BOUNDS FOR SERRE'S OPEN IMAGE THEOREM

DAVID ZYWINA

Abstract. Consider an elliptic curve E without complex multiplication defined over the rationals. The absolute Galois group of $\mathbb{Q}$ acts on the group of torsion points of E, and this action can be expressed in terms of a Galois representation $\rho_E\colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_2(\widehat{\mathbb{Z}})$. A renowned theorem of Serre says that the image of ρ_E is open, and hence has finite index, in $\operatorname{GL}_2(\widehat{\mathbb{Z}})$. We give the first general bounds of this index in terms of basic invariants of E. For example, the index $[\operatorname{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))]$ can be bounded by a polynomial function of the logarithmic height of the j-invariant of E. As an application of our bounds, we settle an open question on the average of constants arising from the Lang-Trotter conjecture.

1. Introduction

1.1. **Main theorem.** Consider an elliptic curve E defined over $\mathbb{Q}$ which has no complex multiplication. For each positive integer m, let $E[m]$ be the group of m-torsion points in $E(\overline{\mathbb{Q}})$; it is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank 2. The group $E[m]$ has an action by the absolute Galois group $\operatorname{Gal}_\mathbb{Q} := \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ which, after a choice of basis, can be expressed in terms of a Galois representation $\rho_{E,m}\colon \operatorname{Gal}_\mathbb{Q} \to \operatorname{Aut}(E[m]) \cong \operatorname{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Combining these representations together, we obtain a single Galois representation

$$\rho_E\colon \operatorname{Gal}_\mathbb{Q} \to \operatorname{Aut}(E_{\text{tors}}) \cong \operatorname{GL}_2(\widehat{\mathbb{Z}})$$

which describes the Galois action on all the torsion points of E (here $\widehat{\mathbb{Z}}$ is the profinite completion of $\mathbb{Z}$).

A famous theorem of Serre says that $\rho_E(\operatorname{Gal}_\mathbb{Q})$ is open, and hence of finite index, in $\operatorname{GL}_2(\widehat{\mathbb{Z}})$ [Ser72]. Serre's theorem is qualitative in nature and does not give an explicit bound for the index. Our main theorem gives such a bound.

Theorem 1.1. *Let E be a non-CM elliptic curve defined over $\mathbb{Q}$. Let j_E be the j-invariant of E and let $h(j_E)$ be its logarithmic height. Let N be the product of primes for which E has bad reduction and let $\omega(N)$ be the number of distinct prime divisors of N.*

(i) *There are absolute constants C and γ such that*

$$\big[\operatorname{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(\operatorname{Gal}_\mathbb{Q})\big] \le C\big(\max\{1, h(j_E)\}\big)^{\gamma}.$$

(ii) *There is an absolute constant C such that*

$$\big[\operatorname{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(\operatorname{Gal}_\mathbb{Q})\big] \le C\big(68N(1+\log\log N)^{1/2}\big)^{24(\omega(N)+1)}.$$

(iii) *Assuming the Generalized Riemann Hypothesis holds, there is an absolute constant C such that*

$$\big[\operatorname{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(\operatorname{Gal}_\mathbb{Q})\big] \le \big(C(\log N)(\log\log(2N))^3\big)^{24(\omega(N)+1)}.$$

These seem to be the first general bounds of Serre's index that hold for *all* non-CM elliptic curves $E/\mathbb{Q}$. Serre and others have computed the index for several examples, and Jones [Jon10] has shown that the index is 2 for "most" $E/\mathbb{Q}$.

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

Key words and phrases. elliptic curves, Galois representations, open image theorem.

1.2. **Background and overview.** Fix a non-CM elliptic curve E over $\mathbb{Q}$. We first review the well-studied *horizontal* situation, that is, we will consider the groups $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q}) \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for a varying prime ℓ.

Suppose that $\rho_{E,\ell}$ is not surjective; its image is contained in some maximal subgroup M of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. If $\ell > 17$ and $\ell \neq 37$, then $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ is contained in the normalizer of a Cartan subgroup but is not contained in any Cartan subgroup (this uses a major theorem of Mazur to rule out the case where M is a Borel subgroup) [Ser81, §8.4]. The case where M is the normalizer of a *split* Cartan subgroup has recently been ruled out by Bilu, Parent and Rebolledo for all primes $\ell > 13$, see [BPR11]; we will not make use of this result since it is satisfying to handle the split and non-split cases on an equal footing.

Let $c(E) \in [1, +\infty]$ be the smallest number for which $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q}) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all primes $\ell > c(E)$. The main task in [Ser72] is to show that $c(E)$ is finite. Serre then asked whether the constant $c(E)$ can be bounded independent of E [Ser72, §4.3], and moreover whether we always have $c(E) \leq 37$ [Ser81, p. 399] (this would be best possible since there are non-CM elliptic curves over $\mathbb{Q}$ which have a rational isogeny of degree 37 [Vél74]). If $c(E)$ could be bounded independent of E, then $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(\mathrm{Gal}_\mathbb{Q})] \leq C$ for some absolute constant C (see Remark 5.2).

Under GRH, Serre proved that $c(E) \leq c \log N (\log\log 2N)^3$ for some absolute constant c [Ser81]; we will discuss his approach in §3. Using a variant of Serre's method, Kraus proved that $c(E) \leq 68N(1 + \log\log N)^{1/2}$ under the now superfluous assumption that $E/\mathbb{Q}$ is modular [Kra95]; a similar bound was also given by Cojocaru [Coj05]. Masser and Wüstholz have proved that $c(E) \leq C\big(\max\{1, h(j_E)\}\big)^\gamma$ where C and γ are effective absolute constants [MW93]; see §4 for related material. The influence of these results on this paper should be apparent from the nature of the bounds in Theorem 1.1.

We now consider the *vertical* situation, that is, we will examine the groups $\rho_{E,\ell^n}(\mathrm{Gal}_\mathbb{Q}) \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ for a fixed prime ℓ and increasing n. Combining these representations together, we obtain an ℓ-adic representation $\rho_{E,\ell^\infty} \colon \mathrm{Gal}_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{Z}_\ell)$.

In [Ser68, IV-11], Serre proved that the group $G_\ell := \rho_{E,\ell^\infty}(\mathrm{Gal}_\mathbb{Q})$ is open in $\mathrm{GL}_2(\mathbb{Z}_\ell)$. He accomplishes this by showing that G_ℓ, viewed as an ℓ-adic Lie group, has the largest possible Lie algebra. Unfortunately, this does not give a bound for the index $[\mathrm{GL}_2(\mathbb{Z}_\ell) : G_\ell]$.

Consider a prime ℓ satisfying $\ell > 17$ and $\ell \neq 37$. From the horizontal setting, we know that $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ is either $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ or is contained in the normalizer of a Cartan subgroup. If $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q}) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, then one can show that $G_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$; so we will focus on the second case. The following key proposition gives constraints on the image of ρ_{E,ℓ^∞}; its proof is mainly group theoretic and will make up most of §2.

Proposition 1.2. *Let E be a non-CM elliptic curve over $\mathbb{Q}$. Let ℓ be a prime for which $\ell > 17$ and $\ell \neq 37$. Then for every positive integer n, one of the following holds:*

- *$\rho_{E,\ell^n}(\mathrm{Gal}_\mathbb{Q})$ is contained in the normalizer of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$,*
- *$\rho_{E,\ell^\infty}(\mathrm{Gal}_\mathbb{Q}) \supseteq I + \ell^{4n} M_2(\mathbb{Z}_\ell)$.*

We are thus led to consider the problem of effectively bounding the primes ℓ and positive integers n for which $\rho_{E,\ell^n}(\mathrm{Gal}_\mathbb{Q})$ is contained in the normalizer of a Cartan subgroup. We will use the methods of the papers mentioned in the horizontal setting which dealt with the case $n = 1$.

Finally, to obtain our bound for $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(\mathrm{Gal}_\mathbb{Q})]$ we will need the following result which we will prove in §5.

Proposition 1.3. *Let E be an elliptic curve over $\mathbb{Q}$. Let M be a positive integer with the following property: if ℓ is a prime greater than 17 and not 37 and $n \geq 1$ is an integer for which $\rho_{E,\ell^n}(\mathrm{Gal}_\mathbb{Q})$*

is contained in the normalizer of a Cartan subgroup, then ℓ^n divides M. With such an M, there is an absolute constant C such that $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(\mathrm{Gal}_{\mathbb{Q}})] \leq CM^{24}$.

For example, in Proposition 3.3(ii) we will prove that there is an M as in Proposition 1.3 satisfying $M \leq \big(68N(1+\log\log N)^{1/2}\big)^{\omega(N)+1}$. Theorem 1.1(ii) then follows immediately from the above proposition.

Remark 1.4.

(i) The constants C in Theorem 1.1 are not easily computed because, in the proof of Proposition 1.3, we have applied Faltings theorem to several modular curves to control the contribution from the small primes. Besides this, our bounds are effective; for example it will be clear from the proof that the index $\big[\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) : \rho_{E,m}(\mathrm{Gal}_{\mathbb{Q}})\big]$ is bounded by $(68N(1+\log\log N)^{1/2})^{24(\omega(N)+1)}$ for all positive integers m relatively prime to $37\prod_{\ell\leq 17}\ell$.

(ii) Serre's theorem is stated more generally for non-CM elliptic curves E over a number field K. We expect Theorem 1.1(i) to hold for all such E/K except with a constant C now depending on the field K. The methods used in the proofs of Theorem 1.1(ii) and (iii) seem unlikely to extend to a general number field K.

1.3. **Lang-Trotter constants on average.** We now give a quick application of Theorem 1.1. Fix an integer r and let E be an elliptic curve defined over $\mathbb{Q}$. For each prime p of good reduction, we obtain an elliptic curve E_p over $\mathbb{F}_p$ by reduction modulo p. Let $a_p(E)$ be the trace of the Frobenius automorphism of $E_p/\mathbb{F}_p$; it is the integer for which $|E_p(\mathbb{F}_p)| = p+1-a_p(E)$. We define $\pi_{E,r}(x)$ to be the number of primes $p \leq x$ of good reduction for which $a_p(E) = r$.

For example, if $r = 0$, then $\pi_{E,0}(x)$ counts the number of supersingular primes $p \leq x$ of E (except possibly undercounting at $p = 2$ and $p = 3$). When $r = 1$, the function $\pi_{E,1}(x)$ counts the number of *anomalous* primes of E up to x [Maz72]. For the CM elliptic curve $E\colon Y^2 = X^3 - X$ we have $a_p(E) = \pm 2$ if and only if $p = n^2+1$, so $\pi_{E,-2}(x) + \pi_{E,2}(x)$ counts the number of primes $p \leq x$ that are of the form n^2+1. The following conjecture of Lang and Trotter [LT76] predicts the asymptotics of $\pi_{E,r}(x)$ as $x \to +\infty$.

Conjecture 1.5 (Lang-Trotter)**.** Let E be an elliptic curve over $\mathbb{Q}$ and let r be an integer. Except for the case where $r = 0$ and E has complex multiplication, there is an explicit constant $C_{E,r} \geq 0$ such that $\pi_{E,r}(x) \sim C_{E,r}\frac{\sqrt{x}}{\log x}$ as $x \to +\infty$.

If $C_{E,r} = 0$, then we interpret the conjecture as saying that $\pi_{E,r}(x)$ is a bounded function of x. The constant $C_{E,r}$, as predicted by Lang and Trotter, is expressed in terms of the image of the representation ρ_E. We shall describe it for non-CM curves in §6. The Lang-Trotter conjecture is open for every pair (E,r) with $C_{E,r} \neq 0$. Furthermore, there are no known examples of $E/\mathbb{Q}$ and $r \neq 0$ for which $\lim_{x\to\infty} \pi_{E,r}(x) = \infty$ (if E is non-CM, then E has infinitely many supersingular primes by Elkies [Elk87]).

One source of theoretical evidence for the Lang-Trotter conjecture are "on average" versions of it, that is, take the average of the functions $\pi_{E,r}(x)$ over a family of elliptic curves E and show that it is compatible with what one expects from the Lang-Trotter conjecture. For real numbers $A, B \geq 2$, let $\mathcal{F}(A,B)$ be the set of pairs $(a,b) \in \mathbb{Z}^2$ with $|a| \leq A$ and $|b| \leq B$ such that $4a^3 + 27b^2 \neq 0$. For each $(a,b) \in \mathcal{F}(A,B)$, let $E(a,b)$ be the elliptic curve over $\mathbb{Q}$ defined by the Weierstrass equation $y^2 = x^3 + ax + b$.

Theorem 1.6 (David-Pappalardi [DP99])**.** *Fix $\varepsilon > 0$. Let $A = A(x)$ and $B = B(x)$ be functions of $x \geq 2$ for which $A, B > x^{1+\varepsilon}$. Then*

$$\frac{1}{|\mathcal{F}(A,B)|}\sum_{(a,b)\in\mathcal{F}(A,B)} \pi_{E(a,b),r}(x) \sim C_r\frac{\sqrt{x}}{\log x}$$

as $x \to +\infty$*, where* $C_r := \dfrac{2}{\pi}\displaystyle\prod_{\ell | r}\Big(1-\frac{1}{\ell^2}\Big)^{-1}\prod_{\ell\nmid r}\frac{\ell(\ell^2-\ell-1)}{(\ell-1)(\ell^2-1)}$.

So averaging the function $\pi_{E,r}(x)$ over the family $\mathcal{F}(A,B)$, with A and B sufficiently large in terms of x, we obtain a quantity with the expected order of magnitude ([DP99] also give a version with explicit error terms). Since conjecturally $\pi_{E(a,b),r}(x) \sim C_{E(a,b),r}\sqrt{x}/\log x$, it is thus natural to ask, as David and Pappalardi did in §2 of [DP99], whether C_r is the average of the constants $C_{E(a,b),r}$. So that the average is well-defined, we will arbitrarily define $C_{E,0} = 0$ when E has complex multiplication. In §6, building off the work of N. Jones, we shall prove the following theorem:

Theorem 1.7. *There is an absolute constant* $\delta > 0$ *such that*

$$\frac{1}{|\mathcal{F}(A,B)|}\sum_{(a,b)\in\mathcal{F}(A,B)} C_{E(a,b),r} = C_r + O\bigg(\frac{\log^{\delta}(AB)}{\sqrt{\min\{A,B\}}}\bigg)$$

where the implicit constant depends only on r*.*

Thus as long as A and B are not that different in magnitude, the average of the constants $C_{E(a,b),r}$ over the pairs $(a,b)\in\mathcal{F}(A,B)$ will be well-aproximated by C_r. In particular,

$$\lim_{A\to+\infty}\frac{1}{|\mathcal{F}(A,A^{\beta})|}\sum_{(a,b)\in\mathcal{F}(A,A^{\beta})} C_{E(a,b),r} = C_r$$

for any real number $\beta > 0$.

Theorem 1.7 is a special case of a theorem of Jones [Jon09] which has the additional hypothesis that there exists an absolute constant c such that $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all non-CM elliptic curves E over $\mathbb{Q}$ and primes $\ell > c$. This extra assumption is needed by Jones to control the "error term"; the potential problem being that a few elliptic curves with extremely large constants $C_{E,r}$ might over contribute in the average.

We will use Theorem 1.1(i) to control the constants $C_{E,r}$. The connection with our result is that $C_{E,r} \leq [\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(\mathrm{Gal}_{\mathbb{Q}})]\cdot C_r$ for all non-CM elliptic curves $E/\mathbb{Q}$ and integers r.

Other "on average" results using Theorem 1.1 can be found in [ADHT12].

Acknowledgments. Thanks to David Zureick-Brown for his helpful comments.

2. Group theory

2.1. **Cartan subgroups.**

Fix an odd prime ℓ and let $\mathcal{A}$ be a free commutative étale $\mathbb{Z}_\ell$-algebra of rank 2. Up to isomorphism, there are two such algebras; we will say that $\mathcal{A}$ is split or non-split if $\mathcal{A}/\ell\mathcal{A}$ is isomorphic to $\mathbb{F}_\ell\times\mathbb{F}_\ell$ or $\mathbb{F}_{\ell^2}$, respectively. The algebra $\mathcal{A}$ has a unique automorphism σ of order 2 which induces the natural involution on $\mathcal{A}/\ell\mathcal{A}$ (i.e., the involution $(x,y)\mapsto(y,x)$ or $x\mapsto x^{\ell}$, respectively).

The algebra $\mathcal{A}$ acts on itself by (left) multiplication, so a choice of $\mathbb{Z}_\ell$-basis for $\mathcal{A}$ gives an embedding $\iota\colon \mathcal{A}\hookrightarrow \mathrm{End}_{\mathbb{Z}_\ell}(\mathcal{A})\approx M_2(\mathbb{Z}_\ell)$ of $\mathbb{Z}_\ell$-algebras. Denote the image of ι by R. For a positive integer n, the subgroup $C(\ell^n) := (R/\ell^n R)^\times$ of $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ is a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$. Up to conjugation in $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$, there are two kinds of Cartan subgroups; $C(\ell^n)$ is split or non-split if R is split or non-split, respectively. The Cartan subgroup $C(\ell^n)$ is its own centralizer in $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$. We will denote the normalizer of $C(\ell^n)$ in $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ by $C^+(\ell^n)$; the index of $C(\ell^n)$ in $C^+(\ell^n)$ is 2 and the non-identity coset of $C^+(\ell^n)/C(\ell^n)$ is represented by the image of the involution $\sigma\in\mathrm{End}_{\mathbb{Z}_\ell}(\mathcal{A})\approx M_2(\mathbb{Z}_\ell)$ in $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$.

More concretely, the group $\{\left(\begin{smallmatrix} a & 0\\ 0 & b\end{smallmatrix}\right) : a,b\in(\mathbb{Z}/\ell^n\mathbb{Z})^\times\}$ is a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ and the matrix $\left(\begin{smallmatrix} 0 & 1\\ 1 & 0\end{smallmatrix}\right)$ lies in its normalizer. With a fixed non-square $\varepsilon\in(\mathbb{Z}/\ell^n\mathbb{Z})^\times$, the group

$\{\left(\begin{smallmatrix} a & \varepsilon b \\ b & a \end{smallmatrix}\right) : a, b \in \mathbb{Z}/\ell^n\mathbb{Z},\ (a,b) \not\equiv (0,0) \pmod{\ell}\}$ is a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ and the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ lies in its normalizer.

Lemma 2.1. *Let α be an element of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ for which $\mathrm{tr}(\alpha)^2 - 4\det(\alpha) \not\equiv 0 \pmod{\ell}$, and let R be the $\mathbb{Z}_\ell$-subalgebra of $M_2(\mathbb{Z}_\ell)$ generated by α. Fix an integer $n \geq 1$ and let $\overline{\alpha}$ be the image of α in $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$.*

- (i) *The ring R is a free commutative étale $\mathbb{Z}_\ell$-algebra of rank 2.*
- (ii) *The centralizer of $\overline{\alpha}$ in $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ is the Cartan subgroup $C(\ell^n) := (R/\ell^n R)^\times$.*
- (iii) *If g is an element of $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ for which $g\overline{\alpha}g^{-1}$ belongs to $C(\ell^n)$, then g belongs to $C^+(\ell^n)$.*
- (iv) *Let H be a cyclic subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ generated by a matrix of the form $h = I + \ell^i A$ with $1 \leq i < n$. Suppose that H is stable under conjugation by $\overline{\alpha}$ and that $A \pmod{\ell}$ is a non-zero element of $R/\ell R$. Then $H \subseteq C(\ell^n)$.*
- (v) *The image of $B \in C(\ell)$ in $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ has order greater than 2 if and only if $\mathrm{tr}(B)^2 - 4\det(B) \neq 0$ and $\mathrm{tr}(B) \neq 0$.*

Proof. (i) We claim that $\{I, \alpha\}$ is a basis of R as a $\mathbb{Z}_\ell$-module; it is generated by $\{I, \alpha\}$ by the Cayley-Hamilton theorem, so it suffices to show that they are linearly independent. Suppose that $aI + b\alpha = 0$ with $a, b \in \mathbb{Z}_\ell$ not both zero. By dividing by an appropriate power of ℓ, we may assume that a or b is non-zero modulo ℓ. Reducing modulo ℓ, we find that $\alpha \pmod{\ell}$ must be a scalar matrix which contradicts our assumption that $\mathrm{tr}(\alpha)^2 - 4\det(\alpha) \not\equiv 0 \pmod{\ell}$. That R is an étale $\mathbb{Z}_\ell$-algebra follows from $\mathrm{tr}(\alpha)^2 - 4\det(\alpha) \in \mathbb{Z}_\ell^\times$.
(ii) Suppose that $g \in \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ commutes with $\overline{\alpha}$. It thus also commutes with $C(\ell^n) = (R/\ell^n R)^\times$ since $R/\ell^n R$ is the group generated by I and $\overline{\alpha}$. Therefore $g \in C(\ell^n)$, since $C(\ell^n)$ is its own centralizer in $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$.
(iii) Fix an element $m \in C^+(\ell^n) - C(\ell^n)$; it does not commute with $\overline{\alpha}$ by (ii). Since $\mathrm{tr}(\overline{\alpha})^2 - 4\det(\overline{\alpha}) \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times$ and ℓ is odd, one finds that there are exactly two roots of the polynomial $x^2 - \mathrm{tr}(\overline{\alpha})x + \det(\overline{\alpha})$ in $R/\ell^n R$ that are not scalar matrices; they are $\overline{\alpha}$ and $m^{-1}\overline{\alpha}m$. So if $g\overline{\alpha}g^{-1}$ belongs to $C(\ell^n)$, then it equals $\overline{\alpha}$ or $m^{-1}\overline{\alpha}m$. Thus g or mg centralizes $\overline{\alpha}$, and hence g or mg belongs to $C(\ell^n)$ by (ii). Since $m \in C^+(\ell^n)$ and $C(\ell^n) \subseteq C^+(\ell^n)$, we deduce that $g \in C^+(\ell^n)$.
(iv) The group H is cyclic of order ℓ^{n-i}. Since $\overline{\alpha}h\overline{\alpha}^{-1}$ is also a generator of H, there is a unique $m \in (\mathbb{Z}/\ell^{n-i}\mathbb{Z})^\times$ for which $\overline{\alpha}h\overline{\alpha}^{-1} = h^m$. We have $\overline{\alpha}A\overline{\alpha}^{-1} \equiv A \pmod{\ell}$ since by assumption $A \pmod{\ell}$ lies in $R/\ell R$. Therefore,

$$I + \ell^i A \equiv I + \ell^i \overline{\alpha}A\overline{\alpha}^{-1} = \overline{\alpha}h\overline{\alpha}^{-1} = h^m \equiv I + \ell^i m A \pmod{\ell^{i+1}}$$

and hence $m \equiv 1 \pmod{\ell}$ since $A \bmod \ell$ is non-zero. Conjugation by $\overline{\alpha}$ thus gives a group automorphism of H with order dividing ℓ^{n-i-1}, and hence $\beta := \overline{\alpha}^{\ell^{n-i-1}}$ commutes with H. The order of $\overline{\alpha} \pmod{\ell}$ is relatively prime to ℓ, so we also have $\mathrm{tr}(\beta)^2 - 4\det(\beta) \not\equiv 0 \pmod{\ell}$. Using part (ii), the centralizer of β in $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ is a Cartan subgroup that contains $C(\ell^n)$ (the centralizer of $\overline{\alpha}$) thus $C(\ell^n)$ is the centralizer of β. Therefore, $H \subseteq C(\ell^n)$.
(v) That B belongs to $C(\ell)$ implies that it is diagonalizable in $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$. It is then easy to show that B^2 is a scalar matrix (equivalently, the image of B in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ has order 1 or 2) if and only if $\mathrm{tr}(B)^2 - 4\det(B) = 0$ or $\mathrm{tr}(B) = 0$. □

2.2. **Congruence filtration.** Fix a prime ℓ and a closed subgroup G of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. [We will eventually consider $G = \rho_{E,\ell^\infty}(\mathrm{Gal}_\mathbb{Q})$ for a non-CM elliptic curve $E/\mathbb{Q}$.] For each positive integer n, let $G(\ell^n)$ be the image of G under the reduction modulo ℓ^n homomorphism $\mathrm{GL}_2(\mathbb{Z}_\ell) \to \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$.

For each $n \geq 1$, we let G_n be the subgroup consisting of those $A \in G$ for which $A \equiv I \pmod{\ell^n}$. The groups G_n are normal closed subgroups of G and form a fundamental system of neighbourhoods of 1 in G.

Let $\mathfrak{gl}_2(\mathbb{F}_\ell)$ be the additive group $M_2(\mathbb{F}_\ell)$ and let $\mathfrak{sl}_2(\mathbb{F}_\ell)$ be the subgroup of trace 0 matrices; they are Lie algebras over $\mathbb{F}_\ell$ when equipped with the usual pairing $[A, B] = AB - BA$. For each $n \geq 1$, we have an injective group homomorphism

$$G_n/G_{n+1} \hookrightarrow \mathfrak{gl}_2(\mathbb{F}_\ell), \quad I + \ell^n B \mapsto B \bmod \ell$$

whose image we will denote by $\mathfrak{g}_n$. From the groups $\mathfrak{g}_n$ and $G(\ell)$, we can recover the cardinality of each $G(\ell^i)$, though not necessarily the group. Indeed, for each $i \geq 1$ we have $|G(\ell^{i+1})| = |G(\ell^i)||\mathfrak{g}_i|$, so $|G(\ell^i)| = |G(\ell)| \cdot \prod_{n=1}^{i-1} |\mathfrak{g}_n|$. If $\det(G_n) \subseteq 1 + \ell^{n+1}\mathbb{Z}_\ell$, then $\mathfrak{g}_n \subseteq \mathfrak{sl}_2(\mathbb{F}_\ell)$ (note that $\det(I + \ell^n A) = 1 + \ell^n \operatorname{tr}(A) + \ell^{2n} \det(A)$). In particular, if $\det(G) = 1$, then $\mathfrak{g}_n \subseteq \mathfrak{sl}_2(\mathbb{F}_\ell)$ for all $n \geq 1$.

Let $[G, G]$ be the commutator subgroup of G, that is, the smallest closed normal subgroup of G whose quotient group is abelian; it is a closed subgroup of $\mathrm{SL}_2(\mathbb{Z}_\ell)$.

Lemma 2.2. *Fix an integer $n \geq 1$ (assume that $n \geq 2$ if $\ell = 2$).*

(i) $\mathfrak{g}_n \subseteq \mathfrak{g}_{n+1}$.

(ii) *If $\mathfrak{g}_n = \mathfrak{gl}_2(\mathbb{F}_\ell)$, then $G \supseteq I + \ell^n M_2(\mathbb{Z}_\ell)$.*

(iii) *If $\det(G) = 1$ and $\mathfrak{g}_n = \mathfrak{sl}_2(\mathbb{F}_\ell)$, then $G \supseteq \{A \in \mathrm{SL}_2(\mathbb{Z}_\ell) : A \equiv I \pmod{\ell^n}\}$.*

(iv) *If $\mathfrak{g}_n = \mathfrak{g}_{2n}$, then $\mathfrak{g}_n$ is a Lie subalgebra of $\mathfrak{gl}_2(\mathbb{F}_\ell)$.*

(v) *Let $e = 0$ or 1 if ℓ is odd or even, respectively, and suppose that $\{A \in \mathrm{SL}_2(\mathbb{Z}/\ell^{n+1+e}\mathbb{Z}) : A \equiv I \pmod{\ell^n}\}$ is a subset of $G(\ell^{n+1+e})$. Then $\{A \in \mathrm{SL}_2(\mathbb{Z}_\ell) : A \equiv I \pmod{\ell^{2n+e}}\}$ is a subset of $[G, G]$.*

Proof. (i) Take any $B \in \mathfrak{g}_n$. There exists an $A \in M_2(\mathbb{Z}_\ell)$ such that $A \equiv B \pmod{\ell}$ and $I + \ell^n A \in G$. Taking the ℓ-th power of $I + \ell^n A$ we find that

$$(I + \ell^n A)^\ell \equiv I + \ell^{n+1} A + \tbinom{\ell}{2} \ell^{2n} A^2 \qquad \pmod{\ell^{3n}}.$$

When ℓ is odd, we have $(I + \ell^n A)^\ell \equiv I + \ell^{n+1} A \pmod{\ell^{n+2}}$ and hence $B \equiv A \pmod{\ell}$ belongs to $\mathfrak{g}_{n+1}$ (when $\ell = 2$ we need $n \geq 2$ to guarantee that $(I + \ell^n A)^\ell \equiv I + \ell^{n+1} A \pmod{\ell^{n+2}}$).
(ii) We always have an inclusion $\mathfrak{g}_i \subseteq \mathfrak{gl}_2(\mathbb{F}_\ell)$, so by part (i) and our assumption on $\mathfrak{g}_n$ we deduce that $\mathfrak{g}_i = \mathfrak{gl}_2(\mathbb{F}_\ell)$ for all $i \geq n$. So for all $i \geq n$, we have $|G(\ell^i)| = |G(\ell^n)|\ell^{4(i-n)}$. Since G is a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, this is equivalent to G containing the group $I + \ell^n M_2(\mathbb{Z}_\ell)$.
(iii) The proof is similar to (ii), one shows that $|G(\ell^i)| = |G(\ell^n)|\ell^{3(i-n)}$ for all $i \geq n$.
(iv) Take any $B_1, B_2 \in \mathfrak{g}_n$. There are $A_i \in M_2(\mathbb{Z}_\ell)$ such that $A_i \equiv B_i \pmod{\ell}$ and $g_i := I + \ell^n A_i$ belongs to G. The commutator $g_1 g_2 g_1^{-1} g_2^{-1}$ belongs to $[G, G] \subseteq G$ and equals

$$\begin{aligned}
&(I + \ell^n A_1)(I + \ell^n A_2)(I + \ell^n A_1)^{-1}(I + \ell^n A_2)^{-1} \\
=&\big((I + \ell^n A_2)(I + \ell^n A_1) + \ell^{2n}(A_1 A_2 - A_2 A_1)\big)(I + \ell^n A_1)^{-1}(I + \ell^n A_2)^{-1} \\
=&I + \ell^{2n}(A_1 A_2 - A_2 A_1)(I + \ell^n A_1)^{-1}(I + \ell^n A_2)^{-1} \\
\equiv&I + \ell^{2n}(A_1 A_2 - A_2 A_1) \qquad \pmod{\ell^{3n}}.
\end{aligned}$$

Therefore, $[B_1, B_2] = B_1 B_2 - B_2 B_1 \equiv A_1 A_2 - A_2 A_1 \pmod{\ell}$ is an element of $\mathfrak{g}_{2n}$. Since $\mathfrak{g}_n = \mathfrak{g}_{2n}$ by assumption, we deduce that $\mathfrak{g}_n$ is closed under the Lie bracket $[\cdot, \cdot]$.
(v) Set $S := [G, G]$ and let $\{\mathfrak{s}_i\}_{i \geq 1}$ be the filtration of S; each space $\mathfrak{s}_n$ is contained in $\mathfrak{sl}_2(\mathbb{F}_\ell)$. We claim that $\mathfrak{s}_{2n+e} = \mathfrak{sl}_2(\mathbb{F}_\ell)$. Once this is known, we can deduce the desired result from (iii).

Define the integral matrices $B_1 = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$, $B_2 = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$ and $B_3 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. We have $\det(I + \ell^n B_i) \equiv 1 \pmod{\ell^{n+1+e}}$, so by assumption there are $g_i \in G_n$ such that $g_i \equiv I + \ell^n B_i \pmod{\ell^{n+1+e}}$. From the commutator calculations above, the matrix $h := g_i g_j g_i^{-1} g_j^{-1}$ belongs to $[G, G] \cap (I + \ell^{2n} M_2(\mathbb{Z}_\ell))$ and $h \equiv I + \ell^{2n}[B_i, B_j] \pmod{\ell^{2n+1+e}}$. Observe that $[B_1, B_2] = B_3$, $[B_2, B_3] = 2B_2$ and $[B_3, B_1] = 2B_1$. The matrices $2B_1$, $2B_2$ and B_3 modulo ℓ are thus in $\mathfrak{s}_{2n}$ and they generate $\mathfrak{sl}_2(\mathbb{F}_\ell)$ if ℓ is odd. Therefore, $\mathfrak{s}_{2n} = \mathfrak{sl}_2(\mathbb{F}_\ell)$ for ℓ odd. Now consider $\ell = 2$. The group $[G(\ell^{2n+2}), G(\ell^{2n+2})]$ contains $I + \ell^{2n} 2B_1 = I + \ell^{2n+1} B_1 \pmod{\ell^{2n+2}}$, $I + \ell^{2n} 2B_2 = I + \ell^{2n+1} B_2 \pmod{\ell^{2n+2}}$ and

$(I+\ell^{2n}B_3)^\ell \equiv I+\ell^{2n+1}B_3 \pmod{\ell^{2n+2}}$. Therefore, B_1, B_2 and B_3 modulo ℓ belong to $\mathfrak{s}_{2n+1}$ and hence $\mathfrak{s}_{2n+1} = \mathfrak{sl}_2(\mathbb{F}_\ell)$. □

2.3. **Group theory for Proposition 1.2.** Let G be a closed subgroup of $\operatorname{GL}_2(\mathbb{Z}_\ell)$ where ℓ is an odd prime, and keep the notation introduced §2.2. We now impose the following additional assumptions on G which will hold for the rest of this section:

- $\det(G) = \mathbb{Z}_\ell^\times$,
- $G(\ell) \subseteq \operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is contained in the normalizer of a Cartan subgroup, but is not contained in any Cartan subgroup,
- the image of $G(\ell)$ in $\operatorname{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ contains an element with order at least 5.

The goal of this section is to prove the following:

Proposition 2.3. *Take G as above. For each $n \geq 1$, at least one of the following properties hold:*

- *$G(\ell^n)$ is contained in the normalizer of a Cartan subgroup,*
- *$G \supseteq I + \ell^{4n}M_2(\mathbb{Z}_\ell)$.*

Let $C(\ell)$ be a Cartan subgroup of $\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ such that $G(\ell) \subseteq C^+(\ell)$. Using $[C^+(\ell) : C(\ell)] = 2$ and our assumption that the image of $G(\ell)$ in $\operatorname{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ contains an element of order at least 5, we deduce from Lemma 2.1(v) that there exists an $\alpha \in G$ such that $\alpha \pmod{\ell}$ belongs to $C(\ell)$, $\operatorname{tr}(\alpha)^2 - 4\det(\alpha) \not\equiv 0 \pmod{\ell}$ and $\operatorname{tr}(\alpha) \not\equiv 0 \pmod{\ell}$.

Let R be the $\mathbb{Z}_\ell$-subalgebra of $M_2(\mathbb{Z}_\ell)$ generated by α, and for each $n \geq 1$ define $C(\ell^n) = (R/\ell^n R)^\times$. By Lemma 2.1, R is a free commutative étale $\mathbb{Z}_\ell$-algebra of rank 2 and $C(\ell^n)$ is the unique Cartan subgroup of $\operatorname{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ containing α modulo ℓ^n (in particular, our two Cartan subgroups denoted $C(\ell)$ are the same).

The group G acts on each G_n by conjugation, and hence also acts on the quotient group G_n/G_{n+1} with the subgroup G_1 acting trivially. Therefore, $\mathfrak{g}_n \subseteq \mathfrak{gl}_2(\mathbb{F}_\ell)$ is stable under conjugation by $G(\ell) = G/G_1$. To figure out the possibilities for $\mathfrak{g}_n$, we will first decompose $\mathfrak{gl}_2(\mathbb{F}_\ell)$ into irreducible $\mathbb{F}_\ell[G(\ell)]$-modules (the representation theory is straightforward since $\ell \nmid |G(\ell)|$).

Lemma 2.4.

(i) *As an $\mathbb{F}_\ell[G(\ell)]$-module, with $G(\ell)$ acting by conjugation, $\mathfrak{gl}_2(\mathbb{F}_\ell)$ equals $V_1 \oplus V_2 \oplus V_3$ for non-isomorphic irreducible $\mathbb{F}_\ell[G(\ell)]$-modules V_i. They can be ordered so that $V_1 = \mathbb{F}_\ell \cdot I$, $V_2 = \{A \in R/\ell R : \operatorname{tr}(A) = 0\}$ and $\dim_{\mathbb{F}_\ell} V_3 = 2$.*

(ii) *The space V_3 in (i) is not a Lie subalgebra of $\mathfrak{gl}_2(\mathbb{F}_\ell)$.*

(iii) *The group $\mathfrak{sl}_2(\mathbb{F}_\ell)$ is generated by the set $\{gBg^{-1} - B : g \in G(\ell),\ B \in \mathfrak{gl}_2(\mathbb{F}_\ell)\}$.*

Proof. (i) It is easy to check that the V_1 and V_2 as given in the statement are stable under conjugation by $C^+(\ell)$, and hence also by $G(\ell)$, and thus $\mathfrak{gl}_2(\mathbb{F}_\ell) = V_1 \oplus V_2 \oplus V_3$ for some $\mathbb{F}_\ell[G(\ell)]$-module V_3 with dimension 2 over $\mathbb{F}_\ell$. The $G(\ell)$-action on V_1 is trivial while the action on V_2 is non-trivial (since each element of $C^+(\ell) - C(\ell)$ acts as $-I$ on V_2, and by assumption we have $G(\ell) \subseteq C^+(\ell)$ and $G(\ell) \not\subseteq C(\ell)$).

It remains to show that V_3 is an irreducible $\mathbb{F}_\ell[G(\ell)]$-module. Conjugation gives a faithful action of $G(\ell)/G(\ell)\cap\mathbb{F}_\ell^\times$ on $\mathfrak{gl}_2(\mathbb{F}_\ell)$. Since V_1 and V_2 are one dimensional, to prove that V_3 is an irreducible $\mathbb{F}_\ell[G(\ell)]$-module, it suffices to show that the group $G(\ell)/G(\ell) \cap \mathbb{F}_\ell^\times$ is non-abelian.

Suppose that $G(\ell)/G(\ell) \cap \mathbb{F}_\ell^\times$ is abelian. Let $\bar{\alpha}$ be the image of α in $G(\ell)$ and let m be an element in $G(\ell) - C(\ell)$. The cosets of m and $\bar{\alpha}$ in $G(\ell)/G(\ell)\cap\mathbb{F}_\ell^\times$ commute, so $m\bar{\alpha}m^{-1}\bar{\alpha}^{-1} = \zeta$ for some $\zeta \in \mathbb{F}_\ell^\times$. Since $m\bar{\alpha}m^{-1} = \zeta\bar{\alpha}$, we have $\det(\bar{\alpha}) = \zeta^2\det(\bar{\alpha})$ and hence $\zeta = \pm 1$. If $\zeta = 1$, then m and $\bar{\alpha}$ commute which by Lemma 2.1(ii) contradicts $m \notin C(\ell)$. Therefore $\zeta = -1$ and hence $m\bar{\alpha}m^{-1} = -\bar{\alpha}$. However, this contradicts that $\operatorname{tr}(\bar{\alpha}) \neq 0$. So as desired, the group $G(\ell)/G(\ell) \cap \mathbb{F}_\ell^\times$ is non-abelian.

(ii) First suppose that R is split. After conjugating $R/\ell R$ by an element of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, we may assume that $R = \{\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)\}$. We then have $V_3 = \mathbb{F}_\ell \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) \oplus \mathbb{F}_\ell \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$, but $\left[\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) \right] = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ does not belong to V_3. Now suppose that R is non-split. After conjugating $R/\ell R$ by an element of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, we may assume that $R = \{\left(\begin{smallmatrix} a & \varepsilon b \\ b & a \end{smallmatrix}\right)\}$ where $\varepsilon \in (\mathbb{Z}/\ell\mathbb{Z})^\times$ is a fixed non-square. Then $V_3 = \mathbb{F}_\ell \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \oplus \mathbb{F}_\ell \left(\begin{smallmatrix} 0 & \varepsilon \\ -1 & 0 \end{smallmatrix}\right)$, but $\left[\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & \varepsilon \\ -1 & 0 \end{smallmatrix}\right) \right] = 2 \left(\begin{smallmatrix} 0 & \varepsilon \\ 1 & 0 \end{smallmatrix}\right)$ does not belong to V_3.
(iii) Let W be the subspace of $\mathfrak{sl}_2(\mathbb{F}_\ell)$ generated by the set $\{gBg^{-1} - B : g \in G(\ell),\, B \in \mathfrak{gl}_2(\mathbb{F}_\ell)\}$; note that each element of the set does have trace 0. The space W is stable under conjugation by $G(\ell)$, so by (i) we find that W is either 0, V_2, V_3 or $V_2 \oplus V_3 = \mathfrak{sl}_2(\mathbb{F}_\ell)$. It thus suffices to show that W contain non-zero elements from V_2 and V_3. Fix $i \in \{2, 3\}$. Since V_i has a non-trivial $G(\ell)$-action, there are $v \in V_i$ and $g \in G(\ell)$ such that $gvg^{-1} \neq v$. Therefore, $gvg^{-1} - v$ is a non-zero element of W that belongs to V_i. □

Define the closed subgroup $S = G \cap \mathrm{SL}_2(\mathbb{Z}_\ell)$ of G. For each $n \geq 1$, we define $S_n = G_n \cap \mathrm{SL}_2(\mathbb{Z}_\ell)$. We denote the image of the injective homomorphism

$$S_n/S_{n+1} \hookrightarrow \mathfrak{gl}_2(\mathbb{F}_\ell), \quad 1 + \ell^n B \mapsto B \bmod \ell \tag{2.1}$$

by $\mathfrak{s}_n$; it is a subgroup of $\mathfrak{sl}_2(\mathbb{F}_\ell)$.

Lemma 2.5. *With notation as above,* $\mathrm{tr}(\mathfrak{g}_n) = \mathbb{F}_\ell$ *and* $\mathfrak{s}_n = \mathfrak{g}_n \cap \mathfrak{sl}_2(\mathbb{F}_\ell)$ *for all* $n \geq 1$.

Proof. First of all, we claim that $\det(G_n) = 1 + \ell^n \mathbb{Z}_\ell$ for all $n \geq 1$. It suffices to show that there exists a $g \in G_1$ with $\det(g) \not\equiv 1 \pmod{\ell^2}$, since then $g^{\ell^{n-1}} \in G_n$ and one can then show that $\det(g^{\ell^{n-1}})$ generates $1 + \ell^n \mathbb{Z}_\ell$ as a topological group. Since $\det(G) = \mathbb{Z}_\ell^\times$, there exists a $g \in G$ such that $\det(g) \equiv 1 \pmod{\ell}$ and $\det(g) \not\equiv 1 \pmod{\ell^2}$. Since $\ell \nmid |G(\ell)|$, replacing g by $g^{|G(\ell)|}$, we have $g \equiv I \pmod{\ell}$ and $\det(g) \not\equiv 1 \pmod{\ell^2}$ as desired.

For an element $g \in G_n$ of the form $g = I + \ell^n A$, the condition that $\det(g) \not\equiv 1 \pmod{\ell^{n+1}}$ is equivalent to $\mathrm{tr}(A) \not\equiv 0 \pmod{\ell}$. So $\det(G_n) = 1 + \ell^n \mathbb{Z}_\ell$ implies that $\mathrm{tr}(\mathfrak{g}_n) = \mathbb{F}_\ell$.

We certainly have $\mathfrak{s}_n \subseteq \mathfrak{g}_n \cap \mathfrak{sl}_2(\mathbb{F}_\ell)$, so we need only prove the other inclusion. Take any $B \in \mathfrak{g}_n$ with trace 0, and pick an A such that $I + \ell^n A \in G$ with $A \equiv B \pmod{\ell}$. We have $\det(I + \ell^n A) \equiv 1 \pmod{\ell^{n+1}}$ since $\mathrm{tr}(A) \equiv 0 \pmod{\ell}$, so there exists an element $g \in G_{n+1}$ such that $\det(g) = \det(I + \ell^n A)$. The matrix $s := g^{-1}(I + \ell^n A)$ has determinant 1, and hence belongs to S. It satisfies $s \equiv I + \ell^n A \pmod{\ell^{n+1}}$ since $g \equiv I \pmod{\ell^{n+1}}$, so $B \equiv A \pmod{\ell}$ belongs to $\mathfrak{s}_n$. □

Proof of Proposition 2.3.
Case 1: $\dim_{\mathbb{F}_\ell} \mathfrak{g}_n = 4$.

We have $\mathfrak{g}_n = \mathfrak{gl}_2(\mathbb{F}_\ell)$, so G contains the group $I + \ell^n M_2(\mathbb{Z}_\ell)$ by Lemma 2.2(ii).
Case 2: $\dim_{\mathbb{F}_\ell} \mathfrak{g}_n = 3$.

If $\dim_{\mathbb{F}_\ell} \mathfrak{g}_{2n} = 4$, then Case 1 shows that G contains the group $1 + \ell^{2n} M_2(\mathbb{Z}_\ell)$. So we may assume that $\dim_{\mathbb{F}_\ell} \mathfrak{g}_{2n} = 3$ and hence $\mathfrak{g}_n = \mathfrak{g}_{2n}$. Since $\mathfrak{g}_n$ has dimension 3 over $\mathbb{F}_\ell$, is stable under conjugation by $G(\ell)$, and satisfies $\mathrm{tr}(\mathfrak{g}_n) = \mathbb{F}_\ell$, we deduce from Lemma 2.4(i) that $\mathfrak{g}_n = \mathbb{F}_\ell \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \oplus V_3$. We thus have $\mathfrak{s}_n = V_3$ which is *not* a Lie subalgebra of $\mathfrak{gl}_2(\mathbb{F}_\ell)$ by Lemma 2.4(ii). However, $\mathfrak{g}_n = \mathfrak{g}_{2n}$ and Lemma 2.2(iv) implies that $\mathfrak{g}_n$, and hence also $\mathfrak{s}_n = \mathfrak{g}_n \cap \mathfrak{sl}_2(\mathbb{F}_\ell)$, is a Lie subalgebra of $\mathfrak{gl}_2(\mathbb{F}_\ell)$. This is a contradiction, so we cannot have $\dim_{\mathbb{F}_\ell} \mathfrak{g}_{2n} = 3$.
Case 3: $\dim_{\mathbb{F}_\ell} \mathfrak{g}_n = 2$.

If $\dim_{\mathbb{F}_\ell} \mathfrak{g}_{2n}$ equals 3 or 4, then Cases 1 and 2 above show that G contains the group $1 + \ell^{4n} M_2(\mathbb{Z}_\ell)$. So assume that $\dim_{\mathbb{F}_\ell} \mathfrak{g}_{2n} = 2$.

Let $S(\ell^{2n})$ be the image of S under the reduction modulo ℓ^{2n} map $\mathrm{SL}_2(\mathbb{Z}_\ell) \to \mathrm{SL}_2(\mathbb{Z}/\ell^{2n}\mathbb{Z})$. Let H be the subgroup of $S(\ell^{2n})$ consisting of those matrices congruence to I modulo ℓ^n. Since $\dim_{\mathbb{F}_\ell} \mathfrak{g}_n = \dim_{\mathbb{F}_\ell} \mathfrak{g}_{2n} = 2$, we deduce from Lemma 2.5 and Lemma 2.2(i) that $\dim_{\mathbb{F}_\ell} \mathfrak{s}_i = 1$ for

$n \leq i \leq 2n$. There exists an element $h \in S(\ell^{2n})$ of the form $I + \ell^n A$ with $A \bmod \ell$ non-zero. By cardinality considerations, the group H is generated by h. The group H is normalized by $G(\ell^{2n})$.

Using $\mathfrak{s}_n \subseteq \mathfrak{sl}_2(\mathbb{F}_\ell)$, $\dim_{\mathbb{F}_\ell} \mathfrak{s}_n = 1$, and Lemma 2.4(i), we find that there is only one possibility for $\mathfrak{s}_n$, i.e., $\mathfrak{s}_n = \{B \in R/\ell R : \operatorname{tr}(B) = 0\}$. Since $A \pmod{\ell}$ belongs to $R/\ell R$, we have $H \subseteq C(\ell^{2n})$ by Lemma 2.1(iv). We then have

$$H = \big\{a \in C(\ell^{2n}) : \det(a) \equiv 1 \pmod{\ell^{2n}} \text{ and } a \equiv I \pmod{\ell^n}\big\};$$

the inclusion "$\subseteq$" is now clear and both groups have cardinality ℓ^n. The group $G(\ell^{2n})$ normalizes H, hence it also normalizes $H' := \{a \in C(\ell^{2n}) : a \equiv I \pmod{\ell^n}\} = I + \ell^n R/\ell^{2n}R$ (the group H' is obtained from H by including scalar matrices that are congruent to the identity modulo ℓ^n).

Now take any $g \in G$. For any $a \in R$, we have just shown that there exists an element $b \in R$ such that $g(I + \ell^n a)g^{-1} \equiv I + \ell^n b \pmod{\ell^{2n}}$, and hence $gag^{-1} \equiv b \pmod{\ell^n}$. Therefore, $g \pmod{\ell^n}$ normalizes $R/\ell^n R$ and thus belongs to $C^+(\ell^n)$. We conclude that $G(\ell^n) \subseteq C^+(\ell^n)$.

Case 4: $\dim_{\mathbb{F}_\ell} \mathfrak{g}_n = 1$.

By Lemma 2.5 and Lemma 2.4, we have $\mathfrak{g}_1 = \cdots = \mathfrak{g}_n = \mathbb{F}_\ell \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Let H be the subgroup of $G(\ell^n)$ consisting of those matrices that are congruent to I modulo ℓ. There exists an element $h \in H$ of the form $I + \ell A$ for which $A \equiv I \pmod{\ell}$. By cardinality considerations, the group H is generated by h. The group H is stable under conjugation by $G(\ell^n)$. Therefore by Lemma 2.1(iv), we have $H \subseteq C(\ell^n)$.

Let W be the group of $g \in G(\ell^n)$ for which $g \pmod{\ell}$ belongs to $C(\ell)$; it is an index 2 subgroup of $G(\ell^n)$. Take any $g \in W$. Since $\alpha \pmod{\ell}$ and $g \pmod{\ell}$ commute, the commutator $g\alpha g^{-1}\alpha^{-1} \pmod{\ell^n}$ belongs to $H \subseteq C(\ell^n)$ and hence $g\alpha g^{-1} \pmod{\ell^n}$ is an element of $C(\ell^n)$. By Lemma 2.1(iii), this implies that g is an element of $C^+(\ell^n)$. Since g was arbitrary, we have $W \subseteq C^+(\ell^n)$ and by considering its image modulo ℓ we must have $W \subseteq C(\ell^n)$. Finally, the group $W \subseteq C(\ell^n)$ contains α and is normalized by $G(\ell^n)$, thus $G(\ell^n) \subseteq C^+(\ell^n)$ by Lemma 2.1(iii). □

2.4. **Proof of Proposition 1.2.** We will apply Proposition 2.3 with the group $G := \rho_{E,\ell^\infty}(\operatorname{Gal}_{\mathbb{Q}})$ contained in $\operatorname{GL}_2(\mathbb{Z}_\ell)$. The representation $\det \circ \rho_{E,\ell^\infty} \colon \operatorname{Gal}_{\mathbb{Q}} \to \mathbb{Z}_\ell^\times$ is the ℓ-adic cyclotomic character, and hence $\det(G) = \mathbb{Z}_\ell^\times$. If $G(\ell) = \rho_{E,\ell}(\operatorname{Gal}_{\mathbb{Q}})$ equals $\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, then $G = \operatorname{GL}_2(\mathbb{Z}_\ell)$ by [Ser81, Lemme 15] and the result is immediate for all n. So assume that $G(\ell) \neq \operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, and hence by our assumption $\ell > 17$ and $\ell \neq 37$, the group $G(\ell)$ lies in the normalizer of some Cartan subgroup of $\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ but is not contained in any Cartan subgroup [Ser81, Lemme 16–18]. The image of $G(\ell)$ in $\operatorname{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ contains an element of order greater than 5 by [Ser81, Lemme 18'] and our assumption $\ell > 17$.

We have verified that our G satisfies the assumptions of Proposition 2.3, so for each $n \geq 1$ the group $G(\ell^n) = \rho_{E,\ell^n}(\operatorname{Gal}_{\mathbb{Q}})$ is contained in the normalizer of a non-split Cartan subgroup *or* G contains $I + \ell^{4n} M_2(\mathbb{Z}_\ell)$. This completes the proof of Proposition 1.2.

To obtain better bounds, we will use the following lemma with Proposition 1.2.

Lemma 2.6. *Let E be a non-CM elliptic curve over $\mathbb{Q}$ and let ℓ be a prime greater than 17 and not equal to 37. If $\rho_{E,\ell^\infty}(\operatorname{Gal}_{\mathbb{Q}}) \supseteq I + \ell^n M_2(\mathbb{Z}_\ell)$, then $\rho_{E,\ell^\infty}(\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\text{cyc}})) \supseteq \{A \in \operatorname{SL}_2(\mathbb{Z}_\ell) : A \equiv I \pmod{\ell^n}\}$ where $\mathbb{Q}^{\text{cyc}}$ is the cyclotomic extension of $\mathbb{Q}$.*

Proof. Define $G := \rho_{E,\ell^\infty}(\operatorname{Gal}_{\mathbb{Q}})$; as noted above, G satisfies the conditions of §2.3. Since $\mathbb{Q}^{\text{cyc}}$ is the maximal abelian extension of $\mathbb{Q}$, we have $[G,G] = \rho_{E,\ell^\infty}(\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\text{cyc}}))$. Define $S := [G,G] \subseteq \operatorname{SL}_2(\mathbb{Z}_\ell)$ and for each $n \geq 1$, define S_n and $\mathfrak{s}_n$ as done at (2.1). The commutator map $G \times G_n \to S_n$, $(g, I + \ell^n A) \mapsto g(I + \ell^n A)g^{-1}(I + \ell^n A)^{-1}$ induces a function

$$f \colon G(\ell) \times \mathfrak{g}_n \to \mathfrak{s}_n, \quad (g, B) \mapsto gBg^{-1} - B.$$

Our hypothesis on the image of ρ_{E,ℓ^∞} implies that $\mathfrak{g}_n = \mathfrak{gl}_2(\mathbb{F}_\ell)$. Lemma 2.4(iii) implies that $\mathfrak{s}_n = \mathfrak{sl}_2(\mathbb{F}_\ell)$ and hence $S \supseteq \{A \in \mathrm{SL}_2(\mathbb{Z}_\ell) : A \equiv I \pmod{\ell^n}\}$ by Lemma 2.2(iii). □

3. Quadratic characters arising from non-surjective $\rho_{E,\ell}$

Let E be a non-CM elliptic curve defined over $\mathbb{Q}$. Let N be the product of primes p for which E has bad reduction and let $\omega(N)$ be the number of distinct prime factors of N. We now follow an approach used by Serre [Ser81, §8.4], and then by Kraus [Kra95] and Cojocaru [Coj05].

Let ℓ be a prime satisfying $\ell > 17$ and $\ell \neq 37$ for which $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q}) \neq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. By [Ser81, Lemmas 16–18], $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ is contained in the normalizer of some Cartan subgroup $C(\ell)$ but is not contained in any Cartan subgroup. We can thus define a non-trivial character

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

By [Ser72, p.317], ε_ℓ is unramified at all primes $p \nmid N$.

For each prime $p \nmid N$, let E_p be the reduction of E modulo p and let $a_p(E)$ be the integer satisfying $|E_p(\mathbb{F}_p)| = p + 1 - a_p(E)$. Hasse showed that $|a_p(E)| \leq 2\sqrt{p}$.

Lemma 3.1. *Let ℓ be a prime as above and n a positive integer such that $\rho_{E,\ell^n}(\mathrm{Gal}_\mathbb{Q})$ is contained in the normalizer of a Cartan subgroup. If $p \nmid N$ is a prime for which $\varepsilon_\ell(\mathrm{Frob}_p) = -1$, then $a_p(E) \equiv 0 \pmod{\ell^n}$.*

Proof. By assumption there is a Cartan subgroup $C(\ell^n)$ of $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ such that $\rho_{E,\ell^n}(\mathrm{Gal}_\mathbb{Q}) \subseteq C^+(\ell^n)$. The representation

$$\mathrm{Gal}_\mathbb{Q} \xrightarrow{\rho_{E,\ell^n}} C^+(\ell^n)/C(\ell^n) \xrightarrow{\sim} \{\pm 1\}$$

agrees with ε_ℓ. If $p \nmid N\ell$, then the representation ρ_{E,ℓ^n} is unramified at p. The condition $\varepsilon_\ell(\mathrm{Frob}_p) = -1$ means that $\rho_{E,\ell^n}(\mathrm{Frob}_p) \subseteq C^+(\ell^n) - C(\ell^n)$. We have $\mathrm{tr}(A) \equiv 0 \pmod{\ell^n}$ for all $A \in C^+(\ell^n) - C(\ell^n)$ (this can be checked directly from the explicit description of Cartan subgroups in §2.1). Therefore, $a_p(E) \equiv \mathrm{tr}(\rho_{E,\ell^n}(\mathrm{Frob}_p)) \equiv 0 \pmod{\ell^n}$.

Now suppose that $p = \ell$. By [Ser72, p.317 (c_5)], we have $a_\ell(E) \equiv 0 \pmod{\ell}$, so $a_\ell(E) = 0$ by the Hasse bound (this uses $\ell \geq 5$). □

Take a prime power ℓ^n as in Lemma 3.1 and suppose that $p \nmid N$ is a prime for which $\varepsilon_\ell(\mathrm{Frob}_p) = -1$ and $a_p(E) \neq 0$. Then ℓ^n divides $a_p(E)$, and hence $\ell^n \leq 2\sqrt{p}$ by Hasse's bound. So to bound ℓ^n it suffices to effectively choose such a prime p.

Lemma 3.2. *Let $\varepsilon \colon \mathrm{Gal}_\mathbb{Q} \to \{\pm 1\}$ be a non-trivial character that is unramified at all $p \nmid N$.*

(i) *Assuming the Generalized Riemann Hypothesis (GRH), there exists an absolute constant c and a prime $p \nmid N$ with $p \leq c(\log N)^2(\log\log(2N))^6$ such that $\varepsilon(\mathrm{Frob}_p) = -1$ and $a_p(E) \neq 0$.*

(ii) *There exists a prime $p \nmid N$ with $p \leq 1152 \cdot N^2(1 + \log\log N)$ such that $\varepsilon(\mathrm{Frob}_p) = -1$ and $a_p(E) \neq 0$.*

Proof. For part (i) see the proof of [Ser81, Lemme 19] (the proof uses $\varepsilon = \varepsilon_\ell$ but only needs our assumption that ε is unramified at $p \nmid N$). It uses an effective version of the Chebotarev density theorem.

We now prove (ii) using the argument in [Kra95]. Let E_2 be the elliptic curve defined over $\mathbb{Q}$ obtained by twisting $E_1 := E$ by the character ε. From our assumption on ε, the curve E_2 has good reduction at all primes $p \nmid N$ and for each $p \nmid N$, we have $a_p(E_2) = \varepsilon(\mathrm{Frob}_p)a_p(E_1)$. Thus for $p \nmid N$, the condition $\varepsilon(\mathrm{Frob}_p) = -1$ and $a_p(E) \neq 0$ is equivalent to having $a_p(E_1) \neq a_p(E_2)$.

Let N_i be the conductor of E_i and define $N_i' = N_i \prod_{p|N} p^{d_i(p)}$, where $d_i(p) = 0, 1$ or 2 if E_i has good, multiplicative or additive reduction, respectively, at p. Let M be the least common multiple of N_1' and N_2'. By [Del85, §5 C], there exists a prime $p \nmid N$ satisfying $p \leq \frac{M}{6} \cdot \prod_{p|M} \left(1 + \frac{1}{p}\right)$ and $a_p(E_1) \neq a_p(E_2)$ (this last step uses that E_1 and E_2 are modular [BCDT]).

The integer M has the same prime factors as N and it divides $2^6 3^3 N^2$, so the above prime p is at most $288 \cdot N^2 \prod_{p|N} \left(1 + \frac{1}{p}\right)$. The final bound follows by using $\prod_{p|N} \left(1 + \frac{1}{p}\right) \leq 4(1 + \log\log N)$ [Kra95, Lemme 2]. □

Consider the case $n = 1$. If $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}}) \neq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, then by Lemma 3.2(ii) there is a prime $p \leq 1152 \cdot N^2(1 + \log\log N)$ such that $\varepsilon_\ell(\mathrm{Frob}_p) = -1$ and $a_p(E) \neq 0$. The prime ℓ divides $a_p(E)$ by Lemma 3.1, so by the Hasse bound we have

$$\ell \leq |a_p(E)| \leq 2\sqrt{p} \leq 2\big(1152 \cdot N^2(1 + \log\log N)\big)^{1/2} < 68N(1 + \log\log N)^{1/2}.$$

Therefore $\rho_{E,\ell}$ is surjective for all $\ell \geq 68N(1 + \log\log N)^{1/2}$, which is the main result of [Kra95].

We now consider higher powers of n while keeping track of divisibilities. Cojocaru [Coj05] handles several primes in bounding the product of primes of ℓ for which $\rho_{E,\ell}$ is not surjective.

Proposition 3.3. *Let E be a non-CM elliptic curve over $\mathbb{Q}$. Let N be the product of the primes p for which E has bad reduction.*

(i) *Assuming GRH, there is an absolute constant c and a positive integer*

$$M \leq \big(c(\log N)(\log\log(2N))^3\big)^{\omega(N)+1}$$

such that if $\rho_{E,\ell^n}(\mathrm{Gal}_{\mathbb{Q}})$ is contained in the normalizer of a Cartan subgroup with $\ell > 17$ and $\ell \neq 37$, then ℓ^n divides M.

(ii) *There is a positive integer*

$$M \leq \big(68N(1 + \log\log N)^{1/2}\big)^{\omega(N)+1}$$

such that if $\rho_{E,\ell^n}(\mathrm{Gal}_{\mathbb{Q}})$ is contained in the normalizer of a Cartan subgroup with $\ell > 17$ and $\ell \neq 37$, then ℓ^n divides M.

Proof. If N is odd, define $N_0 = N$, otherwise define $N_0 = 4N$. Let V_1 be the group of characters $(\mathbb{Z}/N_0\mathbb{Z})^\times \to \{\pm 1\}$, which we may view as a vector space over $\mathbb{F}_2$. Let d be the dimension of V_1 over $\mathbb{F}_2$.

We will define a sequence of primes $p_1, \ldots, p_d$ that are relatively prime to N such that $a_{p_i}(E) \neq 0$ for all i and that for every non-trivial character $\alpha \in V_1$, we have $\alpha(p_i) = -1$ for some $i \in \{1, .., d\}$. We proceed recursively on $i = 1, \ldots, d$. Choose a non-trivial character $\alpha_i \in V_i$. Assuming GRH, Lemma 3.2(i) says there is a prime $p_i \nmid N$ satisfying

$$p_i \leq c(\log N)^2(\log\log(2N))^6 \tag{3.1}$$

such that $\alpha_i(p_i) = -1$ and $a_{p_i}(E) \neq 0$. Let V_{i+1} be the subspace of V_i consisting of those characters ε for which $\varepsilon(p_i) = 1$. The space V_{i+1} has dimension $d - i$ over $\mathbb{F}_2$. Since $V_{d+1} = 1$, our sequence of primes $p_1, \ldots, p_d$ has the desired property.

Define the positive integer

$$M = \prod_{i=1}^{d} |a_{p_i}(E)|.$$

Consider ℓ and n as in the statement of the proposition. Since $\varepsilon_\ell \colon \mathrm{Gal}_{\mathbb{Q}} \to \{\pm 1\}$ is unramified at all $p \nmid N$, we may associate to it a Dirichlet character $\varepsilon \colon (\mathbb{Z}/N_0\mathbb{Z})^\times \to \{\pm 1\}$ that satisfies $\varepsilon_\ell(\mathrm{Frob}_p) = \varepsilon(p)$ for all $p \nmid N$. Since ε_ℓ, and hence ε, is non-trivial, there is some $i \in \{1, \ldots, d\}$ for which $\varepsilon_\ell(\mathrm{Frob}_{p_i}) = \varepsilon(p_i) = -1$. By Lemma 3.1, we have $a_{p_i}(E) \equiv 0 \pmod{\ell^n}$, and hence ℓ^n divides M. It remains to bound M. Using Hasse's bound and (3.1), we obtain

$$M \leq \prod_{i=1}^{d} 2\big(c(\log N)^2(\log\log(2N))^6\big)^{1/2} = \big(2c^{1/2}(\log N)(\log\log(2N))^3\big)^d.$$

Part (i) follows by noting that $d \leq \omega(N)+1$.

Part (ii) is proved in the exact same way as (i) except that Lemma 3.2(ii) is used to choose the primes $p_1,\ldots,p_d$. We then have an appropriate M with

$$M \leq \prod\nolimits_{i=1}^{d} 2\big(1152\cdot N^2(1+\log\log N)\big)^{1/2} \leq \big(68N(1+\log\log N)^{1/2}\big)^d \qquad \square$$

Remark 3.4. Let $A(E)$ be the product of the primes ℓ for which $\rho_{E,\ell}$ is not surjective. By Proposition 3.3(ii), we have $A(E) \leq \big(37\prod_{\ell\leq 17}\ell\big)\cdot\big(68N(1+\log\log N)^{1/2}\big)^{\omega(N)+1}$

Theorem 2 of [Coj05] claims that $A(E) \ll N'(\log\log N')^{1/2}$ where N' is the conductor of E, but there seems to be a small gap in the proof. If ℓ is a prime greater than 17 and not 37 for which $\rho_{E,\ell}$ is not surjective, then one can use Lemma 3.2(ii), or something similar, to choose a small prime $p\nmid N$ for which $a_p(E)\neq 0$ and $\varepsilon_\ell(p)=-1$. However, it is not clear why this particular choice of p should work for all such ℓ. To make our proof work, we chose at most $\omega(N)+1$ different primes p_i, which is why our bound is essentially the $(\omega(N)+1)$-th power of that in [Coj05].

4. Masser and Wüstholz approach

Let E be a non-CM elliptic curve defined over $\mathbb{Q}$. Masser and Wüstholz have shown that $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q}) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all $\ell \geq c\big(\max\{1,h(j_E)\}\big)^\gamma$ where c and γ are absolute constants [MW93] (they actually prove an analogous results for elliptic curves over an arbitrary number field, but we will continue our focus on curves over $\mathbb{Q}$). This theorem was later refined by Masser in [Mas98, Theorem 3] where he proved the following: there are absolute constants c and γ, and a positive integer $M \leq c\big(\max\{1,h(j_E)\}\big)^\gamma$ such that $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q}) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all $\ell\nmid M$.

The main tool of Masser and Wüstholz is an effective bound of the minimal possible degree of an isogeny between two isogenous abelian varieties. We will use the following variant [Mas98, p.190 Theorem D]. For a principally polarized abelian variety A over a number field, let $h(A)$ denote its (absolute, logarithmic, semistable) Faltings height.

Theorem 4.1. *Let r and D be positive integers. Then there are constants c and κ, depending only on r and D, with the following property: Suppose that A is a principally polarized abelian variety of dimension r defined over a number field k. Suppose further that A is isomorphic over k to a product $A_1^{e_1}\times\cdots\times A_t^{e_t}$, where $A_1,\ldots,A_t$ are simple, pairwise non-isogenous, and have trivial endomorphism rings. Then there is a positive integer*

$$b(k,A,D) \leq c\big(\max\{[k:\mathbb{Q}],h(A)\}\big)^\kappa$$

such that if A^* is an abelian variety, defined over an extension K of k of relative degree at most D, that is isogenous over K to A, then there is an isogeny over K from A^* to A whose degree divides $b(k,A,D)$.

Our application of this theorem is the following. The proof is the same as [MW93, Lemma 3.2] except using the above refined theorem and considering higher prime powers.

Proposition 4.2. *There are absolute constants c and κ with the following property. Suppose that E is a non-CM elliptic curve defined over $\mathbb{Q}$. Then there is a positive integer $M \leq c\big(\max\{1,h(j_E)\}\big)^\kappa$ such that if $\rho_{E,\ell^n}(\mathrm{Gal}_\mathbb{Q})$ is contained in the normalizer of a Cartan subgroup with $\ell\geq 7$, then ℓ^n divides M.*

Proof. Suppose that $\ell\geq 7$ is a prime for which $\rho_{E,\ell^n}(\mathrm{Gal}_\mathbb{Q})$ is contained in the normalizer of a Cartan subgroup. There is a quadratic extension K of $\mathbb{Q}$ such that $\rho_{E,\ell^n}(\mathrm{Gal}(\overline{\mathbb{Q}}/K))$ is contained in a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$. By [Ser81, Lemme 18'], the image of $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q})$ in $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ contains an element of order at least $(\ell-1)/4$, and in particular of order greater than 1 since $\ell\geq 7$.

Therefore, $\rho_{E,\ell^n}(\mathrm{Gal}(\overline{\mathbb{Q}}/K)) \subseteq \mathrm{Aut}(E[\ell^n]) \cong \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ contains an element α for which $\alpha \pmod{\ell}$ is not a scalar matrix.

Let Γ be the finite subgroup of $A := E\times E$ consisting of pairs of points $(x, \alpha x)$ with $x \in E[\ell^n]$. The group Γ is defined over K, since an arbitrary $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ takes $(x, \alpha x)$ to $(\rho_{E,\ell^n}(\sigma)x, \rho_{E,\ell^n}(\sigma)\alpha x)$, which is $(y, \alpha y)$ for $y = \rho_{E,\ell^n}(\sigma)x$ (we have used that $\rho_{E,\ell^n}(\mathrm{Gal}(\overline{\mathbb{Q}}/K))$ is commutative). Therefore, the abelian variety $A^* := A/\Gamma$ and the natural isogeny $\psi\colon A \to A^*$ are both defined over K. By Theorem 4.1, there is an isogeny $\phi\colon A^* \to A$ defined over K whose degree divides $b(\mathbb{Q}, E \times E, 2)$. The composition $\varepsilon := \phi\circ\psi$ is an endomorphism of $A = E\times E$. Since E is non-CM, there are integers $a, b, c, d \in \mathbb{Z}$ such that $\varepsilon(x, y) = (ax + by, cx + dy)$. Since $\Gamma \subseteq \ker(\varepsilon)$, we have $ax + b\alpha x = 0$ and $cx + d\alpha x = 0$ for all $x \in E[\ell^n]$. Equivalently, $a + b\alpha \equiv 0$ and $c + d\alpha \equiv 0 \pmod{\ell^n}$. Since $\alpha \pmod{\ell}$ is non-scalar, we deduce that ℓ^n divides a, b, c and d. Therefore, ℓ^{4n} divides $\deg\varepsilon = (ad - bc)^2$. Since $\deg\psi = |\Gamma| = \ell^{2n}$ and $\deg\varepsilon = \deg\phi \cdot \deg\psi$, we find that ℓ^{2n} divides $\deg\phi$ and hence also $b(\mathbb{Q}, E \times E, 2)$.

So we shall take $M = b(\mathbb{Q}, E \times E, 2)$, and it remain to prove that M has the desired upper bound. Since $b(\mathbb{Q}, E \times E, 2) \leq c(\max\{1, h(E \times E)\})^\kappa$ for absolute constants c and κ, it suffices to note that $h(E \times E) = 2h(E)$ and that $h(E) \ll \max\{1, h(j_E)\}$ [Sil86, Proposition 2.1]. □

5. Proof of Proposition 1.3 and Theorem 1.1

We first prove the following lemma to deal with the small primes.

Lemma 5.1. *For each prime ℓ, there is an integer $e(\ell) \geq 1$, depending only on ℓ, such that $\rho_{E,\ell^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{cyc}}))$ contains the group $\{A \in \mathrm{SL}_2(\mathbb{Z}_\ell) : A \equiv I \pmod{\ell^{e(\ell)}}\}$ for all non-CM elliptic curves E over $\mathbb{Q}$.*

Proof. Fix a prime ℓ. For each subgroup H of $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ with $\det(H) = (\mathbb{Z}/\ell^n\mathbb{Z})^\times$, we can define a modular curve X_H over $\mathbb{Q}$ which comes with a morphism $\pi\colon X_H \to \mathbb{P}^1_\mathbb{Q}$ to the j-line [DR73, IV-3]. If E is an elliptic curve over $\mathbb{Q}$ with $\rho_{E,\ell^n}(\mathrm{Gal}_\mathbb{Q}) \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ conjugate to a subgroup of H, then there is a rational point $P \in X_H(\mathbb{Q})$ such that $\pi(P)$ equals the j-invariant of E.

Let Γ_H be the congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ consisting of those $A \in \mathrm{SL}_2(\mathbb{Z})$ for which A modulo ℓ^n belongs to H. The genus of X_H is equal to the genus of Γ_H (which is the genus of the Riemann surface obtained by the usual quotient of the upper-half plane by the group Γ_H acting via linear fractional transformations and adding cusps). There are only finitely many congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ of genus 0 or 1, cf. [Den75]. Hence, there exists an integer $f = f(\ell) \geq 1$ such that if H is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell^{f+2}\mathbb{Z})$ for which X_H has genus at most 1, then $H \supseteq \{A \in \mathrm{SL}_2(\mathbb{Z}/\ell^{f+2}\mathbb{Z}) : A \equiv I \pmod{\ell^f}\}$. Apply Faltings' theorem (originally, Mordell's conjecture) to the modular curves X_H with groups $H \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell^{f+2}\mathbb{Z})$ not containing $\{A \in \mathrm{SL}_2(\mathbb{Z}/\ell^{f+2}\mathbb{Z}) : A \equiv I \pmod{\ell^f}\}$, we find that there is a *finite* set $J \subseteq \mathbb{Q}$ such $\rho_{E,\ell^{f+2}}(\mathrm{Gal}_\mathbb{Q}) \supseteq \{A \in \mathrm{SL}_2(\mathbb{Z}/\ell^{f+2}\mathbb{Z}) : A \equiv I \pmod{\ell^f}\}$ for all elliptic curves $E/\mathbb{Q}$ with $j(E) \notin J$. If $E/\mathbb{Q}$ satisfies $j(E) \notin J$, then Lemma 2.2(v) implies that $\rho_{E,\ell^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{cyc}})) \supseteq \{A \in \mathrm{SL}_2(\mathbb{Z}_\ell) : A \equiv I \pmod{\ell^{2f+2}}\}$ (since $\mathbb{Q}^{\mathrm{cyc}}$ is the maximal abelian extension of $\mathbb{Q}$, $\rho_{E,\ell^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{cyc}}))$ is the commutator subgroup of $\rho_{E,\ell^\infty}(\mathrm{Gal}_\mathbb{Q})$). The desired $e(\ell)$ is chosen such that $e(\ell) \geq 2f + 2$ and such that the lemma holds for the finite number of excluded $\overline{\mathbb{Q}}$-isomorphism classes of non-CM elliptic curves over $\mathbb{Q}$. □

Proof of Proposition 1.3. Define the set $Q = \{\ell : \ell \leq 17\} \cup \{37\}$ and let $\mathcal{P}$ be the (finite) set of primes $\ell \notin Q$ for which $\rho_{E,\ell}$ is not surjective. Let K be the compositum of the fields $\{\mathbb{Q}(E[\ell])\}_{\ell\in\mathcal{P}\cup Q}$; it is a finite Galois extension of $\mathbb{Q}$. Define the group $S = \rho_E(\mathrm{Gal}(\overline{\mathbb{Q}}/K\mathbb{Q}^{\mathrm{cyc}}))$. Since $\det\circ\rho_E\colon \mathrm{Gal}_\mathbb{Q} \to \widehat{\mathbb{Z}}^\times$ is the cyclotomic character and is thus surjective, we have

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(\mathrm{Gal}_\mathbb{Q})] = [\mathrm{SL}_2(\widehat{\mathbb{Z}}) : \rho_E(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{cyc}}))] = [K : K \cap \mathbb{Q}^{\mathrm{cyc}}]^{-1}[\mathrm{SL}_2(\widehat{\mathbb{Z}}) : S]. \tag{5.1}$$

So it remains to bound $[\mathrm{SL}_2(\widehat{\mathbb{Z}}) : S]$. For each prime ℓ, let S_ℓ be the image of S under the projection to $\mathrm{SL}_2(\mathbb{Z}_\ell)$. We now describe the groups S_ℓ.

Case 1: Let ℓ be a prime in $\mathcal{P}$.

Define $f(\ell) = \mathrm{ord}_\ell(M) + 1$. Since $\ell^{f(\ell)} \nmid M$, the group $\rho_{E,\ell^{f(\ell)}}(\mathrm{Gal}_\mathbb{Q})$ is not contained in the normalizer of a Cartan subgroup. By Proposition 1.2, we must have $\rho_{E,\ell^\infty}(\mathrm{Gal}_\mathbb{Q}) \supseteq I + \ell^{4f(\ell)} M_2(\mathbb{Z}_\ell)$ and hence $\rho_{E,\ell^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{cyc}}))$ contains $\{A \in \mathrm{SL}_2(\mathbb{Z}_\ell) : A \equiv I \pmod{\ell^{4f(\ell)}}\}$ by Lemma 2.6. Therefore,

$$[\mathrm{SL}_2(\mathbb{Z}_\ell) : S_\ell] \le \left(\ell^{4f(\ell)}\right)^3 \ell^{\mathrm{ord}_\ell([K:K\cap\mathbb{Q}^{\mathrm{cyc}}])} = \left(\ell^{\mathrm{ord}_\ell(M)+1}\right)^{12} \ell^{\mathrm{ord}_\ell([K:K\cap\mathbb{Q}^{\mathrm{cyc}}])}.$$

The prime ℓ divides M, so $[\mathrm{SL}_2(\mathbb{Z}_\ell) : S_\ell] \le \ell^{\mathrm{ord}_\ell([K:K\cap\mathbb{Q}^{\mathrm{cyc}}])}\left(\ell^{\mathrm{ord}_\ell(M)}\right)^{24}$.

Case 2: Let ℓ be a prime in Q.

By Lemma 5.1, there is an integer $e(\ell) \ge 1$, not depending on E, such that $\rho_{E,\ell^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{cyc}}))$ contains $\{A \in \mathrm{SL}_2(\mathbb{Z}_\ell) : A \equiv I \pmod{\ell^{e(\ell)}}\}$. Therefore,

$$[\mathrm{SL}_2(\mathbb{Z}_\ell) : S_\ell] \le \ell^{3e(\ell)} \ell^{\mathrm{ord}_\ell([K:K\cap\mathbb{Q}^{\mathrm{cyc}}])}.$$

Case 3: Let ℓ be a prime not in $\mathcal{P} \cup Q$.

We claim that $S_\ell = \mathrm{SL}_2(\mathbb{Z}_\ell)$. Since ℓ is not in $\mathcal{P}$, we have $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q}) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. No composition series of the group $\mathrm{Gal}(K/\mathbb{Q})$ contains the simple group $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})/\{\pm I\}$ (this follows from the description of the sets "$\mathrm{Occ}(\mathrm{GL}_2(\mathbb{Z}_p))$" in [Ser68, IV-25]). Therefore, the group $\rho_{E,\ell}(\mathrm{Gal}(\overline{\mathbb{Q}}/K))$, and hence also $H := \rho_{E,\ell}(\mathrm{Gal}(\overline{\mathbb{Q}}/K\mathbb{Q}^{\mathrm{cyc}})) \subseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$, contains the group $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})/\{\pm I\}$ in its composition series. The image of H under the quotient $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})/\{\pm I\}$ is thus surjective, so $H = \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ by [Ser68, IV-23 Lemma 2]. By [Ser68, IV-23 Lemma 3], we have $\rho_{E,\ell^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/K\mathbb{Q}^{\mathrm{cyc}})) = \mathrm{SL}_2(\mathbb{Z}_\ell)$.

We now return to the group S. We may view S as a closed subgroup of $\prod_\ell S_\ell \subseteq \prod_\ell \mathrm{SL}_2(\mathbb{Z}_\ell) = \mathrm{SL}_2(\widehat{\mathbb{Z}})$. We will show that $S = \prod_\ell S_\ell$. For each finite set of primes B, let $p_B \colon S \to S_B := \prod_{\ell\in B} S_\ell$ be the projection map. We have $p_B(S) = S_B$ for $B = \mathcal{P} \cup Q$ since the groups S_ℓ with $\ell \in B$ are pro-ℓ by our choice of K (the group $p_B(S)$ is pro-nilpotent and is thus a product of its Sylow subgroups). Now assume that B is a set of primes containing $\mathcal{P} \cup Q$ for which $p_B(S) = S_B$ and fix a prime $\ell_0 \notin B$. We claim that $p_{B\cup\{\ell_0\}}(S) = S_{B\cup\{\ell_0\}}$. Define $N = p_{B\cup\{\ell_0\}}\big(p_{\{\ell_0\}}^{-1}(1)\big)$ and $N' = p_{B\cup\{\ell_0\}}\big(p_B^{-1}(1)\big)$ which are closed normal subgroups of $p_{B\cup\{\ell_0\}}(S)$ that we may also view as subgroups of S_B and S_{ℓ_0}, respectively. By Goursat's lemma, we find that the image of S in $S_B/N \times S_{\ell_0}/N'$ is the graph of an isomorphism $S_B/N \cong S_{\ell_0}/N'$ of profinite groups (cf. [Rib76, §2], it is clear that the isomorphism and its inverse are continuous). The groups $S_{\ell_0} = \mathrm{SL}_2(\mathbb{Z}_{\ell_0})$ and $S_B = \prod_{\ell\in B} S_\ell$ have no isomorphic non-abelian simple groups in their composition series (again see [Ser68, IV-25] and note that ℓ-groups are solvable), so the isomorphism $S_B/N \cong S_{\ell_0}/N'$ is an isomorphism of solvable groups. However, there are no non-trivial abelian quotients of $\mathrm{SL}_2(\mathbb{Z}_{\ell_0})$ [Coj05, Appendix Corollary 7], so $N = S_B$ and $N' = S_{\ell_0}$. Thus $p_{B\cup\{\ell_0\}}(S) = S_B \times S_{\ell_0} = S_{B\cup\{\ell_0\}}$ as claimed. By induction, we have $p_B(S) = S_B$ for any finite set of primes B containing $\mathcal{P} \cup Q$, and since S is profinite we deduce that $S = \prod_\ell S_\ell$.

Returning to the index and using the three cases, we find that

$$[\mathrm{SL}_2(\widehat{\mathbb{Z}}) : S] = \prod_\ell [\mathrm{SL}_2(\mathbb{Z}_\ell) : S_\ell] \le [K : K \cap \mathbb{Q}^{\mathrm{cyc}}] \prod_{\ell\in Q} \ell^{3e(\ell)} \Big(\prod_{\ell\in\mathcal{P}} \ell^{\mathrm{ord}_\ell(M)}\Big)^{24}.$$

By (5.1), we conclude that $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(\mathrm{Gal}_\mathbb{Q})] \le CM^{24}$ where the constant $C := \prod_{\ell\in Q} \ell^{3e(\ell)}$ is absolute. □

Theorem 1.1 is now easy. Part (i) follows immediately by combining Proposition 1.3 and Proposition 4.2. Parts (ii) and (iii) follow by combining Proposition 1.3 with Proposition 3.3(ii) and (i), respectively.

Remark 5.2. Suppose that there exists an absolute constant c such that $\rho_{E,\ell}(\operatorname{Gal}_\mathbb{Q}) = \operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all non-CM elliptic curves E over $\mathbb{Q}$ and primes $\ell > c$. We may assume that c is the smallest such constant. For each prime $\ell \leq c$, let $e(\ell)$ be a positive integer as in Lemma 5.1. The integer $M = \prod_{\ell \leq c} \ell^{e(\ell)}$ satisfies the condition of Proposition 1.3, so $[\operatorname{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(\operatorname{Gal}_\mathbb{Q})] \leq CM^{24}$ where C and M are absolute constants.

6. Lang-Trotter constants

Let E be an non-CM elliptic curve over $\mathbb{Q}$. The predicted constant $C_{E,r}$ of Conjecture 1.5 is

$$C_{E,r} = \frac{2}{\pi} \lim_{m\to\infty} m \frac{|\{A \in \rho_{E,m}(\operatorname{Gal}_\mathbb{Q}) : \operatorname{tr}(A) \equiv r \pmod m\}|}{|\rho_{E,m}(\operatorname{Gal}_\mathbb{Q})|}.$$

where the limit is over all natural numbers m ordered by divisibility, see [LT76, I §4]. Serre's open image theorem is used to prove that this limit converges. The constant $C_{E,r}$ for CM elliptic curves is not studied in [LT76] but can be found in [Jon09, §2.2]. To control the constants $C_{E,r}$ for non-CM $E/\mathbb{Q}$, we will need the following easy lemma.

Lemma 6.1. *Let E be a non-CM elliptic curve over $\mathbb{Q}$. Then $C_{E,r} \leq [\operatorname{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(\operatorname{Gal}_\mathbb{Q})] \cdot C_r$ where C_r is the constant of Theorem 1.6.*

Proof. We have

$$\begin{aligned} C_{E,r} &\leq \frac{2}{\pi} \limsup_{m\to\infty} m \frac{|\{A \in \operatorname{GL}_2(\mathbb{Z}/m\mathbb{Z}) : \operatorname{tr}(A) \equiv r \pmod m\}|}{|\rho_{E,m}(\operatorname{Gal}_\mathbb{Q})|} \\ &= [\operatorname{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(\operatorname{Gal}_\mathbb{Q})] \cdot \frac{2}{\pi} \limsup_{m\to\infty} m \frac{|\{A \in \operatorname{GL}_2(\mathbb{Z}/m\mathbb{Z}) : \operatorname{tr}(A) \equiv r \pmod m\}|}{|\operatorname{GL}_2(\mathbb{Z}/m\mathbb{Z})|} \end{aligned}$$

and this last line equals $[\operatorname{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(\operatorname{Gal}_\mathbb{Q})] \cdot C_r$ by the computations in [LT76, I §4] (with $M = 1$). □

We will now prove Theorem 1.7. Let $\mathcal{S}(A,B)$ be the set of $(a,b) \in \mathcal{F}(A,B)$ for which $[\operatorname{GL}_2(\widehat{\mathbb{Z}}) : \rho_{E(a,b)}(\operatorname{Gal}_\mathbb{Q})] = 2$ (such elliptic curves are called *Serre curves*) and define $\mathcal{N}(A,B) = \mathcal{F}(A,B) - \mathcal{S}(A,B)$. By [Jon09, Theorem 10] with $k = 1$, we have

$$\frac{1}{|\mathcal{F}(A,B)|} \sum_{(a,b)\in\mathcal{S}(A,B)} C_{E(a,b),r} = C_r + O\Big(\frac{1}{A} + \frac{(\log B)^{1/2}(\log A)^{7/2}}{B^{1/2}}\Big) \tag{6.1}$$

where the implicit constant depends only on r.

Now fix a pair $(a,b) \in \mathcal{N}(A,B)$. If $E(a,b)$ is CM, then we have $C_{E(a,b),r} \ll_r 1$ as noted in [Jon09, Lemma 23] (the key point being that there are only finitely many $\overline{\mathbb{Q}}$-isomorphism classes of CM curves over $\mathbb{Q}$). If $E(a,b)$ is non-CM, then by Lemma 6.1 and Theorem 1.1(i), we have

$$C_{E(a,b),r} \ll_r \big(\max\{1, h(j_{E(a,b)})\}\big)^\gamma$$

where γ is an absolute constant. Since $(a,b) \in \mathbb{Z}^2$ with $|a| \leq A$ and $|b| \leq B$, we have

$$h(j_{E(a,b)}) = h([1728(4a)^3, -16(4a^3 + 27b^2)]) \ll \log(\max\{A,B\}) \leq \log(AB)$$

and hence $C_{E(a,b),r} \ll_r \log^\gamma(AB)$. Therefore,

$$\frac{1}{|\mathcal{F}(A,B)|} \sum_{(a,b)\in\mathcal{N}(A,B)} C_{E(a,b),r} \ll_r \frac{|\mathcal{N}(A,B)|}{|\mathcal{F}(A,B)|} \log^\gamma(AB).$$

Jones [Jon10, Theorem 4] has shown that there is an absolute constant $\beta > 0$ such that

$$\frac{|\mathcal{N}(A,B)|}{|\mathcal{F}(A,B)|} \ll \frac{\log^{\beta}(\min\{A,B\})}{\sqrt{\min\{A,B\}}},$$

so

$$\frac{1}{|\mathcal{F}(A,B)|} \sum_{(a,b)\in\mathcal{N}(A,B)} C_{E(a,b),r} \ll_r \frac{\log^{\beta+\gamma}(AB)}{\sqrt{\min\{A,B\}}}. \tag{6.2}$$

Theorem 1.7 follows by adding (6.1) and (6.2) together, and taking $\delta = \max\{4, \beta+\gamma\}$.

References

[ADHT12] Shabnam Akhtari, Chantal David, Heekyoung Hahn, and Lola Thompson, *Distribution of squarefree values of sequences associated with elliptic curves*, 2012. arXiv:1210.3433.

[BPR11] Yu. Bilu, P. Parent, and M. Rebolledo, *Rational points on $X_0^+(p^r)$*, 2011. arXiv:1104.4641.

[BCDT] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor, *On the modularity of elliptic curves over* **Q***: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939.

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

[DP99] Chantal David and Francesco Pappalardi, *Average Frobenius distributions of elliptic curves*, Internat. Math. Res. Notices **4** (1999), 165–183.

[Del85] Pierre Deligne, *Représentations l-adiques*, Astérisque **127** (1985), 249–255. Seminar on arithmetic bundles: the Mordell conjecture (Paris, 1983/84).

[DR73] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), 1973, pp. 143–316. Lecture Notes in Math., Vol. 349.

[Den75] Joseph B. Dennin Jr., *The genus of subfields of $K(n)$*, Proc. Amer. Math. Soc. **51** (1975), 282–288.

[Elk87] Noam D. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over* **Q**, Invent. Math. **89** (1987), no. 3, 561–567.

[Jon09] Nathan Jones, *Averages of elliptic curve constants*, Math. Ann. **345** (2009), no. 3, 685–710.

[Jon10] ______, *Almost all elliptic curves are Serre curves*, Trans. Amer. Math. Soc. **362** (2010), no. 3, 1547–1570.

[Kra95] Alain 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.

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

[Mas98] David Masser, *Multiplicative isogeny estimates*, J. Austral. Math. Soc. Ser. A **64** (1998), no. 2, 178–194.

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

[Maz72] Barry Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.

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

[Ser68] Jean-Pierre Serre, *Abelian l-adic representations and elliptic curves*, McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute, W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[Ser72] ______, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.

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

[Sil86] Joseph H. Silverman, *Heights and elliptic curves*, Arithmetic geometry (Storrs, Conn., 1984), 1986, pp. 253–265.

[Vél74] Jacques Vélu, *Les points rationnels de $X_0(37)$*, Journées Arithmétiques (Grenoble, 1973), 1974, pp. 169–179. Bull. Soc. Math. France Mém., 37.

School of Mathematics, Institute for advanced study, Princeton, NJ 08540
E-mail address: zywina@math.ias.edu