Received: 26 May 2023 | Revised: 29 November 2023 | Accepted: 20 December 2023

DOI: 10.1112/blms.13002

RESEARCH ARTICLE

Bulletin of the London Mathematical Society

On the effective version of Serre's open image theorem

Jacob Mayle[1] | **Tian Wang**[2]

[1]Department of Mathematics, Wake Forest University, Winston-Salem, North Carolina, USA

[2]Max Planck Institute for Mathematics, Bonn, Germany

Correspondence
Jacob Mayle, Department of Mathematics, Wake Forest University, Winston-Salem, NC 27109, USA.
Email: maylej@wfu.edu

Abstract

Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. By Serre's open image theorem, the mod ℓ Galois representation $\overline{\rho}_{E,\ell}$ of E is surjective for each prime number ℓ that is sufficiently large. Under the generalized Riemann hypothesis, we give an explicit upper bound on the largest prime ℓ, linear in the logarithm of the conductor of E, such that $\overline{\rho}_{E,\ell}$ is nonsurjective.

MSC 2020
11G05 (primary), 11F80 (secondary)

1 | INTRODUCTION

Let E be an elliptic curve defined over $\mathbb{Q}$. For a prime number ℓ, let $E[\ell]$ denote the ℓ-torsion subgroup of $E(\overline{\mathbb{Q}})$ and let $T_\ell(E)$ denote the ℓ-adic Tate module of E. Recall that $E[\ell]$ and $T_\ell(E)$ are free modules of rank two over $\mathbb{F}_\ell$ and $\mathbb{Z}_\ell$, respectively, where $\mathbb{F}_\ell$ denotes the finite field with ℓ elements and $\mathbb{Z}_\ell$ denotes the ring of ℓ-adic integers. Fixing bases, we obtain the module isomorphisms

$$E[\ell] \cong \mathbb{F}_\ell \oplus \mathbb{F}_\ell \quad \text{and} \quad T_\ell(E) \cong \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell.$$

The absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts coordinate-wise on elements of $E[\ell]$ and on $T_\ell(E)$. These actions respect the above isomorphisms, and give rise to the *mod ℓ Galois representation* and *ℓ-adic Galois representation* of E, which are denoted, respectively, by

$$\bar{\rho}_{E,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell) \quad \text{and} \quad \rho_{E,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell).$$

The above Galois representations carry a considerable amount of information about E. For instance, consider the reduction E_p of the curve E at a prime number p that is distinct from ℓ. The well-known Néron–Ogg–Shafarevich criterion gives that E has good reduction at p if and only if $\rho_{E,\ell}$ is unramified at p. Further, if E has good reduction at p, then $\operatorname{tr}\rho_{E,\ell}(\mathrm{Frob}_p) = a_p(E)$ and $\det\rho_{E,\ell}(\mathrm{Frob}_p) = p$, where $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ denotes a Frobenius automorphism associated with p and $a_p(E)$ is defined by the equation $\#E_p(\mathbb{F}_p) = p + 1 - a_p(E)$.

Suppose from now on that E is without complex multiplication, that is, assume that the geometric endomorphism ring of E is trivial. A celebrated theorem of Serre [40], known as the open image theorem, establishes that if ℓ is sufficiently large, then $\bar{\rho}_{E,\ell}$ is surjective. Let $c(E)$ denote the least positive integer such that if $\ell > c(E)$, then $\bar{\rho}_{E,\ell}$ is surjective.[†] Serre asked if $c(E) \leqslant 37$ holds for each elliptic curve $E/\mathbb{Q}$ without complex multiplication. This is known as Serre's uniformity question and, following theoretical advances and vast numerical evidence, is now articulated in precise conjectures of Sutherland [47, Conjecture 1.1] and Zywina [53, Conjecture 1.12]. Mazur's landmark work on modular curves implies that $c(E) \leqslant 11$ if E is semistable [34, Theorem 4]. Further progress toward resolving Serre's question has since been made by studying modular curves, which we discuss in §2. In an adjacent direction, there has been progress in bounding $c(E)$ in terms of invariants of E, such as the Faltings height h_E or the conductor N_E of E, which we address in this paper.

Serre's original proof of the open image theorem is ineffective and does not give a bound on $c(E)$. The first unconditional bound on $c(E)$ is due to Masser and Wüstholz [33] who proved in 1993 that there exist absolute constants C_1 and γ such that

$$c(E) \leqslant C_1 h_E^{\gamma}.$$

This bound has subsequently been improved and made explicit in [28, 32, 39]. Under the now superfluous assumption that E is modular [8], in 1995, Kraus [23] bounded $c(E)$ in terms of the conductor of E,

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

where $\operatorname{rad} n := \prod_{p|n} p$ denotes the radical of an integer n. In 2005, Cojocaru [12] proved independently using a similar approach that

$$c(E) \leqslant \frac{4\sqrt{6}}{3} N_E \prod_{p|N_E} \left(1 + \frac{1}{p}\right)^{1/2}.$$

Recently, Zywina [54, Proposition 1.8 and Theorem 1.10] improved the bounds of Kraus and Cojocaru.

Considerably better bounds for $c(E)$ are known under the assumption of the generalized Riemann hypothesis (GRH) for Dedekind zeta functions. Assuming GRH, Serre gave an elegant proof in 1981 [41, Théorème 22] that there exists an absolute, computable constant C_2 such that

$$c(E) \leqslant C_2(\log\operatorname{rad} N_E)(\log\log\operatorname{rad} 2N_E)^3. \tag{1}$$

[†] The choice to define $c(E)$ in terms of $\bar{\rho}_{E,\ell}$ instead of $\rho_{E,\ell}$ is somewhat arbitrary. Indeed, for a prime number $\ell \geqslant 5$, we have that $\bar{\rho}_{E,\ell}$ is surjective if and only if $\rho_{E,\ell}$ is surjective [43, p. IV-23].

Serre mentioned without proof in [44, Note 632.6] that the "log log" term in (1) may be removed by employing an ℓ-adic technique of Faltings [21, §6, pp. 362–363]. The technique and its extension is called the Faltings–Serre method (see [9, Section 2]) and is widely recognized for its important role in establishing various modularity results: such as the modularity of elliptic curves over (infinitely) many imaginary quadratic fields [11, 14, 18, 22, 48], the paramodularity of certain abelian surfaces with a trivial endomorphism ring [7, 9], and the modularity of some Calabi–Yau threefolds [15, 19].

In 2014, Larson and Vaintrob [27, Theorem 1] proved, without applying the Falting–Serre method, that under GRH, there exists an absolute constant C_3 such that

$$c(E) \leqslant C_3 \log N_E. \tag{2}$$

Not only is their bound linear in $\log N_E$, but it also holds over an arbitrary number field K (with C_3 depending only on K). However, even over $\mathbb{Q}$, the bound (2) is ineffective in the sense that no method is presently known for computing C_3. In order to compute C_3 via the proof in [27], one would need to understand the rational points on the modular curve $X_{ns}^{+}(\ell)$ for some prime $\ell \geqslant 53$.

The main result of this paper is an explicit conditional bound on $c(E)$ of the same asymptotic quality as (2) for elliptic curves over $\mathbb{Q}$. Specifically, we shall prove the following.

Theorem 1. *Assume GRH. If $E/\mathbb{Q}$ is an elliptic curve without complex multiplication, then*

$$c(E) \leqslant 964 \log \operatorname{rad}(2N_E) + 5760,$$

where $\operatorname{rad} n := \prod_{p|n} p$ *denotes the radical of an integer n.*

Our proof of Theorem 1 follows the strategy set forth by Serre in [41, Théorème 22] and [44, Note 632.6]. The key improvement comes from the following sharpening of his conditional bound in the effective version of Faltings's isogeny theorem for elliptic curves [41, Théorème 21].

Theorem 2. *Assume GRH. Let $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ be elliptic curves without complex multiplication. Suppose that E_1 and E_2 are not $\mathbb{Q}$-isogenous. Then there exists a prime number p of good reduction for E_1 and E_2 such that $a_p(E_1) \neq a_p(E_2)$ satisfying the inequality*

$$p \leqslant (482 \log \operatorname{rad}(2N_{E_1}N_{E_2}) + 2880)^2.$$

The structure of our paper is as follows. In §3, we give a variant of the effective Chebotarev density theorem due to Bach and Sorenson. We use this tool, together with a refinement of a technique of Faltings, to prove Theorem 2 in §4. With this result in hand, in §5, we follow in the footsteps of Serre's elegant proof of (1) to complete our proof of Theorem 1. Afterward, we illustrate our result with a numerical example in §5.3.

We conclude the introduction with some remarks on extensions of the effective Serre's open image theorem.

We recall from the modularity theorem [49, 52] that Galois representations of elliptic curves over $\mathbb{Q}$ arise from Galois representations of weight 2 cuspidal eigenforms. Therefore, Theorem 1 can also be interpreted as an effective open image theorem for modular forms of weight 2. We refer the reader to [5, 38] for other effective results for higher weight modular forms.

Let K be a number field and E/K be a non-CM elliptic curve. Serre's open image theorem also applies over a number field, so we can define $c(E)$ in a similar way as before. It is known that there is a uniform bound of $c(E)$ for certain families of $\mathbb{Q}$-curves E over a quadratic field K (see [28, 30]).

The main result of this paper is to make explicit the conditional bound of Larson and Vaintrob [27, Theorem 1] for elliptic curves over $\mathbb{Q}$. However, as their bound holds for elliptic curves over number fields, it is natural to ask if we could extend our result to E/K. The approach that we follow relies on Mazur's cyclic isogeny theorem. Generalizing Mazur's result to elliptic curves over arbitrary number fields appears to be challenging. Nonetheless, assuming GRH, if K is among a certain finite set of quadratic fields K, Banwait [3] and Banwait, Najman, and Padurariu [4], building on the earlier work of David [16], Larson and Vaintrob [26], and Momose [35], proved an analog of Mazur's cyclic isogeny theorem for E/K. Thus, it is promising that one may be able to extend our work to give an explicit open image theorem for elliptic curves defined over these quadratic fields.

2 | PROGRESS TOWARD SERRE'S UNIFORMITY QUESTION

The most significant progress toward a resolution of Serre's uniformity question comes from studying rational points on certain modular curves. By doing so, one limits the possibilities for $G_E(\ell) := \operatorname{im} \bar{\rho}_{E,\ell}$, that is, the image of $\bar{\rho}_{E,\ell}$. As $G_E(\ell)$ is a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, in order to describe what is known in this direction, we first state a well-known classification of subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$ (which dates back to Dickson [17]) and give some necessary terminology.

Let ℓ be an odd prime number and fix a nonsquare element $\varepsilon \in \mathbb{F}_\ell^\times$. The *split Cartan subgroup* and *nonsplit Cartan subgroup* of $\mathrm{GL}_2(\mathbb{F}_\ell)$ are, respectively,

$$C_s(\ell) := \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} : a, d \in \mathbb{F}_\ell^\times \right\} \quad \text{and} \quad C_{ns}(\ell) := \left\{ \begin{pmatrix} a & \varepsilon c \\ c & a \end{pmatrix} : a, c \in \mathbb{F}_\ell \text{ and } (a,c) \neq (0,0) \right\}.$$

Let $C_s^+(\ell)$ and $C_{ns}^+(\ell)$ denote the normalizer of $C_s(\ell)$ and $C_{ns}(\ell)$, respectively. One may show that

$$C_s^+(\ell) = C_s(\ell) \cup \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} C_s(\ell) \quad \text{and} \quad C_{ns}^+(\ell) = C_{ns}(\ell) \cup \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} C_{ns}(\ell). \tag{3}$$

Let $B(\ell)$ denote the *Borel subgroup* of $\mathrm{GL}_2(\mathbb{F}_\ell)$, that is, the subgroup of upper triangular matrices,

$$B(\ell) := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, d \in \mathbb{F}_\ell^\times \text{ and } b \in \mathbb{F}_\ell \right\}.$$

Let A_n and S_n denote the alternating and symmetric groups, respectively, on n elements. Finally, for a subgroup G of $\mathrm{GL}_2(\mathbb{F}_\ell)$, let $\overline{G}$ denote the image of G in the projective linear group $\mathrm{PGL}_2(\mathbb{F}_\ell)$. With notation set, we now state the classification. For further details, we refer the reader to [40, §2].

Proposition 3. *Let ℓ be an odd prime. If $G \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$ is a subgroup, then*

(1) *G contains $\mathrm{SL}_2(\mathbb{F}_\ell)$,*
(2) *G is conjugate to a subgroup of $B(\ell)$,*

(3) *G is conjugate to a subgroup of $C_{ns}(\ell)$,*
(4) *G is conjugate to a subgroup of $C_s^+(\ell)$ but not to any subgroup of $C_s(\ell)$,*
(5) *G is conjugate to a subgroup of $C_{ns}^+(\ell)$ but not to any subgroup of $C_{ns}(\ell)$, or*
(6) *$\overline{G}$ is isomorphic to A_4, S_4, or A_5.*

Returning to the world of elliptic curves, recall that by the Weil pairing on E, the composition

$$\det \circ \bar{\rho}_{E,\ell} : \ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathbb{F}_\ell^\times$$

is the mod ℓ cyclotomic character and hence is surjective [46, III.8]. In particular, if $\mathrm{SL}_2(\mathbb{F}_\ell) \subseteq G_E(\ell)$, then, in fact, $G_E(\ell) = \mathrm{GL}_2(\mathbb{F}_\ell)$. Consequently, in order to prove that $\bar{\rho}_{E,\ell}$ is surjective for a particular prime number ℓ, it suffices to rule out possibilities (2) through (6) of Proposition 3 for the group $G_E(\ell)$. For a non-CM elliptic curve, many cases are already ruled out for sufficiently large ℓ. Indeed, Serre ruled out (3) for $\ell > 2$ [40, §5.2] and (6) for $\ell > 13$ [41, Lemme 18]; Mazur ruled out (2) for $\ell > 37$ [34, Theorem 3]; Bilu, Parent, and Rebolledo ruled out (4) for $\ell > 7$ and $\ell \neq 13$ [6, Corollary 1.2]; Balakrishnan, Dogra, Netan, Müller, Tuitman, and Vonk ruled out (4) for $\ell = 13$ [2, Theorem 1.2]. Therefore, all but (5) are ruled out for each prime number $\ell > 37$, as recorded below.

Theorem 4. *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. If ℓ is a prime number such that $\ell > 37$, then either $\bar{\rho}_{E,\ell}$ is surjective or $G_E(\ell)$ is conjugate to a subgroup of $C_{ns}^+(\ell)$ but is not conjugate to any subgroups of $C_{ns}(\ell)$.*

3 | THE EFFECTIVE CHEBOTAREV DENSITY THEOREM

In this section, we offer a modest extension of the version of the effective Chebotarev density theorem given in [1]. This extension will serve as a crucial tool in our proof of Theorem 1. First, let us fix some relevant notation.

Let K be a number field with absolute discriminant d_K and ring of integers $\mathcal{O}_K$. For a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$, we write $\mathfrak{p} \mid p$ to indicate that $\mathfrak{p}$ lies above a prime number p. Let $\upsilon_\mathfrak{p} : K \to \mathbb{Z}$ denote the normalized $\mathfrak{p}$-adic valuation on K. We write $N(\mathfrak{p})$ for the ideal norm of $\mathfrak{p}$, which extends multiplicatively to arbitrary ideals of $\mathcal{O}_K$. One has that $\upsilon_\mathfrak{p}(p) = e_\mathfrak{p}$ and $N(\mathfrak{p}) = p^{f_\mathfrak{p}}$, where $e_\mathfrak{p}$ and $f_\mathfrak{p}$ are the ramification index and inertia degree of $\mathfrak{p}$, respectively.

Assume that $K/\mathbb{Q}$ is Galois. For a prime number p that is unramified in $K/\mathbb{Q}$, write $\left(\frac{p}{K/\mathbb{Q}}\right)$ to denote the Artin symbol of $K/\mathbb{Q}$ at p. Let C be a subset of the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ that is closed under conjugation. Associated with C, consider the counting function

$$\pi_C(x) := \#\left\{ p \leqslant x \ : \ p \text{ is unramified in } K/\mathbb{Q} \text{ and } \left(\frac{p}{K/\mathbb{Q}}\right) \subseteq C \right\}.$$

The Chebotarev density theorem states that

$$\pi_C(x) \sim \frac{\#C}{\#\mathrm{Gal}(K/\mathbb{Q})}\pi(x), \tag{4}$$

where $\pi(x)$ is the prime counting function and $f \sim g$ means that $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$.

Assuming GRH, Lagarias and Odlyzko [24] gave an effective version of the Chebotarev density theorem that provides an error term in (4). Moreover, they showed that there exists an absolute constant k such that the least prime number p with

$$\left(\frac{p}{K/\mathbb{Q}}\right) \subseteq C \tag{5}$$

satisfies the inequality $p \leqslant k(\log d_K)^2$. Oesterlé [37] stated that the absolute constant k may be taken to be 70. Subsequently, Bach and Sorenson offered the following improvement.

Theorem 5. *Assume GRH. Let K be a Galois number field and let $C \subseteq \mathrm{Gal}(K/\mathbb{Q})$ be a nonempty subset that is closed under conjugation. Then there exists a prime number p that is unramified in $K/\mathbb{Q}$ for which (5) holds that satisfies the inequality*

$$p \leqslant (a \log d_K + b[K : \mathbb{Q}] + c)^2,$$

where a, b, and c are absolute constants that may be taken to be 4, 2.5, and 5, respectively, or may be taken to be the improved values given in [1, Table 3] associated with K.

Proof. See [1, Theorem 5.1]. □

For our application, we need an extension of Theorem 5 that allows for the avoidance of a prescribed set of primes.

Corollary 6. *Assume GRH. Let K be a Galois number field, let m be a squarefree positive integer, and set $\tilde{K} := K(\sqrt{m})$. Let $C \subseteq \mathrm{Gal}(K/\mathbb{Q})$ be a nonempty subset that is closed under conjugation. Then there exists a prime number p not dividing m that is unramified in $K/\mathbb{Q}$ for which (5) holds that satisfies the inequality*

$$p \leqslant (\tilde{a} \log d_{\tilde{K}} + \tilde{b}[\tilde{K} : \mathbb{Q}] + \tilde{c})^2, \tag{6}$$

where $\tilde{a}, \tilde{b}, \tilde{c}$ are absolute constants that may be taken to be 4, 2.5, and 5, respectively, or may be taken to be the improved values given in [1, Table 3] associated with $\tilde{K}$.

Proof. Notice that $\tilde{K}$ is Galois over $\mathbb{Q}$ since both K and $\mathbb{Q}(\sqrt{m})$ are Galois over $\mathbb{Q}$. If $\tilde{K} = K$, then each prime number dividing m is ramified in $K/\mathbb{Q}$, so Theorem 5 provides the desired result. Thus, we assume that $\tilde{K} \neq K$. Then $K \cap \mathbb{Q}(\sqrt{m}) = \mathbb{Q}$, so by [25, Theorem VI 1.14], we have that

$$\mathrm{Gal}(\tilde{K}/\mathbb{Q}) \cong \mathrm{Gal}(K/\mathbb{Q}) \times (\mathbb{Z}/2\mathbb{Z}).$$

Let $\mathrm{res} : \mathrm{Gal}(\tilde{K}/\mathbb{Q}) \longrightarrow \mathrm{Gal}(K/\mathbb{Q})$ denote the restriction map and consider the subset $\tilde{C} := \mathrm{res}^{-1}(C)$ of $\mathrm{Gal}(\tilde{K}/\mathbb{Q})$. Since C is closed under conjugation in $\mathrm{Gal}(K/\mathbb{Q})$, $\tilde{C}$ is closed under conjugation in $\mathrm{Gal}(\tilde{K}/\mathbb{Q})$. By applying Theorem 5 to $\tilde{K}$ and $\tilde{C}$, we obtain a prime number p that is unramified in $\tilde{K}$ for which (5) holds and satisfies the inequality (6). Note that $\tilde{K}$ is ramified at the ramified primes of K and at the prime divisors of m (and possibly at 2). Thus, p is unramified

in K and does not divide m. Finally, because $(\frac{p}{\tilde{K}/\mathbb{Q}}) \subseteq \tilde{C}$ and $\mathrm{res}((\frac{p}{\tilde{K}/\mathbb{Q}})) = (\frac{p}{K/\mathbb{Q}})$, we have that $(\frac{p}{K/\mathbb{Q}}) \subseteq C$. □

In the corollary, we see that p is bounded above in terms of $[\tilde{K} : \mathbb{Q}]$ and $\log d_{\tilde{K}}$. In our application, the degree $[\tilde{K} : \mathbb{Q}]$ will be absolutely bounded. Thus, it will remain to bound $\log d_{\tilde{K}}$. For this purpose, we employ the following lemma, which can be found in [41, Proposition 6].

Lemma 7. *If $K/\mathbb{Q}$ is a nontrivial finite Galois extension, then*

$$(\tfrac{1}{2}\log 3)[K : \mathbb{Q}] \leqslant \log d_K \leqslant ([K : \mathbb{Q}] - 1)\log \mathrm{rad}(d_K) + [K : \mathbb{Q}]\log([K : \mathbb{Q}]).$$

Proof. The left-hand inequality follows from the Minkowski bound for the discriminant [41, p. 139]. For the right-hand inequality, let $\mathfrak{D}_K \subseteq \mathcal{O}_K$ denote the different ideal of K and note that

$$d_K = N(\mathfrak{D}_K) = \prod_{p \mid d_K} p^{v_p(N(\mathfrak{D}_K))}.$$

By taking logarithms, we obtain

$$\log d_K = \sum_{p \mid d_K} v_p(N(\mathfrak{D}_K))\log p = \sum_{p \mid d_K} \sum_{\mathfrak{p} \mid p} f_{\mathfrak{p}} v_{\mathfrak{p}}(\mathfrak{D}_K)\log p. \tag{7}$$

For each prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ lying above p, we have that

$$v_{\mathfrak{p}}(\mathfrak{D}_K) = e_{\mathfrak{p}} - 1 + s_{\mathfrak{p}}$$

for some integer $s_{\mathfrak{p}}$ satisfying $0 \leqslant s_{\mathfrak{p}} \leqslant v_{\mathfrak{p}}(e_{\mathfrak{p}})$ (see, e.g., [36, Theorem 2.6, p. 199]). Thus,

$$\sum_{\mathfrak{p} \mid p} f_{\mathfrak{p}} v_{\mathfrak{p}}(\mathfrak{D}_K) = \sum_{\mathfrak{p} \mid p} f_{\mathfrak{p}}(e_{\mathfrak{p}} - 1) + \sum_{\mathfrak{p} \mid p} f_{\mathfrak{p}} s_{\mathfrak{p}} \leqslant [K : \mathbb{Q}] - 1 + \sum_{\mathfrak{p} \mid p} f_{\mathfrak{p}} v_{\mathfrak{p}}(e_{\mathfrak{p}}). \tag{8}$$

Since $K/\mathbb{Q}$ is Galois, $e_{\mathfrak{p}}$ divides $[K : \mathbb{Q}]$. Thus, $v_p(e_{\mathfrak{p}}) \leqslant v_p([K : \mathbb{Q}])$. Hence,

$$\sum_{\mathfrak{p} \mid p} f_{\mathfrak{p}} v_{\mathfrak{p}}(e_{\mathfrak{p}}) = \sum_{\mathfrak{p} \mid p} f_{\mathfrak{p}} e_{\mathfrak{p}} v_p(e_{\mathfrak{p}}) \leqslant v_p([K : \mathbb{Q}]) \sum_{\mathfrak{p} \mid p} f_{\mathfrak{p}} e_{\mathfrak{p}} = v_p([K : \mathbb{Q}])[K : \mathbb{Q}]. \tag{9}$$

Observe that

$$\sum_{p \mid d_K} v_p([K : \mathbb{Q}])[K : \mathbb{Q}]\log p \leqslant [K : \mathbb{Q}]\log[K : \mathbb{Q}]. \tag{10}$$

Applying (8)–(10) to (7), we obtain

$$\log d_K \leqslant ([K : \mathbb{Q}] - 1) \sum_{p \mid d_K} \log p + [K : \mathbb{Q}]\log[K : \mathbb{Q}].$$

The claimed inequality now follows by noting that $\sum_{p \mid d_K} \log p = \log \mathrm{rad}(d_K)$. □

4 | AN EFFECTIVE ISOGENY THEOREM FOR ELLIPTIC CURVES

The objective of this section is to provide an improved conditional bound on the effective version of Faltings's isogeny theorem for elliptic curves. We begin in §4.1 with some preliminaries.

4.1 | Ramified primes

Let $A/\mathbb{Q}$ be an abelian variety. For a positive integer m, let $\mathbb{Q}(A[m])$ denote the m-division field of A, that is, the field obtained by adjoining to $\mathbb{Q}$ the coordinates of all points of $A(\overline{\mathbb{Q}})$ of order dividing m. For a prime number ℓ, we write

$$\mathbb{Q}(A[\ell^\infty]) := \bigcup_{k=1}^{\infty} \mathbb{Q}(A[\ell^k]).$$

We now recall Serre and Tate's extension of the criterion of Néron–Ogg–Shafarevich to abelian varieties in order to specify which primes ramify in the infinite degree algebraic extension $\mathbb{Q}(A[\ell^\infty])/\mathbb{Q}$.

Theorem 8. *Let $A/\mathbb{Q}$ be an abelian variety. For a prime number p, the following are equivalent:*

(1) *A has good reduction at p,*
(2) *$\mathbb{Q}(A[m])/\mathbb{Q}$ is unramified at p for each positive integer m, not divisible by p, and*
(3) *$\mathbb{Q}(A[m])/\mathbb{Q}$ is unramified at p for infinitely many positive integers m, not divisible by p.*

Proof. See [45, Theorem 1]. □

Corollary 9. *Let B_A be the product of ℓ and the primes of bad reduction for A. The extension $\mathbb{Q}(A[\ell^\infty])/\mathbb{Q}$ is ramified at exactly the prime divisors of B_A.*

Proof. First, we note that ℓ is ramified in $\mathbb{Q}(A[\ell^\infty])/\mathbb{Q}$. Indeed, let $\zeta_{\ell^2} \in \overline{\mathbb{Q}}$ be a primitive ℓ^2-root of unity. It follows from the Weil pairing on $E[\ell^2]$ (see the exercise in [42, p. 55]) that

$$\mathbb{Q} \subseteq \mathbb{Q}(\zeta_{\ell^2}) \subseteq \mathbb{Q}(A[\ell^2]) \subseteq \mathbb{Q}(A[\ell^\infty]).$$

Because ℓ ramifies in $\mathbb{Q}(\zeta_{\ell^2})/\mathbb{Q}$, it follows that ℓ ramifies in $\mathbb{Q}(A[\ell^\infty])/\mathbb{Q}$.[†]

We continue the proof by showing that the extension $\mathbb{Q}(A[\ell^\infty])/\mathbb{Q}$ is unramified at exactly the primes not dividing B_A. Let p be a prime number such that $p \nmid B_A$. Then A has good reduction at p, so it follows from the equivalence of (1) and (2) in Theorem 8 that in the chain of subfields

$$\mathbb{Q} \subseteq \mathbb{Q}(A[\ell]) \subseteq \mathbb{Q}(A[\ell^2]) \subseteq \cdots \subseteq \mathbb{Q}(A[\ell^\infty]),$$

the prime p is unramified in $\mathbb{Q}(A[\ell^n])/\mathbb{Q}$ for each $n \geqslant 0$. Thus, p is unramified in $\mathbb{Q}(A[\ell^\infty])/\mathbb{Q}$. Now suppose that p is distinct from ℓ and is unramified in $\mathbb{Q}(A[\ell^\infty])/\mathbb{Q}$. Then, in fact, p is

[†] If $\ell \neq 2$, then it suffices to consider $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_\ell) \subseteq \mathbb{Q}(A[\ell]) \subseteq \mathbb{Q}(A[\ell^\infty])$ to observe that ℓ ramifies in $\mathbb{Q}(A[\ell^\infty])/\mathbb{Q}$.

unramified in $\mathbb{Q}(A[\ell^n])/\mathbb{Q}$ for each $n \geqslant 0$. By the equivalence of (1) and (3) in Theorem 8, p is a prime of good reduction of A, so $p \nmid B_A$. □

Remark 10. Equivalently, $\rho_{A,\ell}$ is ramified at exactly the prime divisors of B_A.

Remark 11. Let $A = E_1 \times E_2$ be the product of two elliptic curves E_1 and E_2, with conductors N_{E_1} and N_{E_2}, respectively. It follows from Theorem 8 that A has good reduction at a prime ℓ if and only if E_1 and E_2 both have good reduction at ℓ. Thus, $\mathrm{rad}(B_A) = \mathrm{rad}(\ell N_{E_1} N_{E_2})$.

4.2 | Effective isogeny theorem

In 1968, Serre proved the isogeny theorem for elliptic curves with nonintegral j-invariant [43, p. IV-14]. This was generalized by Faltings for arbitrary abelian varieties [21, Korollar 2, p. 361]. For elliptic curves $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$, the isogeny theorem gives that E_1 and E_2 are $\mathbb{Q}$-isogenous if and only if for each prime $p \nmid N_{E_1} N_{E_2}$, one has that

$$a_p(E_1) = a_p(E_2). \tag{11}$$

Provided that E_1 and E_2 are without complex multiplication and not $\mathbb{Q}$-isogenous, Serre proved in [41, Théorème 21] that under GRH, the least prime number $p \nmid N_{E_1} N_{E_2}$ for which equality in (11) fails to hold satisfies the inequality

$$p \leqslant C_4 (\log \mathrm{rad}(N_{E_1} N_{E_2}))^2 (\log\log \mathrm{rad}(2 N_{E_1} N_{E_2}))^{12}, \tag{12}$$

for some absolute, computable constant C_4. In this section, we improve upon the bound in (12) by removing the "log log" factor.

We begin by offering a refinement of a proposition due to Serre. Serre mentioned his result, without proof, in [44, Note 632.6]. Much later, he communicated an elegant proof that appears in [10, Theorem 4.7]. Our proof builds on the one appearing in [10] by considering a quotient by scalar matrices as in the proof of [41, Théorème 21']. Our bound on the order of G (as below) coincides with Serre's when $\ell = 2$, which is the prime for which we will apply the result in the proof of Theorem 2. However, it does offer an improvement in the case when $\ell \neq 2$, so we find it worthwhile to include it nonetheless.

Proposition 12. *Let ℓ be a prime number and r be a positive integer. Let Γ be a group and $\rho_1, \rho_2 : \Gamma \longrightarrow \mathrm{GL}_r(\mathbb{Z}_\ell)$ be group homomorphisms. Suppose that there is an element $\gamma \in \Gamma$ such that $\mathrm{tr}\,\rho_1(\gamma) \neq \mathrm{tr}\,\rho_2(\gamma)$. Then there exists a quotient G of Γ and a subset $C \subseteq G$ for which*

(1) *the order of G is at most $\frac{\ell^{2r^2}-1}{\ell-1}$,*
(2) *the set C is nonempty and closed under conjugation in G, and*
(3) *if the image in G of an element $\gamma \in \Gamma$ belongs to C, then $\mathrm{tr}\,\rho_1(\gamma) \neq \mathrm{tr}\,\rho_2(\gamma)$.*

Proof. Let $M := \mathrm{Mat}_{r\times r}(\mathbb{Z}_\ell)$ be the $\mathbb{Z}_\ell$-algebra of the $r \times r$ matrices with coefficients in $\mathbb{Z}_\ell$. Let A denote the $\mathbb{Z}_\ell$-algebra generated by the image of Γ under the product map

$$\rho_1 \times \rho_2 : \Gamma \longrightarrow \mathrm{GL}_r(\mathbb{Z}_\ell) \times \mathrm{GL}_r(\mathbb{Z}_\ell).$$

Let G' be the image of Γ under $\rho_1 \times \rho_2$ in $A/\ell A$. Because of the existence of the identity element in Γ, the algebra A contains the set of scalar matrices

$$\Lambda_{2r} := \{(\mu I_r, \mu I_r) : \mu \in \mathbb{Z}_\ell\}.$$

We write H to denote the image of $\Lambda_{2r} \backslash \ell \Lambda_{2r}$ in $A/\ell A$. Then we have the group isomorphism $H \cong \mathbb{Z}/\ell\mathbb{Z}^\times$, as the image of $(\mu I_r, \mu I_r)$ in $A/\ell A$ is determined by the image of μ in $\mathbb{Z}/\ell\mathbb{Z}$. Clearly, $H \cap G'$ is a normal subgroup of G'. Consider the group $G := G'/(H \cap G')$. From the second isomorphism theorem in group theory, we have $G \cong G'H/H$. Since the rank of A as a free $\mathbb{Z}_\ell$-module is at most $2r^2$ and both $G'H$ and H are groups in $A/\ell A$, we obtain the bound

$$|G| = |G'H/H| \leqslant \frac{\ell^{2r^2} - 1}{\ell - 1}.$$

Let m be the largest nonnegative integer such that for each $\gamma \in \Gamma$, one has that

$$\operatorname{tr} \rho_1(\gamma) \equiv \operatorname{tr} \rho_2(\gamma) \pmod{\ell^m}.$$

As A is a $\mathbb{Z}_\ell$-algebra generated by the image of Γ under $\rho_1 \times \rho_2$, it follows that the congruence $\operatorname{tr} x_1 \equiv \operatorname{tr} x_2 \pmod{\ell^m}$ holds for each $(x_1, x_2) \in A$. We obtain the $\mathbb{Z}_\ell$-module homomorphism $\lambda : A \longrightarrow \mathbb{Z}_\ell$ given by

$$\lambda(x_1, x_2) = \ell^{-m}(\operatorname{tr} x_1 - \operatorname{tr} x_2).$$

Since $\lambda(\ell A) \subseteq \ell\mathbb{Z}_\ell$, we may consider the induced $\mathbb{Z}/\ell\mathbb{Z}$-module homomorphism $\bar{\lambda} : A/\ell A \longrightarrow \mathbb{Z}/\ell\mathbb{Z}$.

Let C be the set of elements in G whose preimages in G' all take nonzero values under $\bar{\lambda}$. From the definition of m and the linearity of the trace map, there exists a $\gamma_0 \in \Gamma$ such that

$$\operatorname{tr} \mu\rho_1(\gamma_0) \not\equiv \operatorname{tr} \mu\rho_2(\gamma_0) \pmod{\ell^{m+1}} \quad \forall \mu \in \mathbb{Z}_\ell^\times.$$

Note that the image of $(\rho_1 \times \rho_2)(\gamma_0)$ in G is contained in C, so C is nonempty. Further, C is closed under conjugation because trace is invariant under conjugation. Finally, suppose that $\gamma \in \Gamma$ is such that the image of γ in G is contained in C. Then $\lambda((\rho_1 \times \rho_2)(\gamma)) \notin \ell\mathbb{Z}_\ell$, and, in particular, $\operatorname{tr} \rho_1(\gamma) \neq \operatorname{tr} \rho_2(\gamma)$. □

We now employ the above proposition, together with the effective Chebotarev density theorem in the form of Corollary 6 to give an improvement on the bound in (12), as recorded in Theorem 2.

Proof of Theorem 2. Let $A := E_1 \times E_2$ and apply Proposition 12 with $\ell := 2$, $r := 2$, $\Gamma := \operatorname{Gal}(\mathbb{Q}(A[2^\infty])/\mathbb{Q})$, and $\rho_i := \rho_{E_i,2}$ for each $i = 1, 2$. Let G and C be as in the conclusion of Proposition 12. Let K be a subfield of $\mathbb{Q}(A[2^\infty])$ for which $\operatorname{Gal}(K/\mathbb{Q}) = G$, which exists by the fundamental theorem of infinite Galois theory. From Proposition 12, the size of G is bounded above by 255. Since $\mathbb{Q}(A[2^\infty]) = \bigcup_k \mathbb{Q}(A[2^k])$, it follows that $K \subseteq \mathbb{Q}(A[2^n])$ for some n. Thus, $[K : \mathbb{Q}]$ divides $[\mathbb{Q}(A[2^n]) : \mathbb{Q}]$, which divides $|\operatorname{GL}_2(\mathbb{Z}/2^n\mathbb{Z})|^2 = (6 \cdot 16^{n-1})^2$. One can check that the largest divisor of $(6 \cdot 16^{n-1})^2$ that is at most 255 is 192. Thus, $|G| = [K : \mathbb{Q}] \leqslant 192$.

Applying Corollary 6 with K and C as above and $m := \mathrm{rad}(2N_{E_1}N_{E_2})$, we obtain a prime number p not dividing m such that $(\frac{p}{K/\mathbb{Q}}) \subseteq C$ that satisfies inequality (6). As $\mathrm{Frob}_p\,|_K = (\frac{p}{K/\mathbb{Q}})$, it follows from Proposition 12 that

$$\operatorname{tr}\rho_{E_1,2}(\mathrm{Frob}_p) \neq \operatorname{tr}\rho_{E_2,2}(\mathrm{Frob}_p).$$

Consequently, $a_p(E_1) \neq a_p(E_2)$. It remains to show that p satisfies the claimed bound.

As in the statement of Corollary 6, let $\tilde{K} := K(\sqrt{m})$. We have that

$$[\tilde{K} : \mathbb{Q}] \leqslant 2[K : \mathbb{Q}] \leqslant 2 \cdot 192 = 384.$$

Thus, by Corollary 6,

$$p \leqslant \left(\tilde{a}\log d_{\tilde{K}} + 384\tilde{b} + \tilde{c}\right)^2.$$

where $\tilde{a}, \tilde{b}, \tilde{c}$ are absolute constants that may be taken to be 4, 2.5, and 5, respectively, or may be taken to be the improved values given in [1, Table 3] associated with $\tilde{K}$.

Thus, if $\log d_{\tilde{K}} \leqslant 100$, then by applying Theorem 5 with the constants 4, 2.5, and 5, we find that

$$p \leqslant (4 \cdot 100 + 2.5 \cdot 384 + 5)^2 = 1\,863\,225.$$

If $100 \leqslant \log d_{\tilde{K}} \leqslant 1000$, then by Theorem 5 with improved constants from [1, Table 3], we find that

$$p \leqslant (1.755 \cdot 1000 + 0.23 \cdot 384 + 6.8)^2 = 3\,422\,944.0144.$$

Next, note that for all real numbers $x \geqslant 1000$, we have that

$$1.257x + 7.3 \geqslant a'x + b'd + c'$$

for all (a', b', c') that appears as any entry in the last three rows of [1, Table 3], where d is the maximal degree for the corresponding column (and $d = 384$ for the last column). Thus, if $\log d_{\tilde{K}} \geqslant 1000$, then

$$p \leqslant (1.257\log d_{\tilde{K}} + 7.3)^2. \tag{13}$$

Therefore, in all cases, we have that

$$p \leqslant \max(3\,422\,944.0144, (1.257\log d_{\tilde{K}} + 7.3)^2). \tag{14}$$

We have that by Remark 11, $K/\mathbb{Q}$ is unramified outside of the prime divisors of $m = \mathrm{rad}(2N_{E_1}N_{E_2})$. As $\tilde{K}$ is the compositum of K and $\mathbb{Q}(\sqrt{m})$, the primes that ramify in $\tilde{K}$ are precisely those that ramify in K or in $\mathbb{Q}(\sqrt{m})$. Thus, since $\mathrm{rad}(d_{\mathbb{Q}(\sqrt{m})}) = \mathrm{rad}(2N_{E_1}N_{E_2})$ and $\mathrm{rad}(d_K) \mid \mathrm{rad}(2N_{E_1}N_{E_2})$,

$$\mathrm{rad}\, d_{\tilde{K}} = \mathrm{rad}(d_K d_{\mathbb{Q}(\sqrt{m})}) = \mathrm{rad}(2N_{E_1}N_{E_2}).$$

Hence, by Lemma 7,

$$\log d_{\tilde{K}} \leqslant 383 \log \operatorname{rad}(2N_{E_1}N_{E_2}) + 384 \log(384). \tag{15}$$

Using the trivial inequality $2N_{E_1}N_{E_2} \geqslant 2$, we observe that

$$(1.257(383 \log \operatorname{rad}(2N_{E_1}N_{E_2}) + 384 \log(384)) + 7.3)^2 \geqslant 3\,422\,944.0144. \tag{16}$$

Considering (14)–(16), we conclude that

$$p \leqslant (1.257(383 \log \operatorname{rad}(2N_{E_1}N_{E_2}) + 384 \log(384)) + 7.3)^2.$$

Partially expanding the right-hand side above gives the claimed bound for p. □

Remark 13. In the proof above, for fields $\tilde{K}$ with $\log d_{\tilde{K}} \leqslant 100$, we use the general bound of [1, Theorem 5.1] rather than the improved bounds appearing in Table 3 of [1]. We do so because Table 3 does not give constants in boxes where some combination of degree and discriminant would violate Minkowski's theorem. This only affects certain entries in the table for which the logarithm of the absolute value of the discriminant is less than 100. For example, the maximal totally real subfield of $\mathbb{Q}(\zeta_7)$ has degree 3 and discriminant 49, yet the table gives no constants for number fields with degree 3–4 for which the logarithm of the absolute value of the discriminant is less than 5.

5 | A BOUND ON THE LARGEST NONSURJECTIVE PRIME

We begin in §5.1 with some necessary background on quadratic Galois characters and quadratic twists of elliptic curves. In §5.2, we put together the pieces to complete the proof of Theorem 1. Finally, we present a numerical example in §5.3 that illustrates the theorem.

5.1 | Quadratic twists

By a *quadratic Galois character*, we mean a surjective group homomorphism

$$\chi : \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \{\pm 1\}.$$

Since $\ker \chi$ is an index two subgroup of $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, there exists a nonzero squarefree integer D such that $\ker \chi = \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{D}))$. Consequently, χ factors through $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})/\ker \chi \cong \operatorname{Gal}(\mathbb{Q}(\sqrt{D})/\mathbb{Q})$,

$$\begin{array}{ccc} \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \xrightarrow{\quad\chi\quad} & \{\pm 1\} \\ & {\scriptstyle \operatorname{res}_D} \searrow \quad \nearrow {\scriptstyle \sim} & \\ & \operatorname{Gal}(\mathbb{Q}(\sqrt{D})/\mathbb{Q}) & \end{array}$$

where res_D denotes the restriction homomorphism. Thus, for each $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$,

$$\chi(\sigma) = \begin{cases} 1 & \sigma(\sqrt{D}) = \sqrt{D} \\ -1 & \sigma(\sqrt{D}) = -\sqrt{D}. \end{cases} \tag{17}$$

We write χ_D to denote the quadratic Galois character described by (17). Note that each quadratic Galois character may be written as χ_D for a unique squarefree integer D.

For a prime number p, let I_p and $I_p(D)$ denote the inertia subgroups of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $\mathrm{Gal}(\mathbb{Q}(\sqrt{D})/\mathbb{Q})$, respectively. One says that χ_D is *unramified* at p if $I_p \subseteq \ker \chi_D$. From the description of χ_D given in (17) and upon noting that $\mathrm{res}_D(I_p) = I_p(D)$, we see that

$$\chi_D \text{ is unramified at } p \iff \mathbb{Q}(\sqrt{D})/\mathbb{Q} \text{ is unramified at } p. \tag{18}$$

If $p \nmid D$, then $(\frac{p}{\mathbb{Q}(\sqrt{D})/\mathbb{Q}})(\sqrt{D}) = (\frac{D}{p})\sqrt{D}$ by [29, p. 88], where $(\frac{D}{p})$ denotes the Legendre symbol of D with respect to p. Thus, from (17), we have that

$$\chi_D\left(\left(\frac{p}{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}\right)\right) = \left(\frac{D}{p}\right). \tag{19}$$

Now consider an elliptic curve $E/\mathbb{Q}$ given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{20}$$

The *quadratic twist* of E by χ_D (or, equivalently, by D) is the elliptic curve $E_D/\mathbb{Q}$ given by

$$y^2 + a_1xy + a_3y = x^3 + \left(a_2D + a_1^2\frac{D-1}{4}\right)x^2 + \left(a_4D^2 + a_1a_3\frac{D^2-1}{2}\right)x + a_6D^3 + a_3^2\frac{D^3-1}{4}. \tag{21}$$

See [13, §4.3] or [46, X.2] for background on quadratic twists. By taking (20) to be a minimal model for E, upon computing and comparing the discriminants of (20) and (21), we find that

$$\mathrm{rad}(N_{E_D}) \quad \text{divides} \quad \mathrm{rad}(2DN_E). \tag{22}$$

Further, if p is a prime number such that $p \nmid 2DN_E$, then by [51, Exercise 4.10] and (19),

$$a_p(E) = \chi_D(\mathrm{Frob}_p)a_p(E_D). \tag{23}$$

We conclude with a lemma about nontrivial quadratic twists (see, e.g., [41, p. 199]).

Lemma 14. *If $D \neq 1$ is squarefree and $E/\mathbb{Q}$ is without complex multiplication, then E and E_D are not $\mathbb{Q}$-isogenous.*

Proof. We know from the Chebotarev density theorem that the natural density of primes p for which $\chi_D(\mathrm{Frob}_p) = -1$ is $\frac{1}{2}$. For such a p, if $p \nmid 2DN_E$, then $a_p(E) = -a_p(E_D)$ by (23). Thus, either $a_p(E) \neq a_p(E_D)$ or $a_p(E) = 0$. The density of primes p for which $p \nmid 2DN_E$ and $a_p(E) = 0$ is 0 by

[41, p. 123] and [20, p. 131]. Thus, there exists a prime $p \nmid 2DN_E$ such that $a_p(E) \neq a_p(E_D)$. As such, E and E_D are not $\mathbb{Q}$-isogenous. □

5.2 | Completing the proof

We now turn to the problem of bounding $c(E)$. Suppose that ℓ is an odd prime such that $G_E(\ell)$ satisfies (5) of Proposition 3. With an appropriate choice of $\mathbb{F}_\ell$-basis of $E[\ell]$ in defining $\bar{\rho}_{E,\ell}$, we may assume that $G_E(\ell) \subseteq \mathcal{C}_{ns}^+(\ell)$ and $G_E(\ell) \nsubseteq \mathcal{C}_{ns}(\ell)$. Following Serre, we consider the quadratic Galois character given by the composition

$$\epsilon_\ell : \ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\bar{\rho}_{E,\ell}} G_E(\ell) \longrightarrow \frac{\mathcal{C}_{ns}^+(\ell)}{\mathcal{C}_{ns}(\ell)} \xrightarrow{\sim} \{\pm 1\}. \tag{24}$$

We list some basic properties of ϵ_ℓ, which are previously noted in [40, p. 317] and [12, p. 18].

Lemma 15. *With the above notation and assumptions, ϵ_ℓ satisfies the following properties.*

(1) *For each prime $p \nmid N_E$, ϵ_ℓ is unramified at p.*
(2) *One has that $\epsilon_\ell = \chi_D$ for some integer $D \mid N_E$.*
(3) *For each prime $p \nmid N_E$, if $\epsilon_\ell(\mathrm{Frob}_p) = -1$, then $a_p(E) \equiv 0 \pmod{\ell}$.*

Proof.

(1) If $p \nmid \ell N_E$, then by Remark 10, $\rho_{E,\ell}$ is unramified at p. In particular, ϵ_ℓ is unramified at p. When $\ell \nmid N_E$ and $p = \ell$, the claimed property follows by a more delicate analysis; see [40, p. 295, Lemme 2].
(2) Let D be the squarefree integer such that $\epsilon_\ell = \chi_D$. It follows from the previous part and (18) that $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ is unramified outside of the prime divisors of N_E. Thus, $D \mid N_E$.
(3) For $p \nmid N_E$, since $\epsilon_\ell(\mathrm{Frob}_p) = -1$, we have that $\bar{\rho}_{E,\ell}(\mathrm{Frob}_p) \in \mathcal{C}_{ns}^+(\ell) \setminus \mathcal{C}_{ns}(\ell)$. From Equation (3), we see that $\mathrm{tr}\,\gamma = 0$ for each $\gamma \in \mathcal{C}_{ns}^+(\ell) \setminus \mathcal{C}_{ns}(\ell)$. Thus, $a_p(E) \equiv \mathrm{tr}(\bar{\rho}_{E,\ell}(\mathrm{Frob}_p)) \equiv 0 \pmod{\ell}$. □

We are now in a position to prove the main theorem.

Proof of Theorem 1. Let ℓ be a prime number such that $\ell > 37$ and $\bar{\rho}_{E,\ell}$ is nonsurjective. By Theorem 4, we know that up to conjugation, $G_E(\ell) \subseteq \mathcal{C}_{ns}^+(\ell)$ yet $G_E(\ell) \nsubseteq \mathcal{C}_{ns}(\ell)$. Consider the quadratic Galois character ϵ_ℓ defined in (24). Let D be the squarefree integer such that $\epsilon_\ell = \chi_D$ and consider the quadratic twist E_D of E. By Lemma 15(2) and (22), we have that

$$\mathrm{rad}(N_{E_D}) \quad \text{divides} \quad \mathrm{rad}(2N_E). \tag{25}$$

For each prime number $p \nmid 2N_E$, by (23), we have that

$$a_p(E) = \epsilon_\ell(\mathrm{Frob}_p) a_p(E_D). \tag{26}$$

By Lemma 14, E and E_D are not $\mathbb{Q}$-isogenous. Thus, there exists a prime number $p \nmid 2N_E$ such that

$$a_p(E) \neq a_p(E_D). \tag{27}$$

Let p_0 be the least prime number such that $p_0 \nmid 2N_E$ and the inequality (27) holds. Applying Theorem 2 to E and E_D and noting (25), we find that

$$p_0 \leqslant (482 \log \operatorname{rad}(2N_E) + 2880)^2.$$

Considering (26) and (27), we see that $\epsilon_\ell(\mathrm{Frob}_{p_0}) = -1$. Thus, by Lemma 15(3), ℓ divides $a_{p_0}(E)$, and so $\ell \leqslant |a_{p_0}(E)|$. The Hasse bound [46, Theorem V.1.1] gives that $|a_{p_0}(E)| \leqslant 2\sqrt{p_0}$. Thus,

$$\ell \leqslant 2\sqrt{p_0} \leqslant 2(482 \log \operatorname{rad}(2N_E) + 2880).$$

Expanding the right-hand side, one obtains the claimed bound. □

5.3 | An example

We illustrate Theorem 1 with a concrete example. Consider the elliptic curve $E/\mathbb{Q}$ with LMFDB [31] label `76204800.ut1`, given by the Weierstrass equation

$$y^2 = x^3 - 198450x - 27\,783\,000.$$

This elliptic curve is without complex multiplication and has conductor

$$N_E = 76204\,800 = 2^8 \cdot 3^5 \cdot 5^2 \cdot 7^2.$$

Assuming the GRH, Theorem 1 tells us that

$$c(E) \leqslant 964 \log(2 \cdot 3 \cdot 5 \cdot 7) + 5760 \approx 10914.61.$$

In about one second total, SageMath's [50] built-in `is_surjective` command confirms that $\bar{\rho}_{E,\ell}$ is surjective for each prime number $\ell \leqslant 10\,915$. Thus, conditional on GRH, $\bar{\rho}_{E,\ell}$ is surjective for all primes ℓ. Calling Zywina's `ExceptionalSet` script [54] on E confirms this unconditionally.

ACKNOWLEDGMENTS

This paper emerged following a series of talks on the effective version of Serre's open image theorem in the Graduate Number Theory Seminar at the University of Illinois Chicago in Spring 2021. Thus, we are thankful to all of the members of the seminar. In addition, we thank Nathan Jones and Sung Min Lee for their helpful comments on an earlier draft of the paper. Further, we thank Jonathan Sorenson for his kind and valuable email response relating to Remark 13. Lastly, we thank the referee for carefully reading our paper and providing several helpful comments.

JOURNAL INFORMATION

The *Bulletin of the London Mathematical Society* is wholly owned and managed by the London Mathematical Society, a not-for-profit Charity registered with the UK Charity Commission. All surplus income from its publishing programme is used to support mathematicians and mathematics research in the form of research grants, conference grants, prizes, initiatives for early career researchers and the promotion of mathematics.

ORCID

Jacob Mayle https://orcid.org/0000-0002-9312-6774
Tian Wang https://orcid.org/0000-0003-2511-1842

REFERENCES

1. E. Bach and J. Sorenson, *Explicit bounds for primes in residue classes*, Math. Comp. **65** (1996), no. 216, 1717–1735. MR 1355006.
2. J. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk, *Explicit Chabauty-Kim for the split Cartan modular curve of level 13*, Ann. of Math. (2) **189** (2019), no. 3, 885–944. MR 3961086
3. B. S. Banwait, *Explicit isogenies of prime degree over quadratic fields*, Int. Math. Res. Not. IMRN **2023** (2023), 1–48.
4. B. S. Banwait, F. Najman, and O. Padurariu, *Cyclic isogenies of elliptic curves over fixed quadratic fields*, arXiv:2206.08891, 2022.
5. N. Billerey and L. V. Dieulefait, *Explicit large image theorems for modular forms*, J. London Math. Soc. (2) **89** (2014), no. 2, 499–523. MR 3188630
6. Y. Bilu, P. Parent, and M. Rebolledo, *Rational points on $X_0^+(p^r)$*, Ann. Inst. Fourier (Grenoble) **63** (2013), no. 3, 957–984. MR 3137477
7. G. Boxer, F. Calegari, T. Gee, and V. Pilloni, *Abelian surfaces over totally real fields are potentially modular*, Publ. Math. Inst. Hautes Études Sci. **134** (2021), 153–501. MR 4349242
8. C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* **Q***: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939. MR 1839918
9. A. Brumer, A. Pacetti, C. Poor, G. Tornaría, J. Voight, and D. S. Yuen, *On the paramodularity of typical abelian surfaces*, Algebra Number Theory **13** (2019), no. 5, 1145–1195. MR 3981316
10. A. Bucur and K. S. Kedlaya, *An application of the effective Sato-Tate conjecture*, Frobenius distributions: Lang-Trotter and Sato-Tate conjectures, Contemp. Math., vol. 663, Amer. Math. Soc., Providence, RI, 2016, pp. 45–56. MR 3502938
11. A. Caraiani and J. Newton, *On the modularity of elliptic curves over imaginary quadratic fields*, 2023.
12. A. C. 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. MR 2118760
13. I. Connell, *Elliptic curve handbook*, 1999. Online notes.
14. J. Cremona and A. Pacetti, *On elliptic curves of prime power conductor over imaginary quadratic fields with class number 1*, Proc. London Math. Soc. (3) **118** (2019), no. 5, 1245–1276. MR 3946721
15. S. Cynk, M. Schütt, and D. van Straten, *Hilbert modularity of some double octic Calabi-Yau threefolds*, J. Number Theory **210** (2020), 313–332. MR 4057530
16. A. David, *Borne uniforme pour les homothéties dans l'image de Galois associée aux courbes elliptiques*, J. Number Theory **131** (2011), no. 11, 2175–2191. MR 2825121
17. L. E. Dickson, *Linear groups: with an exposition of the Galois field theory*, Dover Publications, Inc., New York, 1958. With an introduction by W. Magnus. MR 0104735
18. L. Dieulefait, L. Guerberoff, and A. Pacetti, *Proving modularity for a given elliptic curve over an imaginary quadratic field*, Math. Comp. **79** (2010), no. 270, 1145–1170. MR 2600560
19. L. Dieulefait, A. Pacetti, and M. Schütt, *Modularity of the Consani-Scholten quintic*, Doc. Math. **17** (2012), 953–987. With an appendix by José Burgos Gil and Pacetti. MR 3007681
20. N. D. Elkies, *Distribution of supersingular primes*, Journées Arithmétiques, 1989 (Luminy, 1989), no. 198–200, 1991, pp. 127–132. MR 1144318

21. G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366. MR 718935
22. M. Harris, D. Soudry, and R. Taylor, *l-adic representations associated to modular forms over imaginary quadratic fields. I. Lifting to* $\mathrm{GSp}_4(\mathbf{Q})$, Invent. Math. **112** (1993), no. 2, 377–411. MR 1213108
23. A. Kraus, *Une remarque sur les points de torsion des courbes elliptiques*, C. R. Acad. Sci. Paris Sér. I Math. **321** (1995), no. 9, 1143–1146. MR 1360773
24. J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, Algebraic number fields: *L*-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977, pp. 409–464. MR 0447191
25. S. Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer, New York, 2002. MR 1878556
26. E. Larson and D. Vaintrob, *Determinants of subquotients of Galois representations associated with abelian varieties*, J. Inst. Math. Jussieu **13** (2014), no. 3, 517–559. With an appendix by Brian Conrad. MR 3211798
27. E. Larson and D. Vaintrob, *On the surjectivity of Galois representations associated to elliptic curves over number fields*, Bull. London Math. Soc. **46** (2014), no. 1, 197–209. MR 3161774
28. S. Le Fourn, *Surjectivity of Galois representations associated with quadratic* $\mathbb{Q}$*-curves*, Math. Ann. **365** (2016), no. 1–2, 173–214. MR 3498908
29. F. Lemmermeyer, *Reciprocity laws*, Springer Monographs in Mathematics, Springer, Berlin, 2000. From Euler to Eisenstein. MR 1761696
30. P. Lemos, *Some cases of Serre's uniformity problem*, Math. Z. **292** (2019), no. 1–2, 739–762. MR 3968924
31. The LMFDB Collaboration, *The L-functions and modular forms database*, http://www.lmfdb.org, 2022 [Online; accessed 12 April 2023].
32. D. Lombardo, *Bounds for Serre's open image theorem for elliptic curves over number fields*, Algebra Number Theory **9** (2015), no. 10, 2347–2395. MR 3437765
33. D. Masser and G. Wüstholz, *Galois properties of division fields of elliptic curves*, Bull. London Math. Soc. **25** (1993), no. 3, 247–254. MR 1209248
34. B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162. MR 482230
35. F. Momose, *Isogenies of prime degree over number fields*, Compositio Math. **97** (1995), no. 3, 329–348. MR 1353278
36. J. Neukirch, *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. MR 1697859
37. J. Oesterlé, *Versions effectives du théoreme de Chebotarev sous l'hypothese de Riemann généralisée*, Astérisque **61** (1979), 165–167. MR 4432522
38. B. Peaucelle, *Explicit small image theorems for residual modular representations*, Int. J. Number Theory **18** (2022), no. 5, 1143–1202. MR 4432522
39. F. Pellarin, *Sur une majoration explicite pour un degré d'isogénie liant deux courbes elliptiques*, Acta Arith. **100** (2001), no. 3, 203–243. MR 1865384
40. J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331. MR 387283
41. J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. (1981), no. 54, 323–401. MR 644559
42. J.-P. Serre, *Lectures on the Mordell-Weil theorem*, Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997, Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre. MR 1757192
43. J.-P. Serre, *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. MR 1484415
44. J.-P. Serre, *Oeuvres/Collected papers. III. 1972–1984*, Springer Collected Works in Mathematics, Springer, Heidelberg, 2013. Reprint of the 2003 edition [of the 1986 original MR0926691]. MR 3223094
45. J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517. MR 236190
46. J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR 2514094

47. A. V. Sutherland, *Computing images of Galois representations attached to elliptic curves*, Forum Math. Sigma **4** (2016), Paper No. e4, 79. MR 3482279
48. R. Taylor, *l-adic representations associated to modular forms over imaginary quadratic fields. II*, Invent. Math. **116** (1994), no. 1–3, 619–643. MR 1253207
49. R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), no. 3, 553–572. MR 1333036
50. The Sage Developers, *Sagemath, the Sage Mathematics Software System (Version 9.7)*, 2023. https://www.sagemath.org.
51. L. C. Washington, *Elliptic curves*, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2003. Number theory and cryptography. MR 1989729
52. A. Wiles, *Modular forms, elliptic curves, and Fermat's last theorem*, Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Zürich, 1994), Birkhäuser, Basel, 1995, pp. 243–245. MR 1403925
53. D. Zywina, *On the possible images of the mod ℓ* representations associated to elliptic curves over $\mathbb{Q}$, arXiv:1508.07660, 2015.
54. D. Zywina, *On the surjectivity of* mod ℓ *representations associated to elliptic curves*, Bull. London Math. Soc. **54** (2022), no. 6, 2404–2417. MR 4549128