REDUCTIONS OF POINTS ON ELLIPTIC CURVES

AMIR AKBARY, DRAGOS GHIOCA, AND V. KUMAR MURTY

Abstract. Let E be an elliptic curve defined over $\mathbb{Q}$. Let Γ be a subgroup of rank r of the group of rational points $E(\mathbb{Q})$ of E. For any prime p of good reduction, let $\bar{\Gamma}$ be the reduction of Γ modulo p. Under certain standard assumptions, we prove that for almost all primes p (i.e. for a set of primes of density one), we have

$$|\bar{\Gamma}| \geq \frac{p}{f(p)},$$

where $f(x)$ is any function such that $f(x) \to \infty$, at an arbitrary slow speed, as $x \to \infty$. This provides additional evidence in support of a conjecture of Lang and Trotter from 1977.

1. Introduction

Artin's primitive root conjecture asserts that if $a \in \mathbb{Z} \setminus \{-1\}$ is not a perfect square, then the set of primes p for which $a \pmod{p}$ is a primitive root has positive density. In 1967, Hooley [9] proved this conjecture under the assumption of the Generalized Riemann Hypothesis (GRH).

More generally, we may consider an algebraic group G defined over $\mathbb{Q}$ and Γ a finitely generated subgroup of $G(\mathbb{Q})$. For all but a finite number of primes p, there is a natural reduction map

$$\Gamma \to \bar{G}(\mathbb{F}_p), \tag{1.1}$$

where $\bar{G}$ denotes the reduction of G mod p, and we may ask for the distribution of primes p for which this map is surjective. Thus, in the classical Artin primitive root conjecture, $G = \mathbb{G}_m$ and Γ is the subgroup generated by a.

Lang and Trotter [12] considered the case where G is an elliptic curve E and Γ is a free subgroup of the group of rational points $E(\mathbb{Q})$, and conjectured an explicit formula for the density of primes for which (1.1) is surjective. Significant results on this question were obtained by Gupta and R. Murty in [5] and [6]. In particular, they showed that, assuming GRH, if the rank r of Γ is sufficiently large ($r \geq 6$ in the CM case, and $r \geq 19$ in the non-CM case), then the set of primes for which (1.1) is surjective has a density.

It is also of interest to consider lower bounds on the size of the image in (1.1). Let Γ be a subgroup of $\mathbb{Q}^*$ generated by r non-zero multiplicatively independent rationals $a_1, \cdots, a_r$. For all primes p not dividing the numerators and the denominators of $a_1, \cdots, a_r$, we let $\bar{\Gamma}$ be the reduction of Γ mod p. Erdös and R. Murty [3], and Pappalardi [15] proved the following theorem regarding the size of $\bar{\Gamma}$ as p varies.

Theorem 1.1. *Let $f : \mathbb{R}_+ \longrightarrow \mathbb{R}_+$ be a function such that $f(x) \to \infty$ as $x \to \infty$. For each $d \geq 1$, and for each $a \in \mathbb{Q}$ let $\zeta_{d,a}(s)$ denote the Dedekind zeta function of*

$$\mathbb{Q}(\exp(2\pi i/d), a^{1/d}).$$

2000 *Mathematics Subject Classification.* 11G20, 11G05.

Key words and phrases. Lang-Trotter conjecture, Artin primitive root conjecture, elliptic curves.

Suppose that there exists $a \in \Gamma \backslash \{1\}$ such that GRH holds for $\zeta_{d,a}(s)$. Then for all but $o(x/\log x)$ primes $p \leq x$, we have

$$|\bar{\Gamma}| \geq \frac{p}{f(p)}.$$

We can view this theorem as a variant of the Artin conjecture, as the surjectivity of the map (1.1) is replaced by a sharp lower bound on the size of the image. Note that weakening the surjectivity condition results in a stronger assertion (the density of the set of primes satisfying this new condition equals one).

In this paper we prove an analogue for elliptic curves of Theorem 1.1. More precisely, let E be an elliptic curve defined over $\mathbb{Q}$. For any prime p of good reduction, let $\bar{E}$ be the elliptic curve over $\mathbb{F}_p$ obtained by reducing E modulo p. By Mordell's theorem we know that $E(\mathbb{Q})$ is finitely generated. Let Γ be a subgroup of rank r of $E(\mathbb{Q})$ and let $\bar{\Gamma}$ be the reduction of Γ mod p. One can ask how the size of $\bar{\Gamma}$ grows as $p \to \infty$.

Let $E[m]$ be the group of m-torsion points of E, and P be a point of infinite order in Γ. Then, under the assumption of some standard conjectures for the Kummerian field $K_m = \mathbb{Q}(E[m], \frac{1}{m} \cdot P)$, we show that if the rank of Γ is sufficiently large then the size of $\bar{\Gamma}$ is very large for almost all primes p. More precisely, we have the following.

Theorem 1.2. *Let E be a non-CM elliptic curve defined over $\mathbb{Q}$. Let Γ be a subgroup of rank r of $E(\mathbb{Q})$.*

(a) Assume that the following conditions hold.

(i) $r > 18$ *(in particular this means that we assume that the rank of $E(\mathbb{Q})$ is greater than* 18*).*

(ii) *There is a rational point of infinite order $P \in \Gamma$, such that for any integer $m > 1$, GRH (Generalized Riemann Hypothesis) holds for $K_m = \mathbb{Q}(E[m], \frac{1}{m} \cdot P)$.*

Then for a full density set of primes (i.e. for all but $o(x/\log x)$ primes $p \leq x$), we have

$$|\bar{\Gamma}| \geq \frac{p}{f(p)},$$

where $f : \mathbb{R}_+ \longrightarrow \mathbb{R}_+$ is any function such that $f(x) \to \infty$, at an arbitrary slow speed, as $x \to \infty$.

(b) In (ii) *if in addition to GRH we also assume that AHC (Artin Holomorphy Conjecture) holds for K_m for any integer $m > 1$, then the assertion of part (a) holds as long as $r > 10$ (in particular this means that we assume that the rank of $E(\mathbb{Q})$ is only greater than* 10*).*

This result is optimal in the sense that it is not true for bounded f (see Remark 5.5).

Remarks 1.3.
(a) Using the classical Hasse bound for elliptic curves, we know that $2\sqrt{p} \geq |\#\bar{E}(\mathbb{F}_p) - p - 1|$; thus our result shows that $\bar{\Gamma}$ has almost the same size as $\bar{E}(\mathbb{F}_p)$ for almost all primes p.
(b) The GRH is the assumption that the Dedekind zeta function of K_m has no zeros in the region $\Re(s) > \frac{1}{2}$.
(c) The AHC referred to above is the statement that all Artin L-series of the extension $K_m/\mathbb{Q}$ are analytic at $s \neq 1$.
(d) In the above theorem we can replace the assumption of GRH with a quasi-GRH assumption. More precisely, in part (a) we only need to assume that the Dedekind zeta function of K_m has no zeros in the region $\Re(s) > \alpha$, for any fixed $\alpha < 1 - \frac{10}{r+2}$, and in part (b) we only need to assume that the Dedekind zeta function of K_m has no zeros in the region $\Re(s) > \alpha$, for any fixed $\alpha < 1 - \frac{6}{r+2}$.

(e) It is a "folklore" conjecture that the rank of an elliptic curve defined over $\mathbb{Q}$ can be arbitrarily large. See [18, Conjecture 10.1, p. 234] for more information regarding this conjecture. The following are 5 elliptic curves of rank at least 11 ordered increasingly in terms of their conductors, as given in [4, Table 2]:
$y^2 + y = x^3 - 16359067x + 26274178986$,
$y^2 + xy = x^3 - x^2 - 38099014x + 115877816224$,
$y^2 + xy = x^3 - x^2 - 41032399x + 106082399089$,
$y^2 + xy = x^3 - x^2 - 34125664x + 69523358164$,
$y^2 + xy = x^3 - x^2 - 56880994x + 168642718624$.
In 2006, Elkies found an elliptic curve with rank at least 28.

In case that E has CM, we can establish a result similar to Theorem 1.2 without assuming AHC and for a significantly larger class of finitely generated subgroups of $E(\mathbb{Q})$. More precisely, we prove the following.

Theorem 1.4. *Let E be an elliptic curve defined over $\mathbb{Q}$ which has CM by a maximal order, and let Γ be a subgroup of rank r of $E(\mathbb{Q})$. Assume that the following conditions hold.*

(i) $r > 5$ *(in particular this means that we assume the rank of $E(\mathbb{Q})$ is greater than* 5*).*

(ii) *There is a rational point of infinite order $P \in \Gamma$, such that for any integer $m > 2$, GRH holds for $K_m = \mathbb{Q}(E[m], \frac{1}{m} \cdot P)$.*

Then for a full density set of primes (i.e. for all but $o(x/\log x)$ primes $p \leq x$), we have

$$|\bar{\Gamma}| \geq \frac{p}{f(p)},$$

where f is a function as defined in Theorem 1.2.

Remark 1.5. In Theorem 1.4 we can replace the assumption of GRH with a quasi-GRH assumption; more precisely, we only need to assume that the Dedekind zeta function of K_m has no zeros in the region $\Re(s) > 1 - \frac{4}{r+2}$.

Note that in both Theorems 1.2 and 1.4 we obtain that for a set of primes p of density 1, the reduction $\bar{\Gamma}$ modulo p has at least $\frac{p}{\log_k p}$ elements, where $\log_k$ is the k-th iterate of the logarithm for any positive integer k.

Here we outline the strategy of our proofs. With the notation as in Theorem 1.2, $[\bar{E}(\mathbb{F}_p) : \langle \bar{P} \rangle]$ denotes the index of the cyclic group generated by $\bar{P}$ in $\bar{E}(\mathbb{F}_p)$. To prove our theorem we need to find a suitable upper bound for

$$\#\{p \leq x : m \mid [\bar{E}(\mathbb{F}_p) : \langle \bar{P} \rangle]\}, \tag{1.2}$$

where m is any fixed positive integer. Our main observation is that we can express the divisibility of $[\bar{E}(\mathbb{F}_p) : \langle \bar{P} \rangle]$ by m as a condition in terms of the liftings of the Frobenius corresponding to the prime p in the extension $K_m/\mathbb{Q}$ (see Lemma 3.4). This allows us to deduce an upper bound for (1.2) by applying the Chebotarev density theorem.

This strategy is in line with the conditional proof of Artin's conjecture given by Hooley [9] (see also the work by Gupta and Murty [5, 6] on finding primitive points for reduction of elliptic curves, and also the work of Hall and Voloch [7] for finding primitive points for elliptic curves defined over function fields), however our proof exhibits several new features. A serious new difficulty in considering our problem arises from the fact that (unlike the classical Artin conjecture) we need to deal with the divisibility of the index $[\bar{E}(\mathbb{F}_p) : \langle \bar{P} \rangle]$ by an arbitrary prime power. Our index divisibility criterion (Lemma 3.4) successfully relates the divisibility of the index with a suitable conjugacy class C_m in $\mathrm{Gal}(K_m/\mathbb{Q})$. Unlike the classical Artin's conjecture where the size of the conjugacy class is 1, in our case the size of the conjugacy class is large. Propositions 5.1 and 6.7 establish the upper bounds of correct order of magnitude for C_m in both non-CM and CM cases. Our results provide a clear and complete picture for the distribution of primes p such that the index $[\bar{E}(\mathbb{F}_p) : \langle \bar{P} \rangle]$ has any given divisibility property; therefore, we believe our methods can be used for various related applications of the classical Artin's conjecture in the context of elliptic curves, and possibly for abelian varieties.

The structure of the paper is as follows. To prove our index divisibility criterion we need some information regarding subgroups of $\mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$, where ℓ is a prime. In Section 2 we study the subgroups of $\mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$. In Section 3 we prove our index divisibility criterion (Lemma 3.4). In Section 4 we state an effective version of the Chebotarev density theorem that will be used, together with our criterion, in establishing an upper bound for (1.2) (see Propositions 5.3 and 6.10). In Section 5 we prove Theorem 1.2, while in Section 6 we prove Theorem 1.4.

Notation. For any positive integers m and n, and any prime number ℓ, the notation $\ell^n \mid\mid m$ means that ℓ^n is the largest power of ℓ dividing m. In general, we reserve the letters p and ℓ to denote prime numbers, and unless otherwise specified, $\ell \neq p$.

We use the notation $f(x) = o(g(x))$ if $\lim_{x\to\infty} f(x)/g(x) = 0$; similarly $f(x) = O(g(x))$ (or, equivalently $f(x) \ll g(x)$) if the function $|f(x)/g(x)|$ is bounded as $x \to \infty$.

We define $\mathrm{Li}(x)$ as $\int_2^\infty dt/\log t = x/\log x + o(x/\log x)$.

For any abelian group G, and any prime number ℓ, we let $G[\ell^\infty]$ be the ℓ-primary part of G, i.e. the subgroup of all elements in G which have order a power of ℓ. We denote by R^* the group of units of a commutative ring R.

$\varphi(m)$, $\omega(m)$, and $d(m)$ denote, respectively, Euler's function, the number of distinct prime divisors of m, and the number of positive divisors of m.

For any finite set S, we denote by $|S|$ (or equivalently $\#S$) the cardinality of S.

Acknowledgments. The authors thank the referee for many helpful suggestions which improved the exposition of our results.

2. Subgroups of $\mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$

The results of this short Section are fairly simple; we provide their proofs for the sake of completeness.

Let n be a positive integer, let ℓ be a prime number, and let π_1, π_2 be the projections of $\mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$ onto each coordinate.

Lemma 2.1. *Let $H \subset \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$ be a subgroup of order ℓ^{2n-c} for some $0 \leq c \leq 2n$. Assume $\pi_2(H) \subset \pi_1(H)$. Then there exist unique $0 \leq i \leq j \leq n$, and $d \in \{0, \ldots, \ell^{j-i} - 1\}$ such that $i + j = c$ and H is generated by $(\ell^i, \ell^i d)$ and $(0, \ell^j)$. Furthermore, H is cyclic if and only if $j = n$.*

Proof. Let $i \in \{0, \ldots, n\}$ be such that $\pi_1(H) = \ell^i \cdot \mathbb{Z}/\ell^n\mathbb{Z}$. Let $(\ell^i, b) \in H$, for some $b \in \mathbb{Z}/\ell^n\mathbb{Z}$. Then for every $(x, y) \in H$, there exists $z \in \mathbb{Z}/\ell^n\mathbb{Z}$ such that $\ell^i \cdot z = x$. Therefore, $(0, y - zb) = (x, y) - z \cdot (\ell^i, b) \in H$. Moreover,

$$H_0 := \{w \in \mathbb{Z}/\ell^n\mathbb{Z} : (0, w) \in H\}$$

is a subgroup of $\mathbb{Z}/\ell^n\mathbb{Z}$; thus there exists $j \in \{0, \dots, n\}$ such that $H_0 = \ell^j \cdot \mathbb{Z}/\ell^n\mathbb{Z}$. Because $H_0 \subset \pi_2(H) \subset \pi_1(H)$, we conclude that $i \leq j$. So, H is generated by (ℓ^i, b) and $(0, \ell^j)$. Furthermore, at the expense of subtracting a multiple of ℓ^j from b, we may assume $b \in \{0, \dots, \ell^j - 1\}$. On the other hand, $b \in \pi_2(H) \subset \pi_1(H)$; so, $\ell^i \mid b$. We conclude that there exists $d \in \{0, \dots, \ell^{j-i} - 1\}$ such that $(\ell^i, \ell^i d)$ and $(0, \ell^j)$ generate H.

It is immediate to see that each element of H can be written uniquely as $x \cdot (\ell^i, \ell^i d) + y \cdot (0, \ell^j)$ for some $x \in \{0, \dots, \ell^{n-i} - 1\}$ and $y \in \{0, \dots, \ell^{n-j} - 1\}$; this shows that $|H| = \ell^{2n-(i+j)}$. Finally, H is cyclic if and only if it is generated by $(\ell^i, \ell^i d)$, i.e. if and only if $j = n$. □

For each $0 \leq i \leq j \leq n$, and for each $d \in \{0, \dots, \ell^{j-i} - 1\}$, we let $H_{i,j,d}$ be the subgroup of $\mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$ generated by $(\ell^i, \ell^i d)$ and $(0, \ell^j)$. Similarly, we let $\tilde{H}_{i,j,d}$ be the subgroup of $\mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$ generated by $(\ell^i d, \ell^i)$ and $(\ell^j, 0)$. Note that $H_{i,i,0} = \tilde{H}_{i,i,0}$ for each $i \in \{0, \dots, n\}$. Also, for each $i, j \in \{0, \dots, n\}$ with $i < j$ and for each $d \in \{1, \dots, \ell^{j-i} - 1\}$ coprime with ℓ, there exists a unique $\tilde{d} \in \{1, \dots, \ell^{j-i} - 1\}$ (also coprime with ℓ) such that $H_{i,j,d} = \tilde{H}_{i,j,\tilde{d}}$.

Let $\mathrm{M}(2, \mathbb{Z}/\ell^n\mathbb{Z})$ denote the set of 2×2 matrices with entries in $\mathbb{Z}/\ell^n\mathbb{Z}$, and $\mathrm{null}(\alpha)$ denote the null space of a 2-by-2 matrix $\alpha \in \mathrm{M}(2, \mathbb{Z}/\ell^n\mathbb{Z})$. Then we have the following.

Lemma 2.2. *There are exactly $\ell^{2(i+j)}$ matrices $\alpha \in \mathrm{M}(2, \mathbb{Z}/\ell^n\mathbb{Z})$ such that $H_{i,j,d} \subset \mathrm{null}(\alpha)$.*

Proof. Let

$$\alpha = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$$

such that $H_{i,j,d} \subset \mathrm{null}(\alpha)$. Then

$$\begin{cases} \ell^i(x + dy) & = & 0 \\ \ell^i(z + dt) & = & 0 \end{cases}$$

and

$$\begin{cases} \ell^j y & = & 0 \\ \ell^j t & = & 0 \end{cases}.$$

This means that there are ℓ^j possibilities for each of y and t, while for each fixed $(y, t) \in (\ell^{n-j} \cdot \mathbb{Z}/\ell^n\mathbb{Z}) \times (\ell^{n-j} \cdot \mathbb{Z}/\ell^n\mathbb{Z})$, there are $\ell^i \cdot \ell^i$ choices of (x, z). This finishes the proof of Lemma 2.2. □

3. Index Divisibility Criterion

Let E be an elliptic curve defined over $\mathbb{Q}$, and let $P \in E(\mathbb{Q})$ be a non-torsion point. Let p be a prime of good reduction for E, and let $\bar{E}$ and $\bar{P}$ be the reduction of E and P modulo p. Let ℓ be a prime number. From now on we assume that $p \nmid \ell\Delta$, where Δ is the discriminant of E.

Let $K_{\ell^n} := \mathbb{Q}\left(E[\ell^n], \frac{1}{\ell^n} \cdot P\right)$. We identify $E[\ell^n]$ with $\mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$; also from now on we denote $\mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$ by $(\mathbb{Z}/\ell^n\mathbb{Z})^2$. Let $Q_0 \in E(K_{\ell^n})$ be a fixed ℓ^n-th root of P. Then each $\sigma \in \mathrm{Gal}(K_{\ell^n}/\mathbb{Q})$ can be uniquely represented as (γ, τ) in the semidirect product $\mathrm{GL}(2, \mathbb{Z}/\ell^n\mathbb{Z}) \ltimes (\mathbb{Z}/\ell^n\mathbb{Z})^2$, where for each torsion point $T \in E[\ell^n]$ (seen as a point in $(\mathbb{Z}/\ell^n\mathbb{Z})^2$), we have

$$\sigma(T) := \gamma(T),$$

while for each ℓ^n-th root Q of P, we have

$$\sigma(Q) := \gamma(Q - Q_0) + Q_0 + \tau. \tag{3.1}$$

In (3.1), we used the fact that $Q - Q_0 \in E[\ell^n]$ can also be seen as an element of $(\mathbb{Z}/\ell^n\mathbb{Z})^2$. Finally, note that the composition rule on $\mathrm{Gal}(K_{\ell^n}/\mathbb{Q})$ is the following

$$(\gamma_1, \tau_1) \circ (\gamma_2, \tau_2) = (\gamma_1\gamma_2, \tau_1 + \gamma_1 \cdot \tau_2). \tag{3.2}$$

Due to a similar argument as in [18, Theorem 7.1, Chapter 7], we obtain that p is unramified in K_{ℓ^n}. Let $\sigma_v = (\gamma_v, \tau_v)$ be a lifting of the Frobenius corresponding to p, where v is a nonarchimedean place of K_{ℓ^n} lying above p. By definition for each algebraic integer $x \in K_{\ell^n}$, we have

$$\sigma_v(x) \equiv x^p \pmod{v}.$$

Our goal is to obtain a criterion for the divisibility by ℓ^n (for any positive integer n) of the index of the cyclic subgroup generated by $\bar{P}$ in $\bar{E}(\mathbb{F}_p)$. Lang and Trotter [12] proved the following criterion for the divisibility of the index $[\bar{E}(\mathbb{F}_p) : \langle\bar{P}\rangle]$ by a prime ℓ (hence, $n = 1$ with the above notation).

Lemma 3.1. *Let Id be the identity matrix in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, and let C_ℓ consist of elements $\sigma = (\gamma, \tau) \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \ltimes (\mathbb{Z}/\ell\mathbb{Z})^2$ of $\mathrm{Gal}(K_\ell/\mathbb{Q})$ such that either*

(i) $\gamma = Id$ (i.e., $\mathrm{null}(\gamma - Id) = (\mathbb{Z}/\ell^n\mathbb{Z})^2$),

or

(ii) $\mathrm{null}(\gamma - Id)$ is a non-trivial cyclic group and $\tau \in (\gamma - Id)((\mathbb{Z}/\ell\mathbb{Z})^2)$.

Then for $p \nmid \ell\Delta$, we have $\ell \mid [\bar{E}(\mathbb{F}_p) : \langle\bar{P}\rangle]$ if and only if $\sigma_v \in C_\ell$ for each lifting σ_v of the Frobenius corresponding to p.

Our Lemma 3.4 is a generalization of the above result to the case that $[\bar{E}(\mathbb{F}_p) : \langle\bar{P}\rangle]$ is divisible by a prime power ℓ^n (for an arbitrary positive integer n). Because ℓ^n is an arbitrary prime power, our criterion is more general than the classical Lang-Trotter criterion. First we translate the divisibility of the above index into a geometric condition satisfied by $\bar{P}$ (our result is a generalization of [5, Lemma 1]).

Lemma 3.2. *The index of the group generated by $\bar{P}$ inside $\bar{E}(\mathbb{F}_p)$ is divisible by ℓ^n if and only if $\bar{E}(\mathbb{F}_p)[\ell^\infty] \cap \bar{E}[\ell^n]$ is a group of order ℓ^{2n-c}, where $0 \le c \le n$, and there exist $R \in \bar{E}(\mathbb{F}_p)$ and $T \in \bar{E}[\ell^n]$ such that $\bar{P} = \ell^c R + \ell^c T$.*

Proof of Lemma 3.2. For any $k \ge 1$ we choose generators $T_1^{(k)}$ and $T_2^{(k)}$ of $\bar{E}[\ell^k]$ such that $\bar{E}[\ell^k] = \langle T_1^{(k)}\rangle \oplus \langle T_2^{(k)}\rangle$ and $\ell(T_1^{(k+1)}, T_2^{(k+1)}) = (T_1^{(k)}, T_2^{(k)})$.

Suppose that $\bar{E}(\mathbb{F}_p)[\ell^\infty] \subset \bar{E}[\ell^{n+m}]$ for some $m \ge 0$. Then by Lemma 2.1 and without loss of generality we can assume that

$$\bar{E}(\mathbb{F}_p)[\ell^\infty] = \langle \ell^{i'} T_1^{(n+m)} + \ell^{i'} d' T_2^{(n+m)}\rangle \oplus \langle \ell^{j'} T_2^{(n+m)}\rangle,$$

and

$$\bar{E}(\mathbb{F}_p)[\ell^\infty] \cap \bar{E}[\ell^n] = \langle \ell^i T_1^{(n)} + \ell^i d T_2^{(n)}\rangle \oplus \langle \ell^j T_2^{(n)}\rangle,$$

where $i' \le j'$ and $i \le j$. Note that with these notations we have $c = i + j$.

We have three cases:

Case 1. $i = 0$ and $j \ge 1$. Hence, in this case $c = j \le n$.

First of all, note that $i' \le m$ since $i = 0$.

Secondly, since $j \ge 1$, we have $\bar{E}[\ell^{n-j}] \subseteq \bar{E}(\mathbb{F}_p)[\ell^\infty]$ and $\bar{E}[\ell^{n-j+1}] \not\subseteq \bar{E}(\mathbb{F}_p)[\ell^\infty]$. So $n - j = m + n - j'$. Thus $j' = j + m$ and

$$\bar{E}(\mathbb{F}_p)[\ell^\infty] = \langle \ell^{i'} T_1^{(n+m)} + \ell^{i'} d' T_2^{(n+m)} \rangle \oplus \langle \ell^j T_2^{(n)} \rangle.$$

Next we find a positive integer a coprime with ℓ such that $a\bar{P} \in \bar{E}(\mathbb{F}_p)[\ell^\infty]$, and so

$$a\bar{P} = x(\ell^{i'} T_1^{(n+m)} + \ell^{i'} d' T_2^{(n+m)}) + y(\ell^j T_2^{(n)}), \tag{3.3}$$

for some integers x and y.

Now suppose that ℓ^n divides the index of $\bar{P}$ in $\bar{E}(\mathbb{F}_p)$. Because $(a,\ell) = 1$ this is equivalent with the fact that ℓ^n divides the index of $a\bar{P}$ in $\bar{E}(\mathbb{F}_p)[\ell^\infty]$. Since $\#\bar{E}(\mathbb{F}_p)[\ell^\infty] = \ell^{n+m-i'+n-j}$ and the index of $a\bar{P}$ in $\bar{E}(\mathbb{F}_p)[\ell^\infty]$ is divisible by ℓ^n we obtain that the order of $a\bar{P}$ divides $\ell^{n+m-i'-j}$. So $\ell^{n+m-i'-j}(a\bar{P}) = \bar{\mathcal{O}}$, where $\bar{\mathcal{O}}$ is the point at infinity of $\bar{E}$. Because $i' \leq m$, we get that

$$\ell^{n+m-i'-j} \cdot y(\ell^j T_2^{(n)}) = y\ell^{n+m-i'} T_2^{(n)} = \bar{\mathcal{O}}.$$

Thus, using (3.3), we conclude that

$$x\ell^{n+m-j}\left(T_1^{(n+m)} + d' T_2^{(n+m)}\right) = \bar{\mathcal{O}};$$

so $x = \ell^j x_1$ for some integer x_1. Hence, if the index of the cyclic group generated by $a\bar{P}$ inside $\bar{E}(\mathbb{F}_p)[\ell^\infty]$ is divisible by ℓ^n then

$$\begin{aligned} a\bar{P} &= \ell^j(x_1(\ell^{i'} T_1^{(n+m)} + \ell^{i'} d' T_2^{(n+m)})) + \ell^j(yT_2^{(n)}) \\ &= \ell^j R_0 + \ell^j T_0, \end{aligned}$$

where $R_0 \in \bar{E}(\mathbb{F}_p)[\ell^\infty]$ and $T_0 \in \bar{E}[\ell^n]$. Multiplying the above identity by an integer b such that $ab \equiv 1 \pmod{\ell^j}$ we have $\bar{P} = (1-ab)\bar{P} + \ell^j bR_0 + \ell^j bT_0$, and we can take $R = ((1-ab)/\ell^j)\bar{P} + bR_0$ and $T = bT_0$ to derive that $\bar{P} = \ell^j R + \ell^j T$, as in the conclusion of Lemma 3.2.

Conversely suppose that $\bar{P} = \ell^j R + \ell^j T$ where $R \in \bar{E}(\mathbb{F}_p)$ and $T \in \bar{E}[\ell^n]$. Choose a relatively prime to ℓ such that $aR \in \bar{E}(\mathbb{F}_p)[\ell^\infty]$. We have

$$\ell^{n+m-i'-j}(a\bar{P}) = \ell^{n+m-i'-j}(\ell^j aR + \ell^j aT) = \bar{\mathcal{O}},$$

since $\ell^n T = \bar{\mathcal{O}}$ (also note that $i' \leq m$) and $\ell^{n+m-i'} \cdot (aR) = \bar{\mathcal{O}}$ (note that $\ell^{n+m-i'} \cdot \bar{E}(\mathbb{F}_p)[\ell^\infty] = \{\bar{\mathcal{O}}\}$). So, the order of $a\bar{P}$ in $\bar{E}(\mathbb{F}_p)$ divides $\ell^{m+n-i'-j}$ and thus

$$\ell^n = \frac{\#\bar{E}(\mathbb{F}_p)[\ell^\infty]}{\ell^{m+n-i'-j}} \mid \frac{\#\bar{E}(\mathbb{F}_p)[\ell^\infty]}{\mathrm{ord}(a\bar{P})} \mid \frac{\#\bar{E}(\mathbb{F}_p)}{\mathrm{ord}(a\bar{P})}.$$

Since $(a,\ell) = 1$ this implies that ℓ^n divides the index of $\langle \bar{P} \rangle$ in $\bar{E}(\mathbb{F}_p)$.

Case 2. $i \geq 1$. Hence, in this case $c = i + j$.

Since $i \geq 1$ then an argument similar to Case 1 shows that $i' = i + m$ and $j' = j + m$; furthermore, $d' = d$ and $\bar{E}(\mathbb{F}_p)[\ell^\infty] \subset \bar{E}[\ell^n]$. Thus (3.3) can be written as

$$a\bar{P} = x(\ell^i T_1^{(n)} + \ell^i dT_2^{(n)}) + y(\ell^j T_2^{(n)}).$$

Now, if ℓ^n divides the index of $\langle \bar{P} \rangle$ in $\bar{E}(\mathbb{F}_p)$, then ℓ^n divides the index of $\langle a\bar{P} \rangle$ in $\bar{E}(\mathbb{F}_p)[\ell^\infty]$, and so $\ell^{n-i-j}(a\bar{P}) = \bar{\mathcal{O}}$ which implies that $\ell^j \mid x$ and $\ell^i \mid y$. Hence there exist integers x_1 and y_1 such that

$$a\bar{P} = \ell^{i+j}(x_1(T_1^{(n)} + dT_2^{(n)}) + y_1 T_2^{(n)})) = \ell^{i+j} T_0,$$

where $T_0 \in \bar{E}[\ell^n]$. Multiplying the above identity by an integer b such that $ab \equiv 1 \pmod{\ell^{i+j}}$ we have $\bar{P} = (1-ab)\bar{P} + \ell^{i+j} bT_0$, and we can take $R = ((1-ab)/\ell^{i+j})\bar{P}$ and $T = bT_0$ to obtain that $\bar{P} = \ell^{i+j}R + \ell^{i+j}T$, as in the conclusion of Lemma 3.2. Note that if $\ell^n \mid [\bar{E}(\mathbb{F}_p) : \langle \bar{P}\rangle]$, then $\#\bar{E}(\mathbb{F}_p)[\ell^\infty] \geq \ell^n$, and so $c \leq n$.

Conversely suppose that $\bar{P} = \ell^{i+j}R + \ell^{i+j}T$ where $R \in \bar{E}(\mathbb{F}_p)$ and $T \in \bar{E}[\ell^n]$. Choose a relatively prime to ℓ such that $aR \in \bar{E}(\mathbb{F}_p)[\ell^\infty]$. An argument similar to Case 1 shows that ℓ^n divides the index of $\langle \bar{P}\rangle$ in $\bar{E}(\mathbb{F}_p)$ (note that in this case $a\bar{P} = \ell^{i+j}aR + \ell^{i+j}aT$ and $aR \in \bar{E}(\mathbb{F}_p)[\ell^\infty] \subset \bar{E}[\ell^n]$).

Case 3. $i = 0$ and $j = 0$. So $c = 0$.

In this case $\bar{E}(\mathbb{F}_p)[\ell^\infty]$ has order $2n + 2m - i' - j'$ (and $i' \leq j' \leq m$); thus $\bar{E}(\mathbb{F}_p)[\ell^\infty] \cap \bar{E}[\ell^n]$ has order ℓ^{2n}, and the order of $\bar{P}$ can be at most $n + m - i'$. So ℓ^n divides the index of $\langle \bar{P}\rangle$ always. The second condition in the conclusion of lemma holds trivially (simply, let $R = \bar{P}$ and $T = \bar{\mathcal{O}}$). □

With the above notation, and also using Lemma 3.2, we can prove the following criterion.

Lemma 3.3. *Let $\sigma_v = (\gamma_v, \tau_v)$ be a lifting of the Frobenius corresponding to p. Then the index of $\langle \bar{P}\rangle$ in $\bar{E}(\mathbb{F}_p)$ is divisible by ℓ^n if and only if the group $\bar{E}(\mathbb{F}_p) \cap \bar{E}[\ell^n]$ has order ℓ^{2n-c}, where $0 \leq c \leq n$, and for each place v of K_{ℓ^n} lying above p, we have $\ell^{n-c}\tau_v \in (\gamma_v - Id)\left((\mathbb{Z}/\ell^n\mathbb{Z})^2\right)$.*

Proof. Let v be a fixed nonarchimedean place of K_{ℓ^n} lying above the prime p, and for any point $U \in E(K_{\ell^n})$, we let $\tilde{U}$ be the reduction of U modulo v; note that if $U \in E(\mathbb{Q})$, then $\tilde{U}$ is the usual reduction of U modulo p (i.e. $\tilde{P} = \bar{P}$). As shown in [18, Proposition 3.1(b)], since $(\ell, p) = 1$ then $E[\ell^n]$ has trivial intersection with the kernel of reduction modulo v. Therefore $\widetilde{E[\ell^n]} = \bar{E}[\ell^n]$ and we may identify $\bar{E}[\ell^n]$ with $\{\tilde{S} : S \in E[\ell^n]\}$, and thus extend the identification between $E[\ell^n]$ and $(\mathbb{Z}/\ell^n\mathbb{Z})^2$ to an identification between $\bar{E}[\ell^n]$ and $(\mathbb{Z}/\ell^n\mathbb{Z})^2$.

If $\bar{E}(\mathbb{F}_p)[\ell^\infty] \cap \bar{E}[\ell^n]$ is a group of order ℓ^{2n-c} (for some $c \leq n$), and $\ell^n \mid [\bar{E}(\mathbb{F}_p) : \langle \bar{P}\rangle]$ then Lemma 3.2 yields that there exist $R \in \bar{E}(\mathbb{F}_p)$ and $T \in \bar{E}[\ell^n]$ such that $\bar{P} = \ell^c R + \ell^c T$. Since $\bar{P} = \tilde{P}$ and $T = \tilde{S}$ for some $S \in E[\ell^n]$, we have

$$\tilde{P} = \ell^c R + \tilde{S}. \tag{3.4}$$

Then, using $\tilde{P} = \ell^c \cdot \ell^{n-c}\tilde{Q}_0$ in (3.4) we obtain that there exists $\tilde{S}_1 \in \bar{E}[\ell^c] \subset \bar{E}[\ell^n]$ such that

$$\ell^{n-c}\tilde{Q}_0 = R + \tilde{S} + \tilde{S}_1. \tag{3.5}$$

We let $\tilde{S}_2 := \tilde{S} + \tilde{S}_1 \in \bar{E}[\ell^n]$, and then apply the Frobenius to (3.5). Noting that the reduction modulo v of σ_v equals the Frobenius corresponding to the prime p, and that $R \in \bar{E}(\mathbb{F}_p)$ is fixed by the Frobenius, and that $\sigma_v(Q_0) = Q_0 + \tau_v$ we obtain

$$\ell^{n-c}\tilde{Q}_0 + \ell^{n-c}\tau_v = R + \gamma_v(\tilde{S}_2). \tag{3.6}$$

We subtract (3.5) from (3.6) and conclude that

$$\ell^{n-c}\tau_v \in (\gamma_v - \mathrm{Id})((\mathbb{Z}/\ell^n\mathbb{Z})^2). \tag{3.7}$$

Conversely suppose that (3.7) holds. Then there exists $\tilde{S} \in \bar{E}[\ell^n]$ such that

$$\ell^{n-c}\tau_v = \gamma_v(\tilde{S}) - \tilde{S}.$$

Adding $\ell^{n-c}\tilde{Q}_0$ to both sides of the above equation yields

$$\ell^{n-c}\tilde{Q}_0 + \ell^{n-c}\tau_v = \ell^{n-c}\tilde{Q}_0 + \gamma_v(\tilde{S}) - \tilde{S}. \tag{3.8}$$

Using (3.1), we can rewrite (3.8) as

$$\ell^{n-c}\widetilde{\sigma_v(Q_0)} - \widetilde{\sigma_v(S)} = \ell^{n-c}\tilde{Q}_0 - \tilde{S}.$$

Hence $R := \ell^{n-c}\tilde{Q}_0 - \tilde{S}$ is fixed by the Frobenius (note that σ_v is the corresponding lifting of the Frobenius), which yields that $R \in \bar{E}(\mathbb{F}_p)$. Thus

$$\tilde{P} = \ell^c R + \ell^c \tilde{S},$$

where $\tilde{P} = \bar{P}$, $R \in \bar{E}(\mathbb{F}_p)$ and $\tilde{S} \in \bar{E}[\ell^n]$. Lemma 3.2 yields the conclusion of Lemma 3.3. □

For any fixed prime p, all liftings σ_v of the Frobenius are conjugate. We denote by σ_p the collection of all σ_v's for all places v lying above p.

Using Lemma 3.3, we obtain the following generalization of the Lang-Trotter criterion (note that $T \in \bar{E}[\ell^n]$ is fixed by γ_v and thus it is fixed by σ_v if and only if $T \in \bar{E}(\mathbb{F}_p)$). We denote by Id the identity matrix in $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$.

Lemma 3.4. *Let C_{ℓ^n} consist of elements $\sigma = (\gamma, \tau)$ of $\mathrm{Gal}(K_{\ell^n}/\mathbb{Q})$ such that $\mathrm{null}(\gamma - Id)$ is a subgroup of $(\mathbb{Z}/\ell^n\mathbb{Z})^2$ of order ℓ^{2n-c} (for some $0 \le c \le n$), and $\ell^{n-c}\tau \in (\gamma - Id)((\mathbb{Z}/\ell^n\mathbb{Z})^2)$. Then for $p \nmid \ell\Delta$, the index $[\bar{E}(\mathbb{F}_p) : \langle\bar{P}\rangle]$ is divisible by ℓ^n if and only if $\sigma_p \subseteq C_{\ell^n}$.*

Using (3.2) one can show that C_{ℓ^n} is closed under conjugation.

For any integer $m \ge 1$, let $K_m := \mathbb{Q}(E[m], \frac{1}{m}\cdot P)$, and let $G_m := \mathrm{Gal}(K_m/\mathbb{Q})$. Let C_m be the set of elements of G_m with the property that for each $\ell^n \parallel m$, the restriction of C_m to K_{ℓ^n} lies in C_{ℓ^n} (which is defined as in Lemma 3.4). Clearly, C_m is closed under conjugation (because each C_{ℓ^n} is closed under conjugation). By Lemma 3.4, for $(p, m\Delta) = 1$, we have

$$m \mid [\bar{E}(\mathbb{F}_p) : \langle\bar{P}\rangle] \iff \sigma_p \subseteq C_m.$$

4. Chebotarev density theorem

The following is an effective version of the Chebotarev theorem (see [10, Theorem 1.1] and [17, Theorem 4] for a proof of the first assertion, and [14, Corollary 3.7] for a proof of the second assertion).

Proposition 4.1. (Effective Chebotarev) *Let $K/\mathbb{Q}$ be a finite Galois extension with Galois group G. Let $C \subset G$ be closed under conjugation, and assume the GRH for $K/\mathbb{Q}$. Define*

$$\Pi_C(x, K/\mathbb{Q}) := \#\{p \le x : p \text{ a prime of } \mathbb{Q} \text{ unramified in } K \text{ such that } \sigma_p \subseteq C\}$$

where σ_p is the Frobenius conjugacy class corresponding to p in $\mathrm{Gal}(K/\mathbb{Q})$. Then

$$\Pi_C(x, K/\mathbb{Q}) = \frac{|C|}{|G|}\mathrm{Li}\ x + O\left(|C|x^{1/2}\log\left(|G|\left(\prod_{p\in P(K/\mathbb{Q})} p\right)x\right)\right),$$

where $P(K/\mathbb{Q})$ is the set of rational primes which ramify in K, and the constant appearing in the O-notation is absolute.

Moreover if we assume that both GRH and AHC hold for $K/\mathbb{Q}$, then we have the following version of the above asymptotic with the improved error term.

$$\Pi_C(x, K/\mathbb{Q}) = \frac{|C|}{|G|}\mathrm{Li}\ x + O\left(|C|^{1/2}x^{1/2}\log\left(|G|\left(\prod_{p\in P(K/\mathbb{Q})} p\right)x\right)\right),$$

where $P(K/\mathbb{Q})$ is defined above, and the constant appearing in the O-notation is absolute.

5. The non-CM Case

Throughout this section we assume that E is a non-CM elliptic curve defined over $\mathbb{Q}$. We know that $K_m = \mathbb{Q}(E[m], \frac{1}{m}\cdot P)$ is a Galois extension of $\mathbb{Q}$, and that only primes of bad reduction for E and those dividing m can ramify in K_m (this follows from a similar argument as the one in [18, Theorem 7.1, pages 184-185]). Let $G(m)$ be the semi-direct product $\mathrm{GL}(2,\mathbb{Z}/\ell^n\mathbb{Z}) \ltimes (\mathbb{Z}/\ell^n\mathbb{Z})^2$ of $\mathrm{GL}(2,\mathbb{Z}/m\mathbb{Z})$ and $(\mathbb{Z}/m\mathbb{Z})^2$. Then

$$|G(m)| = m^6\prod_{\ell|m}\left(1-\frac{1}{\ell}\right)^2\left(1+\frac{1}{\ell}\right), \tag{5.1}$$

and the Galois group G_m of K_m over $\mathbb{Q}$ is a subgroup of $G(m)$.

Proposition 5.1. *Let E be a non-CM elliptic curve defined over $\mathbb{Q}$, and let $m > 1$ be an integer. Let C_m be the subset of G_m defined after Lemma 3.4. Then*

$$|C_m| < m^4\cdot\prod_{\ell|m}\left(1+\frac{1}{\ell}+\frac{8}{\ell^2}\right).$$

Proof. By definition, $|C_m| \le \prod_{\ell^n||m}|C_{\ell^n}|$ (since K_m is the compositum of all fields K_{ℓ^n} for $\ell^n \mid\mid m$). So, it is enough to show that for each prime ℓ, we have

$$|C_{\ell^n}| < \ell^{4n}\cdot\left(1+\frac{1}{\ell}+\frac{8}{\ell^2}\right). \tag{5.2}$$

For an element $\sigma = (\gamma,\tau) \in C_{\ell^n}$ we know that $\mathrm{null}(\gamma-\mathrm{Id})$ is a subgroup of $(\mathbb{Z}/\ell^n\mathbb{Z})^2$ of order ℓ^{2n-c} (for some $0\le c\le n$), and $\ell^{n-c}\tau \in (\gamma-\mathrm{Id})((\mathbb{Z}/\ell^n\mathbb{Z})^2)$. Then either $\mathrm{null}(\gamma-\mathrm{Id}) = H_{i,j,d}$, or $\mathrm{null}(\gamma-\mathrm{Id}) = \tilde{H}_{i,j,d}$ for some $0\le i\le j\le n$, and $d\in\{0,\ldots,\ell^{j-i}-1\}$; thus $c = i+j$. Therefore we have two possibilities, either $\mathrm{null}(\gamma-\mathrm{Id})$ is a cyclic subgroup of $(\mathbb{Z}/\ell^n\mathbb{Z})^2$ of order ℓ^n and $\tau\in(\gamma-\mathrm{Id})(\mathbb{Z}/\ell^n\mathbb{Z})^2$ (in this case $j = n$ and $i = 0$) or $\mathrm{null}(\gamma-\mathrm{Id})$ is a non-cyclic subgroup of $(\mathbb{Z}/\ell^n\mathbb{Z})^2$ of order ℓ^{2n-c}, and $\ell^{n-c}\tau\in(\gamma-\mathrm{Id})(\mathbb{Z}/\ell^n\mathbb{Z})^2$ (in this case $j\le n-1$).

There are $\ell^n+\ell^{n-1}$ different cyclic subgroups of $(\mathbb{Z}/\ell^n\mathbb{Z})^2$ of order ℓ^n (they are generated by either $(1,d)$ for any $d\in\mathbb{Z}/\ell^n\mathbb{Z}$, or by $(d',1)$ for any $d'\in\mathbb{Z}/\ell^n\mathbb{Z}$ divisible by ℓ). As shown in Lemma 2.2, for each such cyclic subgroup H, there are at most ℓ^{2n} matrices $\gamma\in\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ such that $H\subset\mathrm{null}(\gamma-\mathrm{Id})$.

On the other hand, for each fixed γ such that $\mathrm{null}(\gamma-\mathrm{Id})$ is cyclic of order ℓ^n, we have

$$|(\gamma-\mathrm{Id})(\mathbb{Z}/\ell^n\mathbb{Z})^2| = \ell^n.$$

Thus there are ℓ^n possibilities for $\tau\in(\mathbb{Z}/\ell^n\mathbb{Z})^2$ such that $(\gamma,\tau)\in C_{\ell^n}$. Therefore, we conclude that the number of pairs $(\gamma,\tau)\in C_{\ell^n}$ for which $\mathrm{null}(\gamma-\mathrm{Id})$ is cyclic is bounded from above by

$$(\ell^n+\ell^{n-1})\cdot\ell^{2n}\cdot\ell^n = \ell^{4n}\cdot(1+1/\ell).$$

Assume now that null$(\gamma - \mathrm{Id})$ is not cyclic (hence $j \le n-1$); without loss of generality, we may assume null$(\gamma - \mathrm{Id}) = H_{i,j,d}$. By Lemma 2.2, there are at most ℓ^{2i+2j} matrices $\gamma \in \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ such that null$(\gamma - \mathrm{Id}) = H_{i,j,d}$. Furthermore, for each such γ, we have

$$|(\gamma - \mathrm{Id})((\mathbb{Z}/\ell^n\mathbb{Z})^2)| = \ell^{i+j},$$

which means that there are $\ell^{2n-(i+j)}$ possibilities for τ such that $(\gamma, \tau) \in C_{\ell^n}$. Therefore the number of pairs $(\gamma, \tau) \in C_{\ell^n}$ for which null$(\gamma - \mathrm{Id})$ is non-cyclic is bounded from above by

$$\begin{aligned}
2 \sum_{\substack{0\le i\le j\le n-1,\ i+j\le n \\ 0\le d\le \ell^{j-i}-1}} \ell^{2(i+j)} \cdot \ell^{2n-(i+j)} &= 2 \sum_{\substack{0\le i\le j\le n-1 \\ i+j\le n}} \ell^{2n+2j} \\
&= 2\ell^{2n}\left(2\ell^{2n-2} + 3\ell^{2n-4} + \cdots\right) \\
&< 2\ell^{4n-2} \sum_{k=0}^{\infty} (k+2)/\ell^{2k} \\
&= 2\ell^{4n-2}\left(-1 + 3\sum_{k=0}^{\infty} 1/\ell^{2k} + \sum_{k=1}^{\infty} k/(\ell^2)^{k+1}\right) \\
&= 2\ell^{4n-2}\left(-1 + (3\ell^2/(\ell^2-1)) + (1/(\ell^2-1))^2\right) \\
&\le 2\ell^{4n-2}\left(-1 + 4 + (1/(2^2-1))^2\right) \\
&< 8\ell^{4n-2}.
\end{aligned}$$

Combining the counting of pairs $(\gamma, \tau) \in C_{\ell^n}$ in both cases: null$(\gamma - \mathrm{Id})$ cyclic, or not cyclic finishes the proof of Proposition 5.1. □

The following result is proved in [2] or [11, Theorem 5.2, pages 122-127] (see also [16] for a comprehensive discussion which generalizes to semiabelian varieties).

Proposition 5.2. (Bachmakov) *If E does not have complex multiplication, then the index of $G_m = \mathrm{Gal}(K_m/\mathbb{Q})$ in $G(m)$ is bounded by a constant $i(E)$ depending only on E.*

Now we are ready to provide a good upper bound for the density of the set of primes p for which the index $[\bar{E}(\mathbb{F}_p) : \langle \bar{P} \rangle]$ is divisible by some arbitrary integer m.

Proposition 5.3. *Let E be a non-CM elliptic curve over $\mathbb{Q}$ with discriminant Δ, let P be a point of infinite order in $E(\mathbb{Q})$, and let $m > 1$ be an integer. We have the following.*

(a) Suppose that GRH holds for $K_m = \mathbb{Q}(E[m], \frac{1}{m} \cdot P)$. Then

$$\#\{p \le x \,:\, p \nmid m\Delta \text{ and } m \mid [\bar{E}(\mathbb{F}_p) : \langle \bar{P} \rangle]\} \le C(E)\frac{\mathrm{Li}\, x}{\varphi(m)^2} + O(m^4(\log\log m)x^{1/2}\log mx),$$

where $C(E)$ is a constant depending only on the elliptic curve E, and the constant in the above O-notation also depends only on E.

(b) Suppose that GRH and AHC hold for $K_m = \mathbb{Q}(E[m], \frac{1}{m} \cdot P)$. Then

$$\#\{p \le x \,:\, p \nmid m\Delta \text{ and } m \mid [\bar{E}(\mathbb{F}_p) : \langle \bar{P} \rangle]\} \le C(E)\frac{\mathrm{Li}\, x}{\varphi(m)^2} + O(m^2(\log\log m)^{1/2}x^{1/2}\log mx),$$

where $C(E)$ is a constant depending only on the elliptic curve E, and the constant in the above O-notation also depends only on E.

Proof. (a) By Lemma 3.4, Proposition 4.1 (under GRH) and Proposition 5.2, we have

$$\begin{aligned}\#\{p \le x : p \nmid m\Delta \text{ and } m \mid [\bar{E}(\mathbb{F}_p) : \langle \bar{P} \rangle]\} &\le \#\{p \le x,\ p \text{ unramified in } K_m,\ \sigma_p \subset C_m\} \\ &\le i(E)\frac{|C_m|}{|G(m)|}\mathrm{Li}\, x \\ &\quad +O\left(|C_m| x^{1/2} \log\left(|G(m)|\left(\prod_{p\in P(K_m/\mathbb{Q})} p\right) x\right)\right).\end{aligned}$$

Because the only primes which can ramify in $K_m/\mathbb{Q}$ are the ones which divide $m\Delta$, we obtain

$$\prod_{p\in P(K_m/\mathbb{Q})} p \le m\Delta.$$

The conclusion of Proposition 5.3 follows by applications of (5.1) and Proposition 5.1 in the above inequality. Indeed, for each prime number ℓ, we have

$$\frac{1+\frac{1}{\ell}+\frac{8}{\ell^2}}{1+\frac{1}{\ell}} = 1 + \frac{8}{\ell^2+\ell},$$

and so, $\prod_{\ell \text{ prime}}\left(1+\frac{8}{\ell^2+\ell}\right)$ is convergent. On the other hand, $\prod_{\ell \mid m}\left(1+\frac{1}{\ell}\right) \ll \log\log m$ (see [8, Theorem 328]). Hence

$$\frac{|C_m|}{|G(m)|} \ll \frac{1}{\varphi(m)^2}, \text{ and } |C_m| \ll m^4 \log\log m,$$

and the conclusion of Proposition 5.3 follows.

(b) The proof is exactly similar to part (a). Under the assumptions of GRH and AHC, we apply the version of the Chebotarev theorem given in Proposition 4.1 which improves our error term. □

We are now ready to prove our Theorem 1.2. Our strategy is to compute densities of the sets of primes p for which the index of the reduction $\bar{\Gamma}$ of Γ modulo p is divisible by some fixed integer m. When m is large, we will use the following result, which follows from an application of the pigeonhole principle, coupled with the use of basic properties of canonical heights associated to elliptic curves. A proof of this result is given in the proof of [1, Proposition 1.2]. For the completeness of our arguments we sketch its proof here.

Proposition 5.4. *Let E be any elliptic curve defined over $\mathbb{Q}$. Let Γ be a subgroup of $E(\mathbb{Q})$ of rank r. Then for each positive real number z, we have*

$$\#\{p \textit{ prime}: \ |\bar{\Gamma}| < z\} = O\left(\frac{z^{1+\frac{2}{r}}}{\log z}\right),$$

where $\bar{\Gamma}$ denotes the reduction of Γ modulo p.

Proof. Clearly, it suffices to prove our result for free subgroups; so, let $\{Q_1, Q_2, \cdots, Q_r\}$ be a basis of Γ. We consider the set

$$S = \{n_1Q_1 + n_2Q_2 + \cdots + n_rQ_r;\ 0 \le n_i \le z^{\frac{1}{r}}\}.$$

Since Q_1, Q_2, $\cdots$, Q_r are linearly independent, then the number of elements of S exceeds

$$([z^{\frac{1}{r}}]+1)^r > z.$$

Now if p is a prime such that $|\bar{\Gamma}| < z$, then there are two distinct elements of S, say P and Q such that $\bar{P} = \bar{Q}$ in $\bar{E}(\mathbb{F}_p)$. In other words there are integers $|m_i| \leq z^{\frac{1}{r}}$ such that

$$m_1Q_1 + \cdots + m_rQ_r \neq \mathcal{O} \text{ in } E(\mathbb{Q}),$$

however

$$m_1\bar{Q}_1 + \cdots + m_r\bar{Q}_r = \bar{\mathcal{O}} \text{ in } \bar{E}(\mathbb{F}_p),$$

where $\mathcal{O}$ denotes the identity element. Let $R = m_1Q_1 + \cdots + m_rQ_r$ in $E(\mathbb{Q})$. Then R is a rational point in $E(\mathbb{Q})$, and so has a representation in the form

$$R = \left(\frac{m}{e^2}, \frac{n}{e^3}\right),$$

where m, n, and e are integers with $e > 0$ and $(m, e) = (n, e) = 1$ (see [20, page 68]). Since under reduction mod p, R maps to $\bar{\mathcal{O}}$, we conclude that $p \mid e$. So for fixed $\{m_i\}_{1\leq i\leq r}$ as above the number of primes satisfying $|\bar{\Gamma}| < z$ is bounded by

$$\omega(e) \ll \frac{\log e}{\log\log e} \ll \frac{h_x(R)}{\log h_x(R)},$$

where $\omega(e)$ is the number of distinct prime divisors of e and

$$h_x(R) = h_x\left(\left(\frac{m}{e^2}, \frac{n}{e^3}\right)\right) = \log\max\{|m|, |e^2|\},$$

is the x-height of R. Recall that the canonical height

$$\hat{h}(R) = \lim_{n\to\infty} \frac{h_x(2^nR)}{2^{2n}}$$

is a quadratic form on E, and it gives a bilinear pairing $\langle\ ,\ \rangle$ with $\hat{h}(R) = \langle R, R\rangle$ (see [18], page 229, Theorem 9.3). Moreover we know that $\hat{h} = h_x + O(1)$, where $O(1)$ depends on E only. So we have

$$\omega(e) \ll \frac{\log e}{\log\log e} \ll \frac{h_x(R)}{\log h_x(R)} = \frac{\hat{h}(R) + O(1)}{\log\left(\hat{h}(R) + O(1)\right)} \ll \frac{\langle R, R\rangle}{\log\langle R, R\rangle}.$$

So for fixed $|m_i| \leq z^{\frac{1}{r}}$, we have $\omega(e) \ll z^{\frac{2}{r}}/\log z$.

The number of possible values for e is bounded by the number of possible R. Noting the range of the m_i (i.e. $|m_i| \leq z^{\frac{1}{r}}$) , we conclude that the number in question is $O\left(z^{1+\frac{2}{r}}/\log z\right)$. □

The main difficulty in the proof of our Theorem 1.2 comes from the case when m is not very large, and it is not square-free; in that case we will use our Proposition 5.3 to derive our main result for non-CM elliptic curves. In fact, our paper is the first one in the literature which deals with the case when the index of $\bar{\Gamma}$ in $\bar{E}(\mathbb{F}_p)$ is divisible by an arbitrary integer m.

Proof of Part (a) of Theorem 1.2. For any prime number p, let $i_p = [\bar{E}(\mathbb{F}_p) : \bar{\Gamma}]$, let $j_p = [\bar{E}(\mathbb{F}_p) : \langle\bar{P}\rangle]$, let $N_p = \#\bar{E}(\mathbb{F}_p)$ and let $g(x) := \frac{1}{3}\inf\{f(y) : \frac{x}{\log x} \leq y \leq x\}$. Note that

$i_p \mid j_p$ and $g(x) \to \infty$ as $x \to \infty$. Using the classical Hasse bound for estimating N_p, we obtain $3p \geq N_p \geq \frac{p}{3}$, and so

$$\begin{aligned}
\#\{p \leq x : p \nmid \Delta \text{ and } |\bar{\Gamma}| < p/f(p)\} &= \#\{p \leq x : p \nmid \Delta,\ i_p > \frac{N_p}{p} f(p)\} \\
&\leq \#\{p \leq x : p \nmid \Delta,\ i_p > \frac{1}{3} f(p)\} \\
&\leq \#\{p \leq x : p \nmid \Delta,\ i_p > g(x)\} + \pi(x/\log x) \\
&\leq \#\{p \leq x : p \nmid \Delta,\ i_p > g(x)\} + o\left(\frac{x}{\log x}\right) \\
&\leq |\mathcal{B}_1| + |\mathcal{B}_2| + o\left(\frac{x}{\log x}\right),
\end{aligned}$$

where

$$\begin{aligned}
\mathcal{B}_1 &= \{p \leq x : p \nmid \Delta,\ i_p \in (x^{\frac{2}{r+2}} \log x, 3x]\}; \text{ and} \\
\mathcal{B}_2 &= \{p \leq x : p \nmid m\Delta,\ m \mid i_p, \text{ for some } m \in (g(x), x^{\frac{2}{r+2}} \log x]\}.
\end{aligned}$$

Observe that in the definition of $\mathcal{B}_1$ we used the fact that $i_p \leq N_p \leq 3p \leq 3x$. Also, observe that in $\mathcal{B}_2$ we can impose the condition $p \nmid m$ since the number of primes $p \leq x$ such that $p \mid i_p$ is $O(1)$ (because $N_p \leq 3p$, and there are at most finitely many primes p such that one of the points P, $2P$ or $3P$ reduces to $\bar{\mathcal{O}}$ modulo p). Finally, note that in the definition of $\mathcal{B}_2$ we may replace the condition $m \mid i_p$ with the weaker condition $m \mid j_p$, and find an upper bound for $\mathcal{B}_2$ in that case. Proposition 5.4 applied for $z := \frac{x^{r/(r+2)}}{\log x}$ yields

$$\#\mathcal{B}_1 = O\left(\frac{x}{(\log x)^{(r+2)/r} \cdot (r/(r+2) \cdot \log x - \log\log x)}\right) = o\left(\frac{x}{\log x}\right).$$

Let α be any sufficiently small real number in the interval $(0,1)$ (see inequality (5.3)). For $\#\mathcal{B}_2$, by Part (a) of Proposition 5.3, and employing the fact that $m/\varphi(m) \ll \log\log m \ll m^{\alpha/2}$ (see [8, Theorem 328]), and using that $\log m \ll m^{\alpha}$, we have the following estimate:

$$\begin{aligned}
\#\mathcal{B}_2 &\ll \sum_{g(x) < m \leq x^{2/(r+2)} \log x} \left(\frac{(\log\log m)^2}{m^2} \frac{x}{\log x} + O(m^4 (\log\log m) x^{1/2} \log mx)\right) \\
&\ll \frac{x}{\log x} \cdot \left(\sum_{g(x) \leq m < +\infty} \frac{1}{m^{2-\alpha}}\right) + O\left(x^{1/2+\alpha} \cdot \sum_{1 \leq m \leq x^{2/(r+2)+\alpha}} m^{4+\alpha/2}\right) \\
&\ll \frac{x}{\log x \cdot g(x)^{1-\alpha}} + O\left(x^{\frac{1}{2}+\alpha+\left(5+\frac{\alpha}{2}\right)\cdot\left(\frac{2}{r+2}+\alpha\right)}\right) \\
&= o\left(\frac{x}{\log x}\right).
\end{aligned}$$

In the last estimate we used the fact that $g(x) \to +\infty$ as $x \to +\infty$, and that $r > 18$, which means that there exists $\alpha > 0$ such that

$$\frac{1}{2} + \alpha + \left(5 + \frac{\alpha}{2}\right) \cdot \left(\frac{2}{r+2} + \alpha\right) < 1. \tag{5.3}$$

Finally, by putting together the estimates for $\#\mathcal{B}_1$ and $\#\mathcal{B}_2$, we conclude the proof of Theorem 1.2 (a). □

Proof of Part (b) of Theorem 1.2. The proof is almost identical to Part (a). The only difference is that in this case by employing Part (b) of Proposition 5.3, we have

$$\#\mathcal{B}_2 \ll \frac{x}{\log x \cdot g(x)^{1-\alpha}} + O\left(x^{\frac{1}{2}+\alpha+\left(3+\frac{\alpha}{4}\right)\cdot\left(\frac{2}{r+2}+\alpha\right)}\right).$$

The right-hand-side of this inequality is $o(x/\log x)$, since $g(x) \to \infty$ as $x \to \infty$, and since for $r > 10$ and for α sufficiently small and positive, we have

$$\frac{1}{2} + \alpha + \left(3 + \frac{\alpha}{4}\right) \cdot \left(\frac{2}{r+2} + \alpha\right) < 1.$$

□

Remark 5.5. From [5, Page 35] we know that for any sufficiently large prime ℓ, we have

$$\#\{p \leq x : p \nmid \ell\Delta,\ \ell \mid [\bar{E}(\mathbb{F}_p) : \bar{\Gamma}]\} \sim \frac{1 + O(1/\ell)}{\ell^{r+1}(1 - 1/\ell)^2(1 + 1/\ell)} \frac{x}{\log x},$$

as $x \to \infty$. This shows that for such fixed ℓ we have $i_p = [\bar{E}(\mathbb{F}_p) : \bar{\Gamma}] \geq \ell$ for a positive proportion of p. This justifies our claim that Theorem 1.2 is optimal in the sense that it is false for any bounded function f. A similar claim is also true for Theorem 1.4.

6. The CM case

Let E be a CM elliptic curve defined over $\mathbb{Q}$, and let K be the quadratic extension of $\mathbb{Q}$, over which the ring $\mathrm{End}(E)$ of all endomorphisms of E is defined. We assume that there exists a ring isomorphism between $\mathrm{End}(E)$ and the ring of algebraic integers $\mathfrak{O}_K$ in K. For simplicity we denote $\mathfrak{O}_K$ by $\mathfrak{O}$. In particular, there exists an analytic group isomorphism between $\mathbb{C}/\mathfrak{O}$ and $E(\mathbb{C})$. For each $\alpha \in \mathfrak{O}$, we let $[\alpha] \in \mathrm{End}(E)$ be the endomorphism which corresponds to the multiplication-by-α-map on $\mathbb{C}/\mathfrak{O}$.

By [13, Lemma 6], we know that $K \subset \mathbb{Q}(E[\ell^n]) \subset K_{\ell^n} = \mathbb{Q}(E[\ell^n], \frac{1}{\ell^n} \cdot P)$ (where $P \in E(\mathbb{Q})$) whenever $\ell^n > 2$. As in Section 3, let p be a prime number such that $(p, \ell\Delta) = 1$; hence p is a prime of good reduction for E.

In this section we assume that $\ell^n > 2$. We have the usual injection of $G_{\ell^n} := \mathrm{Gal}(K_{\ell^n}/\mathbb{Q})$ into $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \ltimes (\mathbb{Z}/\ell^n\mathbb{Z})^2$. Moreover, for the subgroup $\tilde{G}_{\ell^n} := \mathrm{Gal}(K_{\ell^n}/K)$ of G_{ℓ^n}, we have an embedding into $(\mathfrak{O}/\ell^n\mathfrak{O})^* \ltimes \mathfrak{O}/\ell^n\mathfrak{O}$ (see [19, proof of Theorem 2.3, page 109]). By abuse of notation, we identify G_{ℓ^n} with its isomorphic image inside $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \ltimes (\mathbb{Z}/\ell^n\mathbb{Z})^2$; similarly, we identify $\tilde{G}_{\ell^n}$ with its isomorphic image inside $(\mathfrak{O}/\ell^n\mathfrak{O})^* \ltimes \mathfrak{O}/\ell^n\mathfrak{O}$. In particular, this means that we fix an embedding of $(\mathfrak{O}/\ell^n\mathfrak{O})^*$ into $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$.

Let $N\mathfrak{a} = \#(\mathfrak{O}/\mathfrak{a}\mathfrak{O})$ denote the norm of any nonzero ideal $\mathfrak{a}$ of $\mathfrak{O}$; then $N\mathfrak{a}$ is completely multiplicative. Let $\tilde{G}(m) = (\mathfrak{O}/m\mathfrak{O})^* \ltimes \mathfrak{O}/m\mathfrak{O}$. Then

$$|\tilde{G}(m)| = m^2\Phi(m) = m^4 \prod_{\substack{\mathfrak{p}|(m) \\ \mathfrak{p}\in\mathrm{Spec}(\mathfrak{O})}} \left(1 - \frac{1}{N\mathfrak{p}}\right), \tag{6.1}$$

where $\Phi(m)$ is the number field analogue of the Euler function.

We use the criterion given in Lemma 3.3 for the divisibility by ℓ^n of the index $[\bar{E}(\mathbb{F}_p) : \langle \bar{P} \rangle]$ (where $\bar{E}$ is the reduction of E modulo p, and $P \in E(\mathbb{Q})$). If $\ell^n \mid [\bar{E}(\mathbb{F}_p) : \langle \bar{P} \rangle]$, then for each nonarchimedean place v of K_{ℓ^n} lying above p, the corresponding lift (γ_v, τ_v) of the Frobenius belongs to the set $C_{\ell^n} \subset G_{\ell^n}$ which contains all $(\gamma, \tau) \in \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \ltimes (\mathbb{Z}/\ell^n\mathbb{Z})^2$ satisfying the following conditions:

(1) there exists an integer $c \in \{0, \dots, n\}$ such that $\#\mathrm{null}(\gamma - 1) = \ell^{2n-c}$; and
(2) $\ell^{n-c}\tau \in (\gamma - 1) \cdot E[\ell^n]$.

Notation 6.1. *For any commutative ring R, and for each element $\alpha \in R$, we denote by* $\mathrm{null}(\alpha)$ *the set of all $\beta \in R$ such that $\alpha\beta = 0$.*

Let $\tilde{C}_{\ell^n} \subset \tilde{G}_{\ell^n}$ be the set of all elements $(\gamma, \tau) \in (\mathfrak{O}/\ell^n\mathfrak{O})^* \ltimes \mathfrak{O}/\ell^n\mathfrak{O}$ such that

(1) there exists an integer $c \in \{0, \dots, n\}$ such that $\#\mathrm{null}(\gamma - 1) = \ell^{2n-c}$; and
(2) $\ell^{n-c}\tau \in (\gamma - 1) \cdot E[\ell^n]$.

Using (3.2), it is immediate to check that both C_{ℓ^n} and $\tilde{C}_{\ell^n}$ are closed under conjugation.

Our first goal here is to bound the size of $\tilde{C}_{\ell^n}$. We note that $\mathfrak{O}$ is a principal ideal domain (PID), because it is the endomorphism ring of a CM elliptic curve defined over $\mathbb{Q}$ (see [18, Appendix C, Example 11.3.1]).

Proposition 6.2. *With the above notation, $\#\tilde{C}_{\ell^n} \le 3n^2\ell^{2n}$.*

Proof. Let $(\gamma, \tau) \in \tilde{C}_{\ell^n}$, and assume $\#\mathrm{null}(\gamma - 1) = \ell^{2n-c}$. We have three cases depending if ℓ splits, is inert, or it is ramified in $\mathfrak{O}$.

Case 1. ℓ splits in $\mathfrak{O}$.

Using that $\mathfrak{O}$ is a PID, we obtain

$$\mathfrak{O}/\ell^n\mathfrak{O} \xrightarrow{\sim} (\mathfrak{O}/\lambda_1^n\mathfrak{O}) \times (\mathfrak{O}/\lambda_2^n\mathfrak{O}), \tag{6.2}$$

where $\ell = \lambda_1 \cdot \lambda_2$, and each λ_i is a prime element in $\mathfrak{O}$; also, $\#(\mathfrak{O}/\lambda_i\mathfrak{O}) = \ell$ for each i. Finally, we represent ℓ under the isomorphism (6.2) as $(\lambda_1 u_1, \lambda_2 u_2)$, where $u_i \in (\mathfrak{O}/\lambda_i^n\mathfrak{O})^*$ for each i.

Under the isomorphism from (6.2), we may also write

$$\gamma - 1 = \left(\lambda_1^{n-d_1} \cdot \gamma_1, \lambda_2^{n-d_2} \cdot \gamma_2\right), \tag{6.3}$$

where $\gamma_i \in (\mathfrak{O}/\lambda_i^n\mathfrak{O})^*$ for $i = 1, 2$, and $0 \le d_1, d_2 \le n$. Thus

$$\#\mathrm{null}(\gamma - 1) = \prod_{i=1}^{2} \#\left(\mathfrak{O}/\lambda_i^{n-d_i}\mathfrak{O}\right) = \prod_{i=1}^{2} \ell^{n-d_i} = \ell^{2n-d_1-d_2}.$$

Hence $c = d_1 + d_2$. Furthermore, for each fixed d_1 and d_2 as above, there are at most

$$\prod_{i=1}^{2} \#\left(\mathfrak{O}/\lambda_i^{d_i}\mathfrak{O}\right) = \ell^{d_1+d_2}$$

elements $\gamma \in \mathfrak{O}/\ell^n\mathfrak{O}$ satisfying (6.3). Moreover,

$$\#\left((\gamma - 1) \cdot \mathfrak{O}/\ell^n\mathfrak{O}\right) = \prod_{i=1}^{2} \#\left(\lambda_i^{n-d_i} \cdot \mathfrak{O}/\lambda_i^n\mathfrak{O}\right) = \ell^{d_1+d_2}.$$

For each $\beta \in (\gamma-1)\cdot\mathfrak{O}/\ell^n\mathfrak{O} = \left(\lambda_1^{n-d_1}\cdot\mathfrak{O}/\lambda_1^n\mathfrak{O}, \lambda_2^{n-d_2}\cdot\mathfrak{O}/\lambda_2^n\mathfrak{O}\right)$, there are $\ell^{2n-2d_1-2d_2}$ solutions τ of the equation

$$\ell^{n-c}\tau = \left(\lambda_1^{n-d_1-d_2}u_1^{n-d_1-d_2}, \lambda_2^{n-d_1-d_2}u_2^{n-d_1-d_2}\right)\cdot\tau = \beta.$$

So, the number of pairs $(\gamma,\tau)\in\tilde{C}_{\ell^n}$ is bounded from above by

$$\sum_{0\le d_1+d_2\le n} \ell^{d_1+d_2}\cdot\ell^{d_1+d_2}\cdot\ell^{2n-2d_1-2d_2} \le \binom{n+2}{2}\cdot\ell^{2n}. \tag{6.4}$$

Case 2. ℓ is inert in $\mathfrak{O}$.

First we note that $\#(\mathfrak{O}/\ell\mathfrak{O}) = \ell^2$. Secondly, we can write $\gamma-1=\ell^{n-d}\cdot\gamma_1$ for a unique $d\in\{0,\dots,n\}$ and some $\gamma_1\in(\mathfrak{O}/\ell^n\mathfrak{O})^*$. Then

$$\#\mathrm{null}(\gamma-1) = \#\mathrm{null}(\ell^{n-d}) = \#\left(\ell^d\cdot\mathfrak{O}/\ell^n\mathfrak{O}\right) = \#\left(\mathfrak{O}/\ell^{n-d}\mathfrak{O}\right) = \ell^{2(n-d)}.$$

Because $\#\mathrm{null}(\gamma-1)=\ell^{2n-c}$, we conclude that $c=2d$, and so, $d\le\frac{n}{2}$. In addition, for each $0\le d\le n/2$, the number of $\gamma = 1+\ell^{n-d}\gamma_1$ (regardless if $\gamma_1\in(\mathfrak{O}/\ell^n\mathfrak{O})^*$ or not) is

$$\#\left(\mathfrak{O}/\ell^d\mathfrak{O}\right) = \ell^{2d}.$$

We also obtain that

$$\#\left((\gamma-1)\cdot\mathfrak{O}/\ell^n\mathfrak{O}\right) = \#\left(\ell^{n-d}\cdot\mathfrak{O}/\ell^n\mathfrak{O}\right) = \#\left(\mathfrak{O}/\ell^d\mathfrak{O}\right) = \ell^{2d}.$$

For each $\beta\in(\gamma-1)\cdot\mathfrak{O}/\ell^n\mathfrak{O} = \ell^{n-d}\cdot\mathfrak{O}/\ell^n\mathfrak{O}$, there exist precisely $\ell^{2(n-c)}=\ell^{2n-4d}$ elements $\tau\in\mathfrak{O}/\ell^n\mathfrak{O}$ such that

$$\ell^{n-c}\tau = \ell^{n-2d}\tau = \beta.$$

So, the number of pairs $(\gamma,\tau)\in\tilde{C}_{\ell^n}$ is bounded above by

$$\sum_{0\le d\le n/2} \ell^{2d}\cdot\ell^{2n-4d}\cdot\ell^{2d} \le (n/2+1)\cdot\ell^{2n}. \tag{6.5}$$

Case 3. ℓ is ramified in $\mathfrak{O}$.

In this case, we let $\ell\mathfrak{O}=(\lambda)^2$ for some prime element $\lambda\in\mathfrak{O}$. We obtain

$$\mathfrak{O}/\ell^n\mathfrak{O} \xrightarrow{\sim} \mathfrak{O}/\lambda^{2n}\mathfrak{O}.$$

Moreover, there exists $u\in\left(\mathfrak{O}/\lambda^{2n}\mathfrak{O}\right)^*$ such that $\ell=\lambda^2u$; also, note that $\#\left(\mathfrak{O}/\lambda\mathfrak{O}\right)=\ell$.

Under the above isomorphism for $\mathfrak{O}/\ell^n\mathfrak{O}$, let $\gamma-1=\lambda^{2n-d}\gamma_1$, where $\gamma_1\in(\mathfrak{O}/\lambda^{2n}\mathfrak{O})^*$ and $0\le d\le 2n$. Then

$$\#\mathrm{null}(\gamma-1) = \#\mathrm{null}(\lambda^{2n-d}) = \ell^{2n-d},$$

which means that $d=c\le n$. Furthermore, there are at most ℓ^d elements γ of the above form. We also compute easily that

$$\#\left((\gamma-1)\cdot\mathfrak{O}/\ell^n\mathfrak{O}\right) = \#\left(\lambda^{2n-d}\mathfrak{O}/\lambda^{2n}\mathfrak{O}\right) = \ell^d.$$

Now, for each $\beta\in(\gamma-1)\cdot\mathfrak{O}/\ell^n\mathfrak{O} = \lambda^{2n-d}\cdot\mathfrak{O}/\lambda^{2n}\mathfrak{O}$, there are ℓ^{2n-2d} solutions τ for the equation

$$\ell^{n-c}\tau = \lambda^{2n-2d}u^{n-d}\cdot\tau = \beta.$$

Thus, the number of pairs $(\gamma, \tau) \in \tilde{C}_{\ell^n}$ is bounded from above by

$$\sum_{0 \le d \le n} \ell^d \cdot \ell^d \cdot \ell^{2n-2d} \le (n+1) \cdot \ell^{2n}. \tag{6.6}$$

Summarizing (6.4), (6.5), and (6.6), we obtain $\#\tilde{C}_{\ell^n} \le 3n^2\ell^{2n}$, as desired. □

Next we show that a similar bound as in Proposition 6.2 holds for the conjugacy class C_{ℓ^n}.

Proposition 6.3. *There exists an absolute, effective constant $a > 1$ such that $\#C_{\ell^n} \le an^2\ell^{2n}$.*

For example, we could take $a = 100$ in Proposition 6.3. Before proceeding to the proof of Proposition 6.3 we prove the following technical result which will be used later in our proof.

Lemma 6.4. *Let d be a nonzero integer, let ℓ be a prime number, and let n be a positive integer. Then the number of pairs $(A, B) \in (\mathbb{Z}/\ell^n\mathbb{Z})^2$ satisfying $A^2 + dB^2 \equiv 1 \pmod{\ell^n}$ is bounded from above by $8\ell^n$.*

Proof. Let $S = \{(A, B) \in (\mathbb{Z}/\ell^n\mathbb{Z})^2 : A^2 + dB^2 \equiv 1 \pmod{\ell^n}\}$. Clearly, $S \subset (S_1 \cup S_2)$, where S_1 contains the pairs $(A, B) \in S$ for which $A \in (\mathbb{Z}/\ell^n\mathbb{Z})^*$, while S_2 contains the pairs $(A, B) \in S$ for which $B \in (\mathbb{Z}/\ell^n\mathbb{Z})^*$. The conclusion of Lemma 6.4 follows from the next two Claims.

Claim 6.5. *If ℓ is odd, then $|S_1| \le 2\ell^n$; if $\ell = 2$, then $|S_1| \le 2^{n+2}$.*

Proof of Claim 6.5. For each fixed $B \in \mathbb{Z}/\ell^n\mathbb{Z}$, we have $(A, B) \in S_1$ if and only if $A \in (\mathbb{Z}/\ell^n\mathbb{Z})^*$ and $A^2 \equiv 1 - dB^2 \pmod{\ell^n}$. Because A is a unit, and there are exactly 2 elements in $(\mathbb{Z}/\ell^n\mathbb{Z})^*$ of order dividing 2 (if $\ell > 2$), and there are exactly 4 elements in $(\mathbb{Z}/2^n\mathbb{Z})^*$ of order dividing 2 (if $n \ge 3$), we conclude the proof of Claim 6.5. □

Now, if $\ell \mid d$, then actually $S = S_1$; thus, from Claim 6.5 we conclude that $|S| \le 4\ell^n$, as desired.

So, from now on, assume that $(\ell, d) = 1$.

Claim 6.6. *If $(\ell, d) = 1$, then $|S_2| \le 4\ell^n$.*

Proof of Claim 6.6. This follows from a similar argument as in the proof of Claim 6.5, only that this time we fix $A \in \mathbb{Z}/\ell^n\mathbb{Z}$, and then count the number of possible solutions $B \in (\mathbb{Z}/\ell^n\mathbb{Z})^*$ such that $dB^2 \equiv 1 - A^2 \pmod{\ell^n}$. Because $(d, \ell) = 1$, we obtain the desired conclusion. □

Therefore, if $(\ell, d) = 1$, then $|S| \le |S_1| + |S_2| \le 8\ell^n$. □

Now we are ready to prove Proposition 6.3.

Proof of Proposition 6.3. Using Proposition 6.2, we only need to bound the cardinality of $C_{\ell^n} \setminus \tilde{C}_{\ell^n}$. We will prove that

$$\#(C_{\ell^n} \setminus \tilde{C}_{\ell^n}) = O\left(\ell^{2n}\right), \tag{6.7}$$

where the O-constant is absolute and effective.

Let $H_{\ell^n} := \mathrm{Gal}(\mathbb{Q}(E[\ell^n])/\mathbb{Q})$ and $\tilde{H}_{\ell^n} := \mathrm{Gal}(\mathbb{Q}(E[\ell^n])/K)$, and let $\sigma = (\gamma, \tau) \in C_{\ell^n} \setminus \tilde{C}_{\ell^n}$ such that $\mathrm{null}(\gamma - 1) = \ell^{2n-c}$, for some $c \in \{0, \dots, n\}$. Because $(\gamma, \tau) \notin \tilde{G}_{\ell^n}$ we get that $\gamma \in H_{\ell^n} \setminus \tilde{H}_{\ell^n}$. We fix an embedding of K_{ℓ^n} into $\mathbb{C}$. Let θ be the usual complex conjugation map on $\mathbb{C}$; by abuse of notation, we denote also by θ its restriction to a nontrivial automorphism of K_{ℓ^n} (note that $K \subset K_{\ell^n}$ is a quadratic imaginary field). Each element in $H_{\ell^n} \setminus \tilde{H}_{\ell^n}$ can be uniquely represented as $\tilde{\gamma}\theta$. Because $\tilde{\gamma} \in \tilde{H}_{\ell^n}$, and $\tilde{H}_{\ell^n}$ embeds into $(\mathfrak{O}/\ell^n\mathfrak{O})^*$, then there exists $m_{\tilde{\gamma}} \in \mathfrak{O}$ (coprime with ℓ) such that the restriction of $\tilde{\gamma}$ on $E[\ell^n]$ is the same as the action of the endomorphism $[m_{\tilde{\gamma}}]$ of E given by multiplication by $m_{\tilde{\gamma}}$ on $\mathbb{C}/\mathfrak{O}$ (more precisely, $m_{\tilde{\gamma}} \equiv \tilde{\gamma} \pmod{\ell^n\mathfrak{O}}$).

Let $\wp$ be the usual Weierstrass function associated to the lattice $\mathfrak{O} \subset \mathbb{C}$; then for every $z \in \mathbb{C}$ we have

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(\mathfrak{O})\wp(z) - g_3(\mathfrak{O}),$$

where

$$g_2(\mathfrak{O}) := \sum_{\omega \in \mathfrak{O}\setminus\{0\}} \frac{1}{\omega^4} \text{ and } g_3(\mathfrak{O}) := \sum_{\omega \in \mathfrak{O}\setminus\{0\}} \frac{1}{\omega^6}.$$

Because $\mathfrak{O}$ is invariant under taking complex conjugates, we obtain that $g_2(\mathfrak{O}), g_3(\mathfrak{O}) \in \mathbb{R}$. Let E_0 be the elliptic curve given by the equation over $\mathbb{R}$:

$$y^2 = 4x^3 - g_2(\mathfrak{O})x - g_3(\mathfrak{O}).$$

Because E is an elliptic curve defined over $\mathbb{Q}$, then there exist $a, b \in \mathbb{Q}$ such that the Weierstrass equation of E over $\mathbb{Q}$ is

$$y^2 = x^3 + ax + b. \tag{6.8}$$

We know that E has complex multiplication by $\mathfrak{O}$; hence there exists $\beta \in \mathbb{C}^*$ such that E is isomorphic to E_0 over $\mathbb{C}$ through the morphism $f : E_0 \longrightarrow E$ given by

$$f(x, y) := (4\beta^2 x, 4\beta^3 y).$$

Thus

$$-4\beta^4 g_2(\mathfrak{O}) = a \text{ and } -16\beta^6 g_3(\mathfrak{O}) = b. \tag{6.9}$$

Case 1. $b = 0$.

Then (6.9) yields $g_3(\mathfrak{O}) = 0$, and

$$\beta^4 = \frac{-a}{4g_2(\mathfrak{O})},$$

which means that either $\beta \in \mathbb{R}$, or $\beta \in \left(\frac{1+i}{\sqrt{2}}\right) \cdot \mathbb{R}$ (note that we may choose any β which satisfies (6.9)). So, either

$$\theta(\beta) = \beta; \text{ or}$$

$$\theta(\beta^2) = -\beta^2 \text{ and } \theta(\beta^3) = i \cdot \beta^3. \tag{6.10}$$

Also in this case, (6.8) yields that the equation of E is given by $y^2 = x^3 + ax$, and so, E has the following endomorphism:

$$(x, y) \mapsto (-x, iy), \tag{6.11}$$

whose square is the automorphism $[-1]$ on E. Thus $\mathfrak{O} = \mathbb{Z}[i]$, and under a suitable identification of $\mathrm{End}(E)$ with $\mathbb{Z}[i]$, the endomorphism from (6.11) corresponds to $i \in \mathbb{Z}[i]$.

We will prove (6.7) in this case, i.e. if $\mathfrak{O} = \mathbb{Z}[i]$. Assume (6.10) holds; a similar argument would work if β were fixed by θ. Now, if (6.10) holds, then for any $T \in E[\ell^n]$, we have

$$\tilde{\gamma}\theta(T) = \left(4\beta^2\wp(im_{\tilde{\gamma}}\overline{\alpha}), 4\beta^3\wp'(im_{\tilde{\gamma}}\overline{\alpha})\right), \tag{6.12}$$

where $\alpha \in \frac{1}{\ell^n} \cdot \mathfrak{O}$ satisfies

$$T = \left(4\beta^2\wp(\alpha), 4\beta^3\wp'(\alpha)\right).$$

Indeed, because E is defined over $\mathbb{Q}$, then also $\theta(T) \in E[\ell^n]$. Furthermore, because $(\overline{\wp(z)}, \overline{\wp'(z)}) = (\wp(\overline{z}), \wp'(\overline{z}))$ we get

$$\begin{aligned} \theta(T) &= \left(4\overline{\beta^2}\wp(\overline{\alpha}), 4\overline{\beta^3}\wp'(\overline{\alpha})\right) \\ &= \left(-4\beta^2\wp(\overline{\alpha}), 4\beta^3 i\wp'(\overline{\alpha})\right) \\ &= \left(4\beta^2\wp(i\overline{\alpha}), 4\beta^3\wp'(i\overline{\alpha})\right), \end{aligned}$$

where in the above equalities we used (6.10) and (6.11). Then (6.12) holds because the action of $\tilde{\gamma}$ on the torsion points is induced by multiplication by $m_{\tilde{\gamma}}$ on $\mathbb{C}/\mathfrak{O}$.

Because $\#\text{null}(\tilde{\gamma}\theta - 1) = \ell^{2n-c}$ then there are ℓ^{2n-c} distinct $\alpha = \frac{x+yi}{\ell^n}$ with $0 \le x, y \le \ell^n - 1$ such that $im_{\tilde{\gamma}}\overline{\alpha} - \alpha \in \mathfrak{O}$. So, letting $m_{\tilde{\gamma}} := A + Bi$, we obtain

$$Ay \equiv (1+B)x \pmod{\ell^n}\text{; and} \tag{6.13}$$

$$Ax \equiv (1-B)y \pmod{\ell^n}. \tag{6.14}$$

Assume $\ell > 2$. Then at least one of $(1+B)$ and $(1-B)$ is coprime with ℓ (note that ℓ is a prime number). Without loss of generality, we assume $(1+B, \ell) = 1$. Then given any $y \in \mathbb{Z}/\ell^n\mathbb{Z}$ there exists a unique $x \in \mathbb{Z}/\ell^n\mathbb{Z}$ satisfying (6.13). So, $\text{null}(\tilde{\gamma}\theta - 1)$ has at most ℓ^n elements, i.e. $c = n$ in Lemma 3.4. Furthermore, in order for (6.13) and (6.14) have ℓ^n solutions simultaneously, we need

$$A^2 + B^2 \equiv 1 \pmod{\ell^n}. \tag{6.15}$$

Using Lemma 6.4, there are at most $8\ell^n$ solutions $(A, B) \in (\mathbb{Z}/\ell^n\mathbb{Z})^2$ to (6.15). Hence each $\gamma \in C_{\ell^n} \setminus \tilde{C}_{\ell^n}$ satisfies $\#\text{null}(\gamma - 1) = \ell^n$, and there are at most $8\ell^n$ such γ's. Moreover, for each such γ there are ℓ^n elements $\tau \in \mathfrak{O}/\ell^n\mathfrak{O}$ such that $\tau \in (\gamma-1)\cdot\mathfrak{O}/\ell^n\mathfrak{O}$ (because $\#\text{null}(\gamma-1) = \ell^n$, while $\#\mathfrak{O}/\ell^n\mathfrak{O} = \ell^{2n}$). So,

$$\#(C_{\ell^n} \setminus \tilde{C}_{\ell^n}) \le 8\ell^{2n}.$$

Assume $\ell = 2$. Then at least one of $(1+B)$ and $(1-B)$ is not divisible by 4. If B is even, then, arguing as above, we obtain that there are at most 2^{2n+3} corresponding pairs $(\gamma, \tau) \in C_{\ell^n} \setminus \tilde{C}_{\ell^n}$.

If B is odd, without loss of generality, we assume $(1-B, 2^n) = 2$. Then given any $x \in \mathbb{Z}/2^n\mathbb{Z}$, there are at most 2 solutions $y \in \mathbb{Z}/2^n\mathbb{Z}$ satisfying (6.14). So, there are at most 2^{n+1} solutions (x, y) solving simultaneously (6.13) and (6.14); thus $c \ge n-1$ with the notation as in Lemma 3.4. Furthermore, in order to have at least 2^n solutions (x, y) to the system formed by (6.13) and (6.14) we need

$$A^2 + B^2 \equiv 1 \pmod{2^{n-1}}. \tag{6.16}$$

There are at most 2^{n+4} solutions $(A, B) \in (\mathbb{Z}/2^n\mathbb{Z})^2$ satisfying (6.16) (after applying Lemma 6.4 to (6.16), and then noting that each solution (A, B) modulo 2^{n-1} has at most 4 liftings to solutions modulo 2^n).

For each one of these at most 2^{n+4} elements $\gamma \in H_{2^n} \setminus \tilde{H}_{2^n}$ such that $\#\text{null}(\gamma - 1) \ge 2^n$, we have at most 2^n elements in $(\gamma - 1) \cdot E[2^n]$. Therefore, for a fixed such γ there are at most $4 \cdot 2^n$

elements $\tau \in E[2^n]$ such that $2\tau \in (\gamma - 1) \cdot E[2^n]$ (note that $c \geq n-1$ in the criterion from Lemma 3.4 in this case). Hence

$$\#(C_{2^n} \setminus \tilde{C}_{2^n}) \leq 2^{2n+3} + 2^{n+4} \cdot 2^{n+2} = 72 \cdot 2^{2n}.$$

Case 2. $b \neq 0$.

Then (6.9) yields that also $g_3(\mathfrak{O}) \neq 0$, and so,

$$\beta^2 = \sqrt[3]{-b/(16 g_3(\mathfrak{O}))} \in \mathbb{R}.$$

Thus $\beta \in \mathbb{R}$ or $\beta \in i \cdot \mathbb{R}$; either way, we have

$$\theta(\beta) = \pm\beta. \tag{6.17}$$

We will prove (6.7) if $\mathfrak{O} = \mathbb{Z}[i\sqrt{d}]$ for some square-free positive integer $d > 1$ (a similar argument works for all other cases). Actually, because $\mathfrak{O}$ is a PID, then $d = 2$ is the only possibility in this case. However, for any of the remaining quadratic number fields, we have $\mathfrak{O} = \mathbb{Z}[(1 + i\sqrt{d})/2]$, and so, any integral element is of the form

$$\frac{A + Bi\sqrt{d}}{2}, \text{ where } A \equiv B \pmod 2,$$

which allows us to reduce our computations to the case $\mathbb{Z}[i\sqrt{d}]$.

So, in Case 2., we claim that for any $T \in E[\ell^n]$, we have

$$\tilde{\gamma}\theta(T) = \left(4\beta^2 \wp(\pm m_{\tilde{\gamma}}\overline{\alpha}), 4\beta^3 \wp'(\pm m_{\tilde{\gamma}}\overline{\alpha})\right), \tag{6.18}$$

where $\alpha \in \frac{1}{\ell^n} \cdot \mathfrak{O}$ satisfies

$$T = \left(4\beta^2 \wp(\alpha), 4\beta^3 \wp'(\alpha)\right).$$

Indeed, because $\wp$ is even and $\wp'$ is odd, we get

$$\begin{aligned} \theta(T) &= \left(4\overline{\beta^2}\wp(\overline{\alpha}), 4\overline{\beta^3}\wp'(\overline{\alpha})\right) \\ &= \left(4\beta^2 \wp(\overline{\alpha}), \pm 4\beta^3 \wp'(\overline{\alpha})\right) \\ &= \left(4\beta^2 \wp(\pm\overline{\alpha}), 4\beta^3 \wp'(\pm\overline{\alpha})\right), \end{aligned}$$

where in the above equalities we used (6.17). Then (6.18) holds because the action of $\tilde{\gamma}$ on the torsion points is induced by multiplication by $m_{\tilde{\gamma}}$ on $\mathbb{C}/\mathfrak{O}$.

Because $\#\text{null}(\tilde{\gamma}\theta - 1) = \ell^{2n-c}$ then there are ℓ^{2n-c} distinct $\alpha = \frac{x + yi\sqrt{d}}{\ell^n}$ with $0 \leq x, y \leq \ell^n - 1$ such that $\pm m_{\tilde{\gamma}}\overline{\alpha} - \alpha \in \mathfrak{O}$. Without loss of generality, assume that we have a minus sign in the last relation. So, letting $m_{\tilde{\gamma}} := A + Bi\sqrt{d}$, we obtain

$$Bdy \equiv -(A+1)x \pmod{\ell^n}; \text{ and} \tag{6.19}$$

$$Bx \equiv (A-1)y \pmod{\ell^n}. \tag{6.20}$$

By employing a similar argument as in Case 1., we finish the proof of Proposition 6.3. □

Using that $\#C_m \leq \prod_{\ell^n || m} \#C_{\ell^n}$, we obtain the following result (note that $\#C_2 \leq [K_2 : \mathbb{Q}] \leq 12$, as the case $\ell^n = 2$ is the only one not explicitly covered by Propositions 6.2 and 6.3).

Proposition 6.7. *Let C_m be the conjugacy class of G_m defined as before, and let E have CM. Then there exists an effective absolute constant a such that $|C_m| \leq a^{\omega(m)} d^2(m) m^2$.*

The following result is proved in [11, Theorem 5.2, pages 122-127] (see also [2] and [16]); note that for $m \geq 3$, we have $K \subset K_m$, and moreover, any endomorphism of E is defined over K.

Proposition 6.8. *Let $m \geq 3$. If E has complex multiplication, then the index of $\tilde{G}_m = \mathrm{Gal}(K_m/K)$ in $\tilde{G}(m)$ is bounded by a constant $i(E)$ depending only on E.*

The following result is proved in [6, Proposition 1].

Proposition 6.9. *Let $m \geq 3$. If E has CM, then AHC holds for the extension $K_m/\mathbb{Q}$.*

Now we can prove the counterpart in the CM case of Proposition 5.3.

Proposition 6.10. *Let $m \geq 3$, let E be a CM elliptic curve over $\mathbb{Q}$ with discriminant Δ, and let P be a point of infinite order in $E(\mathbb{Q})$. Moreover suppose that GRH holds for $K_m = \mathbb{Q}(E[m], \frac{1}{m} \cdot P)$. Then*

$$\#\{p \leq x : p \nmid m\Delta \text{ and } m \mid [\bar{E}(\mathbb{F}_p) : \langle \bar{P} \rangle]\} \leq C(E) \frac{a^{\omega(m)} d^2(m)}{\Phi(m)} \operatorname{Li} x + O(m a^{\omega(m)/2} d(m) x^{1/2} \log mx),$$

where $C(E)$ is a constant depending only on the elliptic curve E, and the constant in the O-notation also depends only on E.

Proof. By Lemma 3.4, Proposition 4.1, Proposition 6.8, and Proposition 6.9, we have

$$\begin{aligned}
\#\{p \leq x : p \nmid m\Delta \text{ and } m \mid [\bar{E}(\mathbb{F}_p) : \langle \bar{P} \rangle]\} &\leq \#\{p \leq x,\ p \text{ unramified in } K_m,\ \sigma_p \subseteq C_m\} \\
&\leq \frac{i(E)}{2} \frac{|C_m|}{|\tilde{G}(m)|} \operatorname{Li} x \\
&\quad + O\left(|C_m|^{1/2} x^{1/2} \log \left(|\tilde{G}(m)| \left(\prod_{p \in P(K_m/\mathbb{Q})} p \right) x \right) \right).
\end{aligned}$$

The assertion of the proposition follows by applications of (6.1) and Proposition 6.7 in the above inequality. □

The following result, which is a consequence of applying the normal order method and the large sieve in an imaginary quadratic field, is proved in [1, Theorem 4.1].

Proposition 6.11. *Let E be a CM elliptic curve. Let $0 < \delta < 1$ and let $\epsilon_1(x)$ and $\epsilon_2(x)$ be such that*

$$\lim_{x \to \infty} \epsilon_1(x) = \lim_{x \to \infty} \epsilon_2(x) = 0.$$

Let

$$H\left(x, x^{\delta - \epsilon_1(x)}, x^{\delta + \epsilon_2(x)}\right) = \#\{p \leq x : \exists u \text{ such that } u \mid \#\bar{E}(\mathbb{F}_p) \text{ and } x^{\delta - \epsilon_1(x)} < u < x^{\delta + \epsilon_2(x)}\}.$$

Then we have

$$H(x, x^{\delta - \epsilon_1(x)}, x^{\delta + \epsilon_2(x)}) = o\left(\frac{x}{\log x}\right)$$

as $x \to \infty$.

Now we are ready to prove our main result in the case of CM elliptic curves.

Proof of Theorem 1.4. Let a be the constant occurring in Proposition 6.7. An elementary analytic estimation yields the following

$$\sum_{m\le x} a^{\omega(m)/2} d(m) \le \sum_{m\le x} d(m)^{(\log_2 a)/2+1} \ll x(\log x)^{\beta}, \tag{6.21}$$

for a positive integer $\beta > 2$. Also,

$$\frac{m^2}{\Phi(m)} \cdot a^{\omega(m)} d(m)^2 \ll m^{\alpha} \text{ for any } \alpha > 0. \tag{6.22}$$

Following the notation for the function $g(x)$, and for the index i_p of $\bar{\Gamma}$ in $\bar{E}(\mathbb{F}_p)$ as introduced in the proof of Theorem 1.2, we have

$$\#\{p \le x : p \nmid \Delta \text{ and } |\bar{\Gamma}| < p/f(p)\} \ \le \ |\mathcal{B}_1'| + H\left(x, \frac{x^{\frac{2}{r+2}}}{(\log x)^{\beta}}, x^{\frac{2}{r+2}} \log x\right) + |\mathcal{B}_2'| + o\left(\frac{x}{\log x}\right),$$

where $\mathcal{B}_1' = \{p \le x : p \nmid \Delta, i_p \in [x^{\frac{2}{r+2}} \log x, 3x]\}$, and $\mathcal{B}_2' = \{p \le x : p \nmid m\Delta,\ m \mid i_p, \text{ for some } m \in (g(x), \frac{x^{\frac{2}{r+2}}}{(\log x)^{\beta}}]\}$.

From the proof of Theorem 1.2 (note that Proposition 5.4 holds for *all* elliptic curves) and Proposition 6.11 we have

$$|\mathcal{B}_1'| = o\left(\frac{x}{\log x}\right), \text{ and } H\left(x, \frac{x^{\frac{2}{r+2}}}{(\log x)^{\beta}}, x^{\frac{2}{r+2}} \log x\right) = o\left(\frac{x}{\log x}\right) \text{ and so,}$$

$$\#\{p \le x : p \nmid \Delta \text{ and } |\bar{\Gamma}| < p/f(p)\} = |\mathcal{B}_2'| + o\left(\frac{x}{\log x}\right).$$

As in proof of Theorem 1.2, we note that in the definition of $\mathcal{B}_2'$ we may replace the condition $m \mid i_p$ with the weaker condition $m \mid j_p$, and find an upper bound for $\mathcal{B}_2'$ in that case (where $j_p = [\bar{E}(\mathbb{F}_p) : \langle \bar{P} \rangle]$).

Let α be any real number between 0 and 1. For $\#\mathcal{B}_2'$, by Proposition 6.10, and using inequalities (6.21) and (6.22), we have

$$\begin{aligned}
\#\mathcal{B}_2' &\ll \sum_{g(x)<m\le x^{2/(r+2)}/(\log x)^{\beta}} \left(\frac{1}{m^{2-\alpha}} \frac{x}{\log x} + O(m a^{\omega(m)/2} d(m) x^{1/2} \log mx)\right) \\
&\ll \frac{x}{\log x} \cdot \left(\sum_{g(x)\le m<+\infty} \frac{1}{m^{2-\alpha}}\right) + O\left(x^{1/2} \log x \cdot \sum_{1\le m\le x^{2/(r+2)}/(\log x)^{\beta}} m a^{\omega(m)/2} d(m)\right) \\
&\ll \frac{x}{\log x \cdot g(x)^{1-\alpha}} + O\left(\frac{x^{\frac{1}{2}+\frac{4}{r+2}}}{(\log x)^{\beta-1}}\right) \\
&= o\left(\frac{x}{\log x}\right),
\end{aligned}$$

as long as $r \ge 6$ (note that $\beta > 2$ by our choice). □

References

[1] A. Akbary and V. K. Murty, Reduction mod p of subgroups of the Mordell-Weil group of an elliptic curve, *Int. J. of Number Theory*, **5** (2009), 465–487.

[2] M. Bachmakov, Cohomology of abelian varieties over a number field, *Uspehi Mat. Nauk*, **27** (1972), no. 6 (168), 25–66.

[3] P. Erdös and M. R. Murty, On the order of a (mod p), *CRM Proceedings and Lecture Notes*, Volume **19**, 1999, 87–97.

[4] N. D. Elkies and M. Watkins, Elliptic curves of large rank and small conductor, *Lecture Notes in Computer Science*, Volume **3076**, 2004, 42–56.

[5] R. Gupta and M. R. Murty, Primitive points on elliptic curves, *Compositio Math.* **58** (1986), 13–44.

[6] R. Gupta and M. R. Murty, Cyclicity and generation of points mod p on elliptic curves, *Invent. Math.* **101** (1990), 225–235.

[7] C. Hall and J. F. Voloch, Towards Lang-Trotter for elliptic curves over function fields, *Pure Appl. Math. Q.* **2** (2006), no. 1, part 1, 163–178.

[8] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, 5th edition, Oxford Science Publications, 1979.

[9] C. Hooley, On Artin's conjecture, *J. reine angew. Math.* **225** (1967), 209–220.

[10] J. Lagarias and A. Odlyzko, Effective versions of the Chebotarev density theorem, *Algebraic Number Fields, Fröhlich (ed.)*, 1977, 409–464.

[11] S. Lang, Elliptic curves: Diophantine Analysis, Springer Verlag, Berlin-New York, 1978. xi+261 pp.

[12] S. Lang and H. Trotter, Primitive points on elliptic curves, *Bull. Amer. Math. Soc.* **83** (1977), 289–292.

[13] M. R. Murty, On Artin's conjecture, *J. Number Theory* **16** (1983), 147–168.

[14] M. R. Murty, V. K. Murty, and N. Saradha, Modular forms and the Chebotarev density theorem, *American J. Math.* **110** (1988), 253-281.

[15] F. Pappalardi, On the order of finitely generated subgroups of $\mathbb{Q}^*$ (mod p) and divisors of $p-1$, *J. Number Theory* **57** (1996), 207–222.

[16] K. Ribet, Kummer theory on extensions of abelian varieties by tori, *Duke Math. J.* **46** (1979), no. 4, 745–761.

[17] J.-P. Serre, Quelques applications du théorème de densité de Chebotarev, *Publ. Math. IHES* **54** (1981), 323–401.

[18] J. H. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, 1986.

[19] J. H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Springer-Verlag, 1994.

[20] J. H. Silverman and J. Tate, Rational Points on Elliptic Curves, Springer-Verlag, 1992.

Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, AB T1K 3M4, Canada

E-mail address: amir.akbary@uleth.ca

Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, AB T1K 3M4, Canada

E-mail address: dragos.ghioca@uleth.ca

Department of Mathematics, University of Toronto, 40 St. George Street, Toronto, ON M5S 2E4, Canada

E-mail address: murty@math.toronto.edu