ELLIPTIC CURVES WITH MAXIMAL GALOIS ACTION ON THEIR TORSION POINTS

DAVID ZYWINA

Abstract. Given an elliptic curve E over a number field k, the Galois action on the torsion points of E induces a Galois representation, $\rho_E\colon \operatorname{Gal}(\bar{k}/k) \to \operatorname{GL}_2(\widehat{\mathbb{Z}})$. For a fixed number field k, we describe the image of ρ_E for a "random" elliptic curve E over k. In particular, if $k \neq \mathbb{Q}$ is linearly disjoint from the cyclotomic extension of $\mathbb{Q}$, then ρ_E will be surjective for "most" elliptic curves over k.

1. Introduction

Fix a number field k and let E be an elliptic curve over k. For each positive integer m, we denote the group of m-torsion of $E(\bar{k})$ by $E[m]$. The group $E[m]$ is non-canonically isomorphic to $(\mathbb{Z}/m\mathbb{Z})^2$ and is equipped with a natural action of the absolute Galois group $G_k := \operatorname{Gal}(\bar{k}/k)$, which may be re-expressed in terms of a Galois representation

$$\rho_{E,m}\colon G_k \to \operatorname{Aut}(E[m]) \cong \operatorname{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

Combining these representations for all m we obtain a single Galois representation

$$\rho_E\colon G_k \to \operatorname{Aut}(E(\bar{k})_{\text{tors}}) \cong \operatorname{GL}_2(\widehat{\mathbb{Z}})$$

which encapsulates the Galois action on the torsion points of E. The main result concerning these representations is the following renowned theorem of Serre [Ser72].

Theorem 1.1 (Serre). *If E/k does not have complex multiplication, then $\rho_E(G_k)$ has finite index in $\operatorname{GL}_2(\widehat{\mathbb{Z}})$.*

Serre's theorem is a qualitative result and does not describe how large the image of ρ_E can be. In particular, can the Galois representation ρ_E ever be surjective? In other words, can every possible group automorphism of the torsion points of E arise as a Galois action?

The first example of a surjective representation ρ_E was given recently by A. Greicius in his Ph.D. thesis (see [Gre07]). Let $\alpha \in \overline{\mathbb{Q}}$ be a root of the polynomial $x^3 + x + 1$, and let $E/\mathbb{Q}(\alpha)$ be the elliptic curve given by the Weierstrass equation $y^2 + 2xy + \alpha y = x^3 - x^2$. Greicius shows that $\rho_E(G_{\mathbb{Q}(\alpha)}) = \operatorname{GL}_2(\widehat{\mathbb{Z}})$.

In this paper we shall describe how large $\rho_E(G_k)$ can be for a "random" elliptic curve E over k.

1.1. **Statement of results.** Denote the ring of integers of k by $\mathcal{O}_k$. For $(a,b) \in \mathcal{O}_k^2$, define $\Delta_{a,b} = -16(4a^3 + 27b^2)$. If $\Delta_{a,b} \neq 0$, then let $E(a,b)$ be the elliptic curve over k defined by the Weierstrass equation

$$Y^2 = X^3 + aX + b.$$

Now fix a norm $\|\cdot\|$ on $\mathbb{R} \otimes_{\mathbb{Z}} \mathcal{O}_k^2 \cong \mathbb{R}^{2[k:\mathbb{Q}]}$. For each real number $x > 0$, we define the set

$$B_k(x) = \big\{(a,b) \in \mathcal{O}_k^2 : \Delta_{a,b} \neq 0,\ \|(a,b)\| \leq x\big\}.$$

Date: August 6, 2009.

2000 *Mathematics Subject Classification.* Primary 11G05; Secondary 11F80, 11N36.

Key words and phrases. elliptic curves, Galois representations, sieve methods.

Thus to each pair $(a,b) \in B_k(x)$, we can associate an elliptic curve $E(a,b)$ over k. The set $B_k(x)$ is finite, and moreover

$$|B_k(x)| \sim \kappa x^{2[k:\mathbb{Q}]} \tag{1.1}$$

as $x \to \infty$, where $\kappa > 0$ is a constant depending on k and $\|\cdot\|$. The following theorem answers a question of Greicius on the surjectivity of the ρ_E ([Gre07, §3.4 Problem 3]). Let $\mathbb{Q}^{\text{cyc}} \subseteq \bar{k}$ be the cyclotomic extension of $\mathbb{Q}$.

Theorem 1.2. *Suppose that* $k \cap \mathbb{Q}^{\text{cyc}} = \mathbb{Q}$ *and* $k \neq \mathbb{Q}$. *Then*

$$\lim_{x\to\infty} \frac{|\{(a,b) \in B_k(x) : \rho_{E(a,b)}(G_k) = \operatorname{GL}_2(\widehat{\mathbb{Z}})\}|}{|B_k(x)|} = 1.$$

Intuitively, the theorem says that for a randomly chosen pair $(a,b) \in \mathcal{O}_k^2$, the corresponding elliptic curve $E(a,b)$ satisfies $\rho_{E(a,b)}(G_k) = \operatorname{GL}_2(\widehat{\mathbb{Z}})$. In particular, with k as in the theorem, there exists an elliptic curve E over k with surjective ρ_E; this was previously unknown except for the case considered by Greicius.

Let $\chi_k \colon G_k \to \widehat{\mathbb{Z}}^\times$ be the cyclotomic character of k. For each elliptic curve E over k, we have $\det \circ \rho_E = \chi_k$. In particular, the assumption $k \cap \mathbb{Q}^{\text{cyc}} = \mathbb{Q}$ (equivalently $\chi_k(G_k) = \widehat{\mathbb{Z}}^\times$) is necessary for Theorem 1.2. For a number field k, we define the group

$$H_k := \{A \in \operatorname{GL}_2(\widehat{\mathbb{Z}}) : \det(A) \in \chi_k(G_k)\}.$$

Given an elliptic curve E over k, we certainly have $\rho_E(G_k) \subseteq H_k$. Our main theorem, which generalizes Theorem 1.2, shows that this is the only general constraint for $k \neq \mathbb{Q}$.

Theorem 1.3. *Let* $k \neq \mathbb{Q}$ *be a number field. Then*

$$\frac{|\{(a,b) \in B_k(x) : \rho_{E(a,b)}(G_k) \neq H_k\}|}{|B_k(x)|} \ll_{k,\|\cdot\|} \frac{\log x}{\sqrt{x}}.$$

Remark 1.4. Theorem 1.3 shows that the proportion of (a,b) in $B_k(x)$ with $\rho_{E(a,b)}(G_k) = H_k$, as a function of x, quickly approaches 1. The implicit constant in the theorem is effective and depends only on k and the fixed norm.

Before continuing, let us introduce some more notation. Let E be an elliptic curve over a field k. For each positive integer m, denote the fixed field in $\bar{k}$ of $\ker(\rho_{E,m})$ by $k(E[m])$.

1.2. The rationals.

For completeness, we let us consider the case $k = \mathbb{Q}$ which was excluded from Theorem 1.3. Let E be an elliptic curve over $\mathbb{Q}$, and let Δ be the discriminant of some Weierstrass model of E over $\mathbb{Q}$. There exists an integer $n \geq 1$ such that $\mathbb{Q}(\sqrt{\Delta}) \subseteq \mathbb{Q}(\mu_n)$, where μ_n is the set of n-th roots of unity (the assumption $k = \mathbb{Q}$ is important here!).

Using that the field $\mathbb{Q}(\sqrt{\Delta})$ lies in both $\mathbb{Q}(E[2])$ and $\mathbb{Q}(\mu_n) \subseteq \mathbb{Q}(E[n])$, Serre deduced that the index $[\operatorname{GL}_2(\mathbb{Z}/2n\mathbb{Z}) : \rho_{E,2n}(G_\mathbb{Q})]$ is *even* (for details, see [Ser72, pp. 310-311]) and in particular $\rho_E(G_\mathbb{Q}) \neq \operatorname{GL}_2(\widehat{\mathbb{Z}})$. Following Lang and Trotter, we make the following definition.

Definition 1.5. An elliptic curve E over $\mathbb{Q}$ is a *Serre curve* if $[\operatorname{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(G_\mathbb{Q})] = 2$.

A Serre curve is thus an elliptic curve E over $\mathbb{Q}$ for which $\rho_E(G_\mathbb{Q})$ is as large as possible. For a Serre curve $E/\mathbb{Q}$, the group $\rho_E(G_\mathbb{Q})$ can be described explicitly in terms of the field $\mathbb{Q}(\sqrt{\Delta})$. N. Jones [Jon06a] (building on work of Duke [Duk97]) has shown that "most" elliptic curves over $\mathbb{Q}$ are Serre curves. The analogue of Theorem 1.3 is then the following.

Theorem 1.6 (Jones)**.** *There is a constant $\beta > 0$ such that*

$$\frac{|\{(a,b) \in B_{\mathbb{Q}}(x) : E(a,b) \text{ is not a Serre curve}\}|}{|B_{\mathbb{Q}}(x)|} \ll_{\|\cdot\|} \frac{(\log x)^{\beta}}{\sqrt{x}}.$$

Remark 1.7. Theorem 1.6 is a special case of [Jon06a, Theorem 4] and will be proven in §7.2. Unlike Jones' version, the constants in our proof will be effective.

1.3. **Overview of proof.** Suppose that E is an elliptic curve over a number field $k \neq \mathbb{Q}$. There is an exact sequence

$$1 \to \mathrm{SL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\widehat{\mathbb{Z}}) \overset{\det}{\to} \widehat{\mathbb{Z}}^{\times} \to 1,$$

and the representation $\det \circ \rho_E \colon G_k \to \widehat{\mathbb{Z}}^{\times}$ is the cyclotomic character χ_k of k. Therefore,

$$\rho_E(G_k) \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = \rho_E(G_{k^{\mathrm{cyc}}}).$$

Thus the equality $\rho_E(G_k) = H_k$ is equivalent to $\rho_E(G_{k^{\mathrm{cyc}}}) = \mathrm{SL}_2(\widehat{\mathbb{Z}})$. A group theoretic argument will show that this in turn is equivalent to having $\rho_{E,m}(G_{k^{\mathrm{cyc}}}) = \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ whenever m is equal to 4, 9, or a prime ≥ 5.

For a prime $m = \ell \geq 5$, the condition $\rho_{E,\ell}(G_{k^{\mathrm{cyc}}}) = \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is equivalent to $\rho_{E,\ell}(G_k) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$. By considering the Frobenius endomorphism for the reduction of E modulo several primes $\mathfrak{p} \subseteq \mathcal{O}_k$, we can determine which conjugacy classes of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ meet $\rho_{E,\ell}(G_k)$. Combining this modulo $\mathfrak{p}$ information together, we will use the large sieve to give an asymptotic upper bound for the growth of

$$|\{(a,b) \in B_k(x) : \rho_{E(a,b),\ell}(G_k) \not\supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})\}|$$

as a function of x; see §5. To understand the distribution of reductions modulo $\mathfrak{p}$, we will use a recent result of Jones; see §3. Of significant importance is a theorem of Masser and Wüstholz, which is needed to bound the number of ℓ's that must be considered.

The conditions at $m = 4$ or 9 are more involved. In particular, for $m = 4$ we will need to impose the condition that $\sqrt{\Delta}$ is not in the cyclotomic extension of k (this avoids the obstruction of §1.2 that always occurs for $k = \mathbb{Q}$). In §6, we again use the large sieve to bound the number of $(a,b) \in B_k(x)$ for which $\sqrt{\Delta_{a,b}}$ (and $\sqrt[3]{\Delta_{a,b}}$ if $\mu_3 \subseteq k$) lie in the cyclotomic extension of k.

Our main theorems will then be deduced in §7.

1.4. **Hilbert irreducibility.** It is useful to recast our theorem in terms of the philosophy of the Hilbert irreducibility theorem. Treating a and b as variables, we obtain an elliptic curve $\mathcal{E} = E(a,b)$ over $k(a,b)$ and as before we have a Galois representation $\rho_{\mathcal{E}} \colon G_{k(a,b)} \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$. It is easy to show that $\rho_{\mathcal{E}}$ has image H_k. For each pair $(a_0, b_0) \in \mathcal{O}_k^2$ with $\Delta_{a,b} \neq 0$, specialization induces an inclusion $\rho_{E(a_0,b_0)}(G_k) \subseteq \rho_{\mathcal{E}}(G_{k(a,b)}) = H_k$. For $k \neq \mathbb{Q}$, our theorem shows that equality holds for most specializations, which is what one would expect from Hilbert's irreducibility theorem. However, this is *not* a direct application of Hilbert's theorem since H_k is an infinite group (the case $k = \mathbb{Q}$ serves as a good warning).

It would be interesting to consider more general families of abelian varieties, and we hope to return to this in future work. See Cojocaru and Hall [CH05] for work on 1-parameter families of elliptic curves.

Acknowledgements. Many thanks to Bjorn Poonen for his careful reading of this paper, helpful comments and assistance. Thanks also to Aaron Greicius and Nathan Jones.

Notation and conventions. For each field k, let $\bar{k}$ be an algebraic closure of k and let $G_k := \operatorname{Gal}(\bar{k}/k)$ be the absolute Galois group of k. For each integer $n \geq 1$, let μ_n be the group of n-th roots of unity in $\bar{k}$. Let k^{cyc} (resp. k^{ab}) be the cyclotomic (resp. maximal abelian) extension of k in $\bar{k}$.

For a number field k, denote its ring of integers by $\mathcal{O}_k$. Let Σ_k be the set of non-zero prime ideals of $\mathcal{O}_k$. For each $\mathfrak{p} \in \Sigma_k$, we have a residue field $\mathbb{F}_\mathfrak{p} = \mathcal{O}_k/\mathfrak{p}$ whose cardinality we denote by $N(\mathfrak{p})$. Let $\Sigma_k(x)$ be the set of primes $\mathfrak{p}$ in Σ_k with $N(\mathfrak{p}) \leq x$. Let $\operatorname{ord}_\mathfrak{p} \colon k^\times \to \mathbb{Z}$ be the surjective discrete valuation corresponding to $\mathfrak{p}$. Denote the absolute discriminant of k by d_k.

Fix a group G. Let G' be the derived subgroup of G, i.e., the minimal normal subgroup of G for which G/G' is abelian. Equivalently, G' is the group generated by the set $\{xyx^{-1}y^{-1} : x, y \in G\}$. The abelianization of G is $G^{\mathrm{ab}} := G/G'$. Profinite groups will always be considered with their profinite topologies.

For a, b in a field k, define $\Delta_{a,b} = -16(4a^3 + 27b^2)$. If $\Delta_{a,b} \neq 0$, then let $E(a, b)$ be the elliptic curve over k defined by the Weierstrass equation $Y^2 = X^3 + aX + b$.

Suppose that f and g are real valued functions of a real variable x. By $f \ll g$ (or $g \gg f$), we mean that there are positive constants C_1 and C_2 such that for all $x \geq C_1$, $|f(x)| \leq C_2|g(x)|$. We use $O(f)$ to represent an unspecified function g with $g \ll f$. The dependencies of the implied constants will always be indicated by subscripts. Also, all implicit constants occurring in this paper are effective.

Finally, the symbols ℓ and p will always denote rational primes.

2. Criterion for maximal Galois action

Proposition 2.1. *Let E be an elliptic curve over a number field k, and let Δ be the discriminant of a Weierstrass model of E over k. Suppose that the following conditions hold:*

(a) $\rho_{E,\ell}(G_k) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ *for every prime* $\ell \geq 5$,
(b) $\rho_{E,4}(G_k) \supseteq \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$ *and* $\rho_{E,9}(G_k) \supseteq \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$,
(c) $\sqrt{\Delta} \notin k^{\mathrm{cyc}}$,
(d) $\mu_3 \not\subseteq k$ *or* $\sqrt[3]{\Delta} \notin k^{\mathrm{cyc}}$.

Then $\rho_E(G_k) = H_k$.

Remark 2.2.

(i) The image of Δ in $k^\times/(k^\times)^{12}$ depends only on the isomorphism class of E/k. Thus for a positive integer r dividing 12, the r-th root of Δ, up to a factor in $\mu_r \cdot k^\times$, is independent of all choices. In particular, conditions (c) and (d) are well-defined.
(ii) The Kronecker-Weber theorem says that $\mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}^{\mathrm{ab}}$, so condition (c) *never* holds for $k = \mathbb{Q}$.

Since $\det \circ \rho_E \colon G_k \to \widehat{\mathbb{Z}}^\times$ is the cyclotomic character of k, we find that $\rho_E(G_k) = H_k$ if and only if $\rho_E(G_{k^{\mathrm{cyc}}}) = \mathrm{SL}_2(\widehat{\mathbb{Z}})$. Applying Lemma A.7 to $\rho_E(G_{k^{\mathrm{cyc}}})$, we have $\rho_E(G_k) = H_k$ if and only if $\rho_{E,m}(G_{k^{\mathrm{cyc}}}) = \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ holds whenever m is 4, 9, or a prime ≥ 5. Proposition 2.1 is then an immediate consequence of the following lemma.

Lemma 2.3. *Let E be an elliptic curve over a number field k with discriminant $\Delta \in k^\times/(k^\times)^{12}$.*

(i) *Let $\ell \geq 5$ be a prime. If $\rho_{E,\ell}(G_k) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$, then $\rho_{E,\ell}(G_{k^{\mathrm{cyc}}}) = \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$.*
(ii) *If $\rho_{E,4}(G_k) \supseteq \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$ and $\sqrt{\Delta} \notin k^{\mathrm{cyc}}$, then $\rho_{E,4}(G_{k^{\mathrm{cyc}}}) = \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$.*
(iii) *If $\rho_{E,9}(G_k) \supseteq \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ and $\sqrt[3]{\Delta} \notin k^{\mathrm{cyc}}$, then $\rho_{E,9}(G_{k^{\mathrm{cyc}}}) = \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$.*
(iv) *If $\rho_{E,9}(G_k) \supseteq \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ and $\mu_3 \not\subseteq k$, then $\rho_{E,9}(G_{k^{\mathrm{cyc}}}) = \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$.*

Proof. Let m be a positive integer such that $\rho_{E,m}(G_k) \supseteq \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$. Since k^{cyc} is an abelian extension of k, we have inclusions

$$\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})' \subseteq \rho_{E,m}(G_k)' \subseteq \rho_{E,m}(G_{k^{\mathrm{cyc}}}) \subseteq \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}). \tag{2.1}$$

(i) Suppose that $m = \ell \geq 5$ is prime. By Lemma A.1 we have $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})' = \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$, so from (2.1) we deduce that $\rho_{E,\ell}(G_{k^{\mathrm{cyc}}}) = \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

(ii) Our assumption $\rho_{E,4}(G_k) \supseteq \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$ implies that $\rho_{E,4}(G_{k(\mu_4)}) = \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$. Thus to prove $\rho_{E,4}(G_{k^{\mathrm{cyc}}}) = \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$, it suffices to show that $k(E[4]) \cap k^{\mathrm{cyc}} = k(\mu_4)$.

In [LT76, Part III §11], it is shown that $\sqrt[4]{\Delta}$ is an element of $k(E[4])$. Using $\sqrt{\Delta} \notin k(\mu_4)$, one finds that $k(\mu_4, \sqrt[4]{\Delta}) \subseteq k(E[4])$ is an abelian extension of $k(\mu_4)$ of degree 4. By Lemma A.1 the group $\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})^{\mathrm{ab}}$ is cyclic of order 4, so $k(E[4]) \cap k(\mu_4)^{\mathrm{ab}} = k(\mu_4, \sqrt[4]{\Delta})$. Therefore

$$k(E[4]) \cap k^{\mathrm{cyc}} = (k(E[4]) \cap k(\mu_4)^{\mathrm{ab}}) \cap k^{\mathrm{cyc}} = k(\mu_4, \sqrt[4]{\Delta}) \cap k^{\mathrm{cyc}} = k(\mu_4), \tag{2.2}$$

where the last equality uses $\sqrt{\Delta} \notin k^{\mathrm{cyc}}$.

(iii) The assumption $\rho_{E,9}(G_k) \supseteq \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ implies that $\rho_{E,9}(G_{k(\mu_9)}) = \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$. By Lemma A.1, the group $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})^{\mathrm{ab}}$ has order 3.

Note that $\sqrt[3]{\Delta}$ is an element of $k(E[3])$ (see [Ade01, Proposition 5.4.3] for example). Arguing as in part (ii), we find that $k(E[9]) \cap k(\mu_9)^{\mathrm{ab}} = k(\mu_9, \sqrt[3]{\Delta})$. Since $\sqrt[3]{\Delta} \notin k^{\mathrm{cyc}}$, we deduce that $k(E[9]) \cap k^{\mathrm{cyc}} = k(\mu_9)$, and hence $\rho_{E,9}(G_{k^{\mathrm{cyc}}}) = \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$.

(iv) The assumptions imply that $\rho_{E,3}(G_k) = \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. One readily checks that $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})' = \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$, and thus $\rho_{E,3}(G_k)' = \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$. Using (2.1), with $m = 3$, gives $\rho_{E,3}(G_{k^{\mathrm{cyc}}}) = \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$.

By Lemma A.1, the group $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})^{\mathrm{ab}}$ has order 3. So from (2.1), with $m = 9$, we find that $\rho_{E,9}(G_{k^{\mathrm{cyc}}})$ is either $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})'$ or $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$. If $\rho_{E,9}(G_{k^{\mathrm{cyc}}}) = \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})'$, then Lemma A.1 implies that $\rho_{E,3}(G_{k^{\mathrm{cyc}}}) \neq \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$. Therefore, $\rho_{E,9}(G_{k^{\mathrm{cyc}}}) = \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$. ☐

We now state a criterion that applies to $k = \mathbb{Q}$.

Lemma 2.4 (Jones)**.** *Let E be an elliptic curve over $\mathbb{Q}$ which satisfies the following properties:*

(a) $\rho_{E,\ell}(G_{\mathbb{Q}}) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ *for every prime* $\ell \geq 5$,
(b) $\rho_{E,72}(G_{\mathbb{Q}}) \supseteq \mathrm{SL}_2(\mathbb{Z}/72\mathbb{Z})$.

Then E is a Serre curve.

Proof. For each $m \geq 1$, we have $\rho_{E,m}(G_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ if and only if $\rho_{E,m}(G_{\mathbb{Q}}) \supseteq \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$. The lemma is now a special case of [Jon06a, Lemma 5]. ☐

3. ELLIPTIC CURVE OVER FINITE FIELDS

Fix a positive integer m and a prime $p \nmid m$. Let E be an elliptic curve over the field $\mathbb{F}_p$. As before, one has a Galois representation $\rho_{E,m}\colon \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, which arises from the Galois action on the m-torsion of E.

Let $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ be the p-th power Frobenius automorphism. For a subset C of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ stable under conjugation, define the set

$$\Omega_C(p) := \left\{(r,s) \in \mathbb{F}_p^2 : \Delta_{r,s} \neq 0,\ \rho_{E(r,s),m}(\mathrm{Frob}_p) \in C\right\}.$$

The following theorem gives a good estimate on the cardinality of this set.

Theorem 3.1 ((Jones))**.** *Fix a positive integer m and a conjugacy class C of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Let d be the element of $(\mathbb{Z}/m\mathbb{Z})^\times$ such that $\det(C) = \{d\}$. Then for all primes p with $p \equiv d \bmod m$,*

$$\frac{|\Omega_C(p)|}{p^2} = \frac{|C|}{|\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})|} + O\left(\frac{m^5}{p^{1/2}}\right).$$

Proof. This follows from Theorem 8 (and Theorem 7) of [Jon06a]. A key ingredient is a generalization of results of Hurwitz, see [Jon06b]. ☐

4. THE LARGE SIEVE

Let K be a number field, Λ a free $\mathcal{O}_K$-module of rank n, and $\|\cdot\|$ a norm on $\Lambda_{\mathbb{R}} = \mathbb{R} \otimes_{\mathbb{Z}} \Lambda$. Fix a subset Y of Λ. Let $x \geq 1$ and $Q > 0$ be real numbers. For every prime ideal $\mathfrak{p} \in \Sigma_K$, let $\omega_{\mathfrak{p}}$ be a real number in the interval $[0, 1)$. Assume the following conditions hold:

1. The set Y is contained in a ball of radius x; i.e., there is an $a_0 \in \Lambda_{\mathbb{R}}$ such that $\|a - a_0\| \leq x$ for all $a \in Y$.
2. For every $\mathfrak{p} \in \Sigma_K(Q)$, the image $Y_{\mathfrak{p}}$ of Y in $\Lambda/\mathfrak{p}\Lambda$ by reduction modulo $\mathfrak{p}$ satisfies
$$|Y_{\mathfrak{p}}| \leq (1 - \omega_{\mathfrak{p}})|\Lambda/\mathfrak{p}\Lambda|.$$

Theorem 4.1 (Large sieve, [Ser97, §12.1])**.** *With assumptions as above, we have*
$$|Y| \ll_{K,\Lambda,\|\cdot\|} \frac{x^{[K:\mathbb{Q}]n} + Q^{2n}}{L(Q)}$$
where
$$L(Q) := \sum_{\substack{\mathfrak{a} \subseteq \mathcal{O}_K \text{ squarefree} \\ N(\mathfrak{a}) \leq Q}} \prod_{\mathfrak{p} | \mathfrak{a}} \frac{\omega_{\mathfrak{p}}}{1 - \omega_{\mathfrak{p}}}.$$

Remark 4.2. We will apply the large sieve with $\Lambda = \mathcal{O}_k^2$ and $\|\cdot\|$ our fixed norm on $\mathbb{R} \otimes_{\mathbb{Z}} \mathcal{O}_k^2$. In §5 and §6, we will take K to be k and $\mathbb{Q}$, respectively.

5. MOST ELLIPTIC CURVES HAVE LARGE ℓ-ADIC GALOIS IMAGES

Throughout this section, fix a number field k.

Definition 5.1. For each positive integer m, define the set
$$B_{k,m}(x) := \{(a, b) \in B_k(x) : \rho_{E(a,b),m}(G_k) \not\supseteq \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})\}.$$

The main goal of this section is to prove the following bound.

Proposition 5.2. *There is an absolute constant $\beta \geq 1$ such that*
$$\frac{|B_{k,4}(x) \cup B_{k,9}(x) \cup \bigcup_{\ell \geq 5} B_{k,\ell}(x)|}{|B_k(x)|} \ll_{k,\|\cdot\|} \frac{(\log x)^{\beta}}{x^{[k:\mathbb{Q}]/2}}.$$

Remark 5.3. For an elliptic curve E over k, we have Galois representations $\rho_{E,\ell^\infty} : G_k \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ coming from the action on the ℓ-power torsion. Proposition 5.2 (with Lemma A.2) shows that for a "random" elliptic curve E over k, we have $\rho_{E,\ell^\infty}(G_k) \supseteq \mathrm{SL}_2(\mathbb{Z}_\ell)$ for all primes ℓ. Since $\det \circ \rho_{E,\ell^\infty} : G_k \to \mathbb{Z}_\ell^\times$ is the ℓ-adic cyclotomic character of k, we find that $\rho_{E,\ell^\infty}(G_k)$ is as "large as possible" for all ℓ.

Remark 5.4. Our proof of Proposition 5.2 is clearly based on Duke's paper [Duk97], which proves the $k = \mathbb{Q}$ case (with Jones [Jon06a] handling 4 and 9).

Unlike Duke's result, the implicit constants in Proposition 5.2 are effective. The source of non-effective constants in [Duk97] is the use of the Siegel-Walfisz theorem. We avoid this by applying the pigeonhole principle in the proof of Lemma 5.10 and then sieving only by conjugacy classes with a fixed determinant.

5.1. **Sieving elliptic curves by Frobenius conjugacy classes.** For a positive integer m and a conjugacy class C of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, define the set

$$Y_C(x) := \{(a,b) \in B_k(x) : \rho_{E(a,b),m}(G_k) \cap C = \emptyset\}.$$

For $d \in (\mathbb{Z}/m\mathbb{Z})^\times$, let $\Sigma_k^1(Q; d, m)$ be the set of $\mathfrak{p} \in \Sigma_k(Q)$ with degree 1 (i.e., $N(\mathfrak{p})$ prime) and $N(\mathfrak{p}) \equiv d \bmod m$.

Proposition 5.5. *Let m be a positive integer and C a conjugacy class of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Let d be the unique element of $(\mathbb{Z}/m\mathbb{Z})^\times$ such that $\det(C) = \{d\}$, and assume that $d \in \chi_k(G_k) \bmod m \subseteq (\mathbb{Z}/m\mathbb{Z})^\times$. Then*

$$\frac{|Y_C(x)|}{|B_k(x)|} \ll_{k,\|\cdot\|} \left(\frac{|C|}{|\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})|} |\Sigma_k^1(x^{[k:\mathbb{Q}]/2}; d, m)| + O_k(m^5 x^{[k:\mathbb{Q}]/4}) \right)^{-1}.$$

Proof. Let Λ be the $\mathcal{O}_k$-module $\mathcal{O}_k^2$. We have already chosen a norm $\|\cdot\|$ on $\Lambda_\mathbb{R} := \mathbb{R} \otimes_\mathbb{Z} \mathcal{O}_k^2$, and the set $B_k(x) \subseteq \Lambda_\mathbb{R}$ lies in a ball of radius x. Let $Q := x^{[k:\mathbb{Q}]/2}$.

For each $\mathfrak{p} \in \Sigma_k^1(Q; d, m)$, define

$$\Omega_\mathfrak{p} = \{(r,s) \in \mathbb{F}_\mathfrak{p}^2 : \Delta_{r,s} \neq 0,\ \rho_{E(r,s),m}(\mathrm{Frob}_{N(\mathfrak{p})}) \in C\}$$

and $\omega_\mathfrak{p} = |\Omega_\mathfrak{p}|/N(\mathfrak{p})^2$. Let $Y_\mathfrak{p}$ be the image of $Y_C(x)$ in $\mathbb{F}_\mathfrak{p}^2$ via reduction modulo $\mathfrak{p}$.

Suppose that $(a,b) \in B_k(x)$ satisfies $(a,b) \bmod \mathfrak{p} \in \Omega_\mathfrak{p}$; then $E(a,b)$ has good reduction at $\mathfrak{p}$ and $\rho_{E(a,b),m}(\mathrm{Frob}_\mathfrak{p}) \subseteq C$. So $\rho_{E(a,b),m}(G_k) \cap C \neq \emptyset$, and thus $(a,b) \notin Y_C(x)$. This shows that

$$Y_\mathfrak{p} \subseteq \mathbb{F}_\mathfrak{p}^2 - \Omega_\mathfrak{p},$$

and hence $|Y_\mathfrak{p}| \leq (1 - \omega_\mathfrak{p})|\Lambda/\mathfrak{p}\Lambda|$.

For $\mathfrak{p} \notin \Sigma_k^1(Q; d, m)$, define $\omega_\mathfrak{p} = 0$. By the large sieve (Theorem 4.1),

$$|Y_C(x)| \ll_{k,\|\cdot\|} \frac{x^{2[k:\mathbb{Q}]}}{L(Q)}, \tag{5.1}$$

where

$$L(Q) := \sum_{\substack{\mathfrak{a} \subseteq \mathcal{O}_k \text{ squarefree} \\ N(\mathfrak{a}) \leq Q}} \prod_{\mathfrak{p} | \mathfrak{a}} \frac{\omega_\mathfrak{p}}{1 - \omega_\mathfrak{p}} \geq \sum_{\mathfrak{p} \in \Sigma_k^1(Q;d,m)} \omega_\mathfrak{p}.$$

For $\mathfrak{p} \in \Sigma_k^1(Q; d, m)$, Theorem 3.1 gives

$$\omega_\mathfrak{p} = \frac{|C|}{|\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})|} + O(m^5/N(\mathfrak{p})^{1/2}).$$

Therefore

$$\begin{aligned} L(Q) &\geq \sum_{\mathfrak{p} \in \Sigma_k^1(Q;d,m)} \left(\frac{|C|}{|\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})|} + O(m^5/N(\mathfrak{p})^{1/2}) \right) \\ &= \frac{|C|}{|\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})|} |\Sigma_k^1(Q; d, m)| + O_k(m^5 Q^{1/2}). \end{aligned}$$

The assumption $d \in \chi_k(G_k) \bmod m$ is needed to guarantees that $L(Q) \gg_{k,m} 1$. The proposition follows by combining our lower bound of $L(Q)$ and (1.1) with (5.1). $\square$

5.2. **Galois image modulo an integer.** The following proposition shows that for a "random" elliptic curve E over k, $\rho_{E,m}$ has large image.

Proposition 5.6. *For a positive integer m,*

$$\frac{|B_{k,m}(x)|}{|B_k(x)|} \ll_{k,\|\cdot\|,m} \frac{\log x}{x^{[k:\mathbb{Q}]/2}}.$$

Proof. Let $C_1, \ldots, C_n$ be the conjugacy classes of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ with determinant 1. By Lemma A.9, we have $B_{k,m}(x) \subseteq \bigcup_{i=1}^n Y_{C_i}(x)$. Proposition 5.5 gives

$$\frac{|B_{k,m}(x)|}{|B_k(x)|} \le \sum_{i=1}^n \frac{|Y_{C_i}(x)|}{|B_k(x)|} \ll_{k,\|\cdot\|} \sum_{i=1}^n \Big(\frac{|C_i|}{|\operatorname{SL}_2(\mathbb{Z}/m\mathbb{Z})|}|\Sigma_k^1(x^{[k:\mathbb{Q}]/2};1,m)| + O_k(m^5 x^{[k:\mathbb{Q}]/4})\Big)^{-1}.$$

Using $|\Sigma_k^1(x^{[k:\mathbb{Q}]/2};1,m)| \gg_{k,m} x^{[k:\mathbb{Q}]/2}/\log x$, we deduce that

$$\frac{|B_{k,m}(x)|}{|B_k(x)|} \ll_{k,\|\cdot\|,m} \sum_{i=1}^n \big(x^{[k:\mathbb{Q}]/2}/\log x\big)^{-1} \ll_m \frac{\log x}{x^{[k:\mathbb{Q}]/2}}. \qquad \square$$

5.3. **Galois image modulo primes.** Let h be the absolute logarithmic height on $\mathbb{P}^1(\overline{\mathbb{Q}})$. For an elliptic curve E, let $j(E)$ be its j-invariant. The following theorem bounds the number of ℓ's that we need to consider (in particular, it gives an effective version of a result of Serre [Ser72]).

Theorem 5.7 (Masser-Wüstholz [MW93])**.** *Let E be an elliptic curve defined over a number field k, and assume that E does not have complex multiplication. There are positive absolute constants c and γ such that if $\ell > c\big(\max\{[k:\mathbb{Q}], h(j(E))\}\big)^\gamma$, then $\rho_{E,\ell}(G_k) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$.*

Lemma 5.8. *If $(a,b) \in B_k(x)$, then $h(j(E(a,b))) \ll_{k,\|\cdot\|} \log x$.*

Proof. Let Σ_k^∞ be the set of archimedean places of k. For each $v \in \Sigma_k^\infty$, let $|\cdot|_v$ be an absolute value on the completion k_v of k at v. On $\prod_{v\in\Sigma_k^\infty} k_v^2$, we have a norm $\|(a_v,b_v)_v\|_1 = \sup_{v\in\Sigma_k^\infty}|a_v|_v + \sup_{v\in\Sigma_k^\infty}|b_v|_v$. Using the natural isomorphism $\mathbb{R}\otimes_\mathbb{Z}\mathcal{O}_k^2 \cong \prod_{v\in\Sigma_k^\infty} k_v^2$, we may view $\|\cdot\|_1$ as a norm on $\mathbb{R}\otimes_\mathbb{Z}\mathcal{O}_k^2$. Recall that $j(E(a,b)) = -1728(4a)^3/\Delta_{a,b}$. Since a and b are integral, we have

$$h(j(E(a,b))) = h([-1728(4a)^3 : \Delta_{a,b}]) \ll_k \sum\nolimits_{v\in\Sigma_k^\infty} \log(\max\{1728\cdot 4^3|a|_v^3, |\Delta_{a,b}|_v\})$$

and thus $h(j(E(a,b))) \ll_k \log\|(a,b)\|_1$. The norms $\|\cdot\|$ and $\|\cdot\|_1$ are equivalent, so

$$h(j(E(a,b))) \ll_k \log\|(a,b)\|_1 \ll_{k,\|\cdot\|} \log\|(a,b)\| \le \log x. \qquad \square$$

Lemma 5.9. *There is a constant $c_k > 0$ (depending only on k) and an absolute constant $\gamma > 0$ such that*

$$\big\{(a,b)\in B_k(x) : \rho_{E(a,b),\ell}(G_k) \not\supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \text{ for some prime } \ell \ge 5\big\} = \bigcup_{5\le\ell\le c_k(\log x)^\gamma} B_{k,\ell}(x).$$

Proof. For an elliptic curve E/k with complex multiplication, we have $\rho_{E,\ell}(G_k) \not\supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for every prime $\ell \ge 5$. The lemma follows by combining Theorem 5.7 and Lemma 5.8. $\square$

Lemma 5.10. *Assume that $5 \le \ell \le c_k(\log x)^\gamma$, where c_k and γ are the constants from Lemma 5.9. Then*

$$\frac{|B_{k,\ell}(x)|}{|B_k(x)|} \ll_{k,\|\cdot\|} \frac{(\log x)^{7\gamma+1}}{x^{[k:\mathbb{Q}]/2}}.$$

Proof. We may assume that ℓ satisfies $k\cap\mathbb{Q}(\mu_\ell)=\mathbb{Q}$ (this excludes only a finite number of ℓ, which can be handled with Proposition 5.6). Define the set $\Sigma_k^1(x):=\{\mathfrak{p}\in\Sigma_k(x) : N(\mathfrak{p}) \text{ is prime}\}$. By the pigeonhole principle, there is an element $d\in(\mathbb{Z}/\ell\mathbb{Z})^\times=\chi_k(G_k) \bmod \ell$ such that

$$|\Sigma_k^1(x^{[k:\mathbb{Q}]/2};d,\ell)|\geq\frac{1}{\ell-1}|\Sigma_k^1(x^{[k:\mathbb{Q}]/2})|+O_k(1)\gg_k\frac{1}{\ell-1}x^{[k:\mathbb{Q}]/2}/\log x.$$

Let $C_1,\dots,C_n$ be the conjugacy classes of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ with $\det(C_i)=d$. Combining Lemma A.8 and Proposition 5.5, we have

$$\begin{aligned}\frac{|B_{k,\ell}(x)|}{|B_k(x)|}\leq\sum_{i=1}^n\frac{|Y_{C_i}(x)|}{|B_k(x)|}&\ll_{k,\|\cdot\|}\sum_{i=1}^n\left(\frac{|C_i|}{|\,\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})|}|\Sigma_k^1(x^{[k:\mathbb{Q}]/2};d,\ell)|+O_k(\ell^5x^{[k:\mathbb{Q}]/4})\right)^{-1}\\&\ll_{k,\|\cdot\|}\sum_{i=1}^n\left(\frac{|C_i|}{|\,\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}x^{[k:\mathbb{Q}]/2}/\log x+O_k(\ell^5x^{[k:\mathbb{Q}]/4})\right)^{-1}.\end{aligned}$$

The bounds $n\leq\ell^3$, $1\leq|C_i|$, and $\ell\leq c_k(\log x)^\gamma$ imply

$$\frac{|B_{k,\ell}(x)|}{|B_k(x)|}\ll_{k,\|\cdot\|}n\ell^4\frac{\log x}{x^{[k:\mathbb{Q}]/2}}\ll_k\frac{(\log x)^{7\gamma+1}}{x^{[k:\mathbb{Q}]/2}}.$$ □

5.4. **Proof of Proposition 5.2.** Using Lemmas 5.9 and 5.10, we obtain the following bounds:

$$\frac{|\bigcup_{\ell\geq5}B_{k,\ell}(x)|}{|B_k(x)|}\leq\sum_{5\leq\ell\leq c_k(\log x)^\gamma}\frac{|B_{k,\ell}(x)|}{|B_k(x)|}\ll_{k,\|\cdot\|}\sum_{5\leq\ell\leq c_k(\log x)^\gamma}\frac{(\log x)^{7\gamma+1}}{x^{[k:\mathbb{Q}]/2}}\ll_k\frac{(\log x)^{8\gamma+1}}{x^{[k:\mathbb{Q}]/2}}.$$

By Proposition 5.6 (with $m=4$ and 9), we have

$$\frac{|B_{k,4}(x)\cup B_{k,9}(x)|}{|B_k(x)|}\ll_{k,\|\cdot\|}\frac{\log x}{x^{[k:\mathbb{Q}]/2}}.$$

The proposition follows immediately with $\beta=8\gamma+1$.

6. DISCRIMINANTS

Proposition 6.1. *Fix a number field $k\neq\mathbb{Q}$, an integer $r\geq2$, and assume that k contains μ_r. Then*

$$\frac{|\{(a,b)\in B_k(x):\sqrt[r]{\Delta_{a,b}}\in k^{\mathrm{cyc}}\}|}{|B_k(x)|}\ll_{k,\|\cdot\|,r}\frac{\log x}{\sqrt{x}}.$$

Remark 6.2. From Proposition 6.1, we find that conditions (c) and (d) of Proposition 2.1 hold for "most" elliptic curves over a fixed number field $k\neq\mathbb{Q}$.

For the rest of this section, we shall fix k and r as in Proposition 6.1. Let $d=[k:\mathbb{Q}]$. Let S be the finite set of rational primes which satisfies the following conditions with minimal value $\prod_{p\in S}p$;

- S contains the primes dividing $6r$,
- S contains the primes that are ramified in k,
- $\mathcal{O}_S$ is a principal ideal domain, where $\mathcal{O}_S$ is the ring of S'-integers of k and $S'=\{\mathfrak{p}\in\Sigma_k : \mathfrak{p}|p,\ \text{ for some } p\in S\}$.

Note that the above choice of S depends only on k and r.

Lemma 6.3. *Fix a prime $p\notin S$, an element $\Delta\in k^\times$, and let $\mathfrak{P}_1\dots,\mathfrak{P}_n$ be the prime ideals of $\mathcal{O}_{k(\sqrt[r]{\Delta})}$ lying over p. If $\sqrt[r]{\Delta}\in k^{\mathrm{cyc}}$, then*

$$e(\mathfrak{P}_1/p)=\cdots=e(\mathfrak{P}_n/p),$$

where $e(\mathfrak{P}_i/p)$ is the ramification index of $\mathfrak{P}_i$ over p.

Proof. Since $\sqrt[r]{\Delta} \in k^{\rm cyc} = \mathbb{Q}^{\rm cyc} \cdot k$, one can show that there is a field $L \subseteq \mathbb{Q}^{\rm cyc}$ such that $k(\sqrt[r]{\Delta}) = L \cdot k$. Since p is unramified in k, we find that $e(\mathfrak{P}_i/p) = e(\mathfrak{P}_i \cap \mathcal{O}_L/p)$. The value $e(\mathfrak{P}_i \cap \mathcal{O}_L/p)$ is independent of i, since L is a Galois extension of $\mathbb{Q}$. ☐

Lemma 6.4. *Let $\mathcal{B} \subseteq \mathcal{O}_S^\times$ be a set of representatives for the cosets of $\mathcal{O}_S^\times/(\mathcal{O}_S^\times)^r$. Then for any $\Delta \in \mathcal{O}_k$ with $\sqrt[r]{\Delta} \in k^{\rm cyc}$, there are $m \in \mathbb{Z}$, $\alpha \in \mathcal{O}_S$, and $\beta \in \mathcal{B}$ such that $\Delta = m\alpha^r\beta$.*

Proof. Fix $\Delta \in \mathcal{O}_k$ with $\sqrt[r]{\Delta} \in k^{\rm cyc}$. We first show that Δ can be written in the form $m\alpha^r\beta$, for some $m \in \mathbb{Z}$, $\alpha \in \mathcal{O}_S$, and $\beta \in \mathcal{O}_S^\times$. We may assume that Δ is non-zero. Since $\mathcal{O}_S$ is a principal ideal domain, there is an element $\alpha \in \mathcal{O}_S$ such that $0 \leq \mathrm{ord}_\mathfrak{p}(\Delta/\alpha^r) < r$ for all $\mathfrak{p} \notin S'$.

Take any prime $p \notin S$ and let $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ be the prime ideals of $\mathcal{O}_S$ lying over p. Suppose that some $\mathfrak{p}_i$ divides Δ/α^r in $\mathcal{O}_S$. Since $0 < \mathrm{ord}_\mathfrak{p}(\Delta/\alpha^r) < r$, we deduce that the extension $k(\sqrt[r]{\Delta})/k$ is ramified at $\mathfrak{p}_i$. By Lemma 6.3, we find that $k(\sqrt[r]{\Delta})/k$ is ramified at all the primes $\mathfrak{p}_1, \dots, \mathfrak{p}_g$, and hence $p\mathcal{O}_S = \mathfrak{p}_1 \dots \mathfrak{p}_g$ divides Δ/α^r in $\mathcal{O}_S$. Dividing by p and repeating the above process, we find that there is an integer $m \geq 1$ such that $\beta := \Delta/(m\alpha^r)$ is an element of $\mathcal{O}_S^\times$. We may assume that β is in $\mathcal{B}$ after multiplying α by an appropriate element of $\mathcal{O}_S^\times$. ☐

For each $\beta \in \mathcal{O}_S^\times$, define the sets

$$W_\beta := \{(a,b) \in \mathcal{O}_k^2 : \Delta_{a,b} = m\alpha^r\beta, \text{ for some } m \in \mathbb{Z},\ \alpha \in \mathcal{O}_S\}$$

and $W_\beta(x) := W_\beta \cap B_k(x)$. For a set $\mathcal{B}$ as in Lemma 6.4, we have

$$\{(a,b) \in B_k(x) : \sqrt[r]{\Delta_{a,b}} \in k^{\rm cyc}\} \subseteq \bigcup_{\beta \in \mathcal{B}} W_\beta(x).$$

The set $\mathcal{B}$ is finite (since the abelian group $\mathcal{O}_S^\times$ is finitely generated), so

$$|\{(a,b) \in B_k(x) : \sqrt[r]{\Delta_{a,b}} \in k^{\rm cyc}\}| \ll_{k,r} \max_{\beta \in \mathcal{O}_S^\times} |W_\beta(x)|. \tag{6.1}$$

Thus to prove Proposition 6.1, it suffices to find bounds for the functions $|W_\beta(x)|$.

Lemma 6.5. *Let $p \nmid 6$ be a prime with $p \equiv 1 \bmod r$. For any $\gamma \in \mathbb{F}_p^\times$,*

$$|\{(a,b) \in \mathbb{F}_p^2 : \Delta_{a,b} = \gamma c^r, \textit{ for some } c \in \mathbb{F}_p\}| = \frac{1}{r}p^2 + O_r(p^{3/2}).$$

Proof. Fix $\gamma \in \mathbb{F}_p^\times$. The equation $\Delta_{a,b} = \gamma c^r$ defines a geometrically irreducible variety X in $\mathbb{A}^3_{\mathbb{F}_p} = \mathrm{Spec}(\mathbb{F}_p[a,b,c])$. Using the Weil conjectures, we find that

$$|X(\mathbb{F}_p)| = p^2 + O_r(p^{3/2}) \tag{6.2}$$

(that the implicit constant in (6.2) depends only on r can be deduced from [Bom78]).

For fixed $(a,b) \in \mathbb{F}_p^2$, if $\Delta_{a,b} = \gamma c^r$ has a solution $c \in \mathbb{F}_p^\times$, then it has exactly r such solutions (this uses the assumption $p \equiv 1 \bmod r$). Most solutions have $c \neq 0$, since $|\{(a,b) \in \mathbb{F}_p^2 : \Delta_{a,b} = 0\}| \ll p$. The lemma is now immediate. ☐

Lemma 6.6. *Take any $\beta \in \mathcal{O}_S^\times$. Let $p \notin S$ be a prime that splits completely in k, and let $W_{\beta,p}$ be the image of W_β in $\mathcal{O}_k^2/p\mathcal{O}_k^2$. Then*

$$|W_{\beta,p}| \leq \Big(\frac{1}{r^{d-1}} + O_{r,d}(p^{-1/2})\Big)|\mathcal{O}_k^2/p\mathcal{O}_k^2|.$$

Proof. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_d \in \Sigma_k$ be the prime ideals lying over p. By the Chinese remainder theorem, we have a natural identification $\mathcal{O}_k/p\mathcal{O}_k = \prod_{i=1}^d \mathbb{F}_{\mathfrak{p}_i}$. Then

$$W_{\beta,p} \subseteq \bigcup_{m \in R} \prod_{i=1}^d \{(a,b) \in \mathbb{F}_{\mathfrak{p}_i}^2 : \Delta_{a,b} = m\alpha^r \cdot (\beta \bmod \mathfrak{p}_i), \text{ for some } \alpha \in \mathbb{F}_{\mathfrak{p}_i}\},$$

where the union is over a set of coset representatives $R \subseteq \mathbb{F}_p^\times$ of $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^r$. We have $p \equiv 1 \bmod r$, since p splits completely in k and by assumption $\mu_r \subseteq k$. By Lemma 6.5,

$$|W_{\beta,p}| \leq |R|\big(p^2/r + O_r(p^{3/2})\big)^d = p^{2d}/r^{d-1} + O_{r,d}(p^{2d-1/2}). \qquad \square$$

Lemma 6.7. *For $\beta \in \mathcal{O}_S^\times$, $|W_\beta(x)| \ll_{k,\|\cdot\|,r} |B_k(x)|(\log x)/\sqrt{x}$.*

Proof. Let I be the set of primes $p \notin S$ that split completely in k. By Lemma 6.6, for each prime $p \in I$, we have $|W_\beta(x) \bmod p\mathcal{O}_k^2| \leq (1-\omega_p)|\mathcal{O}_k^2/p\mathcal{O}_k^2|$, where $\omega_p = 1 - 1/r^{d-1} + O_{r,d}(p^{-1/2})$. For $p \notin I$, set $\omega_p = 0$.

We may now apply the large sieve. By Theorem 4.1 (with $K = \mathbb{Q}$, $\Lambda = \mathcal{O}_k^2$, $Q = \sqrt{x}$, and our chosen norm $\|\cdot\|$ on $\mathbb{R} \otimes_{\mathbb{Z}} \Lambda$), we have $|W_\beta(x)| \ll_{k,\|\cdot\|} x^{2d}/L(\sqrt{x})$, where

$$L(\sqrt{x}) := \sum_{\substack{J \subseteq I \text{ finite} \\ \prod_{p\in J} p \leq \sqrt{x}}} \prod_{p \in J} \frac{\omega_p}{1-\omega_p}.$$

Using $r \geq 2$ and $d \geq 2$ (since $k \neq \mathbb{Q}$), we have the bound

$$L(\sqrt{x}) \geq \sum_{\substack{J \subseteq I \text{ finite} \\ \prod_{p\in J} p \leq \sqrt{x}}} \prod_{p \in J} \Big(1 + O_{r,d}(p^{-1/2})\Big) \geq \sum_{\substack{p \in I \\ p \leq \sqrt{x}}} \Big(1 + O_{r,d}(p^{-1/2})\Big).$$

The set I has positive density in the primes, so $L(\sqrt{x}) \gg_{r,k} \sqrt{x}/\log x$. The lemma follows by using this bound for $L(\sqrt{x})$ and (1.1) with our upper bound for $|W_\beta(x)|$. $\square$

Proof of Proposition 6.1. Apply Lemma 6.7 to the bound (6.1). $\square$

7. ELLIPTIC CURVES WITH MAXIMAL GALOIS ACTION

7.1. **Proof of Theorem 1.3.** Define the sets

$$\begin{aligned} Y_1(x) &= B_{k,4}(x) \cup B_{k,9}(x) \cup \bigcup\nolimits_{\ell \geq 5} B_{k,\ell}(x), \\ Y_2(x) &= \{(a,b) \in B_k(x) : \sqrt{\Delta_{a,b}} \in k^{\text{cyc}}\}, \\ Y_3(x) &= \{(a,b) \in B_k(x) : \mu_3 \subseteq k \text{ and } \sqrt[3]{\Delta_{a,b}} \in k^{\text{cyc}}\}. \end{aligned}$$

By Proposition 2.1, we have $\{(a,b) \in B_k(x) : \rho_{E(a,b)}(G_k) \neq H_k\} \subseteq Y_1(x) \cup Y_2(x) \cup Y_3(x)$, and thus

$$|\{(a,b) \in B_k(x) : \rho_{E(a,b)}(G_k) \neq H_k\}| \leq |Y_1(x)| + |Y_2(x)| + |Y_3(x)|.$$

By Proposition 5.2, we have $|Y_1(x)|/|B_k(x)| \ll_{k,\|\cdot\|} (\log x)^\beta/x^{[k:\mathbb{Q}]/2}$, where $\beta \geq 1$ is an absolute constant. By Proposition 6.1, we have

$$\frac{|Y_2(x)|}{|B_k(x)|} \ll_{k,\|\cdot\|} \frac{\log x}{\sqrt{x}} \quad \text{and} \quad \frac{|Y_3(x)|}{|B_k(x)|} \ll_{k,\|\cdot\|} \frac{\log x}{\sqrt{x}}.$$

Combining everything together gives:

$$\frac{|\{(a,b) \in B_k(x) : \rho_{E(a,b)}(G_k) \neq H_k\}|}{|B_k(x)|} \ll_{k,\|\cdot\|} \max\left\{\frac{(\log x)^\beta}{x^{[k:\mathbb{Q}]/2}}, \frac{\log x}{\sqrt{x}}\right\} \ll \frac{\log x}{\sqrt{x}},$$

where the last bound uses $k \neq \mathbb{Q}$.

7.2. **Proof of Theorem 1.6.** The theorem is easily deduced by combining the criterion of Lemma 2.4 with Proposition 5.2 and Proposition 5.6 (with $m = 72$).

APPENDIX A. GROUP THEORY FOR SL_2

In this appendix, we collect several basic facts about the groups $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$. We will need to pay special attention to the primes 2 and 3.

A.1. **Abelianizations.**

Lemma A.1. *Let m be a positive integer, and define $b := \gcd(m, 12)$. Reduction modulo b induces an isomorphism $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})^{\mathrm{ab}} \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{Z}/b\mathbb{Z})^{\mathrm{ab}}$. The group $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})^{\mathrm{ab}}$ is cyclic of order b.*

Proof. It is well-known that the group $\mathrm{PSL}_2(\mathbb{Z}) := \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$ has a presentation $\langle A, B : A^2 = 1, B^3 = 1\rangle$, thus $\mathrm{PSL}_2(\mathbb{Z})^{\mathrm{ab}}$ is a cyclic group of order 6. Under the quotient map, $\mathrm{SL}_2(\mathbb{Z})'$ surjects on to $\mathrm{PSL}_2(\mathbb{Z})'$, so $\mathrm{SL}_2(\mathbb{Z})^{\mathrm{ab}}$ has order 6 or 12.

For each positive integer m, reduction modulo m gives a surjective homomorphism $\mathrm{SL}_2(\mathbb{Z}) \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ (see [Shi94, Lemma 1.38]). We leave it to the reader to verify that the groups $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})^{\mathrm{ab}}$, $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})^{\mathrm{ab}}$ and $\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})^{\mathrm{ab}}$ are cyclic of order 2, 3 and 4 respectively. We deduce that $\mathrm{SL}_2(\mathbb{Z})^{\mathrm{ab}}$ is cyclic of order 12 and that reduction modulo 12 induces an isomorphism $\mathrm{SL}_2(\mathbb{Z})^{\mathrm{ab}} \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{Z}/12\mathbb{Z})^{\mathrm{ab}}$. The lemma is easily deduced from this isomorphism. $\square$

A.2. **Reductions.**

Lemma A.2. *Let ℓ be a prime, $n \geq 1$ an integer, and H a subgroup of $\mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$.*

(i) *If $\ell \geq 5$ and the image of H modulo ℓ is $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$, then $H = \mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$.*

(ii) *If $n \geq 2$ and the image of H modulo ℓ^2 is $\mathrm{SL}_2(\mathbb{Z}/\ell^2\mathbb{Z})$, then $H = \mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$.*

Proof. Part (i) is due to Serre, see [Ser98, IV-23 Lemma 3]. We now prove (ii). By induction, it suffices to show that for each $r \geq 2$, no *proper* subgroup of $\mathrm{SL}_2(\mathbb{Z}/\ell^{r+1}\mathbb{Z})$ reduces modulo ℓ^r to the full group $\mathrm{SL}_2(\mathbb{Z}/\ell^r\mathbb{Z})$. Let G be any subgroup of $\mathrm{SL}_2(\mathbb{Z}/\ell^{r+1}\mathbb{Z})$ such that $G \bmod \ell^r = \mathrm{SL}_2(\mathbb{Z}/\ell^r\mathbb{Z})$. It suffices to show that G contains the abelian group $\mathfrak{s} := \{A \in \mathrm{SL}_2(\mathbb{Z}/\ell^{r+1}\mathbb{Z}) : A \equiv I \bmod \ell^r\}$.

The group $\mathfrak{s}$ has a natural structure as a $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$-module; i.e., conjugate by any lift to $\mathrm{SL}_2(\mathbb{Z}/\ell^{r+1}\mathbb{Z})$. As an $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$-module, $\mathfrak{s}$ is generated by

$$I + \ell^r \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) \quad \text{and} \quad I + \ell^r \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right).$$

Since $G \bmod \ell = \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$, we find that $G \cap \mathfrak{s}$ is a $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$-submodule of $\mathfrak{s}$. Take any $B \in \{\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)\}$. We shall now show that $I + \ell^r B \in G$, which will complete the proof of (ii). By assumption, there exists a $g \in G$ such that $g \equiv I + \ell^{r-1}B \bmod \ell^r$. Taking ℓ-th powers, and using $r \geq 2$ and $B^2 = 0$, we find that $I + \ell^r B = g^\ell \in G$. $\square$

Remark A.3. Lemma A.2(i) is not true for $\ell = 2$ and 3 (see [Ser98, IV-28 Exercises 2 and 3]).

A.3. **Goursat's lemma.**

For a finite group G, let $\mathcal{J}(G)$ be the set of non-abelian simple groups, up to isomorphism, which occur in some/any composition series of G.

Lemma A.4 ((Goursat's lemma))**.** *Let $G_1, \ldots, G_n$ be finite groups, and assume that for each $i \neq j$, $\mathcal{J}(G_i) \cap \mathcal{J}(G_j) = \emptyset$ and $\gcd(|G_i^{\mathrm{ab}}|, |G_j^{\mathrm{ab}}|) = 1$. Let H be a subgroup of $G_1 \times \cdots \times G_n$ such that $\mathrm{pr}_i(H) = G_i$ for every projection $\mathrm{pr}_i \colon G_1 \times \cdots \times G_n \to G_i$. Then $H = G_1 \times \cdots \times G_n$.*

Proof. By induction, we may reduce to the case $n = 2$. Define $N_1 = \mathrm{pr}_1(H \cap (G_1 \times \{1\}))$ and $N_2 = \mathrm{pr}_2(H \cap (\{1\} \times G_2))$ which are normal subgroups of G_1 and G_2 respectively. The image of H in $G_1/N_1 \times G_2/N_2$ is the graph of an isomorphism

$$G_1/N_1 \cong G_2/N_2; \tag{A.1}$$

this fact is usually called *Goursat's lemma* (see [Rib76, Lemma 5.2.1]). We deduce that $\mathcal{J}(G_1/N_1) \subseteq \mathcal{J}(G_1) \cap \mathcal{J}(G_2) = \emptyset$, thus the group G_1/N_1 is solvable. The groups G_1 and G_2 have no common abelian quotients besides 1 (this follows from the assumption $\gcd(|G_1^{\mathrm{ab}}|, |G_2^{\mathrm{ab}}|) = 1$), so from (A.1) and the solvability, we deduce that $G_1 = N_1$ and $G_2 = N_2$. From the definition of the N_i, we find that H contains $\{1\} \times G_2$ and $G_1 \times \{1\}$, hence $H = G_1 \times G_2$. ☐

Lemma A.5 ([Lan02, XIII Theorem 8.4]). *For $\ell \geq 5$, $\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z}) := \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})/\{\pm I\}$ is a non-abelian simple group of order $(\ell^3 - \ell)/2$. The groups $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ and $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ are solvable.*

Lemma A.6. *Let m and n be relatively prime positive integers and let H be a subgroup of $\mathrm{SL}_2(\mathbb{Z}/mn\mathbb{Z})$. Then $H = \mathrm{SL}_2(\mathbb{Z}/mn\mathbb{Z})$ if and only if H surjects onto $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ and $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ by reduction modulo m and n, respectively.*

Proof. Using Lemma A.5 and the solvability of ℓ-groups, we deduce that for any positive integer d, $\mathcal{J}(\mathrm{SL}_2(\mathbb{Z}/d\mathbb{Z})) = \{\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \ell | d, \ell \geq 5\}$. Since m and n are relatively prime, we have $\mathcal{J}(\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})) \cap \mathcal{J}(\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})) = \emptyset$. By Lemma A.1,

$$\gcd(|\,\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})^{\mathrm{ab}}|, |\,\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})^{\mathrm{ab}}|) = \gcd(m, n, 12) = 1.$$

The lemma is now a direct consequence of Lemma A.4. ☐

Lemma A.7. *Let H be a closed subgroup of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$. Then $H = \mathrm{SL}_2(\widehat{\mathbb{Z}})$ if and only if $H \bmod 4 = \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$, $H \bmod 9 = \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$, and $H \bmod \ell = \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all $\ell \geq 5$.*

Proof. We have $H = \mathrm{SL}_2(\widehat{\mathbb{Z}})$ if and only if $H \bmod m = \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ holds for all positive integers m. By Lemmas A.2 and A.6, this equivalent to having $H \bmod m = \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ whenever m is 4, 9, or a prime ≥ 5. ☐

A.4. **Conjugacy classes with fixed determinant.**

Lemma A.8. *Let ℓ be a prime and H a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$. Fix an element $d \in \mathbb{F}_\ell^\times$. If $H \cap C \neq \emptyset$ for every conjugacy class C of $\mathrm{GL}_2(\mathbb{F}_\ell)$ with $\det(C) = \{d\}$, then $H \supseteq \mathrm{SL}_2(\mathbb{F}_\ell)$.*

Proof. First suppose that $d = b^2$ for some $b \in \mathbb{F}_\ell^\times$. The group H then contains an element conjugate in $\mathrm{GL}_2(\mathbb{F}_\ell)$ to $b \cdot \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. In particular, $|H| \equiv 0 \bmod \ell$. By [Ser72, Proposition 15] (which needs the condition $|H| \equiv 0 \bmod \ell$), we deduce that either H is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ or H contains $\mathrm{SL}_2(\mathbb{F}_\ell)$. If H was contained in a Borel subgroup, then the main hypothesis of the lemma would imply that every semisimple matrix in $\mathrm{GL}_2(\mathbb{F}_\ell)$ of determinant d is diagonalizable over $\mathbb{F}_\ell$; which is false. Therefore, $H \supseteq \mathrm{SL}_2(\mathbb{F}_\ell)$.

Now suppose that d is not a square in $\mathbb{F}_\ell^\times$. Without loss of generality, we may assume that H contains the scalar matrices in $\mathrm{GL}_2(\mathbb{F}_\ell)$. Since d is not a square, we have $\det(H) = \mathbb{F}_\ell^\times$.

We shall now show that $H = \mathrm{GL}_2(\mathbb{F}_\ell)$. Let H_d be the set of elements of H with determinant d. The main hypothesis of the lemma implies that

$$\{A \in \mathrm{GL}_2(\mathbb{F}_\ell) : \det(A) = d\} = \bigcup_{g \in \mathrm{GL}_2(\mathbb{F}_\ell)/H} g H_d g^{-1}. \tag{A.2}$$

By counting both sides, we find that the expression (A.2) must be a disjoint union. Therefore

$$\bigcup_{h \in H_d} \{g \in \mathrm{GL}_2(\mathbb{F}_\ell) : g h g^{-1} \in H\} \subseteq H. \tag{A.3}$$

Using (A.2) and (A.3), we find that H contains both split and non-split Cartan subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$ (see [Ser72, §2.1] for definitions). Using Propositions 17 and 14 of [Ser72], we deduce that $H = \mathrm{GL}_2(\mathbb{F}_\ell)$. ☐

Lemma A.9. *Let m be a positive integer and let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. If $H \cap C \neq \emptyset$ for every conjugacy class C of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ with determinant 1, then $H \supseteq \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$.*

Proof. By replacing H with $H \cap \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$, we may assume that H is a subgroup of $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$. By Lemma A.6, it suffices to consider the case where m is a prime power. By Lemma A.2, we may further assume that m is 4, 9, or a prime. The case where m is prime, is a consequence of Lemma A.8.

We may thus assume that $m = \ell^2$, where $\ell = 2$ or 3. There is an exact sequence

$$1 \to \mathfrak{s} \to \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) \overset{\text{mod } \ell}{\to} \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \to 1.$$

Since $\mathfrak{s}$ is abelian, it has a natural $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$-action; i.e., lift to an element of $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ and act via conjugate on $\mathfrak{s}$. By the prime case of the lemma, we find that the image of H modulo ℓ is $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Therefore $H \cap \mathfrak{s}$ is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$.

If $\ell = 3$, then $H \cap \mathfrak{s}$ contains an element conjugate in $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ to $A := \left(\begin{smallmatrix} 1 & 3 \\ 3 & 1 \end{smallmatrix}\right)$. The conjugacy classes of A in $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ and $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ are equal and have cardinality 12. Since $H \cap \mathfrak{s}$ is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$, we deduce that $H \cap \mathfrak{s}$ contains at least 12 elements. Since $|\mathfrak{s}| = 27$, we conclude that $H \cap \mathfrak{s} = \mathfrak{s}$ and hence $H = \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$.

If $\ell = 2$, then $H \cap \mathfrak{s}$ contains $B := \left(\begin{smallmatrix} 3 & 0 \\ 0 & 3 \end{smallmatrix}\right)$ which is in the center of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$. Also $H \cap \mathfrak{s}$ must contain at least one element not in $\{I, B\}$. Since $|\mathfrak{s}| = 8$, we have

$$[\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z}) : H] = [\mathfrak{s} : H \cap \mathfrak{s}] \in \{1, 2\}.$$

Suppose that $[\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z}) : H] = 2$. Then H is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$ with quotient cyclic of order 2. However, by Lemma A.1 there is only one index 2 subgroup of $\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$, and when reduced modulo 2, it does not have image $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$. Therefore $[\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z}) : H] = 1$. ☐

REFERENCES

[Ade01] Clemens Adelmann, *The decomposition of primes in torsion point fields*, Lecture Notes in Mathematics, vol. 1761, Springer-Verlag, Berlin, 2001. ↑2

[Bom78] E. Bombieri, *On exponential sums in finite fields. II*, Invent. Math. **47** (1978), no. 1, 29–39. ↑6

[CH05] Alina Carmen Cojocaru and Chris Hall, *Uniform results for Serre's theorem for elliptic curves*, Int. Math. Res. Not. **50** (2005), 3065–3080. ↑1.4

[Duk97] William Duke, *Elliptic curves with no exceptional primes*, C. R. Acad. Sci. Paris Sér. I Math. **325** (1997), no. 8, 813–818. ↑1.2, 5.4

[Gre07] Aaron Greicius, *Elliptic curves with surjective global Galois representation*, Ph.D. thesis, University of California, Berkeley, 2007. ↑1, 1.1

[Jon06a] Nathan Jones, *Almost all elliptic curves are Serre curves* (2006). arXiv:math/0611096v1 [math.NT]. ↑1.2, 1.7, 2, 3, 5.4

[Jon06b] ———, *Trace formulas and class number sums* (2006). arXiv:math/0610959v1 [math.NT]. ↑3

[Lan02] S. Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. ↑A.5

[LT76] Serge Lang and Hale Trotter, *Frobenius distributions in* GL_2*-extensions*, Springer-Verlag, Berlin, 1976. Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers; Lecture Notes in Mathematics, Vol. 504. ↑2

[MW93] D. W. Masser and G. Wüstholz, *Galois properties of division fields of elliptic curves*, Bull. London Math. Soc. **25** (1993), no. 3, 247–254. ↑5.7

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

[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, 5.3, A.4, A.4

[Ser97] ———, *Lectures on the Mordell-Weil theorem*, 3rd ed., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt; With a foreword by Brown and Serre. ↑4.1

[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. ↑A.2, A.3

[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; Kano Memorial Lectures, 1. ↑A.1

E-mail address: `zywina@math.upenn.edu`

Department of Mathematics, University of Pennsylvania, Philadelphia, PA 19104-6395, USA