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 $\rho_{E,\ell}\colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_2(\mathbb{F}_\ell)$. An important theorem of Serre says that $\rho_{E,\ell}$ is surjective for all sufficiently large ℓ. In this paper, we describe an algorithm based on Serre's proof that can quickly determine the finite set of primes ℓ 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 a free $\mathbb{F}_\ell$-vector space of dimension 2 and there is a natural action of the absolute Galois group $\operatorname{Gal}_\mathbb{Q} := \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 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

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

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 integer $n \geq 1$ for which $\rho_{E,\ell}$ is surjective for all primes $\ell > n$. Serre has asked whether the constant $c(E)$ can be bounded independent of E [Ser72, §4.3], and moreover whether $c(E) \leq 37$ always holds [Ser81, p. 399]. We pose a slightly stronger conjecture; first define the set of pairs

$$S_0 := \big\{ (17, -17^2\cdot 101^3/2), (17, -17\cdot 373^3/2^{17}), (37, -7\cdot 11^3), (37, -7\cdot 137^3\cdot 2083^3) \big\}.$$

Denote by j_E the j-invariant of $E/\mathbb{Q}$. When $(\ell, j_E) \in S_0$, 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 $(\ell, j_E) \notin S_0$, then $\rho_{E,\ell}(\operatorname{Gal}_\mathbb{Q}) = \operatorname{GL}_2(\mathbb{F}_\ell)$.*

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 $\ell > 11$ since using [Zyw15], we can easily compute the group $\rho_{E,\ell}(\operatorname{Gal}_\mathbb{Q})$, up to conjugacy in $\operatorname{GL}_2(\mathbb{F}_\ell)$, for all the primes $\ell \leq 11$.

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

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 $\mathbb{F}_p$-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 $\operatorname{tr}(\rho_{E,\ell}(\operatorname{Frob}_p)) \equiv a_p(E) \pmod{\ell}$ and $\det(\rho_{E,\ell}(\operatorname{Frob}_p)) \equiv p \pmod{\ell}$, where $\operatorname{Frob}_p \in \operatorname{Gal}_\mathbb{Q}$ 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.

2010 *Mathematics Subject Classification.* Primary 11G05; Secondary 11F80.

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 p that satisfy one of the following conditions:

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

Take any odd prime p for which E has Kodaira symbol I_0 or I_0^*. Equivalently, $E/\mathbb{Q}$ 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 odd primes such that E has Kodaira symbol I_0 or I_0^* and such that the integer $a_i := |a_{p_i}(E_{p_i})|$ is non-zero. Note that the set of such primes p_i has density 1, cf. [Ser81, Théorèm 20].

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

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

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.

Let $r \geq 1$ be the smallest integer for which the linear equation $A_r x = b_r$ has no solution. By Dirichlet's theorem for primes in arithmetic progressions, there is an integer $i_0 \geq 1$ such that $\alpha_{i_0,j} = 0$ for all $1 \leq j \leq d$ and $\beta_{i_0} = 1$. So $r \leq i_0$ and in particular r is well-defined.

Let S be the set of primes ℓ such that $\ell \leq 13$, $(\ell, j_E) \in S_0$, or $a_i \equiv 0 \pmod{\ell}$ for some $1 \leq i \leq r$; it is finite since S_0 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 $\ell \notin S$.*

We will explain in §6 how to test the surjectivity of $\rho_{E,\ell}$ for the finitely many primes $\ell \in S$.

Example 1.3. We have used Theorem 1.2 to verify Conjecture 1.1 for all elliptic curves $E/\mathbb{Q}$ with conductor at most 350000 (`Magma` code is given in Appendix A). In fact, for all such curves $E/\mathbb{Q}$ our computations show that $p_r \leq 71$. By the Hasse bound, we have $a_i \leq 2\sqrt{p_i} \leq 2\sqrt{71} < 17$ for $1 \leq i \leq r$. Therefore, the set $S - \{2,3,5,7,11,13\}$ is either empty or is $\{\ell\}$ when $(\ell, j_E) \in S_0$. In particular, we did not need to directly check the surjectivity of $\rho_{E,\ell}$ for any exceptional primes $\ell > 13$.

There are of course 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).

Remark 1.4.

(i) The set S does not change if we replace E by a quadratic twist and hence it depends only on j_E.
(ii) In practice, 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. (Contrast this with §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.)

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. *The denominator of j_E is of the form $p_1^{e_1}\cdots p_s^{e_s}$ with distinct primes p_i and $e_i > 0$. If $\rho_{E,\ell}$ is not surjective for a prime $\ell > 13$ with $(\ell, j_E) \notin S_0$, 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 $p_i^2 - 1$ and e_i with $1 \le i \le s$. Let S be the set of primes ℓ such that $\ell \le 13$, $(\ell, j_E) \in S_0$, 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 1.8 sufficed for all $E/\mathbb{Q}$ with $j_E \notin \mathbb{Z}$ (i.e., there were no primes $\ell \in S$ that needed to be checked individually). The integral j-invariants that needed to be considered were handled with 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. Note that if $(\ell, j_E) \in S_0$, then $\ell = 17$. The first bound is immediate from Proposition 1.6 since $\max S \le \max\{17, g\}$. Suppose that p is a prime satisfying $v_p(j_E) < 0$ and $\rho_{E,\ell}$ is not surjective for a prime $\ell > 17$. By Theorem 1.5, we have $p \equiv \pm 1 \pmod{\ell}$. Since $p+1$ and $p-1$ are not primes, we must have $\ell \le (p+1)/2$. By Theorem 1.5, the denominator d is divisible by p^ℓ and is thus at least $(\ell-1)^\ell$. Hence, $\ell \le \ell \log(\ell - 1) \le \log d$. □

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

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

where $\mathrm{rad}(N_E) = \prod_{p | N_E} p$. Using a similar approach, Cojocaru [Coj05] showed that $c(E)$ is at most $\frac{4}{3}\sqrt{6} \cdot N_E \prod_{p|N_E}(1 + 1/p)^{1/2} + 1$. 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*

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

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

Suppose that we are in the excluded case where $E/\mathbb{Q}$ has multiplicative reduction at a prime p. Then the bound $c(E) \le \max\{37, (p+1)/2\}$ 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. Computations were done in `Magma` [BCP97].

2. The character ε_ℓ

Fix a non-CM elliptic curve $E/\mathbb{Q}$ and a prime $\ell > 13$ with $(\ell, j_E) \notin S_0$ 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 $\ell^2 - 1$ 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 $(\ell, j_E) \notin S_0$ is a famous 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 $(\ell, j_E) \in S_0$. 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. Let $q_1, \ldots, q_d$ be the primes from §1.1.

Lemma 2.2.

(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 $v_p(j_E) < 0$. Using a Tate curve, we shall show in §4 that ε_ℓ is unramified at p (and moreover that $\varepsilon_\ell(\mathrm{Frob}_p) \equiv p \pmod{\ell}$); the proof will use the definition of ε_ℓ but none of the successive lemmas in this section.

• 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].

Let Φ_p be the image of I_p under $\rho_{E,\ell}$. 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. Moreover, one knows that Φ_p is isomorphic to a subgroup of $\mathrm{Aut}(\widetilde{E})$ where $\widetilde{E}/\overline{\mathbb{F}}_p$ is the reduction of E/L, cf. [Ser72, §5.6]. We have $\Phi_p \subseteq \mathrm{SL}_2(\mathbb{F}_\ell)$ since $\det\circ\rho_{E,\ell}$ is ramified only at the prime ℓ. In particular, if there is an element in Φ_p with order 2, then it is $-I$.

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.

Consider $p = 3$. The group $\mathrm{Aut}(\widetilde{E})$ is now either cyclic of order 2, 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). 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.

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 $\mathrm{SL}_2(\mathbb{F}_3)$. We have $j_E = c_4^3/\Delta$ and hence $v_2(j_E) = 3v_2(c_4) - v_2(\Delta)$. Checking all the cases in the corollary to Théorème 3 of [Kra90], we find 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 $|\Phi_p| \neq 24$.

Now suppose that $p \notin \{q_1, \ldots, q_d\}$. From the above computations and our choice of q_j, we find that Φ_p has order 2, 3 or 6. If Φ_p has order 2 or 6, then $-I \in \Phi_p$. 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 $p \in \{q_1, \ldots, q_d\}$ (and $p \neq \ell$). Then Φ_p is cyclic of order 4, or has order 12 ($p = 3$), or has order 8 ($p = 2$). In all these cases, Φ_p contains an element g of order 4. The element g^2 of order 2 in C must be $-I$. This completes the proof of (ii). □

Remark 2.3. 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 2.2(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 2.2(ii), so ε_ℓ is indeed ramified at p.

Lemma 2.4. *There are unique integers $e_1,\dots,e_d \in \{0,1\}$ 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. There is a unique squarefree integer D such that $\varepsilon_\ell(\mathrm{Frob}_p) = \left(\frac{-D}{p}\right)$ 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 2.2. 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 2.5. *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

Replacing $E/\mathbb{Q}$ by a quadratic twist does not change the set S or the set of primes ℓ for which $\rho_{E,\ell}$ is not surjective. We may thus assume that E has no odd primes p with Kodaira type I_0^*. So for each p_i, we have $a_i = |a_{p_i}(E)|$.

Suppose that $\ell\notin S$ is a prime 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 2.4, there are unique $e_1,\dots,e_d\in\{0,1\}$ 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 2.5 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 $\{\pm1\}\cong\mathbb{F}_2$, 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 $\mathbb{F}_2^d$. This is a contradiction since the equation $A_r x = b_r$ has no solution by 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 p that divides the denominator of j_E. Everything that follows is a local argument, so by base extending we shall view E as an elliptic curve over $\mathbb{Q}_p$; we have a Galois representation $\rho_{E,\ell}\colon \mathrm{Gal}_{\mathbb{Q}_p}\to \mathrm{GL}_2(\mathbb{F}_\ell)$. There exists an element $q\in\mathbb{Q}_p$ with $v_p(q) = -v_p(j_E) > 0$ such that

$$j_E = (1+240\sum\nolimits_{n\ge1} n^3q^n/(1-q^n))^3/(q\prod\nolimits_{n\ge1}(1-q^n)^{24}) = q^{-1}+744+196884q+\cdots;$$

let $\mathscr{E}/\mathbb{Q}_p$ be the Tate curve associated to q, cf. [Sil94, V§3]. It is an elliptic curve with j-invariant j_E and the group $\mathscr{E}(\overline{\mathbb{Q}}_p)$ 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 $\mathscr{E}[\ell]$ 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 chosen 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 $\mathscr{E}[\ell]$, we have $\rho_{\mathscr{E},\ell}(\sigma) = \left(\begin{smallmatrix} \alpha(\sigma) & \beta(\sigma) \\ 0 & 1 \end{smallmatrix}\right)$ for $\sigma \in \mathrm{Gal}_{\mathbb{Q}_p}$. The curves E and $\mathscr{E}$ 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 $\sigma \in \mathrm{Gal}_{\mathbb{Q}_p}$.

Now assume that $\rho_{E,\ell}$ is not surjective for a prime $\ell > 13$ with $(\ell, j_E) \notin S_0$. By Proposition 2.1, the image of $\rho_{E,\ell}$ is contained in the normalizer N of a non-split Cartan subgroup C of $\mathrm{GL}_2(\mathbb{F}_\ell)$. Let $\varepsilon_\ell\colon \mathrm{Gal}_{\mathbb{Q}} \to \{\pm 1\}$ be the corresponding quadratic character.

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 $\sigma \in \mathrm{Gal}_{\mathbb{Q}_p}$. If $\ell = p$, then $\alpha(\mathrm{Gal}_{\mathbb{Q}_p}) = \mathbb{F}_\ell^\times$ which is impossible since $\ell > 13$ and α takes values in $\{\pm 1\}$. So $\ell \neq p$ and hence $\alpha(\mathrm{Frob}_p) \equiv p \pmod{\ell}$. Therefore, ε_ℓ is unramified at p and $\varepsilon_\ell(\mathrm{Frob}_p) \equiv \alpha(\mathrm{Frob}_p) \equiv p \pmod{\ell}$. In particular, we must have $p \equiv \pm 1 \pmod{\ell}$.

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 $e = -v_p(j_E) = v_p(q) = \ell v_p(q^{1/\ell}) \in \ell\mathbb{Z}$.

5. Proof of Theorem 1.10

Suppose that $\rho_{E,\ell}$ is not surjective for a prime $\ell > 13$ with $(\ell, j_E) \notin S_0$. 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 $\rho_{E',\ell}(I_p) = \rho_{E,\ell}(I_p)$. We always have $\pm\rho_{E',\ell}(I_p) = \pm\rho_{E,\ell}(I_p)$. So if ε_ℓ is ramified at p, then Lemma 2.2(ii) implies that $\rho_{E',\ell}(I_p) = \pm\rho_{E',\ell}(I_p) = \pm\rho_{E,\ell}(I_p) = \rho_{E,\ell}(I_p)$. ☐

By Lemma 5.1, the elliptic curves E and E' 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 $\varepsilon \neq 1$ (by Lemma 2.4) 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*

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

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 $\{W_{p^e}\}_{p^e \| N}$. 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 $K = \mathrm{div}(\omega)$ 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,

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

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 $\mathrm{ord}_P(\omega) = \mathrm{ord}_{i\infty}(\omega)$. Therefore,

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

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 $\mathrm{ord}_{i\infty}(\omega) = n - 1$, and hence

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

If n is prime, then we are done. If n is composite with $a_n(f) \ne a_n(g)$, then $a_q(f) \ne a_q(g)$ 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 $n \le \frac{N}{6}\prod_{p|N}(1+\frac{1}{p})$ such that $a_n(f) \ne a_n(g)$. 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 $a_q(E) = a_q(f) \ne a_q(g) = a_q(E')$. 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 $a_q(E) \ne a_q(E') = \varepsilon_\ell(\mathrm{Frob}_q)a_q(E)$, we deduce that $\varepsilon_\ell(\mathrm{Frob}_q) = -1$ and $a_q(E) \ne 0$. By Lemma 2.5, we find that $a_q(E) \equiv 0 \pmod{\ell}$. The Hasse bound then implies that

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

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

6. Remaining primes

Fix a non-CM elliptic curve $E/\mathbb{Q}$. In this section, we explain how to determine whether $\rho_{E,\ell}$ is surjective for a fixed prime ℓ. Combined with Theorem 1.2 (or possibly Proposition 1.6), this gives a method to compute the (finite) set of primes ℓ for which $\rho_{E,\ell}$ is not surjective. We will also mention the surjectivity of the ℓ-adic representations of E in §6.5.

6.1. **Primes $\ell \leq 11$.** Let $\mathscr{E}$ be the elliptic curve over $\mathbb{Q}$ defined by the Weierstrass equation $y^2 + y = x^3 - x^2 - 7x + 10$ and let $\mathscr{O}$ be the point at infinity. The Mordell-Weil group $\mathscr{E}(\mathbb{Q})$ is an infinite cyclic group generated by the point $(4,5)$. Let $J\colon \mathscr{E} \to \mathbb{A}^1_{\mathbb{Q}} \cup \{\infty\}$ be the morphism given by

$$J(x,y) = (f_1 f_2 f_3 f_4)^3/(f_5^2 f_6^{11}),$$

where

$$f_1 = x^2 + 3x - 6, \qquad f_2 = 11(x^2-5)y + (2x^4 + 23x^3 - 72x^2 - 28x + 127),$$
$$f_3 = 6y + 11x - 19, \qquad f_4 = 22(x-2)y + (5x^3 + 17x^2 - 112x + 120),$$
$$f_5 = 11y + (2x^2 + 17x - 34), \qquad f_6 = (x-4)y - (5x-9).$$

For $\ell \leq 11$, the following gives a criterion to determine whether $\rho_{E,\ell}$ is surjective or not.

Proposition 6.1. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve.*

(i) *The representation $\rho_{E,2}$ is not surjective if and only if $j_E = 256(t+1)^3/t$ or $j_E = t^2 + 1728$ for some $t \in \mathbb{Q}$.*

(ii) *The representation $\rho_{E,3}$ is not surjective if and only if $j_E = 27(t+1)(t+9)^3/t^3$ or $j_E = t^3$ for some $t \in \mathbb{Q}$.*

(iii) *The representation $\rho_{E,5}$ is not surjective if and only if*

$$j_E = \frac{5^3(t+1)(2t+1)^3(2t^2-3t+3)^3}{(t^2+t-1)^5}, \quad j_E = \frac{5^2(t^2+10t+5)^3}{t^5} \quad \text{or} \quad j_E = t^3(t^2+5t+40)$$

for some $t \in \mathbb{Q}$.

(iv) *The representation $\rho_{E,7}$ is not surjective if and only if*

$$j_E = \frac{t(t+1)^3(t^2-5t+1)^3(t^2-5t+8)^3(t^4-5t^3+8t^2-7t+7)^3}{(t^3-4t^2+3t+1)^7},$$
$$j_E = \frac{64t^3(t^2+7)^3(t^2-7t+14)^3(5t^2-14t-7)^3}{(t^3-7t^2+7t+7)^7} \quad \text{or}$$
$$j_E = \frac{(t^2+245t+2401)^3(t^2+13t+49)}{t^7}$$

for some $t \in \mathbb{Q}$.

(v) *The representation $\rho_{E,11}$ is not surjective if and only if $j_E \in \{-11^2, -11\cdot 131^3\}$ or $j_E = J(P)$ for some $P \in \mathscr{E}(\mathbb{Q}) - \{\mathscr{O}\}$.*

(vi) *If j_E is an integer, then $\rho_{E,11}$ is not surjective if and only if $j_E \in \{-11^2, -11\cdot 131^3\}$. If j_E is not an integer and $\rho_{E,11}$ is not surjective, then the denominator of j_E is of the form $p_1^{e_1}\cdots p_s^{e_s}$ with p_i distinct primes such that $p_i \equiv \pm 1 \pmod{11}$ and $e_i \equiv 0 \pmod{11}$.*

Proof. Parts (i)–(v) are consequence of the theorems from [Zyw15]; one need only consider the maximal subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$. Note that the normalizer of a split Cartan subgroup in $\mathrm{GL}_2(\mathbb{F}_3)$ is not a maximal subgroup. The normalizer of a split Cartan subgroup in $\mathrm{GL}_2(\mathbb{F}_5)$ lies in a maximal subgroup of $\mathrm{GL}_2(\mathbb{F}_5)$ whose image in $\mathrm{PGL}_2(\mathbb{F}_5)$ is isomorphic to $\mathfrak{S}_4$.

The curve $\mathscr{E}$ and the map J come from Halberstadt's description of $X_{\mathrm{ns}}^+(11)$ in [Hal98]. In particular, the group $\rho_{E,11}(\mathrm{Gal}_\mathbb{Q})$ is conjugate to a subgroup of the normalizer of a non-split Cartan subgroup of

$\mathrm{GL}_2(\mathbb{F}_{11})$ if and only if $j_E = J(P)$ for some $P \in \mathscr{E}(\mathbb{Q}) - \{\mathcal{O}\}$. In [ST12], it is shown that if $J(P)$ is an integer with $P \in \mathscr{E}(\mathbb{Q}) - \{\mathcal{O}\}$, then $J(P)$ is the j-invariant of a CM elliptic curve; this proves the first part of (vi). For the second part of (vi), note that the proof of Theorem 1.5 applies verbatim. □

Remark 6.2. In [Zyw15], we give explicit polynomials $A, B, C \in \mathbb{Q}[X]$ of degree 55 such that $j_E = J(P)$ for some point $P \in \mathscr{E}(\mathbb{Q}) - \{\mathcal{O}\}$ if and only if the polynomial $A(X)j_E^2 + B(X)j_E + C(X) \in \mathbb{Q}[X]$ has a root. So it straightforward to determine whether $j_E = J(P)$ for some $P \in \mathscr{E}(\mathbb{Q}) - \{\mathcal{O}\}$.

6.2. The prime $\ell = 13$.

Proposition 6.3.

(i) *The representation $\rho_{E,13}$ is not surjective if*

$$j_E = 2^4 \cdot 5 \cdot 13^4 \cdot 17^3 / 3^{13},$$
$$j_E = -2^{12} \cdot 5^3 \cdot 11 \cdot 13^4 / 3^{13},$$
$$j_E = 2^{18} \cdot 3^3 \cdot 13^4 \cdot 127^3 \cdot 139^3 \cdot 157^3 \cdot 283^3 \cdot 929 / (5^{13} \cdot 61^{13}), \quad \textit{or}$$
$$j_E = (t^2 + 5t + 13)(t^4 + 7t^3 + 20t^2 + 19t + 1)^3 / t \quad \textit{for some } t \in \mathbb{Q}.$$

(ii) *The representation $\rho_{E,13}$ is surjective if and only if all the following conditions hold:*
- *there is a prime $p \nmid 13N_E$ such that $a_p(E) \not\equiv 0 \pmod{13}$ and such that $a_p(E)^2 - 4p$ is a non-zero square modulo 13,*
- *there is a prime $p \nmid 13N_E$ such that $a_p(E) \not\equiv 0 \pmod{13}$ and such that $a_p(E)^2 - 4p$ is a non-square modulo 13,*
- *there is prime $p \nmid 13N_E$ such that the image of $a_p(E)^2/p$ in $\mathbb{F}_{13}$ is not 0, 1, 2 and 4, and is not a root of $x^2 - 3x + 1$.*

Proof. Part (i) is explained in [Zyw15]; the first three exceptional j-invariants come from [BC14]. Part (ii) is a direct consequence of Proposition 19 of [Ser72] and the Chebotarev density theorem. □

Consider a non-CM elliptic curve $E/\mathbb{Q}$. Suppose that j_E is not one of those given in Proposition 6.3(i); if it was then $\rho_{E,13}$ would not be surjective. Conjecturally, the representation $\rho_{E,13}$ will be surjective and hence this should be checkable using the criterion of Proposition 6.3(ii).

If the surjectivity is unknown even after computing $a_p(E)$ for many primes $p \nmid 13N_E$, then one can do a direct computation. The representation $\rho_{E,13}$ is surjective if and only if the image of $\rho_{E,13}(\mathrm{Gal}_\mathbb{Q})$ in $\mathrm{GL}_2(\mathbb{F}_{13})/\{\pm I\}$ is the full group $\mathrm{GL}_2(\mathbb{F}_{13})/\{\pm I\}$. 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 13; it is the monic polynomial $f(X) \in \mathbb{Q}[X]$ whose roots are the x-coordinates of the elements of order 13 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 be computed directly. (For example, this was how the author found the interesting j-invariants $2^4 \cdot 5 \cdot 13^4 \cdot 17^3/3^{13}$ and $-2^{12} \cdot 5^3 \cdot 11 \cdot 13^4/3^{13}$ before [BC14] was available.)

Alternatively, if $\rho_{E,13}$ was not surjective, then one could construct a new rational point on one of the explicit genus 3 curves in [BC14] or [Bar14].

6.3. A surjectivity criterion for primes $\ell > 13$.

Fix a prime $\ell > 13$.

Proposition 6.4. *The representation $\rho_{E,\ell}$ is surjective if and only if $(\ell, j_E) \notin S_0$ 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 $(\ell, j_E) \in S_0$. So assume that $(\ell, j_E) \notin S_0$. 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 $tr(g)^2 - 4\det(g)$ 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. There are matrices $A \in \mathrm{GL}_2(\mathbb{F}_\ell)$ so that $\mathrm{tr}(A) \neq 0$ and $\mathrm{tr}(A)^2 - 4\det(A)$ is a non-zero square. That primes p as in the statement of the proposition occur is then a consequence of the Chebotarev density theorem. □

Now assume that $(\ell, j_E) \notin S_0$. By computing $a_p(E)$ for more and more primes $p \nmid N_E\ell$, one expects to be able to use the criterion of Proposition 6.4 to prove that $\rho_{E,\ell}$ is surjective. If not, then we would have a counterexample to Conjecture 1.1.

6.4. **Further comments for $\ell > 13$.** Suppose that after computing $a_p(E)$ for more and more primes p, the criterion of §6.3 is inconclusive (in practice, the criterion of Proposition 6.4 works quickly).

We now explain how to determine if $\rho_{E,\ell}$ is surjective; its image can be computed directly using the division polynomial at ℓ. Note that if Conjecture 1.1 is true, then the material in this section should never be needed!

Lemma 6.5. *Suppose that E has no primes of multiplicative reduction and that $\ell > 13$ is a prime with $(\ell, j_E) \notin S_0$. Set $\mathscr{B} := N_E/6 \cdot \prod_{p|N_E}(1+1/p)$. Then $\rho_{E,\ell}$ is not surjective if and only if there is a non-trivial quadratic character χ that is unramified at all primes $p \nmid N_E$ and satisfies $\chi(p) = 1$ or $a_p(E) \equiv 0 \pmod{\ell}$ for all primes $p \nmid N_E$ with $p \leq \mathscr{B}$.*

Proof. First suppose that $\rho_{E,\ell}$ is not surjective. Let $\varepsilon_\ell \colon \mathrm{Gal}_\mathbb{Q} \to \{\pm 1\}$ be the corresponding character from §2. The character ε_ℓ is non-trivial and unramified at $p \nmid N_E$ by Lemmas 2.2(i) and 2.4. Let χ be the primitive Dirichlet quadratic character corresponding to ε_ℓ; we have $\chi(p) = \varepsilon_\ell(\mathrm{Frob}_p)$ for each $p \nmid N_E$. The character χ is non-trivial since ε_ℓ is non-trivial. By Lemma 2.5, we have $\chi(p) = \varepsilon(\mathrm{Frob}_p) = 1$ or $a_p(E) \equiv 0 \pmod{\ell}$ for all $p \nmid N_E$ (and in particular, this holds if $p \leq \mathscr{B}$).

Now suppose that there is a non-trivial quadratic character χ that is unramified at primes $p \nmid N_E$ and satisfies $\chi(p) = 1$ or $a_p(E) \equiv 0 \pmod{\ell}$ for all primes $p \nmid N_E$ with $p \leq \mathscr{B}$. Let $f = \sum_{n\geq 1} a_n(f)q^n \in S_2(\Gamma_0(N_E))$ be the newform corresponding to $E/\mathbb{Q}$ by modularity. Since E has no primes of multiplicative reduction, we have $a_n(f) = 0$ whenever $(N_E, n) \neq 1$. Let $g = \sum_{n\geq 1} \chi(n)a_n(f)q^n$ be the twist of f by χ; it is also a cusp form of level N_E. Using our assumption on χ, we have $a_p(f) \equiv \chi(p)a_p(f) = a_p(g) \pmod{\ell}$ for all primes $p \leq \mathscr{B}$. We have $\mathscr{B} = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N_E)]/6$, so Theorem 1 of [Stu87] implies that $a_p(E) = a_p(f) \equiv a_p(g) = \chi(p)a_p(E) \pmod{\ell}$ for all primes p (one need only consider prime index Fourier coefficients since they are multiplicative and defined recursively on prime powers). In particular, $a_p(E) \equiv 0 \pmod{\ell}$ whenever $p \nmid N_E$ satisfies $\chi(p) = -1$. Since χ is non-trivial, we deduce that the set of primes $p \nmid N_E$ for which $a_p(E) \equiv 0 \pmod{\ell}$ has natural density at least $1/2$. By the Chebotarev density theorem, we have $|\{A \in \rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q}) : \mathrm{tr}(A) = 0\}|/|\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})| \geq 1/2$. It easy to check that this inequality fails if $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q}) = \mathrm{GL}_2(\mathbb{F}_\ell)$. Therefore, $\rho_{E,\ell}$ is not surjective. □

If $v_2(j_E) < 0$, then $\rho_{E,\ell}$ is surjective by Theorem 1.5; so assume that $v_2(j) \geq 0$. After replacing E by its quadratic twist by $\prod_{p\|N_E} p$, we may assume that E has no primes of multiplicative reduction (if $\rho_{E,\ell}$ is not surjective, then its image lies in the normalizer of a Cartan subgroup and this does change if we change E by a quadratic twist). Lemma 6.5 then gives a way to compute if $\rho_{E,\ell}$ is surjective; there are a bounded number of $a_p(E)$ to compute and there are only finitely many possible characters χ.

6.5. **ℓ-adic surjectivity.** For each integer $n \geq 1$, let $E[\ell^n]$ be the group of ℓ^n-torsion in $E(\overline{\mathbb{Q}})$. The Tate module $T_\ell(E)$ of E is the inverse limit of the groups $E[\ell^n]$ with respect to the transition maps $E[\ell^{n+1}] \to E[\ell^n]$, $P \mapsto \ell P$. The Tate module $T_\ell(E)$ is a free $\mathbb{Z}_\ell$-module of rank 2 with a natural $\mathrm{Gal}_\mathbb{Q}$-action. Let $\rho_{E,\ell^\infty} \colon \mathrm{Gal}_\mathbb{Q} \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(E)) \cong \mathrm{GL}_2(\mathbb{Z}_\ell)$ be the representation describing this Galois action.

Using the results of this paper, and the following lemma, it is straightforward to compute the (finite) set of primes ℓ for which ρ_{E,ℓ^∞} is not surjective.

Lemma 6.6. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve.*

(i) *The representation $\rho_{E,2^\infty}$ is not surjective if and only if $\rho_{E,2}$ is not surjective or j_E is of the form*
$$-4t^3(t+8), \quad -t^2+1728, \quad 2t^2+1728 \quad \text{or} \quad -2t^2+1728$$
for some $t \in \mathbb{Q}$.

(ii) *The representation $\rho_{E,3^\infty}$ is not surjective if and only if $\rho_{E,3}$ is not surjective or*
$$j_E = -\frac{3^7(t^2-1)^3(t^6+3t^5+6t^4+t^3-3t^2+12t+16)^3(2t^3+3t^2-3t-5)}{(t^3-3t-1)^9}$$
for some $t \in \mathbb{Q}$.

(iii) *If $\ell \geq 5$, then ρ_{E,ℓ^∞} is not surjective if and only if $\rho_{E,\ell}$ is not surjective.*

Proof. For the 2-adic and 3-adic cases, see [DD12] and [Elk06], respectively. When $\ell \geq 5$, the lemma follows from Lemma 3.4 of [Ser98, IV §3.4]. □

Appendix A. Some code

Given a non-CM elliptic curve $E/\mathbb{Q}$, the following Magma function outputs a finite set of primes S such that the representation $\rho_{E,\ell}$ is surjective for all primes $\ell \notin S$. It uses the algorithm of §1.1 if j_E is an integer and uses §1.2 otherwise. (Note that we could then use §6 to quickly determine the set of primes ℓ for which $\rho_{E,\ell}$ is not surjective.)

```
ExceptionalSet:=function(E)
     j:=jInvariant(E); den:=Denominator(j);
     S:={2,3,5,7,13};
     if j in {-11^2,-11*131^3} then S:=S join {11}; end if;
     if j in {-297756989/2, -882216989/131072} then  S:=S join {17};  end if;
     if j in {-9317, -162677523113838677} then  S:=S join {37}; end if;
     if den ne 1 then
          ispow,b,e:=IsPower(den);
          if ispow then
               P:={p: p in PrimeDivisors(e) | p ge 11};
               if P ne {} then
                    g:=GCD({&*P} join {p^2-1 : p in PrimeDivisors(b)});
                    S:= S join {ell : ell in PrimeDivisors(g) | ell ge 11};
               end if;
          end if;
     else
          D:=Discriminant(E);
          Q:=PrimeDivisors( GCD(Numerator(j-1728),Numerator(D)*Denominator(D)));
          Q:=[q: q in Q | q ne 2 and IsOdd(Valuation(j-1728,q))];
          if Valuation(j,2) in {3,6,9} then Q:=[2] cat Q; end if;
          p:=2;
          alpha:=[]; beta:=[];
          repeat
               a:=0;
               while a eq 0 do
                    p:=NextPrime(p);  K:=KodairaSymbol(E,p);
                    if K eq KodairaSymbol("I0") then
                         a:=TraceOfFrobenius(E,p);
```

```
                    elif K eq KodairaSymbol("I0*") then
                         a:=TraceOfFrobenius(QuadraticTwist(E,p),p);
                    end if;
               end while;
               S:=S join {ell : ell in PrimeDivisors(a) | ell gt 13};
               alpha:= alpha cat [[(1-KroneckerSymbol(q,p)) div 2 : q in Q]];
               beta:= beta cat [ [(1-KroneckerSymbol(-1,p)) div 2] ];
               A:=Matrix(GF(2),alpha);  b:=Matrix(GF(2),beta);
          until IsConsistent(Transpose(A),Transpose(b)) eq false;
     end if;
     return S;
end function;
```

The following code verifies Conjecture 1.1 for all elliptic curves $E/\mathbb{Q}$ in Cremona's database [Cre]; currently this includes all curves of conductor at most 350000.

```
D:=CremonaDatabase();   LargestConductor(D);
for N in [1..LargestConductor(D)] do
for E in EllipticCurves(D,N) do
if not HasComplexMultiplication(E) then
        S:={p: p in ExceptionalSet(E) | p gt 13};
        if S ne {} then   print jInvariant(E), " ", S;   end if;
end if;
end for;
end for;
```

References

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

[BC14] Barinder Singh Banwait and John Cremona, *Tetrahedral Elliptic Curves and the local-global principle for Isogenies* (2014). arXiv:1306.6818 [math.NT]. ↑6.2

[Bar14] Burcu Baran, *An exceptional isomorphism between modular curves of level 13*, J. Number Theory **145** (2014), 273–300. ↑6.2

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Computational algebra and number theory (London, 1993). ↑1.3

[BK75] B. J. Birch and W. Kuyk (eds.), *Modular functions of one variable. IV*, Lecture Notes in Mathematics, Vol. 476, Springer-Verlag, Berlin, 1975. ↑

[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://homepages.warwick.ac.uk/~masgaj/ftp/data/. ↑A

[DD12] Tim Dokchitser and Vladimir Dokchitser, *Surjectivity of mod* 2^n *representations of elliptic curves*, Math. Z. **272** (2012), no. 3-4, 961–964. ↑6.5

[Elk06] N.D. Elkies, *Elliptic curves with* 3*-adic Galois representation surjective mod* 3 *but not mod* 9 (2006). arXiv:math/0612734 [math.NT]. ↑6.5

[Hal98] Emmanuel Halberstadt, *Sur la courbe modulaire* $X_{ndép}(11)$, Experiment. Math. **7** (1998), no. 2, 163–174. ↑6.1

[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, 6.2

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

[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. ↑6.5

[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. ↑4, 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). http://modular.math.washington.edu/Tables/surj/. ↑1.1

[Stu87] Jacob Sturm, *On the congruence of modular forms*, Number theory (New York, 1984), Lecture Notes in Math., vol. 1240, Springer, Berlin, 1987, pp. 275–280. ↑6.4

[ST12] René Schoof and Nikos Tzanakis, *Integral points of a modular curve of level 11*, Acta Arith. **152** (2012), no. 1, 39–49. ↑6.1

[Sut12] Andrew V. Sutherland, *Computing the image of Galois* (talk), 2012. http://www-math.mit.edu/~drew/CNTA12.pdf. ↑

[Zyw15] David Zywina, *The possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$* (2015). preprint. ↑1, 1, 6.1, 6.2, 6.2

Department of Mathematics, Cornell University, Ithaca, NY 14853, USA
E-mail address: zywina@math.cornell.edu
URL: http://www.math.cornell.edu/~zywina