This is a ``preproof'' accepted article for *Canadian Mathematical Bulletin*
This version may be subject to change during the production process.
DOI: 10.4153/S0008439525101173

IMPROVED BOUNDS FOR SERRE'S OPEN IMAGE THEOREM

IMIN CHEN AND JOSHUA SWIDINSKY

Abstract. Let E be an elliptic curve over the rationals which does not have complex multiplication. Serre showed that the adelic representation attached to $E/\mathbb{Q}$ has open image, and in particular there is a minimal natural number C_E such that the mod ℓ representation $\bar{\rho}_{E,\ell}$ is surjective for any prime $\ell > C_E$. Assuming the Generalized Riemann Hypothesis, Mayle-Wang gave explicit bounds for C_E which are logarithmic in the conductor of E and have explicit constants. The method is based on using effective forms of the Chebotarev density theorem together with the Faltings-Serre method, in particular, using the 'deviation group' of the 2-adic representations attached to two elliptic curves.

By considering quotients of the deviation group and a characterization of the images of the 2-adic representation $\rho_{E,2}$ by Rouse and Zureick-Brown, we show in this paper how to further reduce the constants in Mayle-Wang's results. Another result of independent interest are improved effective isogeny theorems for elliptic curves over the rationals.

1. Introduction

Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication. Serre showed in [15] that the adelic representation attached to $E/\mathbb{Q}$ has open image, in particular, there is a minimal natural number C_E such that the mod ℓ representation $\bar{\rho}_{E,\ell}$ is surjective for any prime $\ell > C_E$.

In determining effective bounds on C_E, one typically uses effective versions of the Chebotarev density theorem under the assumption of the Generalized Riemann Hypothesis (GRH) as was first done by Serre. The bounds on C_E usually depend on the radical $\mathrm{rad}(N_E)$ of the conductor N_E of E over $\mathbb{Q}$. In Serre's original treatment [16], the following theorem was shown. By GRH, we mean the conjecture which applies to the Artin L-functions of Galois extensions L/K where L and K are number fields.

Theorem 1.1. [16, Theorem 21] *Assume GRH. Let E and E' be two elliptic curves defined over $\mathbb{Q}$. Suppose that E and E' are not $\mathbb{Q}$-isogenous. Then there exists a prime p of good reduction for E and E' such that $a_p(E) \neq a_p(E')$ and satisfying the inequality*

$$p \leq C_1(\log \mathrm{rad}(N_E N_{E'}))^2(\log\log \mathrm{rad}(2N_E N_{E'}))^{12}, \tag{1.1}$$

where C_1 is an absolute constant.

Based on the method used, the constant C_1 here is unfortunately rather large. Recent work of Mayle-Wang [10] has given an explicit result on the smallest prime which achieves $a_p(E) \neq a_p(E')$. The constants are quite small, and like Serre's result, depend on only knowledge of the primes of bad reduction of the two elliptic curves E and E'.

Date: August 25, 2025.
2020 *Mathematics Subject Classification.* 11G05, 11F80.

Theorem 1.2. [10, Theorem 2] *Assume GRH. Let E and E' be two elliptic curves over $\mathbb{Q}$ without complex multiplication. Suppose E and E' are not $\mathbb{Q}$-isogenous. Then there exists a prime p of good reduction for E and E' such that $a_p(E) \neq a_p(E')$ and satisfying the inequality*

$$p \leq (482 \log \operatorname{rad}(2N_E N_{E'}) + 2880)^2, \tag{1.2}$$

where N_E and $N_{E'}$ denote the conductors of E and E', respectively.

The method is based on using effective forms of the Chebotarev density theorem together with the Faltings-Serre method, in particular, by studying the 'deviation group' $\delta(G)$ of the 2-adic representations attached to two elliptic curves.

In our work, we explain how to replace $\delta(G)$ with smaller quotients in Mayle-Wang's original arguments. Using these smaller quotients allows us to prove an improved effective isogeny theorem for elliptic curves over $\mathbb{Q}$ with a certain condition on the mod 2 representations.

Theorem 1.3. *Assume GRH. Let E and E' be two elliptic curves over $\mathbb{Q}$. Suppose E and E' are not $\mathbb{Q}$-isogenous. Assume the mod 2 representations $\bar{\rho}_{E,2}$ and $\bar{\rho}_{E',2}$ are not isomorphic, or if they are isomorphic that they are absolutely irreducible. Then there exists a prime p of good reduction for E and E' such that $a_p(E) \neq a_p(E')$ and satisfying the inequality*

$$p \leq (124 \log \operatorname{rad}(2N_E N_{E'}) + 561)^2. \tag{1.3}$$

Remark 1.4. Mayle-Wang, in Theorem 1.2, include a hypothesis that the elliptic curves E and E' be without complex multiplication; in Proposition 5.1 and Theorem 1.3, we have dropped this assumption. All we require here is the existence of a prime of good reduction such that $a_p(E) \neq a_p(E')$, which is satisfied once we assume the two elliptic curves are not $\mathbb{Q}$-isogenous, a consequence of Faltings' Theorem [7] (see translation in [6]).

The representation $\bar{\rho}_{E,\ell}$ is absolutely irreducible if and only if its image does not lies in a non-split Cartan subgroup or a Borel subgroup. In the case of $\ell = 2$, $\bar{\rho}_{E,\ell}$ is absolutely irreducible if and only if it is surjective.

We also prove another improved effective isogeny theorem which applies for elliptic curves over $\mathbb{Q}$ which are quadratic twists of each other and do not have complex multiplication.

Theorem 1.5. *Assume GRH. Let E and E' be two elliptic curves over $\mathbb{Q}$ which are quadratic twists of each other and do not have complex multiplication. In addition, assume $\bar{\rho}_{E,2}$ is irreducible and the image of $\rho_{E,2}$ contains $-I$. Suppose E and E' are not $\mathbb{Q}$-isogenous. Then there exists a prime p of good reduction for E and E' such that $a_p(E) \neq a_p(E')$ and satisfying the inequality*

$$p \leq (124 \log \operatorname{rad}(2N_E N_{E'}) + 561)^2. \tag{1.4}$$

This version requires the results of Rouse and Zureick-Brown [13] which characterizes the images of the 2-adic representations attached to an elliptic curve over $\mathbb{Q}$.

Using Theorem 1.2, Mayle-Wang [10, Theorem 1] prove the following bound for Serre's open image theorem.

Theorem 1.6. *Assume GRH. Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication. Then*

$$C_E \leq 964 \log \operatorname{rad}(2N_E) + 5760.$$

https://doi.org/10.4153/S0008439525101173 Published online by Cambridge University Press

A consequence of our improved effective isogeny Theorems 1.3 and 1.5 is an improvement in the constants for Serre's open image theorem.

Theorem 1.7. *Assume GRH. Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication. Then*

$$C_E \leq 248 \log \operatorname{rad}(2N_E) + 1122.$$

The `Magma` computational algebra system [2] was used for verifying assertions in this paper. The electronic resources are available from

https://github.com/ichensfuca/ChenSwidinsky.

Acknowledgements

We thank the anonymous referee for useful comments and suggestions which improved the constants in Theorem 1.7 and computational efficiency of the verifications.

2. Explicit forms of the Chebotarev density theorem

Let L/K be a finite Galois extension with Galois group G. Define the counting function $\pi_C(x, L/K)$, for a conjugacy class C of the Galois group G of L/K, to be the function

$$\pi_C(x, L/K) = \left| \left\{ \mathfrak{p} \text{ a prime of } K \mid \mathfrak{p} \text{ unramified in } L/K, \left(\frac{L/K}{\mathfrak{p}}\right) = C, \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}) \leq x \right\} \right|,$$

where for a prime $\mathfrak{p}$ of K unramified in L/K, the notation

$$\left(\frac{L/K}{\mathfrak{p}}\right) \tag{2.1}$$

denotes the Artin symbol which gives the Frobenius conjugacy class at $\mathfrak{p}$ in G.

Theorem 2.1 (Chebotarev Density Theorem)**.** *Let $\pi_C(x, L/K)$ be as above. Then,*

$$\pi_C(x, L/K) \sim \frac{|C|}{|G|} \operatorname{Li}(x),$$

Effective versions of Chebotarev's Density Theorem exist as well and we shall be applying results in which the constants are explicitly computable in terms of the absolute discriminant d_L of L as well as the degree n_L of L over $\mathbb{Q}$. The first of these was given by Lagarias and Odlyzko [8]. Their result relies on the validity of GRH.

We now state the first explicit form of Theorem 2.1.

Theorem 2.2. [8, Theorem 1.1] *There exists an effectively computable positive absolute constant c_1 such that if GRH holds for the Dedekind zeta function of L, then for every $x \geq 2$,*

$$\left| \pi_C(x, L/K) - \frac{|C|}{|G|} \operatorname{Li}(x) \right| \leq c_1 \left(\frac{|C|}{|G|} x^{1/2} \log(|d_L| x^{n_L}) + \log |d_L| \right).$$

An important corollary, one that we shall make use of, is finding an x_0 such that $\pi_C(x_0, L/K) > 0$.

https://doi.org/10.4153/S0008439525101173 Published online by Cambridge University Press

Corollary 2.3. [8, Corollary 1.2] *There exists an effectively computable positive absolute constant c_2 such that if GRH holds for the Artin L-functions of $L/\mathbb{Q}$, $L \neq \mathbb{Q}$, then for every conjugacy class C of G there exists a prime ideal $\mathfrak{p}$ of K unramified in $L/\mathbb{Q}$ such that*

$$\left(\frac{L/K}{\mathfrak{p}}\right) = C$$

and

$$N_{K/\mathbb{Q}}(\mathfrak{p}) \leq c_2(\log|d_L|)^2(\log\log|d_L|)^4.$$

If $L = \mathbb{Q}$, then $\mathfrak{p} = (2)$ is a solution.

The above is a non-nullity result about $\pi_C(x, L/K)$; it asserts the size of x we must take to ensure that $\pi_C(x, L/K)$ is nonzero, that is, there is some unramified prime ideal $\mathfrak{p}$ of K whose Artin symbol hits C and with norm smaller than x.

Theorem 2.4. [11, Théorème 4] *There exists an effectively computable positive absolute constant c_3 such that if GRH and Artin's Conjecture (AC) hold for the Artin L-functions of $L/\mathbb{Q}$, $L \neq \mathbb{Q}$, then for every conjugacy class C of G, we have that*

$$\pi_C(x, L/K) \geq 1$$

for all $x \geq 2$ such that $x \geq c_3(\log|d_L|)^2$.

Oesterlé [11, Théorème 4] finds that $c_3 = 70$, although his proof was seemingly never published. An improvement to Lagarias and Odlyzko is given by Bach-Sorenson [1]:

Theorem 2.5. [1, Theorem 5.1] *Assume GRH. Let $K/\mathbb{Q}$ be a Galois extension of number fields, with $K \neq \mathbb{Q}$. Let d_K denote the discriminant of K. Let n_K denote the degree of K. Let $C \subseteq \mathrm{Gal}(K/\mathbb{Q})$ be a nonempty subset closed under conjugation. Then, there is a prime p of $\mathbb{Q}$ unramified in $K/\mathbb{Q}$ with*

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

satisfying

$$p \leq (a\log|d_K| + bn_K + c)^2$$

for some triple (a, b, c) taken from [1, Table 3] *according to the quantities $\log|d_K|$ and n_K. We may take $a = 4$, $b = 2.5$, and $c = 5$ to cover all cases of $\log|d_K|$ and $n_K = [K : \mathbb{Q}]$.*

A corollary to the above is given in Mayle-Wang [10, Corollary 6] when we need to pick the prime p to be coprime to a given positive integer m.

Corollary 2.6. [10, Corollary 6] *Assume GRH. Let $K/\mathbb{Q}$ be a Galois extension of number fields, with $K \neq \mathbb{Q}$. Let m be a positive integer, and set $\tilde{K} = K(\sqrt{m})$. Denote $d_{\tilde{K}}$ to be the absolute value of the discriminant of $\tilde{K}$. Let $n_{\tilde{K}}$ denote the degree of $\tilde{K}$. 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 $K/\mathbb{Q}$ with $\left(\frac{K/\mathbb{Q}}{p}\right) \subseteq C$ and satisfying*

$$p \leq (\tilde{a}\log|d_{\tilde{K}}| + \tilde{b}n_{\tilde{K}} + \tilde{c})^2,$$

for some triple $(\tilde{a}, \tilde{b}, \tilde{c})$ taken from [1, Table 3] *according to the quantities $\log|d_{\tilde{K}}|$ and $n_{\tilde{K}}$. We may take $\tilde{a} = 4$, $\tilde{b} = 2.5$, and $\tilde{c} = 5$ to cover all cases of $\log|d_{\tilde{K}}|$ and $n_{\tilde{K}} = [\tilde{K} : \mathbb{Q}]$.*

https://doi.org/10.4153/S0008439525101173 Published online by Cambridge University Press

$n_{\tilde{K}}$	$(\bar{a}, \bar{b}, \bar{c})$
2	$(1.446, 0.23, 6.8)$
3-4	$(1.527, 0.17, 6.4)$
5-9	$(1.629, 0.11, 6.1)$
10-14	$(1.667, 0.09, 6.0)$
15-49	$(1.745, 0.04, 5.8)$
50-128	$(1.755, 0, 5.7)$

TABLE 1. Triples $(\bar{a}, \bar{b}, \bar{c})$ as appearing in Proposition 2.7.

For a fixed n_K, we say a triple (a, b, c) is bigger than a triple (a', b', c') (resp. a triple (a', b', c') is smaller than a triple (a, b, c)) if

$$(a' \log |d_K| + b' n_K + c')^2 \leq (a \log |d_K| + b n_K + c)^2$$

for all values of $\log |d_K|$ in a row of [1, Table 3].

We give our own version of Theorem 2.5 and Corollary 2.6. The idea is to collapse [1, Table 3] into a 1-dimensional table, removing the condition on $\log |d_{\tilde{K}}|$ so that each triple is valid for a range of $n_{\tilde{K}}$. We do this by picking a "pivot" triple for each column, for which all triples appearing before the pivot are absorbed into a special constant $p_0(n_{\tilde{K}})$, and all triples appearing after are checked to be smaller than the pivot triple.

The pivot triple in each column of [1, Table 3] is chosen to be the first one so that (2.4) holds.

Proposition 2.7. *Assume GRH. Let $K/\mathbb{Q}$ be a Galois extension of number fields with $K \neq \mathbb{Q}$. Let m be a positive integer, and set $\tilde{K} = K(\sqrt{m})$. Denote $d_{\tilde{K}}$ to be the discriminant of $\tilde{K}$. Let $n_{\tilde{K}}$ denote the degree of $\tilde{K}/\mathbb{Q}$. Let $C \subseteq \mathrm{Gal}(K/\mathbb{Q})$ be a nonempty subset that is closed under conjugation. Then there exists a triple $(\bar{a}, \bar{b}, \bar{c})$ taken from Table 1, a special constant $p_0(n_{\tilde{K}})$, and a prime number p not dividing m that is unramified in $K/\mathbb{Q}$ with $\left(\frac{K/\mathbb{Q}}{p}\right) \subseteq C$ and satisfying*

$$p \leq \max((\bar{a} \log |d_{\tilde{K}}| + \bar{b} n_{\tilde{K}} + \bar{c})^2, p_0(n_{\tilde{K}})) \tag{2.2}$$

$$\leq (\bar{a} \cdot ((n_0 - 1) \log \mathrm{rad}(d_{\tilde{K}}) + n_0 \log n_0) + \bar{b} \cdot n_0 + \bar{c})^2, \tag{2.3}$$

where $n_0 = \max(72, n_{\tilde{K}})$. If we only have an upper bound for $n_{\tilde{K}} \leq n_1$, then we have to replace each of $\bar{a}, \bar{b}, \bar{c}$ with the maximum of their values over entries in Table 1 with $n_{\tilde{K}} \leq n_1$, respectively, and n_0 with $\max(72, n_1)$.

Proof. We have written a program in `Magma` which verifies the required inequalities (2.2). For inequality (2.3), there are two parts to check. The program checks that

$$p_0(n_{\tilde{K}}) \leq (\bar{a} \cdot ((n_0 - 1) \log 2 + n_0 \log n_0) + \bar{b} \cdot n_0 + \bar{c})^2, \tag{2.4}$$

and the inequality

$$(\bar{a} \log |d_{\tilde{K}}| + \bar{b} n_{\tilde{K}} + \bar{c})^2 \leq (\bar{a} \cdot ((n_0 - 1) \log \mathrm{rad}(d_{\tilde{K}}) + n_0 \log n_0) + \bar{b} \cdot n_0 + \bar{c})^2 \tag{2.5}$$

follows from Lemma 2.8. □

https://doi.org/10.4153/S0008439525101173 Published online by Cambridge University Press

Lemma 2.8. [10, Lemma 7] *If $K/\mathbb{Q}$ is a nontrivial finite Galois extension, then*

$$\left(\frac{1}{2}\log 3\right)[K:\mathbb{Q}] \leq \log|d_K| \leq ([K:\mathbb{Q}]-1)\log \mathrm{rad}(d_K) + [K:\mathbb{Q}]\log([K:\mathbb{Q}]),$$

where d_K is the absolute value of the discriminant of K.

3. The deviation group $\delta(G)$

In this section, we wish to construct a finite group, called the *deviation group*, denoted $\delta(G)$, from which we can find a finite subset that will determine if the two representations are isomorphic or not.

Our treatment of the deviation group will follow the exposition given in Ignasi's thesis [12]. We note that Ignasi's exposition is, itself, taken from Chênevert's thesis [5], whose work follows the work of Serre [17] (the propositions and lemmas which appear here, with the exception of Lemma 3.8, can also be found in [5, Chapter 5]).

Let G be a group, and L be a finite extension of $\mathbb{Q}_\ell$, for ℓ prime, with ring of integers $\mathcal{O}_\lambda$, maximal ideal λ, and residue field $k = \mathcal{O}_\lambda/\lambda\mathcal{O}_\lambda$. We let π be a uniformizer, so $\lambda = \pi\mathcal{O}_\lambda$. Let $\rho_1, \rho_2 : G \to \mathrm{GL}_n(\mathcal{O}_\lambda)$ be two λ-adic representations. We begin by extending the map $\rho_1 \times \rho_2 : G \to \mathrm{GL}_n(\mathcal{O}_\lambda) \times \mathrm{GL}_n(\mathcal{O}_\lambda)$ from G to the group ring $\mathcal{O}_\lambda[G]$.

We define the map $\rho : \mathcal{O}_\lambda[G] \to M_n(\mathcal{O}_\lambda) \oplus M_n(\mathcal{O}_\lambda)$ to be

$$\rho\left(\sum a_i g_i\right) = \left(\sum a_i \rho_1(g_i), \sum a_i \rho_2(g_i)\right).$$

Let M be the full image of ρ inside $M_n(\mathcal{O}_\lambda) \oplus M_n(\mathcal{O}_\lambda)$, and consider the composition map $\delta : G \xrightarrow{\rho} M^\times \to (M/\lambda M)^\times$.

Definition 3.1. [12, Definition 2.1.1] The image $\delta(G)$ of G inside $(M/\lambda M)^\times$ is called the *deviation group* of the pair of representations ρ_1, ρ_2.

Remark 3.2. Since M is a subalgebra of $R = M_n(\mathcal{O}_\lambda) \times M_n(\mathcal{O}_\lambda)$, it might be tempting to think $\delta(G)$ is a subgroup of $(R/\lambda R)^\times = \mathrm{GL}_n(k) \times \mathrm{GL}_n(k)$ but this may not be the case. See the remark after [12, Definition 2.1.1].

The deviation group turns out to be finite, as described by the following proposition.

Proposition 3.3. [12, Proposition 2.1.2] *The group $\delta(G)$ is finite, and in particular we have $|\delta(G)| \leq |k|^{2n^2}$.*

Proof. Note that M is a submodule of the free $\mathcal{O}_\lambda$-module $M_n(\mathcal{O}_\lambda) \oplus M_n(\mathcal{O}_\lambda)$. Since $\mathcal{O}_\lambda$ is a local ring, M is free and is of rank r, where r satisfies

$$r \leq \mathrm{rank}(M_n(\mathcal{O}_\lambda) \oplus M_n(\mathcal{O}_\lambda)) = 2n^2.$$

Given M is a $\mathcal{O}_\lambda$-module, $M/\lambda M$ is a k-algebra of dimension r. Hence,

$$|\delta(G)| \leq |(M/\lambda M)^\times| \leq |k|^r \leq |k|^{2n^2}$$

as claimed. □

https://doi.org/10.4153/S0008439525101173 Published online by Cambridge University Press

Remark 3.4. A similar bound on $|\delta(G)|$ is employed by Mayle-Wang in their proof of Theorem 1.2, although they do not explicitly mention the deviation group. See the proof in [10, Theorem 2].

Let us turn our attention now to the practical use of $\delta(G)$, that being its ability to help us determine when two representations are isomorphic.

Proposition 3.5. [12, Proposition 2.1.3] *Let $\Sigma \subseteq G$ be a subset that surjects onto $\delta(G)$. Then, $\rho_1 \sim \rho_2$ if and only if $\mathrm{tr}(\rho_1(g)) = \mathrm{tr}(\rho_2(g))$ for all $g \in \Sigma$.*

Before we introduce the next proposition, some further explanations are needed (following [12]). We assume now the representations $\rho_1, \rho_2 : G \to \mathrm{GL}_n(\mathcal{O}_\lambda)$ are not isomorphic, that is, they are not conjugate in $\mathrm{GL}_n(\mathcal{O}_\lambda)$, but that the residual representations $\bar{\rho}_1$ and $\bar{\rho}_2$ obtained from ρ_1 and ρ_2 by reduction modulo λ are isomorphic. We then have an equality $\bar{\rho}_1 = P\bar{\rho}_2 P^{-1}$ for some matrix $P \in M_n(k)$.

Define β to be the largest integer such that ρ_1 and ρ_2 are conjugate modulo λ^β, that is, there is a matrix $P \in \mathrm{GL}_n(\mathcal{O}_\lambda)$ such that $\rho_1 \equiv P\rho_2 P^{-1} \pmod{\lambda^\beta}$; we then have $\beta \geq 1$, since $\bar{\rho}_1 \cong \bar{\rho}_2$. In addition, there is an integer $\alpha \geq 1$ such that $\mathrm{tr}(\rho_1) \equiv \mathrm{tr}(\rho_2) \pmod{\lambda^\alpha}$ and $\mathrm{tr}(\rho_1) \not\equiv \mathrm{tr}(\rho_2) \pmod{\lambda^{\alpha+1}}$; in particular, ρ_1 and ρ_2 are not conjugate modulo $\lambda^{\alpha+1}$, so $\beta \leq \alpha$. Given that ρ_1 and ρ_2 are conjugate modulo λ^β but not conjugate modulo $\lambda^{\beta+1}$, if we replace ρ_2 with a conjugate we may assume $\rho_1 \equiv \rho_2 \pmod{\lambda^\beta}$ but $\rho_1 \not\equiv \rho_2 \pmod{\lambda^{\beta+1}}$.

Hence, for any $g \in G$, we have

$$\rho_2(g) - \rho_1(g) \equiv 0 \pmod{\lambda^\beta} \Rightarrow \rho_2(g) - \rho_1(g) = \theta_g \pi^\beta \tag{3.1}$$

for some $\theta_g \in M_n(\mathcal{O}_\lambda)$ and π a uniformizer of $\mathcal{O}_\lambda$. Rearranging, we get an equation for $\rho_2(g)$ of the form

$$\rho_2(g) = (I_n + \theta_g \pi^\beta \rho_1(g)^{-1})\rho_1(g), \tag{3.2}$$

where I_n is the $n \times n$ identity matrix. Let $\theta : G \to M_n(\mathcal{O}_\lambda)$ be the map $g \to \theta_g \rho_1(g)^{-1}$, and notice that (3.2) becomes

$$\rho_2(g) = (I_n + \pi^\beta \theta(g))\rho_1(g). \tag{3.3}$$

Proposition 3.6. [12, Proposition 2.2.1] *Let $\rho_1, \rho_2 : G \to \mathrm{GL}_n(\mathcal{O}_\lambda)$ be representations that are not isomorphic, and suppose $\bar{\rho}_1, \bar{\rho}_2 : G \to \mathrm{GL}_n(k)$ are isomorphic. Let β be the largest integer such that ρ_1 and ρ_2 are conjugate modulo λ^β, and as above, assume ρ_2 has been replaced by a conjugate such that $\rho_1 \equiv \rho_2 \pmod{\lambda^\beta}$. Let*

$$\begin{aligned} \varphi : G &\to M_n(k) \rtimes \mathrm{GL}_n(k) \\ g &\mapsto (\theta(g) \pmod{\lambda}, \rho_1(g) \pmod{\lambda}) \end{aligned} \tag{3.4}$$

where the semidirect product is with respect to the action of $\mathrm{GL}_n(k)$ on $M_n(k)$ by conjugation, that is multiplication is given by

$$(A, B) \cdot (C, D) = (A + BCB^{-1}, BD).$$

Then φ is a group homomorphism which factors through the deviation group $\delta(G)$.

Remark 3.7. The homomorphism $\delta(G) \twoheadrightarrow \varphi(G)$ may not be injective. See [12, Remark 2.2.2].

https://doi.org/10.4153/S0008439525101173 Published online by Cambridge University Press

Lastly, we state a general lemma regarding determinants of matrices that we shall employ later.

Lemma 3.8. [12, Lemma 2.2.3] *Let R be a discrete valuation ring with uniformizer π, and F its field of fractions. For any $A \in \mathrm{GL}_n(F)$,*

$$\det(I_n + \pi A) = 1 + \pi \operatorname{tr}(A) + O(\pi^2).$$

It can be difficult to compute the exact size of $\delta(G)$, or find a tighter upper bound for it. We will, in the following section, work to replace $\delta(G)$ with $\varphi(G)$ in the case of 2-adic representations. The codomain of φ is easily understood, and hence a bound for $|\varphi(G)|$ is easily computable. This is what allows us to prove Theorem 1.3.

4. The tools of Mayle-Wang

The methodology of Mayle-Wang relies on the following proposition that is due to Serre (a proof of which can be found in [3, Theorem 4.7]). The proposition which follows is a refined version of Serre's original argument due to Mayle-Wang [10, Proposition 12] in which we have reworked the statement and proof to follow the work and notation done in Section 3. We note that the statement is similar to that of Proposition 3.5: here, we show that if the representations are not isomorphic, then their traces must disagree on some finite set. While the proofs are very similar, the advantage of the following proposition is that it is in a form to which we may readily apply Chebotarev.

Proposition 4.1. [10, Proposition 12] *Let n be a positive integer. Let G be a group and $\rho_1, \rho_2 : G \to \mathrm{GL}_n(\mathcal{O}_\lambda)$ be representations, and $\delta(G)$ the deviation group of G of the two representations ρ_1 and ρ_2. Suppose that there exists an element $g \in G$ such that $\operatorname{tr}\rho_1(g) \neq \operatorname{tr}\rho_2(g)$. Then there exists a subset $C \subseteq \delta(G)$ for which*

(1) the set C is non-empty and closed under conjugation by $\delta(G)$, and
(2) if the image in $\delta(G)$ of an element $g \in G$ belongs to C, then $\operatorname{tr}\rho_1(g) \neq \operatorname{tr}\rho_2(g)$.

Proof. Let $R := M_n(\mathcal{O}_\lambda) \times M_n(\mathcal{O}_\lambda)$. Let M denote the $\mathcal{O}_\lambda$-subalgebra of R generated by the image of G under the product map

$$\rho_1 \times \rho_2 : G \to \mathrm{GL}_n(\mathcal{O}_\lambda) \times \mathrm{GL}_n(\mathcal{O}_\lambda).$$

Recall that $\delta(G)$ is the image of G under $\rho_1 \times \rho_2$ in $M/\lambda M$.

Let α be the largest nonnegative integer such that for each $g \in G$, one has that

$$\operatorname{tr}(\rho_1(g)) \equiv \operatorname{tr}(\rho_2(g)) \pmod{\lambda^\alpha}.$$

As M is a $\mathcal{O}_\lambda$-subalgebra generated by the image of G under $\rho_1 \times \rho_2$, it follows that the congruence $\operatorname{tr} x_1 \equiv \operatorname{tr} x_2 \pmod{\lambda^\alpha}$ holds for each pair $(x_1, x_2) \in M$. We obtain the $\mathcal{O}_\lambda$-module homomorphism $\phi : M \to \mathcal{O}_\lambda$ given by

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

Since $\phi(\lambda M) \subseteq \lambda\mathcal{O}_\lambda$, we may consider the induced $\mathcal{O}_\lambda/\lambda\mathcal{O}_\lambda$-module homomorphism $\bar{\phi} : M/\lambda M \to \mathcal{O}_\lambda/\lambda\mathcal{O}_\lambda$.

https://doi.org/10.4153/S0008439525101173 Published online by Cambridge University Press

Let $C = \delta(G) \setminus \ker \bar{\phi}$ be the set of elements in $\delta(G)$ whose image under $\bar{\phi}$ in $M/\lambda M$ all are nonzero. From the definition of α and the linearity of the trace map, there exists $g_0 \in G$ such that

$$\operatorname{tr}(\rho_1(g_0)) \not\equiv \operatorname{tr}(\rho_2(g_0)) \pmod{\lambda^{\alpha+1}}.$$

Note that the image of $(\rho_1 \times \rho_2)(g_0)$ in $\delta(G)$ is contained in C, so C is nonempty. Also, C is closed under conjugation since the trace map is invariant under conjugation.

Finally, suppose that $g \in G$ is such that the image of g in $\delta(G)$ is contained in C. Then, $\phi(\rho_1 \times \rho_2(g)) \notin \lambda\mathcal{O}_\lambda$, and in particular $\operatorname{tr}\rho_1(g) \neq \operatorname{tr}\rho_2(g)$. □

Remark 4.2. In the notation $\delta(G)$ and $\varphi(G)$ we suppress the dependence on the representations ρ_1 and ρ_2 as they are usually fixed in the context.

We now give an analogous version of Proposition 4.1 in the case where the mod 2 representations are isomorphic and absolutely irreducible. This allows us to replace $\delta(G)$ in Proposition 4.1 with $\varphi(G)$ from Proposition 3.6, a set which is easier to estimate the size of. The idea to replace $\delta(G)$ with $\varphi(G)$ comes from Chênevert [5, pg. 114], in which he gives a remark that, in the 2-adic case, Serre [17] implies that $\delta(G) \cong \varphi(G)$. However, in a conversation with Chênevert, Serre mentions he might not have proven the map $\delta(G) \to \varphi(G)$ was an isomorphism, but, in an unpublished letter to Tate, that the α in the proof of Proposition 3.5 is equal to the β coming from the construction of the function φ if the residual representation is surjective. We show, in the 2-adic case, that $\alpha = \beta$, and that we can replace $\delta(G)$ in Proposition 4.1 with $\varphi(G)$ and get the same conclusion, that is, there is a subset $C \subseteq \varphi(G)$ that is a conjugacy class, and if $g \in G$ is such that $\varphi(g) \in C$, then $\operatorname{tr}\rho_1(g) \neq \operatorname{tr}\rho_2(g)$.

In order to prove this special case, we require a theorem of Carayol [4].

Theorem 4.3. [4, Theorem 1] *Let A be a local ring, R an A-algebra, and let $\rho_1, \rho_2 : R \to M_n(A)$ be two representations of R of the same dimension n. Suppose that the residual representation $\bar{\rho} : R \otimes_A F \to M_n(F)$, where F is the residue field of A, is absolutely irreducible. Suppose that the traces for ρ_1 and ρ_2 are the same for every $r \in R$. Then, ρ_1 and ρ_2 are isomorphic as representations, that is, there exists a matrix $Q \in \mathrm{GL}_n(A)$ such that $\rho_1(r) = Q\rho_2(r)Q^{-1}$ for all $r \in R$.*

We now prove the special case.

Proposition 4.4. *Let n be a positive integer. Let G be a group and $\rho_1, \rho_2 : G \to \mathrm{GL}_n(\mathbb{Z}_2)$ be representations, and suppose their reductions $\bar{\rho}_1, \bar{\rho}_2$ are isomorphic and absolutely irreducible. Suppose that there exists an element $g \in G$ such that $\operatorname{tr}\rho_1(g) \neq \operatorname{tr}\rho_2(g)$. Then there exists a subset $C \subseteq \varphi(G)$ for which*

(1) the set C is non-empty and closed under conjugation by $\varphi(G)$, and
(2) if the image in $\varphi(G)$ of an element $g \in G$ belongs to C, then $\operatorname{tr}\rho_1(g) \neq \operatorname{tr}\rho_2(g)$.

Proof. Our setup begins, as it did, in Section 3. Let α be the largest nonnegative integer such that for each $g \in G$, we have

$$\operatorname{tr}(\rho_1(g)) \equiv \operatorname{tr}(\rho_2(g)) \pmod{2^\alpha} \quad \text{and} \quad \operatorname{tr}(\rho_1(g)) \not\equiv \operatorname{tr}(\rho_2(g)) \pmod{2^{\alpha+1}}.$$

In addition, we let β be the largest integer such that ρ_1 and ρ_2 are conjugate modulo 2^β, that is, there is a matrix $P \in \mathrm{GL}_n(\mathbb{Z}_2)$ such that $\rho_1 \equiv P\rho_2 P^{-1} \pmod{2^\beta}$. As demonstrated

https://doi.org/10.4153/S0008439525101173 Published online by Cambridge University Press

before, we have $\beta \leq \alpha$. Also, given that ρ_1 and ρ_2 are conjugate modulo 2^β but not conjugate modulo $2^{\beta+1}$, if we replace ρ_2 with a conjugate $P\rho_2 P^{-1}$ for $P \in \mathrm{GL}_n(\mathbb{Z}_2)$, we may assume

$$\rho_1 \equiv P\rho_2 P^{-1} \pmod{2^\beta} \text{ and } \rho_1 \not\equiv P\rho_2 P^{-1} \pmod{2^{\beta+1}}. \tag{4.1}$$

This implies $P\rho_2(g)P^{-1} - \rho_1(g) \equiv 0 \pmod{2^\beta}$ for any $g \in G$. In particular, we get $P\rho_2(g)P^{-1} - \rho_1(g) = \theta_g 2^\beta$ for some $\theta_g \in M_n(\mathbb{Z}_2)$, which we can write as

$$\theta_g = \frac{P\rho_2(g)P^{-1} - \rho_1(g)}{2^\beta}. \tag{4.2}$$

In particular, note that

$$\mathrm{tr}(\theta_g) = 2^{-\beta}(\mathrm{tr}(P\rho_2(g)P^{-1}) - \mathrm{tr}(\rho_1(g))) = 2^{-\beta}(\mathrm{tr}(\rho_2(g)) - \mathrm{tr}(\rho_1(g))) \tag{4.3}$$

by the invariance of trace under conjugation.

We now show $\alpha = \beta$. Extend the maps ρ_1, ρ_2 to the group ring $\mathbb{Z}/2^\alpha\mathbb{Z}[G]$ by $\rho_i(\sum a_j g_j) = \sum a_j \rho_i(g_j)$, for $i = 1, 2$ and $a_j \in \mathbb{Z}/2^\alpha\mathbb{Z}$ and $g_j \in G$. Then, notice that

$$\begin{aligned} \mathrm{tr}(\rho_1(\sum a_j g_j)) \pmod{2^\alpha} &\equiv \mathrm{tr}(\sum a_j \rho_1(g_j)) \pmod{2^\alpha} \\ &\equiv \sum a_j \,\mathrm{tr}(\rho_1(g_j)) \pmod{2^\alpha} \\ &\equiv \sum a_j \,\mathrm{tr}(\rho_2(g_j)) \pmod{2^\alpha} \\ &\equiv \mathrm{tr}(\rho_2(\sum a_j g_j)) \pmod{2^\alpha}. \end{aligned} \tag{4.4}$$

Since we satisfy the hypotheses of Theorem 4.3 with $A = \mathbb{Z}/2^\alpha\mathbb{Z}$ and $R = \mathbb{Z}/2^\alpha\mathbb{Z}[G]$, we can find a matrix $Q \in \mathrm{GL}_n(\mathbb{Z}/2^\alpha\mathbb{Z})$ such that $\rho_1(g) \equiv Q\rho_2(g)Q^{-1} \pmod{2^\alpha}$ for all $g \in G$. However, β is the largest integer such that ρ_1 and ρ_2 are conjugate modulo 2^β, so $\alpha \leq \beta$, implying $\alpha = \beta$.

Recall, from (3.4), the map $\varphi : G \to M_n(\mathbb{F}_2) \rtimes \mathrm{GL}_n(\mathbb{F}_2)$ is defined by

$$\varphi(g) = (\theta(g) \pmod 2, \rho_1(g) \pmod 2)) = ([\theta_g \rho_1(g)^{-1}]_2, [\rho_1(g)]_2). \tag{4.5}$$

We note our use of the notation $[N]_2$, for $N \in M_n(\mathbb{Z}_2)$, to denote the residue class of N modulo 2.

Define the map $\phi' : M_n(\mathbb{F}_2) \rtimes \mathrm{GL}_n(\mathbb{F}_2) \to \mathbb{F}_2$ by

$$\phi'((A, B)) = \mathrm{tr}(AB) \tag{4.6}$$

where the product of matrices is taken to be the action of $\mathrm{GL}_n(\mathbb{F}_2)$ on $M_n(\mathbb{F}_2)$, and the trace is considered to be modulo 2. By (4.5), notice

$$\begin{aligned} \phi'(\varphi(g)) &= \mathrm{tr}([\theta_g \rho_1(g)^{-1}]_2 [\rho_1(g)]_2) \\ &= \mathrm{tr}([\theta_g \rho_1(g)^{-1} \rho_1(g)]_2) \\ &= \mathrm{tr}([\theta_g]_2) \\ &= [\mathrm{tr}(\theta_g)]_2 \\ &= [2^{-\alpha}(\mathrm{tr}(\rho_2(g)) - \mathrm{tr}(\rho_1(g)))]_2 \end{aligned} \tag{4.7}$$

https://doi.org/10.4153/S0008439525101173 Published online by Cambridge University Press

where we have used (4.3) above (with β replaced with α, since $\alpha = \beta$) and the fact that, for a matrix $N \in M_n(\mathbb{Z}_2)$ with $\operatorname{tr}(N) = \sum_{i=1}^{n} a_{ii}$ for entries $a_{ii} \in \mathbb{Z}_2$ along the diagonal, we have

$$\begin{aligned} \operatorname{tr}([N]_2) &= \sum_{i=1}^{n} [a_{ii}]_2 \\ &= \left[\sum_{i=1}^{n} a_{ii} \right]_2 \\ &= [\operatorname{tr}(N)]_2 \end{aligned} \tag{4.8}$$

which shows the final equality (noting our use of $[x]_2$ in (4.8) to denote the residue class of a 2-adic integer $x \in \mathbb{Z}_2$).

Let C be the set of elements in $\varphi(G)$ that take a nonzero value under the map ϕ'. From the definition of α and the linearity of the trace map, there exists $g_0 \in G$ such that

$$\operatorname{tr}(\rho_1(g_0)) \not\equiv \operatorname{tr}(\rho_2(g_0)) \pmod{2^{\alpha+1}}.$$

Note that the image of g_0 in $\varphi(G)$ is inside C, so C is nonempty. In addition, let $\phi(h) \in \phi(G)$ for some $h \in G$; then, given φ is a homomorphism (Proposition 3.6) and by (4.7) and the invariance under conjugation of the trace map,

$$\begin{aligned} \phi'(\varphi(h)\varphi(g)\varphi(h)^{-1}) &= \phi'(\varphi(hgh^{-1})) \\ &= [2^{-\alpha}(\operatorname{tr}(\rho_2(hgh^{-1})) - \operatorname{tr}(\rho_1(hgh^{-1})))]_2 \\ &= [2^{-\alpha}(\operatorname{tr}(\rho_2(h)\rho_2(g)\rho_2(h)^{-1}) - \operatorname{tr}(\rho_1(h)\rho_1(g)\rho_1(h)^{-1}))]_2 \\ &= [2^{-\alpha}(\operatorname{tr}(\rho_2(g)) - \operatorname{tr}(\rho_1(g)))]_2 \\ &= \phi'(\varphi(g)) \\ &\neq 0, \end{aligned} \tag{4.9}$$

so C is closed under conjugation. Finally, suppose that $g \in G$ is such that the image of g in $\varphi(G)$ is contained in C. Then, $\phi'(\varphi(g)) \neq 0$, in particular $\operatorname{tr}\rho_1(g) \neq \operatorname{tr}\rho_2(g)$. □

5. Improved bounds for the effective isogeny theorem

For a prime ℓ and an elliptic curve E, we define

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

We begin with the proof of Proposition 5.1. We note that the work which follows is the same as that of Mayle-Wang [10], except for our use of Proposition 2.7 and Table 1.

Let E and E' be two elliptic curves over $\mathbb{Q}$ and let $A = E \times E'$. Let $G = \operatorname{Gal}(\mathbb{Q}(A[2^\infty])/\mathbb{Q})$. We may regard the 2-adic representations $\rho_{E,2}$ and $\rho_{E',2}$ as representations of G instead of $G_\mathbb{Q}$ since $\mathbb{Q}(E[2^\infty])$ and $\mathbb{Q}(E'[2^\infty])$ are subfields of $\mathbb{Q}(A[2^\infty])/\mathbb{Q}$.

The representation $\rho_{A,2} = \rho_{E,2} \times \rho_{E',2}$ is a continuous homomorphism $G \to \mathrm{GL}_2(\mathbb{Z}_2) \times \mathrm{GL}_2(\mathbb{Z}_2)$ with image being M as defined in the proof of Proposition 4.1. Since $2M$ is closed

https://doi.org/10.4153/S0008439525101173 Published online by Cambridge University Press

inside M, we see that $\delta(G)$ is a closed subgroup of G and hence by the fundamental theorem of infinite Galois theory corresponds to a finite Galois extension $K/\mathbb{Q}$ with $K \subseteq \mathbb{Q}(A[2^\infty])/\mathbb{Q}$.

Since $K \subseteq \mathbb{Q}(A[2^n])$ for some $n \in \mathbb{N}$, we have that

$$|\delta(G)| = [K : \mathbb{Q}] \mid [\mathbb{Q}(A[2^n]) : \mathbb{Q}] \mid |\operatorname{GL}_2(\mathbb{Z}/2^n\mathbb{Z})|^2 = (6 \cdot 16^{n-1})^2, \tag{5.1}$$

for some $n \in \mathbb{N}$ and by [10, Proposition 12],

$$|\delta(G)| \leq 255. \tag{5.2}$$

The set $\varphi(G)$ (defined in Proposition 3.6) is a subset of a very explicit semi-direct product, and estimating $|\varphi(G)|$ gives a smaller bound.

Proposition 5.1. *Assume GRH. Let E and E' be two elliptic curves over $\mathbb{Q}$. Suppose E and E' are not $\mathbb{Q}$-isogenous. Let $\delta(G)$ be the deviation group of G with respect to the 2-adic representations $\rho_{E,2}$ and $\rho_{E',2}$.*

Choose the triple $(\bar{a}, \bar{b}, \bar{c})$ from Table 1 for $n_0 = \max(72, 2|\delta(G)|)$. Then there exists a prime p of good reduction for E and E' such that $a_p(E) \neq a_p(E')$ such that

$$p \leq (\bar{a}((2|\delta(G)| - 1)\log \operatorname{rad}(2N_E N_{E'}) + 2|\delta(G)|\log(2|\delta(G)|)) + 2|\delta(G)|\bar{b} + \bar{c})^2. \tag{5.3}$$

Furthermore, if E and E' are such that their mod 2 representations are isomorphic and absolutely irreducible, then we may replace $|\delta(G)|$ with $|\varphi(G)|$.

Proof. Let $\mathcal{O}_\lambda = \mathbb{Z}_2$. Let $A = E \times E'$ and apply Proposition 4.1 with $\ell = 2$, $n = 2$, $G = \operatorname{Gal}(\mathbb{Q}(A[2^\infty])/\mathbb{Q})$, and the 2-adic representations $\rho_1 = \rho_{E,2}$ and $\rho_2 = \rho_{E',2}$. By Faltings' theorem [7], since the two elliptic curves E and E' are not $\mathbb{Q}$-isogenous, ρ_1 and ρ_2 are not isomorphic; therefore, by Serre [14, pg. IV-15], there is some prime p such that $a_p(E) \neq a_p(E')$. By Proposition 4.1, there exists a conjugacy class $C \subseteq \delta(G)$ obeying the stated conclusion of this proposition.

Let K be the subfield of $\mathbb{Q}(A[2^\infty])$ for which $\operatorname{Gal}(K/\mathbb{Q}) = \delta(G)$. Choosing $m = \operatorname{rad}(N_E N_{E'})$, Proposition 2.7 produces a prime p not dividing m such that $\left(\frac{K/\mathbb{Q}}{p}\right) \subseteq C$ and

$$p \leq (\bar{a} \cdot ((n_0 - 1)\log \operatorname{rad}(d_{\tilde{K}}) + n_0 \log n_0) + \bar{b} \cdot n_0 + \bar{c})^2, \tag{5.4}$$

where $n_0 = \max(72, 2|\delta(G)|)$ and $\bar{a}, \bar{b}, \bar{c}$ are the maximum of their values over entries in Table 1 with $n_{\tilde{K}} \leq 2|\delta(G)|$, respectively. It follows from Proposition 4.1 that

$$\operatorname{tr} \rho_{E,2}(\operatorname{Frob}_p) \neq \operatorname{tr} \rho_{E',2}(\operatorname{Frob}_p),$$

and consequently $a_p(E) \neq a_p(E')$.

The abelian variety A has good reduction at some prime q if and only if both E and E' have good reduction at q. Thus, $K/\mathbb{Q}$ is unramified outside of the prime divisors of $m = N_E N_{E'}$. 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 $\mathbb{Q}(\sqrt{m})$. Since $\operatorname{rad}(d_{\mathbb{Q}(\sqrt{m})}) \mid \operatorname{rad}(2m) = \operatorname{rad}(2N_E N_{E'})$, and $\operatorname{rad}(d_K) \mid \operatorname{rad}(2N_E N_{E'})$, we have that

$$\operatorname{rad}(d_{\tilde{K}}) = \operatorname{rad}(d_K d_{\mathbb{Q}(\sqrt{m})}) \mid \operatorname{rad}(2N_E N_{E'}). \tag{5.5}$$

https://doi.org/10.4153/S0008439525101173 Published online by Cambridge University Press

Now, applying Lemma 2.8 to (5.4) gives us

$$p \le (\bar{a}((2|\delta(G)|-1)\log \operatorname{rad}(2N_E N_{E'}) + 2|\delta(G)|\log(2|\delta(G)|)) + 2|\delta(G)|\bar{b}+\bar{c})^2$$

which matches (5.3).

To prove the final statement, note if $\bar{\rho}_{E,2}$ and $\bar{\rho}_{E',2}$ are isomorphic and absolutely irreducible, then we instead apply Proposition 4.4 over Proposition 4.1, in which case $\delta(G)$ is replaced with $\varphi(G)$; in particular, $|\delta(G)|$ can be replaced with $|\varphi(G)|$ in (5.3). □

Now we give a proof of Theorem 1.3.

Proof of Theorem 1.3. We split our analysis into two cases. If the mod 2 representations are not isomorphic, then mod 2 already distinguishes the traces. Define

$$\bar{\rho}_2 : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \tag{5.6}$$

by $\bar{\rho}_2(x) = (\bar{\rho}_{E,2}(x), \bar{\rho}_{E',2}(x))$. Let $G_2 = \bar{\rho}_2(G_{\mathbb{Q}}) \subset \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ be the image of the map $\bar{\rho}_2$. Let

$$C_2 = \{(s, s') \in G_2 \mid \operatorname{tr}(s) \neq \operatorname{tr}(s')\}. \tag{5.7}$$

Apply Proposition 2.7 to the field $L = \mathbb{Q}(E[2], E'[2])$, whose Galois group is G_2, the conjugacy class C_2 given in (5.7), and $m = \operatorname{rad}(N_E N_{E'})$, so that we get a prime p unramified in L and $p \nmid m$ such that $a_p(E) \not\equiv a_p(E') \pmod 2$ (implying $a_p(E) \neq a_p(E')$) and satisfying

$$p \le \max((\bar{a}\log|d_{\tilde{L}}| + \bar{b}n_{\tilde{L}} + \bar{c})^2, p_0(n_{\tilde{L}})) \tag{5.8}$$

$$\le (1.755\,((2n_L - 1)\log\operatorname{rad}(d_{\tilde{L}}) + 2n_L\log(2n_L)) + 0.23\cdot 2n_L + 6.8)\,. \tag{5.9}$$

Taking $[L:\mathbb{Q}] \le |\,\mathrm{GL}_2(\mathbb{F}_2)|^2 = 6^2 = 36$ gives us

$$\begin{aligned} p &\le (1.745\,(71\log\operatorname{rad}(d_{\tilde{L}}) + 72\log 72) + 72\cdot 0.23 + 6.8)^2 \\ &\le (124\log\operatorname{rad}(2N_E N_{E'}) + 561)^2 \end{aligned} \tag{5.10}$$

Next, assume that the mod 2 representations $\rho_1 = \bar{\rho}_{E,2}$ and $\rho_2 = \bar{\rho}_{E',2}$ are isomorphic and absolutely irreducible. Apply Proposition 5.1, and replace $\delta(G)$ with $\varphi(G)$ (since the mod 2 representations are isomorphic and absolutely irreducible) to get a prime p such that $a_p(E) \neq a_p(E')$ and satisfying

$$p \le (\bar{a}((2|\varphi(G)|-1)\log\operatorname{rad}(2N_E N_{E'}) + 2|\varphi(G)|\log(2|\varphi(G)|)) + 2|\varphi(G)|\bar{b}+\bar{c})^2.$$

From (3.2) and Lemma 3.8, we have for any $g \in G$,

$$\begin{aligned} \det(\rho_2(g)) &= \det((I_2 + 2^\beta\theta(g))\rho_1(g)) \\ &= (1 + 2^\beta\operatorname{tr}(\theta(g)) + O(2^{2\beta}))\det(\rho_1(g)). \end{aligned} \tag{5.11}$$

As we have $\det\rho_1 = \det\rho_2$ being the cyclotomic character, so the above can be rewritten as $0 = 2^\beta\operatorname{tr}(\theta(g)) + O(2^{2\beta})$, which, after multiplying through by $2^{-\beta}$ implies

$$\operatorname{tr}(\theta) \equiv 0 \pmod 2.$$

https://doi.org/10.4153/S0008439525101173 Published online by Cambridge University Press

In particular, the map φ from Proposition 3.6 takes values in $M_2^0(\mathbb{F}_2) \rtimes \mathrm{GL}_2(\mathbb{F}_2)$, where $M_2^0(\mathbb{F}_2)$ denotes the matrices with trace 0 with entries in $\mathbb{F}_2$. Therefore, we have $|\varphi(G)| \leq |M_2^0(\mathbb{F}_2) \rtimes \mathrm{GL}_2(\mathbb{F}_2)| = 8 \cdot 6 = 48$. We find from Proposition 2.7 that

$$\begin{aligned} p &\leq (1.745(95 \log \operatorname{rad}(2N_E N_{E'}) + 96 \log(96)) + 96 \cdot 0.23 + 6.8)^2 \\ &\leq (166 \log \operatorname{rad}(2N_E N_{E'}) + 794)^2 \end{aligned} \tag{5.12}$$

We now improve the bound in (5.12) by using the following two results.

Proposition 5.2. *Let G be a group and $\rho_1, \rho_2 : G \to \mathrm{GL}_2(\mathbb{Z}_2)$ be a group homomorphism, and suppose the mod 2 representations $\bar{\rho}_1, \bar{\rho}_2$ are isomorphic. Let Ξ be the elements $g \in G$ such that the characteristic polynomials of $\rho_1(g)$ and $\rho_2(g)$ coincide. Then for $g \in \Xi$, the order of $\delta(g)$ in $\delta(G)$ is ≤ 3.*

Proof. See [5, Proposition 5.5.6]. □

Corollary 5.3. *Let G be a group and $\rho_1, \rho_2 : G \to \mathrm{GL}_2(\mathbb{Z}_2)$ be a group homomorphism, and suppose the mod 2 representations $\bar{\rho}_1, \bar{\rho}_2$ are isomorphic. Let $\pi : \delta(G) \twoheadrightarrow \bar{G}$ be a quotient having a conjugacy class $C \subseteq \bar{G}$ of order > 3. If $g \in G$ is such that $\pi(\delta(g)) \in C$, then $g \notin \Xi$.*

From (5.1) and (5.2), the possible sizes of $\delta(G)$ are

$$1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 32, 36, 48, 64, 72, 96, 128, 144, 192. \tag{5.13}$$

As the possible orders are small, it is possible to enumerate in `Magma` all isomorphism classes of groups of these sizes. The group $\delta(G)$ therefore lies in an explicit finite list which can be computed.

By Corollary 5.3, if $\delta(G)$ has a quotient $\bar{G}$ with an element of order > 3, then we may replace $\delta(G)$ by $\bar{G}$. We check this in `Magma` for each value of $|\delta(G)|$ and find that either $\delta(G)$ has such a quotient with strictly smaller size in the given list of (5.13) or it is in a small list of problematic groups. We list for each size $|\delta(G)|$, the `Magma` labels of the isomorphism classes of the problematic groups of that order.

$\lvert\delta(G)\rvert$	# of isomorphism classes	problematic groups
192	1543	1023, 1025, 1541
144	197	none
128	2328	2326, 2327, 2328
96	231	204
72	50	none
64	267	266, 267
48	52	3, 50
36	14	11
32	51	49, 50, 51

TABLE 2. List of problematic groups

Consider the homomorphism $\varphi : \delta(G) \to M_2^0(\mathbb{F}_2) \rtimes \mathrm{GL}_2(\mathbb{F}_2)$. The possible orders of the image are:

$$1, 2, 3, 4, 6, 8, 12, 16, 24, 48. \tag{5.14}$$

https://doi.org/10.4153/S0008439525101173 Published online by Cambridge University Press

Using `Magma`, we check if $|\delta(G)| \geq 32$, there is no homomorphism from a problematic group to a subgroup of order 24 or 48 in the codomain of φ. Hence, either $|\delta(G)| \leq 24$ or the image of φ is ≤ 16. In either case, we can replace $\delta(G)$ by a quotient of order ≤ 24. Thus, we obtain the same bound as in (5.10) using Proposition 2.7.

□

6. The results of Rouse and Zureick-Brown on 2-adic images

The 2-adic representation $\rho_{E,2} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_2)$ of an elliptic curve E over $\mathbb{Q}$ has open image in $\mathrm{GL}_2(\mathbb{Z}_2)$ and the properties that $\det \rho_{E,2} : G_{\mathbb{Q}} \to \mathbb{Z}_2^{\times}$ is surjective and $\rho_{E,2}(c)$ is an element with determinant -1 and trace 0 for a complex conjugation. With this in mind, the authors in [13] make the following definition:

Definition 6.1. An open subgroup $H \subseteq \mathrm{GL}_2(\mathbb{Z}_2)$ is arithmetically maximal if

(1) $\det : H \to \mathbb{Z}_2^{\times}$ is surjective,
(2) there is an element of H with determinant -1 and trace 0, and
(3) there is no subgroup K satisfying (1) and (2) with $H \subsetneq K$ and so that the genus of X_K is ≥ 2.

The idea behind this definition is that arithmetically maximal subgroups $H \subseteq \mathrm{GL}_2(\mathbb{Z}_2)$ are maximal among the subgroups H satisfying (1) and (2), except possibly when H is contained in a subgroup K such that X_K has genus ≤ 1. For instance, if $H \subsetneq K$ and X_K has genus ≥ 2, it would be easier and sufficient to determine the $\mathbb{Q}$-rationals point X_K rather than X_H.

For an arithmetically maximal subgroup H, either X_H has infinitely many $\mathbb{Q}$-rational points (hence has genus ≤ 1) or X_H has finitely many $\mathbb{Q}$-rational points. The union of the latter cases leads to a finite list of j-invariants.

In [13], it is shown there are 727 arithmetically maximal subgroups $H \subseteq \mathrm{GL}_2(\mathbb{Z}_2)$ up to conjugation such that $-I \in H$. Among these, there are 408 which have genus ≤ 1 and 202 of these are such that X_H has infinitely many $\mathbb{Q}$-rational points.

From [13, Theorem 1.1], we may determine the possible images of $\rho_{E,2}$ when the image of $\rho_{E,2}$ contains $-I$ as follows.

Theorem 6.2. *Let $H \subseteq \mathrm{GL}_2(\mathbb{Z}_2)$ be a subgroup containing $-I$ and let $E/\mathbb{Q}$ be an elliptic curve such that the image of $\rho_{E,2}$ is contained in a conjugate of H. Then one of the following holds:*

(1) The modular curve X_H has infinitely many $\mathbb{Q}$-rational points (hence has genus ≤ 1).
(2) The elliptic curve E has complex multiplication.
(3) The j-invariant of E is one of

$$2^{11}, 2^4 \cdot 17^3, 4097^3/2^4, 257^3/2^8, -857985^3/62^8, 919425^3/496^4, \\ -3 \cdot 18249920^3/17^{16}, 7 \cdot 1723187806080^3/79^{16}. \tag{6.1}$$

We rephrase the above theorem for the purposes of proving the main results of this paper.

https://doi.org/10.4153/S0008439525101173 Published online by Cambridge University Press

Theorem 6.3. *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. Suppose the image of $\rho_{E,2}$ contains $-I$. Then $\rho_{E,2}(G)$ is one of* 202 *arithmetically maximal groups listed in* [13] *which have infinitely many $\mathbb{Q}$-rational points, or the j-invariant of E appears in* (6.1).

7. Improved bounds for Serre's open image theorem

In Theorem 1.3, there is a hypothesis that $\bar{\rho}_{E,2} \simeq \bar{\rho}_{E',2}$ is absolutely irreducible. While we do not have an argument to remove this condition and achieve better bounds than Theorem 1.2, we are able to do so in the case when E and E' are quadratic twists of each other and do not have complex multiplication.

Proof of Theorem 1.5. Suppose E' is a twist of E by a quadratic character χ associated to the extension $\mathbb{Q}(\sqrt{d})$. Then $\rho_{E',2} = \rho_{E,2} \otimes \chi$. Since E does not have complex multiplication, E and E' are not $\mathbb{Q}$-isogenous.

If $\bar{\rho}_{E,2}$ is absolutely irreducible, the result follows from Theorem 5. Assume from here on that $\rho_{E,2}$ is not absolutely irreducible but irreducible.

If $\mathbb{Q}(\sqrt{d})$ is not a subfield of $L = \mathbb{Q}(E[2^\infty])$, then $L(\sqrt{d})$ is a degree 2 extension of L. Hence, the identity automorphism of L extends to an automorphism σ of $L(\sqrt{d})$ such that $\chi(\sigma) = -1$. It follows that $\rho_{E,2}(\sigma) = I$ and $\rho_{E',2}(\sigma) = -I$ where I is the identity element. This means that $\alpha = \beta = 1$ so we may apply the proofs of Theorem 1.3 and Proposition 4.4 (no need for Theorem 4.3) to get the desired conclusion.

Otherwise $\mathbb{Q}(\sqrt{d})$ lies in the field L. In [13] (see Theorem 6.3), the possible 2-adic images $\rho_{E,2}(G)$ of an elliptic curve $E/\mathbb{Q}$ are determined up to conjugacy. Every such image contains the principal congruence subgroup of level 32 and can be regarded as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/2^t\mathbb{Z})$ for $0 \le t \le 5$. In order to apply [13, Lemma 3.3], without loss of generality we take $t \ge 2$.

Let $\Gamma = I + 2^{t+1}M_2(\mathbb{Z}_2) \subseteq N = I + 2^tM_2(\mathbb{Z}_2)$. The character χ corresponds to a subgroup H of index 2 inside $\rho_{E,2}(G)$. Either $\Gamma \subseteq N \subseteq H$ or

$$N/N \cap H \cong NH/H \cong G/H \tag{7.1}$$

so $N/N \cap H$ has order 2. In the latter case, $N \cap H$ is a maximal subgroup of N, hence by [13, Lemma 3.3], we obtain again that $\Gamma \subseteq N \cap H \subseteq H$.

It follows that χ factors through

$$\rho_{E,2}(G)/\Gamma. \tag{7.2}$$

Consider the product representation

$$\rho_2 = \rho_{E,2} \times \rho_{E',2} : G \to \mathrm{GL}_2(\mathbb{Z}_2) \times \mathrm{GL}_2(\mathbb{Z}_2). \tag{7.3}$$

We note that

$$\rho_{E',2}(g) = \begin{cases} \rho_{E,2}(g) & \text{if } \rho_{E,2}(g) \in H \\ -\rho_{E,2}(g) & \text{if } \rho_{E,2}(g) \notin H. \end{cases} \tag{7.4}$$

https://doi.org/10.4153/S0008439525101173 Published online by Cambridge University Press

Let θ be defined as:

$$\theta : \rho_{E,2}(G) \to \rho_{E',2}(G) \tag{7.5}$$
$$\rho_{E,2}(g) \mapsto \begin{cases} \rho_{E,2}(g) & \text{if } \rho_{E,2}(g) \in H \\ -\rho_{E,2}(g) & \text{if } \rho_{E,2}(g) \notin H. \end{cases}$$

The map θ is an isomorphism which is the identity when restricted to $\Gamma \subseteq H$ and

$$\rho_2(G) = (\rho_{E,2} \times \rho_{E',2})(G) \tag{7.6}$$

is the subgroup of $\mathrm{GL}_2(\mathbb{Z}_2) \times \mathrm{GL}_2(\mathbb{Z}_2)$ given by the graph of θ, namely,

$$\{(\rho_{E,2}(g), \theta(\rho_{E,2}(g))) : g \in G\}. \tag{7.7}$$

Hence, it follows that the inclusion

$$\iota : \rho_{E,2}(G) \to \rho(G) \tag{7.8}$$
$$\rho_{E,2}(g) \mapsto (\rho_{E,2}(g), \theta(\rho_{E,2}(g))) \tag{7.9}$$

is an isomorphism. Composing with the homomorphism $\rho_2(G) \to (M/2M)^\times$, we obtain a homomorphism

$$\phi : \rho_{E,2}(G) \to \rho_2(G) \twoheadrightarrow \delta(G) \subseteq (M/2M)^\times. \tag{7.10}$$

Since $\rho_{E,2}(G) \supseteq 1 + 2^t M_2(\mathbb{Z}_2)$, we see that $M = \mathbb{Z}_2[\rho_2(G)] \supseteq 2^t \Delta(M_2(\mathbb{Z}_2))$ where $\Delta : M_2(\mathbb{Z}_2) \to M_2(\mathbb{Z}_2) \times M_2(\mathbb{Z}_2)$ is the diagonal homomorphism. Thus, $2M \supseteq 2^{t+1}\Delta(M_2(\mathbb{Z}_2))$. Thus, we see that the kernel of the map ϕ contains $\Gamma = 1 + 2^{t+1}M_2(\mathbb{Z}_2)$ and hence ϕ factors through

$$\rho_{E,2}(G)/\Gamma. \tag{7.11}$$

Using `Magma`, we check that each one of the 202 possibilities for $\rho_{E,2}(G)$ does not have a quotient which factors through $\rho_{E,2}(G)/\Gamma$ and is isomorphic to one of the problematic groups in Table 2. In the computation, we do not need to check the cases when $\bar{\rho}_{E,2}$ is absolutely irreducible or reducible by our previous assumption.

We conclude that it is possible to replace $\delta(G)$ with a quotient of order ≤ 24. It is also checked that the elliptic curves E over $\mathbb{Q}$ with j-invariant in the finite list of Theorem 6.2 (3) have $C_E \leq 2$. Thus, we obtain the same bound as in (5.10) using Proposition 2.7.

□

Let E^F be the twist of an elliptic curve $E/\mathbb{Q}$ by a quadratic extension $F/\mathbb{Q}$. The splitting fields of the m-division polynomials of E and E^F are equal to a common field $L_m = L_{E,m} = L_{E^F,m}$.

Proof of Theorem 1.7. Let $F/\mathbb{Q}$ be chosen so that F is not contained in the fields $L_{E,2^n}$ for all $n \geq 1$. This is possible as the fields L_{2^n} are unramified outside of $2N_E$. If $-I \notin \rho_{E,2}(G)$, then $-I \notin \bar{\rho}_{E,2^n}(G)$ for all $n \geq 1$. By [18, Corollary 5.25 (b)] we have that $-I \in \bar{\rho}_{E^F,2^n}(G)$ for all $n \geq 1$ and hence $-I \in \rho_{E^F,2}(G)$. Hence, up to replacing E by the quadratic twist E^F, we may assume that $-I \in \rho_{E,2}(G)$ as the set of primes $\ell > 13$ for which $\bar{\rho}_{E^F,\ell}$ is non-surjective is the same as that for $\bar{\rho}_{E,\ell}$ by [19, Lemma 3.1].

https://doi.org/10.4153/S0008439525101173 Published online by Cambridge University Press

Furthermore, by [9, Theorem 1.1] we may assume $\bar{\rho}_{E,2}$ is irreducible otherwise $\bar{\rho}_{E,\ell}$ is surjective for $\ell > 37$.

We now combine Theorems 1.3 and 1.5 with the arguments in [10]. □

References

[1] Bach, E., and Sorenson, J. Explicit bounds for primes in residue classes. *Mathematics of Computation 65*, 216 (1996), 1717–1735. 2, 2.5, 2.6, 2

[2] Bosma, W., Cannon, J., and Playoust, C. The Magma algebra system. I. The user language. *J. Symbolic Comput. 24*, 3-4 (1997), 235–265. Computational algebra and number theory (London, 1993). 1

[3] Bucur, A., and Kedlaya, K. S. An application of the effective sato-tate conjecture. *Contemporary Mathematics 663* (2016), 45–56. 4

[4] Carayol, H. Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet. *Contemprary Mathematics 165* (1994), 213–237. 4, 4.3

[5] Chênevert, G. *Exponential sums, hypersurfaces with many symmetries and Galois representations.* PhD thesis, McGill University, 2008. 3, 4, 5

[6] Cornell, G., and Silverman, J. H. *Arithmetic Geometry.* Springer-Verlag, 1986. 1.4

[7] Faltings, G. Endlichkeitssätze für abelsche varietäten über zahlkörpern. *Inventiones Mathematicae 73* (1983), 349–366. 1.4, 5

[8] Lagarias, J. C., and Odlyzko, A. M. Effective versions of the Chebotarev density theorem. *Algebraic Number Fields 54* (1979), 271–296. 2, 2.2, 2.3

[9] Lemos, P. Serre's uniformity conjecture for elliptic curves with rational cyclic isogenies. *Trans. Amer. Math. Soc. 371*, 1 (2019), 137–146. 7

[10] Mayle, J., and Wang, T. On the effective version of Serre's open image theorem. *Bulletin of the London Mathematical Society* (2024), to appear. 1, 1.2, 1, 2, 2.6, 2.8, 3.4, 4, 4.1, 5, 5, 7

[11] Oesterlé, J. Versions effectives du théorème de Chebotarev sous l'hypothèse de Riemann généralisée. *Astérisque 61* (1979), 165–167. 2.4, 2

[12] Rodríguez, I. S. Comparing galois representations and the Falting-Serre-Livné method. Master's thesis, Universitat de Barcelona, 2020. 3, 3.1, 3.2, 3.3, 3.5, 3, 3.6, 3.7, 3.8

[13] Rouse, J., and Zureick-Brown, D. Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois. *Res. Number Theory 1* (2015), Paper No. 12, 34. 1, 6, 6, 6.3, 7, 7

[14] Serre, J.-P. *Abelian ℓ-Adic Representations and Elliptic Curves.* W. A. Benjamin, Inc., 1968. 5

[15] Serre, J.-P. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math. 15*, 4 (1972), 259–331. 1

[16] Serre, J.-P. Quelques applications du théorème de densité de Chebotarev. *Publications Mathématiques de l'IHÉS 54* (1981), 123–201. 1, 1.1

[17] Serre, J.-P. Résumé des cours de 1984-1985. In *Annuaire du Collège de France.* 1985, pp. 85–90. 3, 4

[18] Sutherland, A. V. Computing images of Galois representations attached to elliptic curves. *Forum Math. Sigma 4* (2016), Paper No. e4, 79. 7

[19] Zywina, D. On the surjectivity of mod ℓ representations associated to elliptic curves. *Bull. Lond. Math. Soc. 54*, 6 (2022), 2404–2417. 7

Department of Mathematics, Simon Fraser University, Burnaby, BC V5A 1S6, Canada.

Email address: ichen@sfu.ca

Department of Mathematics, Simon Fraser University, Burnaby, BC V5A 1S6, Canada.

Email address: joshua_swidinsky@sfu.ca

https://doi.org/10.4153/S0008439525101173 Published online by Cambridge University Press