ON THE SURJECTIVITY OF MOD ℓ REPRESENTATIONS ASSOCIATED TO ELLIPTIC CURVES

DAVID ZYWINA

ABSTRACT. Let E be an elliptic curve over the rationals that does not have complex multiplication. For each prime ℓ, the action of the absolute Galois group on the ℓ-torsion points of E can be given in terms of a Galois representation $\rho_{E,\ell}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\ell)$. An important theorem of Serre says that $\rho_{E,\ell}$ is surjective for all sufficiently large ℓ. In this paper, we describe a simple algorithm based on Serre's proof that can quickly determine the finite set of primes $\ell > 13$ for which $\rho_{E,\ell}$ is not surjective. We will also give some improved bounds for Serre's theorem.

1. INTRODUCTION

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

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

A renowned theorem of Serre shows that $\rho_{E,\ell}$ is surjective for all sufficiently large primes ℓ, cf. [Ser72].

Let $c(E)$ be the smallest positive integer for which $\rho_{E,\ell}$ is surjective for all primes $\ell > c(E)$. Serre has asked whether the constant $c(E)$ can be bounded independent of E [Ser72, §4.3], and moreover whether $c(E) \le 37$ always holds [Ser81, p. 399]. We pose a slightly stronger conjecture; first define the set of pairs

$$\mathscr{S} := \left\{ (17, -17^2\cdot 101^3/2),\ (17, -17\cdot 373^3/2^{17}),\ (37, -7\cdot 11^3),\ (37, -7\cdot 137^3\cdot 2083^3) \right\}.$$

Denote by j_E the j-invariant of $E/\mathbb{Q}$. When $(\ell, j_E) \in \mathscr{S}$, the curve E has an isogeny of degree ℓ and hence $\rho_{E,\ell}$ is not surjective, cf. [Zyw15] for a description of the image of $\rho_{E,\ell}$.

Conjecture 1.1. *If E is a non-CM elliptic curve over $\mathbb{Q}$ and $\ell > 13$ is a prime satisfying $(\ell, j_E) \notin \mathscr{S}$, then $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{F}_\ell)$.*

The main goal of this paper is to give a simple and practical algorithm to compute the finite set of primes ℓ for which $\rho_{E,\ell}$ is not surjective. We will focus on the case $\ell > 13$ since using [Sut16] or [Zyw15], we can easily compute the group $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$, up to conjugacy in $\mathrm{GL}_2(\mathbb{F}_\ell)$, for all the primes $\ell \le 13$.

We will also give improved upper bounds for $c(E)$.

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

Notation. For an elliptic curve $E/\mathbb{Q}$, denote its j-invariant and conductor by j_E and N_E, respectively. For each prime p for which E has good reduction, define the integer $a_p(E) = |E(\mathbb{F}_p)| - (p+1)$, where $E(\mathbb{F}_p)$ is the group of $\mathbb{F}_p$-points of a good model at p. For each good prime $p \neq \ell$, the representation $\rho_{E,\ell}$ is unramified at p and satisfies $\mathrm{tr}(\rho_{E,\ell}(\mathrm{Frob}_p)) \equiv a_p(E) \pmod{\ell}$ and $\det(\rho_{E,\ell}(\mathrm{Frob}_p)) \equiv p \pmod{\ell}$, where $\mathrm{Frob}_p \in \mathrm{Gal}_{\mathbb{Q}}$ is an (arithmetic) Frobenius at p. For primes p for which E has bad reduction, we set $a_p(E) = 0$, 1 or -1, if E has additive, split multiplicative or non-split multiplicative reduction, respectively, at p. Let $v_p \colon \mathbb{Q}_p^{\times} \twoheadrightarrow \mathbb{Z}$ be the valuation for the prime p.

1.1. **An algorithm.** Fix a non-CM elliptic curve $E/\mathbb{Q}$. We now explain how to compute a finite set S of primes such that $\rho_{E,\ell}$ is surjective for all primes $\ell \notin S$.

Let $q_1 < \cdots < q_d$ be the primes q that satisfy one of the following conditions:

- $q = 2$ and $v_q(j_E)$ is 3, 6 or 9,
- $q \geq 3$ and $v_q(j_E - 1728)$ is positive and odd.

We now consider odd primes p for which E has Kodaira symbol I_0 or I_0^*. For such a prime p, $E/\mathbb{Q}$ or its quadratic twist by p has good reduction at p; denote this curve by $E_p/\mathbb{Q}$.

Let $p_1 < p_2 < p_3 < p_4 < \ldots$ be the primes satisfying the following conditions:

- $p_i \nmid 2q_1 \cdots q_d$,
- E has Kodaira symbol I_0 or I_0^* at p_i,
- $a_i := |a_{p_i}(E_{p_i})|$ is non-zero.

Note that the set of primes p_i has density 1, cf. [Ser81, Théorème 20].

For integers $i \geq 1$ and $1 \leq j \leq d$, define the following values in $\mathbb{F}_2$:

$$\alpha_{i,j} = \begin{cases} 0 & \text{if } q_j \text{ is a square modulo } p_i, \\ 1 & \text{otherwise,} \end{cases} \quad \text{and} \quad \beta_i = \begin{cases} 0 & \text{if } -1 \text{ is a square modulo } p_i, \\ 1 & \text{otherwise.} \end{cases}$$

It is easy to compute $\alpha_{i,j}$ and β_i; with respect to the isomorphism $\mathbb{F}_2 \cong \{\pm 1\}$, they are simply Legendre symbols. For each integer $m \geq 1$, let $A_m \in M_{m,d}(\mathbb{F}_2)$ be the $m \times d$ matrix whose (i,j)-th entry is $\alpha_{i,j}$ and let $b_m \in \mathbb{F}_2^m$ be the column vector whose i-th entry is β_i.

For m large enough, the linear equation $A_m x = b_m$ has no solution. Indeed, by Dirichlet's theorem for primes in arithmetic progressions, there is an integer $i_0 \geq 1$ satisfying $\alpha_{i_0,j} = 0$ for all $1 \leq j \leq d$ and $\beta_{i_0} = 1$. So $A_m x = b_m$ has no solutions for $m \geq i_0$.

Let $r \geq 1$ be the smallest integer for which the linear equation $A_r x = b_r$ has no solution. We define S to be the set of primes ℓ such that $\ell \leq 13$, $(\ell, j_E) \in \mathscr{S}$, or $a_i \equiv 0 \pmod{\ell}$ for some $1 \leq i \leq r$. The set S is finite since $\mathscr{S}$ is finite and each a_i is non-zero. We will prove the following in §3.

Theorem 1.2. *The representation $\rho_{E,\ell}$ is surjective for all primes $\ell \notin S$.*

There are earlier results that produce an explicit finite set S that satisfies the conclusion of Theorem 1.2. For example, the bounds of Kraus and Cojocaru mentioned in §1.3 will give such sets S; however, the resulting sets S can be extremely large and testing surjectivity of $\rho_{E,\ell}$ for the finite number of $\ell \in S$ can be time consuming. Stein verified Conjecture 1.1 for curves of conductor at most 30000 using the bound of Cojocaru, cf. [Ste]; the resulting sets S would typically consist of thousands of primes (this should be contrasted with Example 1.3).

We will explain in §6 how to test the surjectivity of $\rho_{E,\ell}$ for the finitely many primes $\ell \in S$ that satisfy $\ell > 13$. We have implemented the above algorithm in `Magma` [BCP97]; code can be found at https://github.com/davidzywina/SurjectivityOfGalois

Example 1.3. We have run the above algorithm on all non-CM elliptic curves $E/\mathbb{Q}$ with conductor at most 500000; they can be found in Cremona's database [Cre]. For all such curves $E/\mathbb{Q}$, we found that $p_r \leq 71$. By the Hasse bound, we have $a_i \leq 2\sqrt{p_i} \leq 2\sqrt{71} < 17$ for $1 \leq i \leq r$. So for each $\ell > 13$ with $(\ell, j_E) \notin \mathscr{S}$, we have $a_i \not\equiv 0 \pmod{\ell}$ for all $1 \leq i \leq r$ and thus $\ell \notin S$. This verifies Conjecture 1.1 for all non-CM elliptic curves $E/\mathbb{Q}$ with conductor at most 500000. This information is now part of Cremona's database.

Remark 1.4.

(i) Replacing E by a quadratic twist does not change the primes q_j, the primes p_i or the integers a_i. In particular, the set S does not change if we replace E by a quadratic twist and hence it depends only on j_E.

In the above algorithm, one could also add the additional condition that E has good reduction at each p_i. The theorem still holds with the new resulting set S (which need not only depend on j_E anymore).

(ii) In principle, the most time consuming part of computing S is to determine the odd primes p for which $v_p(j_E - 1728)$ is positive and odd; note that the curve E has bad reduction at such primes p. However, observe that we do not need to determine all the primes of bad reduction. This complements §1.2, where we find an alternate set S when $j_E \notin \mathbb{Z}$ by only using the primes that divide the denominator of j_E.

(iii) The linear equation $A_m x = b_m$ is equivalent to having $\sum_{j=1}^{d} \alpha_{i,j} x_j = \beta_i$ for all $1 \leq i \leq m$. In the special case $d = 0$, r is the smallest positive integer for which $\beta_r \neq 0$.

1.2. **Non-integral j-invariants.** Let $E/\mathbb{Q}$ be a non-CM elliptic curve. The following, which will be proved in §4, shows that if $\rho_{E,\ell}$ is not surjective, then the denominator of j_E must be of a special form.

Theorem 1.5. *Let $p_1^{e_1} \cdots p_s^{e_s}$ be the factorization of the denominator of j_E, where the p_i are distinct primes with $e_i > 0$. If $\rho_{E,\ell}$ is not surjective for a prime $\ell > 13$ with $(\ell, j_E) \notin \mathscr{S}$, then each p_i is congruent to ± 1 modulo ℓ and each e_i is divisible by ℓ.*

Now suppose that the j-invariant of E is not an integer (the theorem is trivial otherwise). Let g be the greatest common divisor of the integers $(p_i + 1)(p_i - 1)$ and e_i with $1 \leq i \leq s$. Let S' be the set of primes ℓ such that $\ell \leq 13$, $(\ell, j_E) \in \mathscr{S}$, or $g \equiv 0 \pmod{\ell}$. The set S' is finite. The following is a direct consequence of Theorem 1.5.

Proposition 1.6. *If j_E is not an integer, then the representation $\rho_{E,\ell}$ is surjective for all primes $\ell \notin S'$.*

Example 1.7. We have verified Conjecture 1.1 for all non-CM elliptic curves $E/\mathbb{Q}$ in the Stein-Watkins database (it consist of 136,924,520 elliptic curves with conductor up to 10^8). Proposition 1.6 sufficed for all $E/\mathbb{Q}$ with $j_E \notin \mathbb{Z}$, i.e., there were no primes $\ell \in S'$ with $\ell > 13$ and $(\ell, j_E) \notin \mathscr{S}$. The integral j-invariants were handled using the algorithm from §1.1.

We now give some easy bounds for $c(E)$.

Proposition 1.8. *Suppose that j_E is not an integer.*

(i) *We have $c(E) \le \max\{17, g\}$.*
(ii) *We have $c(E) \le \max\{17, (p+1)/2\}$ for every prime p with $v_p(j_E) < 0$.*
(iii) *We have $c(E) \le \max\{17, \log d\}$, where $d \ge 1$ is the denominator of j_E.*

Proof. Take any prime $\ell > 13$ for which $\rho_{E,\ell}$ is not surjective. If $(\ell, j_E) \in \mathscr{S}$, then $\ell = 17$ since j_E is not an integer by assumption. So we may assume that $(\ell, j_E) \notin \mathscr{S}$. Proposition 1.6 implies that $\ell \le g$ since $\max S' \le \max\{17, g\}$.

Take any prime p satisfying $v_p(j_E) < 0$. We have $p \equiv \pm 1 \pmod{\ell}$ by Theorem 1.5. Since $p+1$ and $p-1$ are not primes, we must have $\ell \le (p+1)/2$. By Theorem 1.5, the denominator d of j_E is divisible by p^ℓ and is thus at least $(\ell-1)^\ell$. Hence, $\ell \le \ell \log(\ell-1) \le \log d$.

The proposition follows from the given upper bounds for ℓ. □

Remark 1.9. For any non-CM elliptic curve $E/\mathbb{Q}$, Masser and Wüstholz [MW93] have shown that $c(E) \le c(\max\{1, h(j_E)\})^\gamma$, where c and γ are absolute constants (which if computed are very large) and $h(j_E)$ is the logarithmic height of j_E. Proposition 1.8(iii) gives a simple version in the case $j_E \notin \mathbb{Z}$ since $\log d \le h(j_E)$.

1.3. **A bound.** We now discuss some bounds for $c(E)$ in terms of the conductor. Kraus [Kra95] proved that

$$c(E) \le 68 \operatorname{rad}(N_E)(1 + \log\log \operatorname{rad}(N_E))^{1/2}$$

where $\operatorname{rad}(N_E) = \prod_{p \mid N_E} p$. Using a similar approach, Cojocaru [Coj05] showed that $c(E)$ is at most $\frac{4}{3}\sqrt{6} \cdot N_E \prod_{p \mid N_E}(1+1/p)^{1/2} + 1$. We shall strengthen these bounds with the following theorem which will be proved in §5.

Theorem 1.10. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve that has no primes of multiplicative reduction. Then*

$$c(E) \le \max\left\{37,\ \frac{2\sqrt{3}}{3} N_E^{1/2} \prod_{p \mid N_E} \left(\frac{1}{2} + \frac{1}{2p}\right)^{1/2}\right\}.$$

In particular, $c(E) \le \max\left\{37, N_E^{1/2}\right\}$.

Suppose that we are in the excluded case where $E/\mathbb{Q}$ has multiplicative reduction at a prime p. Then the bound $c(E) \le \max\{17, (p+1)/2\}$ from Proposition 1.8 already gives a sizeable improvement over the bounds of Kraus and Cojocaru.

Acknowledgements. Thanks to Andrew Sutherland and Barinder Singh Banwait. Thanks also to Larry Rolen and William Stein for their corrections of an older version of this paper. Special thanks to the referee who made several suggestions that improved the exposition.

2. The character ε_ℓ

Fix a non-CM elliptic curve $E/\mathbb{Q}$ and a prime $\ell > 13$ with $(\ell, j_E) \notin \mathscr{S}$ such that the representation $\rho_{E,\ell}$ is *not* surjective.

Proposition 2.1 (Serre, Mazur, Bilu-Parent-Rebolledo)**.** *With assumptions as above, the image of $\rho_{E,\ell}$ lies in the normalizer of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$.*

Before explaining the proposition, let us recall some facts about non-split Cartan subgroups. A non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ is the image of a homomorphism $\mathbb{F}_{\ell^2}^\times \hookrightarrow \mathrm{Aut}_{\mathbb{F}_\ell}(\mathbb{F}_{\ell^2}) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$, where the first map comes from acting by multiplication and the isomorphism arises from some choice of $\mathbb{F}_\ell$-basis of $\mathbb{F}_{\ell^2}$. Let C be a non-split Cartan subgroup; it is cyclic of order ℓ^2-1 and is uniquely defined up to conjugacy in $\mathrm{GL}_2(\mathbb{F}_\ell)$. Let N be the normalizer of C in $\mathrm{Aut}_{\mathbb{F}_\ell}(\mathbb{F}_{\ell^2}) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$; it is the subgroup generated by C and the automorphism $a \mapsto a^\ell$ of $\mathbb{F}_{\ell^2}$. In particular, $[N : C] = 2$.

Fix a non-square $\epsilon \in \mathbb{F}_\ell$. After replacing C by a conjugate, one can take C to be the group consisting of matrices of the form $\left(\begin{smallmatrix} a & b\epsilon \\ b & a \end{smallmatrix}\right)$ with $(a,b) \in \mathbb{F}_\ell^2 - \{(0,0)\}$; the group N is then generated by C and the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. For all $g \in N - C$, g^2 is scalar and $\mathrm{tr}(g) = 0$.

Proof of Proposition 2.1. Suppose that $\rho_{E,\ell}$ is not surjective; its image lies in a maximal subgroup H of $\mathrm{GL}_2(\mathbb{F}_\ell)$. We have $\det(\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})) = \mathbb{F}_\ell^\times$ since the character $\det \circ \rho_{E,\ell}$ corresponds to the Galois action on the ℓ-th roots of unity. Therefore, $\det(H) = \mathbb{F}_\ell^\times$. From [Ser72, §2], we find that, up to conjugation, H is one of the following:

(a) a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$,
(b) the normalizer of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$,
(c) the normalizer of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$,
(d) for $\ell \equiv \pm 3 \pmod 8$, a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ that contains the scalar matrices and whose image in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is isomorphic to the symmetric group $\mathfrak{S}_4$.

That $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ is not contained in a Borel subgroup when $\ell > 13$ and $(\ell, j_E) \notin \mathscr{S}$ is a theorem of Mazur, cf. [Maz78]; the modular curves $X_0(17)$ and $X_0(37)$ each have two rational points which are not cusps or CM points and these points are explained by the pairs $(\ell, j_E) \in \mathscr{S}$. Bilu, Parent and Rebolledo have shown that $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ cannot be conjugate to a subgroup as in (b), cf. [BPR13]; they make effective the bounds in earlier works of Bilu and Parent using improved isogeny bounds of Gaudron and Rémond. Serre has shown that $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ cannot be conjugate to a subgroup as in (d), cf. [Ser81, §8.4]. Therefore, the only possibility for H is to be a group as in (c). □

By Proposition 2.1 and our assumption on $\rho_{E,\ell}$, the image of $\rho_{E,\ell}$ is contained in the normalizer N of a non-split Cartan subgroup C of $\mathrm{GL}_2(\mathbb{F}_\ell)$. Following Serre, we define the quadratic character

$$\varepsilon_\ell \colon \mathrm{Gal}_\mathbb{Q} \xrightarrow{\rho_{E,\ell}} N/C \xrightarrow{\sim} \{\pm 1\}.$$

For each prime p, let I_p be an inertia subgroup of $\mathrm{Gal}_\mathbb{Q}$ at p. Recall that ε_ℓ is unramified at p if and only if $\varepsilon_\ell(I_p) = \{1\}$.

We now state several basic lemmas concerning the character ε_ℓ. We first consider some primes for which E has multiplicative reduction.

Lemma 2.2. *Take any prime p for which $v_p(j_E) < 0$.*

(i) *The character ε_ℓ is unramified at p*
(ii) *We have $p \equiv \pm 1 \pmod \ell$ and $v_p(j_E) \equiv 0 \pmod \ell$.*

Proof. Define $\mathrm{Gal}_{\mathbb{Q}_p} = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, where $\overline{\mathbb{Q}}_p$ is a fixed algebraic closure of $\mathbb{Q}_p$. Choosing $\overline{\mathbb{Q}}_p$ to contain $\overline{\mathbb{Q}}$, the restriction map $\mathrm{Gal}_{\mathbb{Q}_p} \to \mathrm{Gal}_\mathbb{Q}$ is an injective homomorphism that we will view as an inclusion. There exists an element $q \in \mathbb{Q}_p$ with $v_p(q) = -v_p(j_E) > 0$ such

that

$$j_E = (1 + 240\sum\nolimits_{n\geq 1} n^3q^n/(1-q^n))^3/(q\prod\nolimits_{n\geq 1}(1-q^n)^{24}) = q^{-1} + 744 + 196884q + \cdots;$$

let $\mathcal{E}/\mathbb{Q}_p$ be the Tate curve associated to q, cf. [Sil94, V§3]. The elliptic curve $\mathcal{E}$ has j-invariant j_E and $\mathcal{E}(\overline{\mathbb{Q}}_p)$ is isomorphic to $\overline{\mathbb{Q}}_p^\times/\langle q\rangle$ as a $\mathrm{Gal}_{\mathbb{Q}_p}$-module. In particular, the ℓ-torsion subgroup $\mathcal{E}[\ell]$ is isomorphic as an $\mathbb{F}_\ell[\mathrm{Gal}_{\mathbb{Q}_p}]$-module to the subgroup of $\overline{\mathbb{Q}}_p^\times/\langle q\rangle$ generated by an ℓ-th root of unity ζ_ℓ and a fixed ℓ-th root $q^{1/\ell}$ of q. Let $\alpha\colon \mathrm{Gal}_{\mathbb{Q}_p} \to \mathbb{F}_\ell^\times$ and $\beta\colon \mathrm{Gal}_{\mathbb{Q}_p} \to \mathbb{F}_\ell$ be the maps defined so that

$$\sigma(\zeta_\ell) = \zeta_\ell^{\alpha(\sigma)} \quad \text{and} \quad \sigma(q^{1/\ell}) = \zeta_\ell^{\beta(\sigma)} q^{1/\ell}$$

for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}_p}$.

So for an appropriate choice of basis for $\mathcal{E}[\ell]$, the representation $\rho_{\mathcal{E},\ell}\colon \mathrm{Gal}_{\mathbb{Q}_p} \to \mathrm{GL}_2(\mathbb{F}_\ell)$ satisfies $\rho_{\mathcal{E},\ell}(\sigma) = \left(\begin{smallmatrix}\alpha(\sigma) & \beta(\sigma)\\ 0 & 1\end{smallmatrix}\right)$ for $\sigma \in \mathrm{Gal}_{\mathbb{Q}_p}$. The curves E and $\mathcal{E}$ are quadratic twists of each other over $\mathbb{Q}_p$ since they are non-CM curves with the same j-invariant. So there is a character $\chi\colon \mathrm{Gal}_{\mathbb{Q}_p} \to \{\pm 1\}$ such that, after an appropriate choice of basis for $E[\ell]$, we have

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

for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}_p}$.

Take any $\sigma \in \mathrm{Gal}_{\mathbb{Q}_p}$. Since C is non-split, the only matrices in C with eigenvalue 1 or -1 are $\pm I$. So if $\rho_{E,\ell}(\sigma)$ belongs to C, then $\alpha(\sigma) = 1$ and $\beta(\sigma) = 0$. If $\rho_{E,\ell}(\sigma)$ belongs to $N - C$, then $\alpha(\sigma) = -1$ since every matrix in $N - C$ has trace 0. This proves that α takes values in $\{\pm 1\}$ and that $\alpha(\sigma) \equiv \varepsilon_\ell(\sigma) \pmod{\ell}$ for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}_p}$. We have $\ell \neq p$, since otherwise $\alpha(\mathrm{Gal}_{\mathbb{Q}_p}) = \mathbb{F}_\ell^\times$ which is impossible since $\ell > 13$ and α takes values in $\{\pm 1\}$.

Since $\ell \neq p$, $\alpha = \det \circ \rho_{E,\ell}|_{\mathrm{Gal}_{\mathbb{Q}_p}}$ is unramified. Since $\alpha(\sigma) \equiv \varepsilon_\ell(\sigma) \pmod{\ell}$ for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}_p}$, we deduce that ε_ℓ is unramified at p. Therefore,

$$\varepsilon_\ell(\mathrm{Frob}_p) \equiv \alpha(\mathrm{Frob}_p) = \det \rho_{E,\ell}(\mathrm{Frob}_p) \equiv p \pmod{\ell}.$$

In particular, we must have $p \equiv \pm 1 \pmod{\ell}$ since $\varepsilon_\ell(\mathrm{Frob}_p) = \pm 1$.

It remains to prove that $e := -v_p(j_E)$ is divisible by ℓ. The matrices I and $-I$ are the only elements of N that have eigenvalue 1 or -1 with multiplicity 2. Since $\alpha(\mathrm{Gal}_{\mathbb{Q}_p(\zeta_\ell)}) = 1$, we must have $\beta(\mathrm{Gal}_{\mathbb{Q}_p(\zeta_\ell)}) = 0$ and hence $q^{1/\ell} \in \mathbb{Q}_p(\zeta_\ell)$. Extend the valuation v_p of $\mathbb{Q}_p$ to $\mathbb{Q}_p(\zeta_\ell)$. Since $\mathbb{Q}_p(\zeta_\ell)/\mathbb{Q}_p$ is an unramified extension (we saw above that $p \neq \ell$), we deduce that $v_p(q^{1/\ell})$ belongs to $\mathbb{Z}$ and hence $e = -v_p(j_E) = v_p(q) = \ell v_p(q^{1/\ell}) \in \ell\mathbb{Z}$. □

Let $q_1, \ldots, q_d$ be the primes from §1.1.

Lemma 2.3.

(i) *The character ε_ℓ is unramified at ℓ and at all primes $p \notin \{q_1, \ldots, q_d\}$.*
(ii) *If $p \in \{q_1, \ldots, q_d\} - \{\ell\}$, then $\rho_{E,\ell}(I_p)$ contains $-I$ and an element of order 4.*

Proof. Take any prime p.

• First suppose that $p = \ell$. Let I'_ℓ be the maximal pro-ℓ subgroup of I_ℓ. We have $\rho_{E,\ell}(I'_\ell) = 1$ since N has cardinality relatively prime to ℓ. The group $\rho_{E,\ell}(I_\ell)$ is cyclic since every finite quotient of the tame inertia group I_ℓ/I'_ℓ is cyclic, see [Ser72, §1.3] for the the structure of I_ℓ/I'_ℓ. Fix a generator g of $\rho_{E,\ell}(I_\ell)$. By the proof of [Ser81, p.397 Lemme 18'], the image $\rho_{E,\ell}(I_\ell)$ in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ contains an element of order at least $(\ell-1)/4 > 2$. The order of the

image of g in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is greater than 2, so g^2 is not a scalar matrix. However, g^2 is a scalar matrix for all $g \in N - C$. So g belongs to C and thus $\rho_{E,\ell}(I_\ell) \subseteq C$. Therefore, ε_ℓ is unramified at ℓ.

• Suppose that $p \neq \ell$ and that E has good reduction at p. We have $\rho_{E,\ell}(I_p) = \{I\} \subseteq C$ since $\rho_{E,\ell}$ is unramified at such primes p. Therefore, ε_ℓ is unramified at p.

• Suppose that $p \neq \ell$ and that $v_p(j_E) < 0$. By Lemma 2.2(i), ε_ℓ is unramified at p.

• Finally suppose that $p \neq \ell$ is a prime for which E bad reduction at p and $v_p(j_E) \geq 0$. Choose a minimal Weierstrass model of $E/\mathbb{Q}$ and let Δ, c_4 and c_6 be the standard invariants attached to this model as given in [Sil09, III §1].

Define the group

$$\Phi_p := \rho_{E,\ell}(I_p) \subseteq N$$

and let $\overline{\Phi}_p$ be the image of Φ_p in $N/\{\pm I\}$. We have $\Phi_p \subseteq \mathrm{SL}_2(\mathbb{F}_\ell)$ since $\det \circ \rho_{E,\ell}$ is ramified only at the prime ℓ. Using $\rho_{E,\ell}$, we can identify Φ_p with $\mathrm{Gal}(L/\mathbb{Q}_p^{\mathrm{un}})$ where L is the smallest extension of $\mathbb{Q}_p^{\mathrm{un}}$ for which E base extended to L has good reduction.

Let $\widetilde{E}/\overline{\mathbb{F}}_p$ be the elliptic curve obtained by reducing E/L. Serre observes in §5.6 of [Ser72] that Φ_p is isomorphic to a subgroup of $\mathrm{Aut}(\widetilde{E})$. We claim that $\overline{\Phi}_p$ is isomorphic to a subgroup of $\mathrm{Aut}(\widetilde{E})/\{\pm 1\}$. Reduction induces an isomorphism $\varphi\colon E[\ell] \xrightarrow{\sim} \widetilde{E}[\ell]$ between the ℓ-torsion subgroups. With respect to the isomorphism φ, the action of an element $\sigma \in \mathrm{Gal}(L/\mathbb{Q}_p^{\mathrm{un}})$ on $E[\ell]$ corresponds to the action of some automorphism of $\widetilde{E}$ on $\widetilde{E}[\ell]$, see the proof of Theorem 2 in [ST68]. Since $\mathrm{Aut}(\widetilde{E})$ acts faithfully on the ℓ-torsion of $\widetilde{E}$, using φ and the implicit isomorphism $E[\ell] \cong \mathbb{F}_\ell^2$ we may identify $\mathrm{Aut}(\widetilde{E})$ with a subgroup A of $\mathrm{GL}_2(\mathbb{F}_\ell)$ that contains Φ_p. We have $-I \in A$ since the automorphism -1 of $\widetilde{E}$ acts as -1 on the ℓ-torsion of $\widetilde{E}$. Therefore, $\overline{\Phi}_p$ is isomorphic to a subgroup of $A/\{\pm I\} \cong \mathrm{Aut}(\widetilde{E})/\{\pm 1\}$ which proves the claim.

Consider $p \geq 5$. The group $\mathrm{Aut}(\widetilde{E})$ is cyclic of order 2, 4 or 6, so Φ_p is cyclic of order 2, 3, 4 or 6. We have $j_E - 1728 = c_6^2/\Delta$, so $v_p(j_E - 1728) \equiv v_p(\Delta) \pmod 2$. From [Ser72, §5.6], we find that Φ_p has order 2, 3 or 6 if and only if $v_p(j - 1728)$ is even. So if $v_p(j - 1728)$ is even, then $\overline{\Phi}_p$ is cyclic of order 1 or 3. If $v_p(j - 1728)$ is odd, then Φ_p is cyclic of order 4.

Consider $p = 3$. The group $\mathrm{Aut}(\widetilde{E})$ is now either cyclic of order 2, 3, 4 or 6, or is a non-abelian group of order 12 (it is a semi-direct product of a cyclic group of order 4 by a distinguished subgroup of order 3). In the cases where Φ_p is cyclic of order 2, 3 or 6, the group $\overline{\Phi}_p$ is cyclic of order 1 or 3. Using that $v_p(j_E - 1728) \equiv v_p(\Delta) \pmod 2$ and Théorème 1 of [Kra90], we find that Φ_p has order 2, 3 or 6 if and only if $v_p(j - 1728)$ is even. So if $v_p(j - 1728)$ is even, then $\overline{\Phi}_p$ is cyclic of order 1 or 3. If $v_p(j - 1728)$ is odd, then Φ_p contains a cyclic group of order 4.

Consider $p = 2$. Then the group $\mathrm{Aut}(\widetilde{E})$, and hence also Φ_p, is isomorphic to a subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$. The group Φ_p is either cyclic of order 2, 3, 4 or 6, isomorphic to the order 8 group of quaternions $\{\pm 1, \pm i, \pm j, \pm k\}$, or is isomorphic to $\mathrm{SL}_2(\mathbb{F}_3)$. In particular, $|\Phi_p| \in \{2, 3, 4, 6, 8, 24\}$. In the cases where Φ_p is cyclic of order 2, 3 or 6, the group $\overline{\Phi}_p$ is cyclic of order 1 or 3. The corollary to Théorème 3 of [Kra90] shows that the values $v_2(c_4)$ and $v_2(\Delta)$ determine whether or not $|\Phi_p|$ lies in the set $\{2, 3, 6, 24\}$. We have $j_E = c_4^3/\Delta$ and hence $v_2(j_E) = 3v_2(c_4) - v_2(\Delta)$. By checking every case in the tables of the corollary to Théorème 3 of [Kra90], we find that Φ_p has order 2, 3, 6 or 24 if and only if $v_2(j_E) \notin \{3, 6, 9\}$. The group

$\mathrm{SL}_2(\mathbb{F}_3)$ is not isomorphic to a subgroup of N since $\mathrm{SL}_2(\mathbb{F}_3)$ is non-abelian and has no index 2 normal subgroups. Since $\Phi_p \subseteq N$, this proves that $|\Phi_p| \neq 24$. So if $v_2(j_E) \notin \{3, 6, 9\}$, then $\overline{\Phi}_p$ is cyclic of order 1 or 3. If $v_2(j_E) \in \{3, 6, 9\}$, then Φ_p contains a group of order 4.

Now suppose that $p \notin \{q_1, \ldots, q_d\}$. From the above computations and our choice of q_j, we find that $\overline{\Phi}_p$ has order 1 or 3. Since $-I \in C$ and $[N : C] = 2$, we deduce that Φ_p is a subgroup of C. Therefore, ε_ℓ is unramified at p. This completes the proof of (i).

Finally suppose that $p \in \{q_1, \ldots, q_d\} - \{\ell\}$. From the above computations and our choice of q_j, we find that there is an element $g \in \Phi_p$ of order 4. Since $[N : C] = 2$, g^2 lies in C and has order 2. We have $g^2 = -I$ since $-I \in C$ and C is cyclic (and hence has at most one element of order 2). This completes the proof of (ii). □

Remark 2.4. If $\ell \equiv 1 \pmod 4$, then we claim that ε_ℓ is ramified at a prime p if and only if $p \in \{q_1, \ldots, q_d\} - \{\ell\}$. One direction of the claim is immediate from Lemma 2.3(i). Now take any prime $p \in \{q_1, \ldots, q_r\} - \{\ell\}$. Suppose that ε_ℓ is unramified at p and hence $\Phi_p := \rho_{E,\ell}(I_p)$ is a subgroup of C. We have $\Phi_p \subseteq C \cap \mathrm{SL}_2(\mathbb{F}_\ell)$ since $\det \circ \rho_{E,\ell}$ is ramified only at ℓ. The group $C \cap \mathrm{SL}_2(\mathbb{F}_\ell)$ has no elements of order 4 since it is cyclic of order $\ell + 1$ and $\ell + 1 \equiv 2 \pmod 4$. This contradicts Lemma 2.3(ii), so ε_ℓ is indeed ramified at p.

Lemma 2.5. *There are unique integers $e_1, \ldots, e_d \in \{0, 1\}$ such that*

$$\varepsilon_\ell(\mathrm{Frob}_p) = \left(\frac{-1}{p}\right) \cdot \prod_{j=1}^{d} \left(\frac{q_j}{p}\right)^{e_j}$$

for all odd primes $p \nmid q_1 \cdots q_d$. In particular, $\varepsilon_\ell \neq 1$.

Proof. Since ε_ℓ is a quadratic character, there is a unique squarefree integer D satisfying $\varepsilon_\ell(\mathrm{Frob}_p) = \left(\frac{-D}{p}\right)$ for all odd primes $p \nmid D$. Let q be any prime dividing D. The character ε_ℓ is ramified at q, so $q = q_j$ for some j by Lemma 2.3. Therefore, D divides $q_1 \cdots q_d$.

It remains to show that D is positive. It suffices to show that $\varepsilon_\ell(c) = -1$, where $c \in \mathrm{Gal}_\mathbb{Q}$ corresponds to complex conjugation under a fixed embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. Set $g := \rho_{E,\ell}(c)$. We have $g^2 = I$ since c has order 2. The matrix g has determinant -1 since the character $\det \circ \rho_{E,\ell}$ corresponds to the Galois action on the ℓ-th roots of unity. The Cartan subgroup C is cyclic since it is non-split, so the only elements of C with order 1 or 2 are I and $-I$. Since $\det(\pm I) = 1$, we deduce that $g \notin C$ and hence $\varepsilon_\ell(c) = -1$ as claimed. □

Lemma 2.6. *Let p be a prime for which E has good reduction. If $a_p(E) \not\equiv 0 \pmod \ell$, then $\varepsilon_\ell(\mathrm{Frob}_p) = 1$.*

Proof. That $a_p(E) \equiv 0 \pmod \ell$ for every good prime p satisfying $\varepsilon(\mathrm{Frob}_p) = -1$ is [Ser72, p.317(c_5)]; for $p \neq \ell$, this follows by noting that $\mathrm{tr}(g) = 0$ for all $g \in N - C$. □

3. Proof of Theorem 1.2

Lemma 3.1. *Consider any quadratic twist $E'/\mathbb{Q}$ of E and any prime $\ell > 13$. Then $\rho_{E,\ell}$ is surjective if and only if $\rho_{E',\ell}$ is surjective.*

Proof. First assume that $\rho_{E,\ell}$ is surjective. The curve E' is a twist of E by a nonzero integer d. Let $\chi\colon \mathrm{Gal}_\mathbb{Q} \to \{\pm 1\}$ be the character that factors through $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \hookrightarrow \{\pm 1\}$. After making appropriate choices of a basis for $E[\ell]$ and $E'[\ell]$, we have $\rho_{E',\ell}(\sigma) = \chi(\sigma)\rho_{E,\ell}(\sigma)$ for

all $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$. Therefore, $\pm\rho_{E',\ell}(\mathrm{Gal}_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{F}_\ell)$. Taking commutator subgroups, we find that $\rho_{E',\ell}(\mathrm{Gal}_{\mathbb{Q}}) \supseteq \mathrm{SL}_2(\mathbb{F}_\ell)$. Since $\det(\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})) = \mathbb{F}_\ell^\times$, we deduce that $\rho_{E',\ell}$ is surjective. This proves one implication of the lemma and the other follows by switching the roles of E and E'. □

Lemma 3.2. *The set S does not change if we replace $E/\mathbb{Q}$ by a quadratic twist. There is a quadratic twist of E that does not have Kodaira symbol I_0^* at any odd prime.*

Proof. Let E' be a quadratic twist of E by a nonzero integer D. We may assume D is squarefree. The elliptic curve E' is also non-CM and has the same j-invariant as E. So the primes $q_1 < \cdots < q_d$ in §1.1 are the same if we replace E by E'.

Consider any odd prime p. If $p \nmid D$ and E has Kodaira symbol I_0 or I_0^* at p, then E' has the same Kodaira symbol at p. If $p|D$ and E has Kodaira symbol I_0 or I_0^* at p, then E' has Kodaira symbol I_0^* or I_0, respectively, at p. In particular, by swapping the role of E and E', we find that E has Kodaira symbol I_0 or I_0^* at p if and only if E' has Kodaira symbol I_0 or I_0^* at p. Moreover, if D is the product of the odd primes for which E has Kodaira symbol I_0^*, then E' does not have Kodaira symbol I_0^* at any odd prime.

Now suppose that for an odd prime p, E has Kodaira symbol I_0 or I_0^* at p. With notation as in §1.1, the curves E_p and E'_p both have good reduction at p and are quadratic twists of each other by a squarefree integer D_0 that is not divisible by p. Therefore, $a_p(E_p) = \pm a_p(E'_p)$. This proves that the primes $p_1 < p_2 < p_3 < p_4 < \ldots$ and integers a_i in §1.1 are the same if we replace E by E'. Examining the algorithm of §1.1, we find that the set S is unchanged if replace E by E'. □

By Lemmas 3.1 and 3.2, we may replace E by a quadratic twist so that it never has Kodaira symbol I_0^* at any odd prime. In particular, for each p_i, we have $a_i = |a_{p_i}(E)|$.

Suppose that there is a prime $\ell \notin S$ for which $\rho_{E,\ell}$ is not surjective. From our choice of ℓ, Proposition 2.1 implies that the image of $\rho_{E,\ell}$ is contained in the normalizer of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$. Let $\varepsilon_\ell\colon \mathrm{Gal}_{\mathbb{Q}} \to \{\pm 1\}$ be the corresponding quadratic character. By Lemma 2.5, there are unique $e_1, \ldots, e_d \in \{0, 1\}$ such that $\varepsilon_\ell(\mathrm{Frob}_p) = \left(\frac{-1}{p}\right) \cdot \prod_{j=1}^d \left(\frac{q_j}{p}\right)^{e_j}$ for all primes $p \nmid 2q_1 \cdots q_d$.

Now consider $p = p_i$ with $1 \le i \le r$. We have $|a_{p_i}(E)| = a_i \not\equiv 0 \pmod{\ell}$ since $\ell \notin S$. Lemma 2.6 implies that $\varepsilon_\ell(\mathrm{Frob}_{p_i}) = 1$ for all $1 \le i \le r$. Therefore,

$$\prod_{j=1}^{d} \left(\frac{q_j}{p_i}\right)^{e_j} = \left(\frac{-1}{p_i}\right)$$

for all $1 \le i \le r$. Using the isomorphism $\{\pm 1\} \cong \mathbb{F}_2$, this is equivalent to having $\sum_{j=1}^d \alpha_{i,j} e_j = \beta_i$ for all $1 \le i \le r$. This shows that the equation $A_r x = b_r$ has a solution in $\mathbb{F}_2^d$. However, this contradicts our choice of r. Therefore, the representation $\rho_{E,\ell}$ must be surjective for all $\ell \notin S$.

4. Proof of Theorem 1.5

Take any prime $\ell > 13$ with $(\ell, j_E) \notin \mathscr{S}$ such that $\rho_{E,\ell}$ is *not* surjective. Take any prime p for which $v_p(j_E) < 0$ and set $e := -v_p(j_E)$. By Lemma 2.2, we have $p \equiv \pm 1 \pmod{\ell}$ and $e \equiv 0 \pmod{\ell}$. The theorem is now immediate.

5. Proof of Theorem 1.10

Suppose that $\rho_{E,\ell}$ is not surjective for a prime $\ell > 13$ with $(\ell, j_E) \notin \mathscr{S}$. We can then define a quadratic character $\varepsilon_\ell\colon \mathrm{Gal}_{\mathbb{Q}} \to \{\pm 1\}$ as in §2. Let $E'/\mathbb{Q}$ be the elliptic curve obtained by twisting $E/\mathbb{Q}$ by ε_ℓ.

Lemma 5.1. *The elliptic curves E and E' have the same conductors.*

Proof. Take any prime p. Lemma 1 of [Kra95] says that E and E' have the same reduction type (i.e., good, additive or multiplicative) at p. This proves that $\mathrm{ord}_p(N_E) = \mathrm{ord}_p(N_{E'})$ for $p \geq 5$. To prove this equality for $p = 2$ and 3, we need to check that the wild part of the conductors of E and E' at p agree; for a description of the wild part of the conductor at p, see [Sil94, IV§10].

For our prime $p \leq 3$, it suffices to show that the groups $\rho_{E,\ell}(I_p)$ and $\rho_{E',\ell}(I_p)$ are conjugate in $\mathrm{GL}_2(\mathbb{F}_\ell)$. After choosing appropriate bases of $E[\ell]$ and $E'[\ell]$, we may assume that $\rho_{E',\ell} = \varepsilon_\ell \cdot \rho_{E,\ell}$. If ε_ℓ is unramified at p, then $\rho_{E',\ell}(I_p) = \rho_{E,\ell}(I_p)$.

So we may assume that ε_ℓ is ramified at p. We clearly have $\pm\rho_{E',\ell}(I_p) = \pm\rho_{E,\ell}(I_p)$, so it suffices to show that $\rho_{E',\ell}(I_p)$ and $\rho_{E,\ell}(I_p)$ both contain $-I$. Since ε_ℓ is ramified at p, Lemma 2.3 implies that $\rho_{E,\ell}(I_p)$ contains $-I$.

We have $\rho_{E',\ell}(\mathrm{Gal}_{\mathbb{Q}}) \subseteq \pm\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}}) \subseteq N$ and in particular $\rho_{E',\ell}$ is not surjective. The character

$$\mathrm{Gal}_{\mathbb{Q}} \xrightarrow{\rho_{E',\ell}} N \to N/C \xrightarrow{\sim} \{\pm 1\}$$

agrees with ε_ℓ since $\rho_{E',\ell} = \varepsilon_\ell \cdot \rho_{E,\ell}$ and $-I \in C$. Note that E is the quadratic twist of E' by ε_ℓ. So by switching the roles of E and E', we find that $\rho_{E',\ell}(I_p)$ contains $-I$. □

By Lemma 5.1, the elliptic curves E and E' have the same conductor; denote it by N. By the modularity theorem (proved by Wiles, Taylor, Breuil, Conrad and Diamond), there are newforms f and $g \in S_2(\Gamma_0(N))$ corresponding to E and E', respectively. Let $a_n(f)$ and $a_n(g)$ be the n-th Fourier coefficient of f and g at the cusp $i\infty$. The following lemma gives a Sturm bound for a prime q that satisfies $a_q(f) \neq a_q(g)$. Note that f and g are distinct since $\varepsilon_\ell \neq 1$ (by Lemma 2.5) and since E and E' are non-CM.

Lemma 5.2. *Let f and g be distinct normalized newforms in $S_2(\Gamma_0(N))$. Then there exists a prime q such that*

$$q \leq \frac{N}{3} \prod_{p \mid N} \left(\frac{1}{2} + \frac{1}{2p}\right) - 1 \tag{5.1}$$

and $a_q(f) \neq a_q(g)$.

Proof. Consider the modular curve $X_0(N)$ defined over $\mathbb{C}$. Its complex points form a Riemann surface obtained by quotienting the complex upper-half plane by $\Gamma_0(N)$ and then compactifying by adding cusps. For each prime power $q = p^e$ such that $p^e \parallel N$, let W_q be a matrix of the form $\left(\begin{smallmatrix} qa & b \\ Nc & qd \end{smallmatrix}\right)$ with $a, b, c, d \in \mathbb{Z}$ that has determinant q. The matrix W_q normalizes $\Gamma_0(N)$ and thus induces an automorphism of $X_0(N)$. Let $W(N)$ be the subgroup of $\mathrm{Aut}(X_0(N))$ generated by the $\{W_{p^e}\}_{p^e \parallel N}$. The group $W(N)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^r$ where r is the number of distinct prime factors of N [AL70, Lemma 9]. The group $W(N)$ permutes the cusps of $X_0(N)$ and the stabilizer of the cusp $i\infty$ is trivial.

For the newform f, consider the holomorphic differential form $\eta = f(z)dz$ on $X_0(N)$. For each automorphism $w \in W(N)$, there is a $\lambda_w(f) \in \{\pm 1\}$ such that $\eta(wz) = \lambda_w(f)\eta(z)$, cf. [AL70, Theorem 3]. Similarly, we have values $\lambda_w(g) \in \{\pm 1\}$ for $w \in W(N)$.

Let H be the set of $w \in W(N)$ for which $\lambda_w(f) = \lambda_w(g)$; it is a subgroup of $W(N)$ of cardinality 2^r or 2^{r-1}. The holomorphic differential form $\omega := (f(z) - g(z))dz$ is non-zero since f and g are distinct. Let $K = \operatorname{div}(\omega)$ be the corresponding (effective) divisor on $X_0(N)$; it has degree $2g_{X_0(N)} - 2$ where $g_{X_0(N)}$ is the genus of $X_0(N)$. Therefore,

$$\sum\nolimits_P \operatorname{ord}_P(\omega) \leq 2g_{X_0(N)} - 2$$

where the sum is over the cusps of $X_0(N)$. For a fixed automorphism $w \in H$, we have a cusp $P = w{\cdot}i\infty$. From our choice of H, we find that $\omega(wz) = \pm\omega(z)$ and thus $\operatorname{ord}_P(\omega) = \operatorname{ord}_{i\infty}(\omega)$. Therefore,

$$2^{r-1} \operatorname{ord}_{i\infty}(\omega) \leq |H| \operatorname{ord}_{i\infty}(\omega) \leq 2g_{X_0(N)} - 2 \leq \frac{N}{6} \prod_{p|N} (1 + 1/p) - 2^r$$

where the last inequality uses an explicit formula for $g_{X_0(N)}$ [Shi94, Prop. 1.40] and that $X_0(N)$ has at least 2^r cusps. Let n be the smallest positive integer for which the Fourier coefficients $a_n(f)$ and $a_n(g)$ disagree. We have $\operatorname{ord}_{i\infty}(\omega) = n - 1$, and hence

$$n \leq \frac{1}{2^r} \frac{N}{3} \prod_{p|N} (1 + 1/p) - 1.$$

If n is prime, then we are done. If n is composite with $a_n(f) \neq a_n(g)$, then $a_q(f) \neq a_q(g)$ for some prime q dividing n (since f and g are normalized eigenforms, we know that their Fourier coefficients are multiplicative and are defined recursively for prime powers indices). □

Remark 5.3. If f and g are distinct modular forms on $\Gamma_0(N)$ of weight 2, then the same proof, but only looking at the cusp $i\infty$, shows that there is an integer $n \leq \frac{N}{6} \prod_{p|N} (1 + \frac{1}{p})$ such that $a_n(f) \neq a_n(g)$. This is the bound used in [Coj05] and [Kra95]; though possibly working with a larger N.

By Lemma 5.2, there is a prime q satisfying (5.1) such that $a_q(E) = a_q(f) \neq a_q(g) = a_q(E')$. Since $a_p(E) = a_p(E') = 0$ for primes of additive reduction, we find that E has either good or multiplicative reduction at q. By assumption, E has no primes of multiplicative reduction, so E has good reduction at q.

Since $a_q(E) \neq a_q(E') = \varepsilon_\ell(\mathrm{Frob}_q) a_q(E)$, we deduce that $\varepsilon_\ell(\mathrm{Frob}_q) = -1$ and $a_q(E) \neq 0$. By Lemma 2.6, we find that $a_q(E) \equiv 0 \pmod{\ell}$. The Hasse bound then implies that

$$\ell \leq |a_q(E)| \leq 2\sqrt{q} \leq 2\sqrt{\frac{N}{3} \prod_{p|N} \left(\frac{1}{2} + \frac{1}{2p}\right)} = \frac{2\sqrt{3}}{3} N^{1/2} \prod_{p|N} \left(\frac{1}{2} + \frac{1}{2p}\right)^{1/2}.$$

Since N is divisible by some prime (there is no elliptic curve over $\mathbb{Q}$ with good reduction everywhere), we have $\ell \leq \frac{2\sqrt{3}}{3} N^{1/2} (\frac{1}{2} + \frac{1}{4})^{1/2} = N^{1/2}$.

6. Remaining primes

Fix a non-CM elliptic curve $E/\mathbb{Q}$ and a prime $\ell > 13$. In this section, we explain how to determine whether $\rho_{E,\ell}$ is surjective. Combined with Theorem 1.2 (or possibly Proposition 1.6), this gives a method to compute the (finite) set of primes $\ell > 13$ for which $\rho_{E,\ell}$ is not surjective.

Proposition 6.1. *The representation $\rho_{E,\ell}$ is surjective if and only if $(\ell, j_E) \notin \mathscr{S}$ and there is a prime $p \nmid N_E\ell$ such that $a_p(E) \not\equiv 0 \pmod{\ell}$ and $a_p(E)^2 - 4p$ is a non-zero square modulo ℓ.*

Proof. As noted in the introduction, the representation $\rho_{E,\ell}$ is not surjective when $(\ell, j_E) \in \mathscr{S}$. So assume that $(\ell, j_E) \notin \mathscr{S}$. First suppose that there is a prime $p \nmid N_E\ell$ such that $a_p(E) \not\equiv 0 \pmod{\ell}$ and $a_p(E)^2 - 4p$ is a non-zero square modulo ℓ. With $g := \rho_{E,\ell}(\mathrm{Frob}_p)$, we have $\mathrm{tr}(g) \neq 0$ and $\mathrm{tr}(g)^2 - 4\det(g)$ is a non-zero square. Let N be the normalizer of a non-split Cartan subgroup C of $\mathrm{GL}_2(\mathbb{F}_\ell)$. For all $A \in N - C$, we have $\mathrm{tr}(A) = 0$. For all $A \in C$, the value $\mathrm{tr}(A)^2 - 4\det(A) \in \mathbb{F}_\ell$ is either zero or a non-square. So $g \notin N$, and hence $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ is not a subgroup of the normalizer of a non-split Cartan. Therefore, $\rho_{E,\ell}$ is surjective by Proposition 2.1.

Now suppose that $\rho_{E,\ell}$ is surjective. Let X be the set of matrices $A \in \mathrm{GL}_2(\mathbb{F}_\ell)$ for which $\mathrm{tr}(A) \neq 0$ and $\mathrm{tr}(A)^2 - 4\det(A)$ is a non-zero square. The set X is nonempty since any matrix $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ with $a + b \neq 0$ and $a \neq b$ lies in X. The set X is stable under conjugation by $\mathrm{GL}_2(\mathbb{F}_\ell)$. Since $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q}) = \mathrm{GL}_2(\mathbb{F}_\ell)$, the set of primes $p \nmid N_E\ell$ for which $\rho_{E,\ell}(\mathrm{Frob}_p) \subseteq X$ has density $|X|/|\mathrm{GL}_2(\mathbb{F}_\ell)| > 0$ by the Chebotarev density theorem. Finally observe that for a prime $p \nmid N_E\ell$ with $\rho_{E,\ell}(\mathrm{Frob}_p) \subseteq X$, we have that $a_p(E)^2 - 4p \equiv \mathrm{tr}(\rho_{E,\ell}(\mathrm{Frob}_p))^2 - 4\det(\rho_{E,\ell}(\mathrm{Frob}_p))$ is a non-zero square mod ℓ and $a_p(E) \equiv \mathrm{tr}(\rho_{E,\ell}(\mathrm{Frob}_p)) \not\equiv 0 \pmod{\ell}$. □

Assuming that Conjecture 1.1 holds, the criterion of Proposition 6.1 will always apply for some p and prove that $\rho_{E,\ell}$ is surjective when $(\ell, j_E) \notin \mathscr{S}$. In practice, one can quickly find a prime p that works. Indeed if $\rho_{E,\ell}$ is surjective, the Chebotarev density theorem shows that the set of primes $p \nmid N_E\ell$ such that $a_p(E) \not\equiv 0 \pmod{\ell}$ and $a_p(E)^2 - 4p$ is a non-zero square modulo ℓ will have density $1/2 + O(1/\ell)$, where the implicit constant depends only on E.

In the unlikely case that $(\ell, j_E) \notin \mathscr{S}$ and the surjectivity is unknown after computing $a_p(E)$ for many primes $p \nmid N_E\ell$, then one can simply do a direct computation. The representation $\rho_{E,\ell}$ is surjective if and only if the image of $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ in $\mathrm{GL}_2(\mathbb{F}_\ell)/\{\pm I\}$ is the full group $\mathrm{GL}_2(\mathbb{F}_\ell)/\{\pm I\}$. For a given Weierstrass equation $y^2 = x^3 + ax + b$ for $E/\mathbb{Q}$ one can compute the division polynomial of E at the prime ℓ; it is the monic polynomial $f(X) \in \mathbb{Q}[X]$ whose roots are the x-coordinates of the elements of order ℓ in $E(\overline{\mathbb{Q}})$. The Galois group of $f(x)$ is isomorphic to the image of $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ in $\mathrm{GL}_2(\mathbb{F}_\ell)/\{\pm I\}$ and can be computed directly.

References

[AL70] A. O. L. Atkin and J. Lehner, *Hecke operators on $\Gamma_0(m)$*, Math. Ann. **185** (1970), 134–160. ↑5

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Computational algebra and number theory (London, 1993). ↑1.1

[BPR13] Yuri Bilu, Pierre Parent, and Marusia Rebolledo, *Rational points on $X_0^+(p^r)$*, Ann. Inst. Fourier (Grenoble) **63** (2013), no. 3, 957–984. ↑2

[Coj05] Alina Carmen Cojocaru, *On the surjectivity of the Galois representations associated to non-CM elliptic curves*, Canad. Math. Bull. **48** (2005), no. 1, 16–31. With an appendix by Ernst Kani. ↑1.3, 5.3

[Cre] J. E. Cremona, *Elliptic Curve Data* (webpage). http://johncremona.github.io/ecdata/. ↑1.3

[Kra90] Alain Kraus, *Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive*, Manuscripta Math. **69** (1990), no. 4, 353–385. ↑2

[Kra95] ———, *Une remarque sur les points de torsion des courbes elliptiques*, C. R. Acad. Sci. Paris Sér. I Math. **321** (1995), no. 9, 1143–1146. ↑1.3, 5, 5.3

[Maz78] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162. ↑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. ↑1.9

[Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331. ↑1, 2, 2, 2

[Ser81] ———, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. **54** (1981), 323–401. ↑1, 1.1, 2, 2

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

[Shi94] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1. ↑5

[Sil94] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. ↑2, 5

[Sil09] ———, *The arithmetic of elliptic curves*, Second, Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. ↑2

[Ste] W. A. Stein, *Images of Galois* (webpage). https://wstein.org/Tables/surj/. ↑1.1

[Sut16] Andrew V. Sutherland, *Computing images of Galois representations attached to elliptic curves*, Forum Math. Sigma **4** (2016), Paper No. e4, 79. ↑1

[Zyw15] David Zywina, *On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$* (2015). arXiv:1508.07660 [math.NT]. ↑1, 1

Department of Mathematics, Cornell University, Ithaca, NY 14853, USA
Email address: zywina@math.cornell.edu
URL: https://pi.math.cornell.edu/~zywina/