2(\mathbb{Z}/N_\ell\ell\mathbb{Z})$ for all primes $\ell \mid N$. Take any $\ell \mid N$. Since the level of $\mathcal{G}$ divides N, we find that the image of G in $\mathrm{GL}_2(\mathbb{Z}/N_\ell\ell\mathbb{Z})$ contains all the matrices that are congruent to I modulo N_ℓ. By [Zyw22b, Lemma 7.2], we deduce that G has level dividing N. □

4. Agreeable groups

4.1. **Agreeable groups.** Recall that a subgroup G of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ is agreeable if it is open, contains all the scalar matrices in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, and each prime dividing the level of G also divides the level of $[G,G]$.

Let G be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and let M be the product of the primes that divide the level of $[G,G] \subseteq \mathrm{SL}_2(\widehat{\mathbb{Z}})$. We define the agreeable closure of G to be the group

$$\mathcal{G} := (\mathbb{Z}_M^\times G_M) \times \prod\nolimits_{\ell \nmid M} \mathrm{GL}_2(\mathbb{Z}_\ell). \tag{4.1}$$

We now give some basic properties of $\mathcal{G}$.

Lemma 4.1.

(i) *We have* $G \subseteq \mathcal{G}$ *and* $[G,G] = [\mathcal{G},\mathcal{G}]$.
(ii) *The group* $\mathcal{G}$ *is the minimal agreeable subgroup of* $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ *that contains* G. *In particular,* G *is agreeable if and only if* $\mathcal{G} = G$.
(iii) *If* M' *is the level of* $[G,G] \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$, *then the level of* $\mathcal{G}$ *divides* $2\operatorname{lcm}(M',4)$.

Proof. The inclusion $G \subseteq \mathcal{G}$ is clear since $G_M \subseteq \mathbb{Z}_M^\times G_M$. The integer M is even since the commutator subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, and hence also of G, has level divisible by 2. Since M is even, we have $[\mathrm{GL}_2(\mathbb{Z}_\ell), \mathrm{GL}_2(\mathbb{Z}_\ell)] = \mathrm{SL}_2(\mathbb{Z}_\ell)$ for all $\ell \nmid M$, cf. Lemma 3.2(ii). Therefore, $[\mathcal{G},\mathcal{G}] = [G_M, G_M] \times \prod_{\ell\nmid M} \mathrm{SL}_2(\mathbb{Z}_\ell) = [G,G]_M \times \prod_{\ell\nmid M} \mathrm{SL}_2(\mathbb{Z}_\ell) = [G,G]$, where the last equality uses that M has the same prime divisors as the level of $[G,G]$. This proves (i).

Since $[G,G] = [\mathcal{G},\mathcal{G}]$, the integer M is also the product of the primes dividing the level of $[\mathcal{G},\mathcal{G}]$. From the definition of the group $\mathcal{G}$, it contains the scalars of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and each primes dividing the level of $\mathcal{G}$ must divide M. Therefore, $\mathcal{G}$ is agreeable.

Take any agreeable subgroup B of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ with $G \subseteq B$. Let N be the product of the primes that divide the level of $[B,B]$. We have $[G,G] \subseteq [B,B]$, so N divides M. Since B is agreeable and $N|M$, we have $B = B_M \times \prod_{\ell\nmid M} \mathrm{GL}_2(\mathbb{Z}_\ell)$. We have $\mathcal{G}_M = \mathbb{Z}_M^\times G_M \subseteq B_M$ since B contains the scalars and $G \subseteq B$. Therefore, $\mathcal{G} \subseteq B$. Part (ii) now follows.

The level of $H := G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ divides M' since $H \supseteq [G,G]$. Note that M and M' have the same prime divisors. Lemma 3.7 implies that $\mathbb{Z}_M^\times H_M$ is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_M)$ whose level divides $2\operatorname{lcm}(M',4)$. Part (iii) follows since $\mathcal{G}$ contains $(\mathbb{Z}_M^\times H_M) \times \prod_{\ell\nmid M} \mathrm{GL}_2(\mathbb{Z}_\ell)$. □

Remark 4.2. In [Zyw22b], we gave a different definition of an *agreeable* subgroup G that insisted on the extra assumption $\det(G) = \widehat{\mathbb{Z}}^\times$. Consider any open subgroup G of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ for which $\det(G) = \widehat{\mathbb{Z}}^\times$. In the notation of [Zyw22b], the group G is agreeable if and only G equals (4.1), cf. §8.3 of [Zyw22b] where the agreeable closure is constructed. In particular, the notions of *agreeable* in this work and in [Zyw22b] are the same for groups with full determinant.

4.2. **Maximal agreeable subgroups.** Fix an agreeable subgroup $\mathcal{G}$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. Let M be the product of the primes that divide the level of $[\mathcal{G},\mathcal{G}]$. In this section, we shall describe the maximal agreeable (proper) subgroups of $\mathcal{G}$. We start by giving some obvious maximal agreeable subgroups.

Lemma 4.3.

(i) *Let* B *be a maximal (proper) open subgroup of* $\mathcal{G}_M$ *satisfying* $B \supseteq \mathbb{Z}_M^\times I$. *Then* $G := B \times \prod_{\ell\nmid M} \mathrm{GL}_2(\mathbb{Z}_\ell)$ *is a maximal agreeable subgroup of* $\mathcal{G}$.
(ii) *For a prime* $p \nmid M$, *let* B *be a maximal (proper) open subgroup of* $\mathrm{GL}_2(\mathbb{Z}_p)$ *that satisfies* $B \supseteq \mathbb{Z}_p^\times I$ *and* $B \not\supseteq \mathrm{SL}_2(\mathbb{Z}_p)$. *Then* $G := \mathcal{G}_M \times B \times \prod_{\ell\nmid pM} \mathrm{GL}_2(\mathbb{Z}_\ell)$ *is a maximal agreeable subgroup of* $\mathcal{G}$.
(iii) *If* $3 \nmid M$, *then* $G := \mathcal{G}_M \times (\mathbb{Z}_3^\times \mathrm{SL}_2(\mathbb{Z}_3)) \times \prod_{\ell\nmid 3M} \mathrm{GL}_2(\mathbb{Z}_\ell)$ *is a maximal agreeable subgroup of* $\mathcal{G}$.

Proof. Since $\mathcal{G}$ is agreeable, we have $\mathcal{G} = \mathcal{G}_M \times \prod_{\ell \nmid M} \mathrm{GL}_2(\mathbb{Z}_\ell)$. In all the cases, the group G is open, contains $\widehat{\mathbb{Z}}^\times I$ and satisfies $G \subseteq \mathcal{G}$. Let N be the product of the primes dividing the level of $[G,G] \subseteq \mathrm{SL}_2(\widehat{\mathbb{Z}})$. We have $M|N$ since $G \subseteq \mathcal{G}$. We have $N = M$, $N = pM$ and $N = 3M$ in parts (i), (ii) and (iii), respectively; in part (iii), we use Lemma 3.2(iii). In all the cases, every prime dividing the level of G also divides N. Thus G is agreeable. In all the cases, one readily sees that G is a maximal subgroup of $\mathcal{G}$. □

After setting some more notations, we will describe the maximal agreeable subgroups of $\mathcal{G}$ that are not covered by Lemma 4.3.

Fix a prime $p \in \{3,5\}$. Let $\mathfrak{S}_p$ and $\mathfrak{A}_p$ be the symmetric and alternating groups, respectively, on p letters. By Lemma 3.4, there is a unique closed normal subgroup W_p of $\mathrm{SL}_2(\mathbb{Z}_p)$ for which $\mathrm{SL}_2(\mathbb{Z}_p)/W_p$ is a finite simple group. The group $\mathrm{SL}_2(\mathbb{Z}_p)/W_p$ is isomorphic to $\mathfrak{A}_p$ (recall the exceptional isomorphism $\mathrm{PSL}_2(\mathbb{F}_5)/\{\pm I\} \cong \mathfrak{A}_5$). The group W_p is also normal in $\mathrm{GL}_2(\mathbb{Z}_p)$. Let

$$\psi_p \colon \mathrm{GL}_2(\mathbb{Z}_p) \to \mathrm{GL}_2(\mathbb{Z}_p)/(\mathbb{Z}_p^\times W_p) \cong \mathfrak{S}_p$$

be the homomorphism obtained by composing the quotient map with a choice of isomorphism (the existence of this isomorphism is a direct computation and requires $p \in \{3,5\}$). The group $\psi_p(\mathrm{SL}_2(\mathbb{Z}_p))$ is equal to the alternating group $\mathfrak{A}_p$. Using the uniqueness of W_p, we find that a closed subgroup B of $\mathrm{GL}_2(\mathbb{Z}_p)$ satisfies $B \supseteq \mathrm{SL}_2(\mathbb{Z}_p)$ if and only if $\psi_p(B) \supseteq \mathfrak{A}_p$.

Lemma 4.4. *Let G be a maximal agreeable subgroup of $\mathcal{G}$ that is not one of the groups described in Lemma 4.3.*

(i) *There is a unique prime $p \in \{3,5\}$ such that $p \nmid M$ and p divides the level of $[G,G]$. We have $G = G_{Mp} \times \prod_{\ell \nmid Mp} \mathrm{GL}_2(\mathbb{Z}_\ell)$.*

(ii) *We have $\mathbb{Z}_p^\times \mathrm{SL}_2(\mathbb{Z}_p) \subseteq G_p \subseteq \mathrm{GL}_2(\mathbb{Z}_p)$. If $p = 3$, then $G_p = \mathrm{GL}_2(\mathbb{Z}_p)$.*

(iii) *There is a homomorphism $\varphi \colon \mathcal{G}_M \to \mathfrak{S}_p$ such that $\varphi(\mathcal{G}_M) = \psi_p(G_p)$ and*

$$G_{Mp} = \{(g_1, g_2) \in \mathcal{G}_M \times G_p : \varphi(g_1) = \psi_p(g_2)\}.$$

Proof. Since G is a maximal agreeable subgroup of $\mathcal{G}$, our assumption that G is not one of the groups from Lemma 4.3 implies that the following hold:

- $G_M = \mathcal{G}_M$,
- $G_\ell \supseteq \mathrm{SL}_2(\mathbb{Z}_\ell)$ for all primes $\ell \nmid M$,
- if $3 \nmid M$, then $G_3 = \mathrm{GL}_2(\mathbb{Z}_3)$.

Since M is even and $G \supseteq \widehat{\mathbb{Z}}^\times I$, we have $\mathbb{Z}_\ell^\times \mathrm{SL}_2(\mathbb{Z}_\ell) \subseteq G_\ell \subseteq \mathrm{GL}_2(\mathbb{Z}_\ell)$ for all $\ell \nmid M$. In particular, (ii) will follow once we prove (i).

Since $G_\ell \supseteq \mathrm{SL}_2(\mathbb{Z}_\ell)$ for all $\ell \nmid M$, Lemma 3.5 implies that the level of $[G,G]$ is not divisible by any prime $\ell \nmid M$ with $\ell > 5$. Since M is even and $[G,G] \subseteq [\mathcal{G},\mathcal{G}]$, we deduce that the product of the primes dividing the level of $[G,G]$ is Mm for a unique $m|15$. We have $m > 1$ since G is a proper subgroup of $\mathcal{G}$ and $G_M = \mathcal{G}_M$. Let $p \in \{3,5\}$ be the largest prime dividing m.

We can view G_{Mp} as a subgroup of $G_M \times G_p$. The projection homomorphisms $\varphi_1 \colon G_{Mp} \to G_M$ and $\varphi_2 \colon G_{Mp} \to G_p$ are surjective. Let B_1 and B_2 be the normal subgroups of G_M and G_p, respectively, for which $\ker(\varphi_2) = B_1 \times \{I\}$ and $\ker(\varphi_1) = \{I\} \times B_2$. Note that G_{Mp} contains $B_1 \times B_2$. We have $\mathbb{Z}_M^\times I \subseteq B_1$ and $\mathbb{Z}_p^\times I \subseteq B_2$ since G contains all the scalars of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. By Goursat's lemma (Lemma 3.1), the

image of G_{Mp} in $(G_M \times G_p)/(B_1 \times B_2) = G_M/B_1 \times G_p/B_2$ is the graph of a group isomorphism $f\colon G_M/B_1 \xrightarrow{\sim} G_p/B_2$.

• First consider the case where $B_2 \not\supseteq \mathrm{SL}_2(\mathbb{Z}_p)$ and hence $\psi_p(B_2) \not\supseteq \mathfrak{A}_p$. In particular, $\psi_p(B_2)$ is a normal subgroup of $\psi_p(G_p) \in \{\mathfrak{A}_p, \mathfrak{S}_p\}$ that does not contain $\mathfrak{A}_p$. Therefore, $\psi_p(B_2) = 1$; equivalently, $B_2 \subseteq \mathbb{Z}_p^\times W_p$. Define the homomorphism

$$\varphi\colon G_M \to G_M/B_1 \xrightarrow{f} G_p/B_2 \to G_p/(\mathbb{Z}_p^\times W_p) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}_p)/(\mathbb{Z}_p^\times W_p) \xrightarrow{\sim} \mathfrak{S}_p,$$

where the last isomorphism with $\mathfrak{S}_p$ is the same as that in our definition of ψ_p. We have $\varphi(G_M) = \psi_p(G_p) \supseteq \mathfrak{A}_p$ and inclusions

$$\begin{aligned} G_{Mp} &= \{(g_1, g_2) \in G_M \times G_p : f(g_1 B_1) = g_2 B_2\} \\ &\subseteq \{(g_1, g_2) \in G_M \times G_p : \varphi(g_1) = \psi_p(g_2)\} =: C. \end{aligned}$$

Define the open subgroup $G' := C \times \prod_{\ell \nmid Mp} \mathrm{GL}_2(\mathbb{Z}_\ell)$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

We claim that G' is agreeable and satisfies $G \subseteq G' \subsetneq \mathcal{G}$. We certainly have $G \subseteq G'$ since $G_{Mp} \subseteq C$. We have $G' \subsetneq \mathcal{G}$ since $C \subsetneq G_M \times G_p \subseteq \mathcal{G}_M \times \mathrm{GL}_2(\mathbb{Z}_\mathfrak{p}) = \mathcal{G}_{Mp}$, where the strict inclusion uses that ψ_p is non-trivial on G_p and the last equality uses that p does not divide the level of $\mathcal{G}$. The inclusion $G' \subseteq \mathcal{G}$ implies that $[G', G'] \subseteq [\mathcal{G}, \mathcal{G}]$ and hence the level of $[G', G']$ is divisible by every prime dividing M. Since M is even, we have $[G', G'] = [C, C] \times \prod_{\ell \nmid Mp} \mathrm{SL}_2(\mathbb{Z}_\ell)$ by Lemma 3.2(ii). So the level of $[G', G']$ is not divisible by any primes $\ell \nmid Mp$. Using that $\psi_p(G_p \cap \mathrm{SL}_2(\mathbb{Z}_p)) = \psi_p(\mathrm{SL}_2(\mathbb{Z}_p)) = \mathfrak{A}_p$, one finds that the level of $C \cap \mathrm{SL}_2(\mathbb{Z}_{Mp})$, and hence also of $[C, C]$, is divisible by p. Combining everything together, we deduce that the product of primes that divide the level of $[G', G']$ is Mp. Observe that the level of G' is divisible only by primes dividing Mp. Since G contains the scalars of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, we have $\mathbb{Z}_{Mp}^\times = \mathbb{Z}_M^\times \times \mathbb{Z}_p^\times \subseteq B_1 \times B_2 \subseteq G_{Mp} \subseteq C$. Therefore, G' contains all the scalars of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. We have now verified that G' is agreeable.

Since G is a maximal agreeable subgroup of $\mathcal{G}$, the previous claim implies that $G' = G$. The lemma is now immediate in this case from our definition of G'.

• Now consider the case where $B_2 \supseteq \mathrm{SL}_2(\mathbb{Z}_p)$. We will prove that this case cannot occur.

We claim that $[G_{Mp}, G_{Mp}] = [G_M, G_M] \times \mathrm{SL}_2(\mathbb{Z}_p)$. It suffices to show that $[G_{Mp}, G_{Mp}] \supseteq \{I\} \times \mathrm{SL}_2(\mathbb{Z}_p)$. Take any $g_1, g_2 \in G_p$ with $\det(g_1) = \det(g_2)$. Since $B_2 \supseteq \mathrm{SL}_2(\mathbb{Z}_p)$, g_1 and g_2 lie in the same coset of G_p/B_2. So there is an $a \in G_M$ such that (a, g_1) and (a, g_2) both lies in G_{Mp}. Taking the commutator of these elements, we find that $(I, g_1 g_2 g_1^{-1} g_2^{-1})$ lies in $[G_{Mp}, G_{Mp}]$. Therefore, $[G_{Mp}, G_{Mp}] \supseteq \{I\} \times C$, where $C \subseteq \mathrm{SL}_2(\mathbb{Z}_p)$ is the closed group generated by the set $\{g_1 g_2 g_1^{-1} g_2^{-1} : g_1, g_2 \in G_p, \det(g_1) = \det(g_2)\}$. It thus suffices to show that $C = \mathrm{SL}_2(\mathbb{Z}_p)$. When $p = 5$, we have $C = \mathrm{SL}_2(\mathbb{Z}_p)$ by Lemma 3.2(i). So assume that $p = 3$. Since C contains the commutator subgroup of $\mathrm{SL}_2(\mathbb{Z}_3)$, the group C has level 1 or 3 by Lemma 3.2(iii). A simple computation shows that the image of C modulo 3 is $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ and hence $C = \mathrm{SL}_2(\mathbb{Z}_3)$. This completes the proof of the claim.

Suppose that $m = p$. The product of the primes dividing the level of $[G, G]$ is $Mm = Mp$. By the above claim, we deduce that $[G, G] = [G_M, G_M] \times \mathrm{SL}_2(\mathbb{Z}_p) \times \prod_{\ell \nmid Mp} \mathrm{SL}_2(\mathbb{Z}_\ell)$ which contradicts that p divides the level of $[G, G]$.

Therefore, $m = 15$ and $p = 5$. We can view $[G_{15M}, G_{15M}]$ as a subgroup of $[G_{5M}, G_{5M}] \times [G_3, G_3]$ whose projection to each factor is surjective. By Goursat's lemma (Lemma 3.1), there are normal subgroups B_1' and B_2' of $[G_{5M}, G_{5M}]$ and $[G_3, G_3]$, respectively, so that the image of $[G_{15M}, G_{15m}]$ in $[G_{5M}, G_{5M}]/B_1' \times [G_3, G_3]/B_2'$ is the graph of an isomorphism. The group $G_3 = \mathrm{GL}_2(\mathbb{Z}_3)$ is prosolvable (since $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ is solvable) and $\mathrm{SL}_2(\mathbb{Z}_5)$ is equal to its own commutator subgroup by Lemma 3.2(i), so we must have $\{I\} \times \mathrm{SL}_2(\mathbb{Z}_5) \subseteq B_1'$. From this we deduce that the level of $[G_{15M}, G_{15M}] \subseteq \mathrm{SL}_2(\mathbb{Z}_{15M})$ is not divisible by 5 which contradicts that $m = 15$. We conclude that the case $B_2 \supseteq \mathrm{SL}_2(\mathbb{Z}_p)$ does not occur. □

4.3. **Special subgroups.** Let $\mathcal{G}$ be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ that contains the scalars $\widehat{\mathbb{Z}}^\times I$. Fix an open group W of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ that satisfies

$$[\mathcal{G}, \mathcal{G}] \subseteq W \subseteq \mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}).$$

The group W is normal in $\mathcal{G}$ and $\mathcal{G}/W$ is abelian since $[\mathcal{G}, \mathcal{G}] \subseteq W \subseteq \mathcal{G}$.

Given an open subgroup U of $\det(\mathcal{G})$, the following theorem gives a criterion that determines whether there exists an open subgroup G of $\mathcal{G}$ for which $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = W$ and $\det(G) = U$. Let N be the least common multiple of the levels of $\mathcal{G}$ and W in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and $\mathrm{SL}_2(\widehat{\mathbb{Z}})$, respectively. Define $N_1 := N$ if N is odd and $N_1 := \mathrm{lcm}(N, 8)$ if N is even.

Theorem 4.5. *Let U be an open subgroup of $\det(\mathcal{G}) \subseteq \widehat{\mathbb{Z}}^\times$ and let $S := U_N[2^\infty]$ be the 2-power torsion subgroup of $U_N \subseteq \mathbb{Z}_N^\times$. Then the following are equivalent:*

(a) *There is an open subgroup $G \subseteq \mathcal{G}$ with $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = W$ and $\det(G) = U$.*
(b) *There is a homomorphism $\beta\colon S \to \mathcal{G}_N/W_N$ such that $\det(\beta(a)) = a$ for all $a \in S$.*
(c) *There is a homomorphism $\beta\colon S \to \mathcal{G}(N_1)/W(N_1)$ such that $\det(\beta(a)) \equiv a \pmod{N_1}$ for all $a \in S$.*

Moreover, if a group G as in (a) exists, then there is such a group whose level divides a power of 2 times the least common multiple of N and the level of $U \subseteq \widehat{\mathbb{Z}}^\times$.

Proof. Define $U' = U_N \times \prod_{\ell \nmid N} \mathbb{Z}_\ell^\times$. We have $U \subseteq U' \subseteq \det(\mathcal{G})$. Note that the conditions (b) and (c) depend only on $U_N = U_N'$. If there is an open subgroup $G' \subseteq \mathcal{G}$ satisfying $G' \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = W$ and $\det(G') = U'$, then the group $G := \{g \in G' : \det(g) \in U\}$ will satisfy (a). Also if the level of G' divides an integer m, then the level of G will divide the least common multiple of m and the level of U. So without loss of generality, we may assume that $U = U_N \times \prod_{\ell \nmid N} \mathbb{Z}_\ell^\times$.

We first assume there is a homomorphism $\beta\colon S \to \mathcal{G}_N/W_N$ as in (b). Recall that for odd ℓ, $\mathbb{Z}_\ell^\times = C(1 + \ell\mathbb{Z}_\ell)$ for a finite cyclic group C of order $\ell - 1$ and $1 + \ell\mathbb{Z}_\ell \cong \mathbb{Z}_\ell$. We have $\mathbb{Z}_2^\times = \pm(1 + 8\mathbb{Z}_2)$ and $1 + 8\mathbb{Z}_2 \cong \mathbb{Z}_2$. Since U_N is an open subgroup of $\mathbb{Z}_N^\times = \prod_{\ell \mid N} \mathbb{Z}_\ell^\times$, we have an internal direct product of groups

$$U_N = S \cdot A_1 \cdot A_2, \tag{4.2}$$

where A_1 is torsion-free $\mathbb{Z}_2$-module of rank at most 1 and A_2 is isomorphic to a product of an odd finite abelian group with $\prod_{\ell \mid N, \ell \neq 2} \mathbb{Z}_\ell$. Fix a $u_1 \in A_1$ that generates A_1 as a $\mathbb{Z}_2$-module and choose an element $g_1 \in \mathcal{G}_N$ for which $\det(g_1) = u_1$. There is a unique continuous homomorphism $t_1\colon A_1 \to \mathcal{G}_N/W_N$ such that $t_1(u_1) = g_1 W_N$. Since $\det(g_1) = u_1$, we have $\det(t_1(a)) = a$ for all $a \in A_1$. The map $A_2 \to A_2$, $a \mapsto a^2$ is an isomorphism of groups whose inverse we denote by

ψ. Define the homomorphism $t_2\colon A_2 \to \mathcal{G}_N/W_N$, $a \mapsto (\psi(a)\cdot I)\cdot W_N$; it satisfies $\det(t_2(a)) = \psi(a)^2 = a$ for all $a \in A_2$. Using the direct product (4.2) with the maps $\beta\colon S \to \mathcal{G}_N/W_N$, t_1 and t_2, we obtain a homomorphism $s_N\colon U_N \to \mathcal{G}_N/W_N$ that satisfies $\det(s_N(a)) = a$ for all $a \in U_N$. For each prime $\ell \nmid N$, we define the homomorphism $s_\ell\colon \mathbb{Z}_\ell^\times \to \mathrm{GL}_2(\mathbb{Z}_\ell)/\mathrm{SL}_2(\mathbb{Z}_\ell)$ by $a \mapsto \left(\begin{smallmatrix}1 & 0\\ 0 & a\end{smallmatrix}\right)\cdot \mathrm{SL}_2(\mathbb{Z}_\ell)$. The map s_ℓ is an isomorphism with inverse given by the determinant; in particular, $\det(s_\ell(a)) = a$ for all $a \in \mathbb{Z}_\ell^\times$. By combining s_N with the s_ℓ for $\ell \nmid N$, we obtain a homomorphism

$$s\colon U = U_N \times \prod\nolimits_{\ell\nmid N} \mathbb{Z}_\ell^\times \to \mathcal{G}_N/W_N \times \prod\nolimits_{\ell\nmid N} \mathrm{GL}_2(\mathbb{Z}_\ell)/\mathrm{SL}_2(\mathbb{Z}_\ell) = \mathcal{G}/W$$

that satisfies $\det(s(a)) = a$ for all $a \in U$ (this uses that the levels of $\mathcal{G}$ and W are not divisible by any prime $\ell \nmid N$). There is a unique subgroup G of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ with $G \supseteq W$ for which G/W is equal to $s(U) \subseteq \mathcal{G}/W$. The group G is closed in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ since s is continuous. We have $\det(G) = \det(s(U)) = U$. Since $\det(s(a)) = a$ for all $a \in U$, we deduce that $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = W$. Using that $\det(G) = U$ is open in $\widehat{\mathbb{Z}}^\times$ and $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = W$ is open in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$, we find that G is an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

We claim that the level of G divides a power of 2 times N. From the definition of s and our s_ℓ, we find that $G \supseteq \{I\} \times \prod_{\ell\nmid N} \mathrm{GL}_2(\mathbb{Z}_\ell)$. Therefore, the level of G is not divisible by any prime $\ell \nmid N$. We have $G_N \supseteq W_N \supseteq \{B \in \mathrm{SL}_2(\mathbb{Z}_N) : B \equiv I \pmod N\}$. Using our choice of t_2, we find that G_N contains the scalar matrices cI for all c in the set $\{a \in U_N : a \equiv 1 \pmod N\} \cap (\{1\} \times \prod_{\ell\mid N, \ell\neq 2} \mathbb{Z}_\ell^\times)$. Therefore,

$$G_N \supseteq \prod\nolimits_{\ell\mid N, \ell = 2} \{I\} \times \prod\nolimits_{\ell\mid N, \ell\neq 2} H_\ell,$$

where $H_\ell := (1 + \ell^{e_\ell}\mathbb{Z}_\ell)\{B \in \mathrm{SL}_2(\mathbb{Z}_\ell) : B \equiv I \pmod{\ell^{e_\ell}}\}$ and ℓ^{e_ℓ} is the largest power of ℓ dividing N. Take any odd prime $\ell | N$. To complete the proof of the claim, it suffices to show that $H_\ell \supseteq \{B \in \mathrm{GL}_2(\mathbb{Z}_\ell) : B \equiv I \pmod{\ell^{e_\ell}}\}$. Take any $B \in \mathrm{GL}_2(\mathbb{Z}_\ell)$ with $B \equiv I \pmod{\ell^{e_\ell}}$. We have $\det(B) \in 1 + \ell^{e_\ell}\mathbb{Z}_\ell = (1 + \ell^{e_\ell}\mathbb{Z}_\ell)^2$, where the equality uses that ℓ is odd. So there is a $u \in 1 + \ell^{e_\ell}\mathbb{Z}_\ell$ for which $\det(B) = u^2$. Define $C := u^{-1}B \in \mathrm{SL}_2(\mathbb{Z}_\ell)$ and note that $C \equiv I \pmod{\ell^{e_\ell}}$. So $B = uC$ is in H_ℓ and the claim follows.

This completes the proof that (b) implies (a). After we prove the reverse implication, the final statement of the theorem will follows from the above claim.

Now suppose that there is a group $G \subseteq \mathcal{G}$ satisfying the properties of (a). Since $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = W$ and $\det(G) = U$, the map $\det\colon G/W \to U$ is an isomorphism of groups whose inverse gives rise to a homomorphism $s\colon U \to G/W \subseteq \mathcal{G}/W$ that satisfies $\det(s(a)) = a$ for all $a \in U$. Let $\iota\colon U_N \to U_N \times \prod_{\ell\nmid N} \mathbb{Z}_\ell^\times = U$ be the homomorphism that is the identity on the U_N factor and trivial on the $\mathbb{Z}_\ell^\times$ factors. Define the homomorphism $s_N\colon U_N \hookrightarrow U \xrightarrow{s} \mathcal{G}/W \to \mathcal{G}_N/W_N$, where the first map is ι and the last map is the N-adic projection. We have $\det(s_N(a)) = a$ for all $a \in U_N$. We have $S \subseteq U_N$, so $\beta := s_N|_S\colon S \to \mathcal{G}_N/W_N$ is a homomorphism satisfying $\det(\beta(a)) = a$ for all $a \in S$. This completes the proof that (a) implies (b).

Now suppose that (c) holds with a homomorphism $\beta\colon S \to \mathcal{G}(N_1)/W(N_1)$.

For any $a \in S$, we claim that there is a $g \in \mathcal{G}_N$ such that $\det(g) = a$ and such that the order of a agrees with the order of gW_N in $\mathcal{G}_N/W_N$. Take any $a \in S$ and denote its order by e. We may assume that $e \geq 2$ since we can take $g = I$ when $e = 1$. Choose a $g_1 \in \mathcal{G}_N$ whose image modulo N_1 represents the coset $\beta(a) \in \mathcal{G}(N_1)/W(N_1)$. We have $\det(g_1) \equiv \det(\beta(a)) \equiv a \pmod{N_1}$. Since $N_1 \equiv 0$

(mod 8) when N_1 is even, we have $(1+N_2\mathbb{Z}_N)^2 = 1+N_1\mathbb{Z}_N$ where $N_2 := N_1 = N$ if N is odd and $N_2 := N_1/2$ if N is even. Therefore, $\det(g_1)a^{-1} = c^{-2}$ for some $c \in 1+N_2\mathbb{Z}_N$. Define $g := cg_1$; it lies in $\mathcal{G}_N$ since $\mathcal{G}$ contains the scalars in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. We have $\det(g) = c^2\det(g_1) = a$. The matrix g^e thus lies in $\mathcal{G}_N \cap \mathrm{SL}_2(\mathbb{Z}_N)$. We have $\beta(a)^e = \beta(a^e) = 1$, so reducing g_1^e modulo N_1 gives the identity coset in $\mathcal{G}(N_1)/W(N_1)$. We have $c^e \equiv 1 \pmod{N_1}$ since $c \equiv 1 \pmod{N_2}$ and $e > 1$ is a power of 2. Therefore, $g^e = c^e g_1^e$ modulo N_1 lies in $W(N_1)$. Since W has level dividing N and $g^e \in \mathrm{SL}_2(\mathbb{Z}_N)$, we deduce that $g^e \in W_N$. So gW_N has order at most e in $\mathcal{G}_N/W_N$. The order is exactly e since $\det(g) = a$ has order e in U_N. This completes the proof of the claim.

Let $\{u_1, \dots, u_r\}$ be a minimal generating set of the finite abelian group S and let e_i be the order of u_i. In particular, we have an isomorphism $\mathbb{Z}/e_1\mathbb{Z} \times \cdots \times \mathbb{Z}/e_r\mathbb{Z} \to S$, $(n_1, \dots, n_r) \mapsto u_1^{n_1} \cdots u_r^{n_r}$. So to define a homomorphism $S \to \mathcal{G}_N/W_N$ as in (b) we need only map each u_i to an element in $\mathcal{G}_N/W_N$ of order e_i that has determinant u_i. Therefore, (b) is true by the previous claim. This proves that (c) implies (b).

Finally, it remains to show that (b) implies (c). This is clear by taking any homomorphism as in (b) and composing with the quotient map $\mathcal{G}_N/W_N \to \mathcal{G}(N_1)/W(N_1)$. □

Remark 4.6. We note that the condition (c) in Theorem 4.5 is straightforward to check in practice since all the groups involved are finite. Now suppose that the conditions of Theorem 4.5 hold. One way to find a group G as in (a), if it exists, is to do a direct search modulo 2^iN for $i = 0, 1, \dots$ (the proof of Theorem 4.5 also gives a constructive way when starting with homomorphism β as in (c)).

4.4. **Proof of Theorem 2.8.** The group $[\mathcal{G},\mathcal{G}]$ is open in $\mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ by Lemma 3.3. Let N be the least common multiple of the levels of $\mathcal{G}$ and $[\mathcal{G},\mathcal{G}]$. Note that N is even since the level of $[\mathcal{G},\mathcal{G}]$ is even. Let W be any of the finitely many of groups satisfying $[\mathcal{G},\mathcal{G}] \subseteq W \subseteq \mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$; its level divides N. To prove the theorem, we need to show that one can find an open subgroup $G \subseteq \mathcal{G}$ such that $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = W$, $[\widehat{\mathbb{Z}}^\times : \det(G)]$ is a power of 2, and the level of G divides N times a power of 2.

There is an open subgroup $U_0 \subseteq \det(\mathcal{G}_N) \subseteq \mathbb{Z}_N^\times$ with $U_0[2^\infty] = 1$ such that $\det(\mathcal{G}_N)$ is generated by its 2-power torsion and U_0; we can may further choose U_0 so that it contains the open and torsion-free subgroup $\{a \in \mathbb{Z}_N^\times : a \equiv I \pmod{2N}\}$. Let S be a subgroup of the 2-power torsion of $\det(\mathcal{G}_N) \subseteq \mathbb{Z}_N^\times$, with maximal cardinality, for which condition (b) of Theorem 4.5 holds, cf. Remark 4.6. Define $U := (S \cdot U_0) \times \prod_{\ell \nmid N} \mathbb{Z}_\ell^\times$; it is an open subgroup of $\det(\mathcal{G})$ and $[\det(\mathcal{G}) : U]$ is a power of 2. The level of U_0, and hence also of U, divides $2N$. By our choice of U, Theorem 4.5 implies that there is an open subgroup $G \subseteq \mathcal{G}$ such that $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = W$, $\det(G) = U$, and the level of G divides a power of 2 times N. By computing in $\mathrm{GL}_2(\mathbb{Z}/2^iN\mathbb{Z})$ for $i \geq 0$, we can find such a group G.

5. Proof of the theorems from §2.3

Note that our proofs of the finiteness of $\mathcal{A}_1$ and $\mathcal{A}_2$ will be given in a manner so that it is clear that they are indeed computable.

5.1. **Proof of Theorem 2.5.** First consider any agreeable subgroup G of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ for which X_G has genus at most 1. Define $H := G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$; it is an open subgroup of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$. The group H contains $-I$ since G contains all the scalars in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. Let N

be the level of H. Define the congruence subgroup $\Gamma_G := \mathrm{SL}_2(\mathbb{Z}) \cap H = \mathrm{SL}_2(\mathbb{Z}) \cap G$ of $\mathrm{SL}_2(\mathbb{Z})$; equivalently, it is the congruence subgroup of level N whose image modulo N agrees with the image of H modulo N. In particular, H can be recovered from Γ_G and we have $-I \in \Gamma_G$. The genus of Γ_G agrees with the genus of G, see Remark 2.4, and hence is at most 1.

There are only finitely many congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ that have genus at most 1 and contain $-I$, cf. [CP03]. Moreover, all such congruence subgroups are explicitly given in [CP03] up to conjugacy in $\mathrm{GL}_2(\mathbb{Z})$; there are 121 and 163 conjugacy classes with genus 0 and 1, respectively.

Now fix one of the finitely many congruence subgroups Γ of $\mathrm{SL}_2(\mathbb{Z})$ that have genus at most 1 and contains $-I$. Let H be the open subgroup of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ corresponding to Γ. We have $-I \in H$. In the rest of the proof, we will explain how to compute the (finitely many) agreeable subgroups G of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ for which $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = H$. The finiteness of $\mathcal{A}_1'$, and hence also of $\mathcal{A}_1$, will be obtained by varying over the finite many Γ. Let N be the level of Γ; it is also the level of H. Define the integer $N_1 := 2\,\mathrm{lcm}(N, 12)$.

Lemma 5.1. *For any agreeable subgroup G of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ with $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = H$, the level of G divides N_1.*

Proof. Define $N_0 = \mathrm{lcm}(N, 12)$. We have $H = H_{N_0} \times \prod_{\ell \nmid N_0} \mathrm{SL}_2(\mathbb{Z}_\ell)$ since the level of H divides N_0. Hence $[H, H] = [H_{N_0}, H_{N_0}] \times \prod_{\ell \nmid N_0} \mathrm{SL}_2(\mathbb{Z}_\ell)$ by Lemma 3.2(i). In particular, the level of $[H, H]$ is divisible only by primes dividing N_0; equivalently, dividing $N_1 = 2N_0$. Consider any agreeable subgroup G of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ for which $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = H$. We have $\mathrm{SL}_2(\widehat{\mathbb{Z}}) \supseteq [G, G] \supseteq [H, H]$, so any prime dividing the level of $[G, G]$ must also divide N_1. Since G is agreeable, we have $G = G_{N_1} \times \prod_{\ell \nmid N_1} \mathrm{GL}_2(\mathbb{Z}_\ell)$. It remains to show that the level of $G_{N_1} \subseteq \mathrm{GL}_2(\mathbb{Z}_{N_1})$ divides N_1. From Lemma 3.7 and our choice of N_1, we find that $\mathbb{Z}_{N_1}^\times H_{N_1}$ is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_{N_1})$ whose level divides N_1. We have $\mathbb{Z}_{N_1}^\times H_{N_1} \subseteq G_{N_1}$ since G contains H and $\widehat{\mathbb{Z}}^\times \cdot I$, and hence the level of G_{N_1} divides N_1. □

We now describe how to compute all the agreeable subgroups G of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ for which $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = H$. By Lemma 5.1, the level of such a group G divides N_1. So we first look for subgroups $\overline{G}$ of $\mathrm{GL}_2(\mathbb{Z}/N_1\mathbb{Z})$ for which $\overline{G} \cap \mathrm{SL}_2(\mathbb{Z}/N_1\mathbb{Z})$ equals the the image of H modulo N_1. There are only finitely many such groups $\overline{G}$ which give rise to finite many candidate groups G of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ which satisfy $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = H$. We can then check which of the candidates G are agreeable.

Finally, suppose there is a group $G \in \mathcal{A}_1$ and a prime $\ell > 19$ for which ℓ divides the level of $[G, G]$. By Lemma 3.5, we have $G_\ell \not\supseteq \mathrm{SL}_2(\mathbb{Z}_\ell)$ and hence the level of $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) \subseteq \mathrm{SL}_2(\widehat{\mathbb{Z}})$ is divisible by ℓ. From our argument above, we find that there is a congruence subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ of genus at most 1 for which ℓ divides the level of Γ. However, the classification of low genus congruence subgroups in [CP03] shows that 19 is the largest possible prime divisor of the level of a congruence subgroup of genus at most 1. Therefore, the level of $[G, G]$ is not divisible by any prime $\ell > 19$ for all $G \in \mathcal{A}_1$.

5.2. **Proof of Theorem 2.6.** First consider any agreeable subgroup G of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ with genus at least 2 that satisfies $G_\ell \supseteq \mathrm{SL}_2(\mathbb{Z}_\ell)$ for all $\ell > 19$. By Lemma 3.5, the level of $[G, G]$ is not divisible by any prime $\ell > 19$. Since G is agreeable, its

level is not divisible by any prime $\ell > 19$. Choose a maximal agreeable group $G \subseteq G' \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ for which G' has genus at least 2. Since the level of G' divides the level of G, we deduce that G' lies in $\mathcal{A}_2'$. This proves part (ii).

Now take any group $G \in \mathcal{A}_2'$. Choose a minimal agreeable group $\mathcal{G}$ of genus at most 1 that satisfies $G \subseteq \mathcal{G}$. Using the definition of $\mathcal{A}_1'$ and $\mathcal{A}_2'$, we find that $\mathcal{G} \in \mathcal{A}_1'$ and that G is a (proper) maximal agreeable subgroup of $\mathcal{G}$. Since we are only interested in groups up to conjugacy, we may assume that $\mathcal{G} \in \mathcal{A}_1$. Since $\mathcal{A}_1$ is finite by Theorem 2.5, to prove the finiteness of $\mathcal{A}_2$ it suffices to show that every group $\mathcal{G} \in \mathcal{A}_1$ has only finitely many maximal agreeable subgroups whose level is not divisible by any prime $\ell > 19$.

Fix a group $\mathcal{G} \in \mathcal{A}_1$ and let M be the product of the primes that divide the level of $[\mathcal{G}, \mathcal{G}]$. We have $\ell \nmid M$ for all $\ell > 19$ by Theorem 2.5. Since $\mathcal{G}$ is agreeable, the level of $\mathcal{G}$ is also not divisible by any prime $\ell > 19$. We now consider the maximal agreeable subgroups G of $\mathcal{G}$ as classified in §4.2. We want to show that there are only finitely many of each type and make clear that they are computable.

If $3 \nmid M$, we obtain a single maximal agreeable subgroup as in Lemma 4.3(iii).

Take any prime $p \nmid M$ with $p \le 19$. The maximal open subgroups $B \subseteq \mathrm{GL}_2(\mathbb{Z}_p)$ with $\mathbb{Z}_p^\times I \subseteq B$ and $\mathrm{SL}_2(\mathbb{Z}_p) \not\subseteq B$, give rise to the maximal agreeable subgroups of $\mathcal{G}$ as in Lemma 4.3(ii). By Lemma 3.6, the group B have level p and are thus easy to enumerate.

A maximal agreeable subgroup of $\mathcal{G}$ as given in Lemma 4.3(i) arises from a maximal proper open subgroup B of $\mathcal{G}_M$ that contain $\mathbb{Z}_M^\times I$. Let N be the least common multiple of 4, M, and the level of $\mathcal{G}$. Lemma 3.8 implies that the level of B divides $N\ell$ for some prime $\ell | N$. So one need only look for maximal subgroups of the image of G in $\mathrm{GL}_2(\mathbb{Z}/N\ell\mathbb{Z})$ for each $\ell | N$.

Now consider any prime $p \in \{3, 5\}$ that does not divide M. We now consider maximal agreeable subgroups of $\mathcal{G}$ as described in Lemma 4.4. By Lemma 4.4, it suffices to compute the open normal subgroups of $\mathcal{G}_M$ for which the quotient is isomorphic to a group $Q \in \{\mathfrak{S}_p, \mathfrak{A}_p\}$ where $Q \neq \mathfrak{A}_p$ when $p = 3$. Let N be the least common multiple of M and the level of $\mathcal{G}$; it has the same prime divisors as M. For any continuous and surjective homomorphism $\mathcal{G}_M \twoheadrightarrow Q$, the kernel contains all $g \in \mathcal{G}_M$ with $g \equiv I \pmod N$ since Q contains no normal ℓ-groups for all $\ell \nmid M$. Therefore, one need only look for normal subgroup of the image of $\mathcal{G}_M$ modulo N that have Q as a quotient group.

5.3. **Proof of Theorem 2.7.** Let $\mathcal{G}$ be the agreeable closure of G_E. Proposition 2.3 implies that G is a minimal element of $\mathcal{A}_1'$, with respect to inclusion, for which G_E is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a subgroup of G. By conjugating G_E, we may assume that $G_E \subseteq G$. Since $\mathcal{G}$ is the minimal agreeable subgroup containing G_E, we have $G_E \subseteq \mathcal{G} \subseteq G$. If $\mathcal{G}$ has genus at most 1, then $\mathcal{G} = G$ since otherwise G is not a minimal element of $\mathcal{A}_1'$ with respect to inclusion. We can now assume that $\mathcal{G}$ has genus at least 2.

We claim that $\mathcal{G}_\ell \supseteq \mathrm{SL}_2(\mathbb{Z}_\ell)$ for all primes $\ell > 19$. Take any prime $\ell > 19$. By assumption, we have $\rho_{E,\ell}(\mathrm{Gal}_K) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ and hence $(G_E)_\ell \supseteq \mathrm{SL}_2(\mathbb{Z}_\ell)$ by Lemma 3.6. The claim follows since $G_E \subseteq \mathcal{G}$ and hence $(G_E)_\ell \subseteq \mathcal{G}_\ell$.

Theorem 2.6(ii) implies that $\mathcal{G}$, and hence also G_E, is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a subgroup of some $G' \in \mathcal{A}_2$. Proposition 2.3 implies that $K_{G'} \subseteq K$ and $j_E \in \pi_{G'}(X_{G'}(K)) \subseteq J_K$, where the last inclusion uses that G' lies in $\mathcal{A}_2$. Since $j_E \notin J_K$ by assumption, the case where $\mathcal{G}$ has genus at least 2 does not occur.

References

[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). ↑1.3

[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. ↑2.7, 5.1, 5.1

[Kaw03] Takashi Kawamura, *The effective surjectivity of mod l Galois representations of 1- and 2-dimensional abelian varieties with trivial endomorphism ring*, Comment. Math. Helv. **78** (2003), no. 3, 486–493. ↑2.7

[LV14] Eric Larson and Dmitry Vaintrob, *On the surjectivity of Galois representations associated to elliptic curves over number fields*, Bull. Lond. Math. Soc. **46** (2014), no. 1, 197–209. ↑2.7

[LMFDB] The LMFDB Collaboration, *The L-functions and modular forms database*. Online database, accessed January 2024. ↑1.1

[Rib76] Kenneth A. Ribet, *Galois action on division points of abelian varieties with real multiplications*, Amer. J. Math. **98** (1976), no. 3, 751–804. ↑3.1

[Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331. ↑1.1, 2.2, 2.7

[Ser81] ———, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. **54** (1981), 323–401. ↑2.7

[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. ↑3.2, 3.2

[Sut16] Andrew V. Sutherland, *Computing images of Galois representations attached to elliptic curves*, Forum Math. Sigma **4** (2016), Paper No. e4, 79. MR3482279 ↑2.7

[Zyw10] David Zywina, *Elliptic curves with maximal Galois action on their torsion points*, Bull. Lond. Math. Soc. **42** (2010), no. 5, 811–826. ↑2.2, 2.8

[Zyw22a] ———, *On the surjectivity of mod ℓ representations associated to elliptic curves*, Bull. Lond. Math. Soc. **54** (2022), no. 6, 2045–2584. ↑2.7

[Zyw22b] ———, *Explicit open images for elliptic curves over* $\mathbb{Q}$ (2022). arXiv:2206.14959 [math.NT]. ↑1.1, 2.4, 2.2, 2.3, 2.5, 2.5, 2.8, 3.2, 3.3, 3.7, 3.3, 4.2

[Zyw24] ———, GitHub repository related to *Open image computations for elliptic curves over number fields*, 2024. https://github.com/davidzywina/AgreeableGroups. ↑2.3, 2.3

Department of Mathematics, Cornell University, Ithaca, NY 14853, USA
Email address: zywina@math.cornell.edu