On the Greatest Prime Divisor of N_p

Amir Akbary*

Abstract

Let E be an elliptic curve defined over $\mathbb{Q}$. For any prime p of good reduction, let E_p be the reduction of E mod p. Denote by N_p the cardinality of $E_p(\mathbb{F}_p)$, where $\mathbb{F}_p$ is the finite field of p elements. Let $P(N_p)$ be the greatest prime divisor of N_p. We prove that if E has CM then for all but $o(x/\log x)$ of primes $p \leq x$,

$$P(N_p) > p^{\vartheta(p)},$$

where $\vartheta(p)$ is any function of p such that $\vartheta(p) \to 0$ as $p \to \infty$. Moreover we show that for such E there is a positive proportion of primes $p \leq x$ for which

$$P(N_p) > p^{\vartheta},$$

where ϑ is any number less than $\vartheta_0 = 1 - \frac{1}{2}e^{-\frac{1}{4}} = 0.6105\cdots$. As an application of this result we prove the following. Let Γ be a free subgroup of rank $r \geq 2$ of the group of rational points $E(\mathbb{Q})$, and Γ_p be the reduction of Γ mod p, then for a positive proportion of primes $p \leq x$, we have

$$|\Gamma_p| > p^{\vartheta_0 - \epsilon},$$

where $\epsilon > 0$.

Keywords: Reduction mod p of elliptic curves, Elliptic curves over finite fields, Brun-Titchmarsh inequality in number fields, Bombieri-Vinogradov theorem in number fields, Abelian extensions of imaginary quadratic number fields.

2000 *Mathematics Subject Classification.* Primary 11G20, Secondary 11N37.

1 Introduction

Let a be a fixed integer and p be a prime. Let $P(p+a)$ be the greatest prime divisor of $p+a$. Many authors studied the problem of finding good lower bounds for $P(p+a)$ as $p \to \infty$. More precisely, for any fixed integer a and real variables x, ϑ, let $N_a(x, x^{\vartheta})$ be the number of $p \leq x$ for which $P(p+a) > x^{\vartheta}$. Then Goldfeld [G] proved that for $\vartheta < c_0 = \frac{7}{12} = .5833\cdots$,

$$N_a(x, x^{\vartheta}) = \sum_{\substack{p \leq x \\ P(p+a) > x^{\vartheta}}} 1 > \eta(\vartheta)\frac{x}{\log x},$$

as $x \to \infty$, where $\eta(\vartheta) > 0$. Over the last 30 years, there has been a lot of effort to find larger values of c_0. This is a list of the major improvements.

*Research of the author is partially supported by NSERC.

(1970)	Motohashi	$c_0 = .6105\cdots$,
(1972)	Hooley	$c_0 = .6197\cdots$,
(1973)	Hooley	$c_0 = .6250\cdots$,
(1982)	Iwaniec	$c_0 = .6381\cdots$,
(1984)	Deshouillers − Iwaniec	$c_0 = .6562\cdots$,
(1985)	Fouvry	$c_0 = .6687\cdots$.

The best result to date is due to Baker and Harman [BH] who improved the value of c_0 to 0.677.

The analogous of the above problem have also been considered for sequences other than the sequence $\{p + a\}$. For example, Stewart [S] has proved that for all sufficiently large primes p,

$$P(2^p - 1) > \frac{1}{2} p (\log p)^{\frac{1}{4}}.$$

Another example is related to the Fourier coefficients a_n of a non-CM normalized eigenform of weight k and level N with integer coefficients. In [MMS], R. Murty, K. Murty, and Saradha showed that under the assumption of the Generalized Riemann Hypothesis (GRH),

$$P(a_p) \geq \exp\left((\log p)^{1-\epsilon}\right)$$

for any $\epsilon > 0$, and for a set of primes p of density 1. Moreover, they proved that unconditionally

$$P(a_p) \geq \exp\left((\log\log p)^{1-\epsilon}\right)$$

for any $\epsilon > 0$, and for a set of primes of density one.

We point out in passing that results on the greatest prime divisor of certain sequences have applications in computational number theory and cryptography. For example the original proof that "Primes is in P" [AKS] uses a result of the form $P(p-1) > p^{\vartheta}$ with $\vartheta > 1/2$.

In this paper we prove an elliptic analogue of such a result. Let E be an elliptic curve defined over $\mathbb{Q}$. For any prime p of good reduction, let E_p be the elliptic curve over the finite field $\mathbb{F}_p$ obtained by reducing E mod p. Let $N_p = \#E_p(\mathbb{F}_p)$. Then we prove the following.

Corollary 5.3 *Let $E/\mathbb{Q}$ have* CM *by $\mathfrak{O}_K$ (i.e complex multiplication by the full ring of integers of an imaginary quadratic field K). Let $\vartheta < \vartheta_0 = 1 - \frac{1}{2}e^{-\frac{1}{4}} = 0.6105\cdots$. Then for a positive proportion of primes $p \leq x$,*

$$P(N_p) > p^{\vartheta}.$$

The method of the proof of this theorem follows closely [G] and [M]. However, in the elliptic setting, the proof involves several new ideas and modifications. The new ingredients include Huxley's extension of the Bombieri-Vinogradov theorem to number fields (Theorem 2.2), a Brun-Titchmarsh type inequality in number fields due to Hinz and Lodemann (Theorem 2.1), and facts from the class field theory of the extension $K \subset K(E[\mathfrak{a}])$. For an ideal $\mathfrak{a}$ of $\mathfrak{O}_K$, $K(E[\mathfrak{a}])$ is obtained by adjoining the coordinates of $\mathfrak{a}$-division points of E to K. We briefly describe the proof's strategy. For a prime ℓ, set

$$\pi_E(x;\ell) = \#\{p \leq x,\ p \text{ is a good prime and } \ell \mid N_p\},$$

where a good prime means a prime of good reduction. Then it is easy to show that

$$\sum_{\substack{p\leq x\\ p \text{ good}}} \sum_{\ell \mid N_p} \log \ell = \sum_{\ell \leq x^+} (\log \ell)\pi_E(x;\ell), \quad (\heartsuit)$$

where $x^+ = (\sqrt{x}+1)^2$ (see Section 4). The estimation of the left-hand side of $(\heartsuit)$ is straightforward. On the right-hand side we employ the number field versions of the Bombieri-Vinogradov theorem,

the Brun-Titchmarch inequality, and properties of the extension $K \subset K(E[\mathfrak{a}])$ to estimate the sum for $\ell \leq x^{\vartheta}$. These estimations imply a lower bound for the sum of the right-hand side of $(\heartsuit)$ for $\ell > x^{\vartheta}$. From this lower bound we deduce our result.

With slight modification of our arguments, we are also able to prove the following.

Corollary 5.5 *Let $E/\mathbb{Q}$ have* CM *by $\mathfrak{O}_K$. Let $\vartheta(p)$ be a function of p such that $\vartheta(p) \to 0$ as $p \to \infty$. Then for all but $o(x/\log x)$ of primes $p \leq x$,*

$$P(N_p) > p^{\vartheta(p)}.$$

Next let Γ be a free subgroup of rank r of the group of rational points $E(\mathbb{Q})$ and let Γ_p be the reduction of Γ mod p. Lang and Trotter [LT] conjectured that the density of primes p for which $\Gamma_p = E_p(\mathbb{F}_p)$ always exists. This conjecture can be considered as an elliptic generalization of the celebrated Artin's primitive root conjecture. So it would be interesting to know how the size of Γ_p grows as $p \to \infty$. In [AM] it is proved that if E has CM by $\mathfrak{O}_K$ then for all but $o(x/\log x)$ of primes $p \leq x$,

$$|\Gamma_p| \geq p^{\frac{r}{r+2}+\epsilon(p)},$$

where $\epsilon(p)$ is any function of p such that $\epsilon(p) \to 0$ as $p \to \infty$.

Here as a consequence of Corollary 5.3 (Theorem 5.2), we prove the following.

Theorem 6.3 *Let $E/\mathbb{Q}$ have* CM *by $\mathfrak{O}_K$. Let $r \geq 2$, and $\epsilon > 0$. Then for a positive proportion of primes $p \leq x$,*

$$|\Gamma_p| > p^{\vartheta_0-\epsilon}.$$

We point out that the above theorem is non-trivial if $r = 2$ or 3 (see Lemma 6.1).

The structure of the paper is as follows. In Section 2 we review some basic facts regarding algebraic number fields and elliptic curves. Section 3 summarizes some important features of the extension $K \subset K(E[\mathfrak{a}])$. In Sections 4 and 5, we prove Theorems 5.2 and 5.4. Section 6 gives the proof of Theorem 6.3.

Notation and Terminology We use p and ℓ to denote rational primes. We write $(\sqrt{x}+1)^2$ as x^+. K and L are number fields. A prime ℓ is called an inert (resp. a split, a ramified) prime in an imaginary quadratic field K if ℓ remains prime (resp. splits completely, ramifies) in K. A prime is called non-inert if it either splits or ramifies. In the sums involving primes of special types (for example ordinary, split, inert, etc.), we write the type of the prime in the index of the sum. For example,

$$\sum_{\substack{p \\ \text{ordinary}}} \sum_{\substack{\ell \\ \text{split}}}$$

is a sum over ordinary primes p and split primes ℓ.

2 Preliminaries

The standard references for this introductory section are [N], [S1], and [S2].

Let K be a number field of degree $n = r_1 + 2r_2$ with r_1 real embeddings and $2r_2$ complex embeddings. Let $\mathfrak{O}_K$ be its ring of integers. For an ideal $\mathfrak{q}$ in $\mathfrak{O}_K$ and integers α and $\beta \in \mathfrak{O}_K$ we write $\alpha \equiv \beta \pmod{\mathfrak{q}}$ if $\alpha - \beta \in \mathfrak{q}$. This equivalence relation defines $N\mathfrak{q}$ residue classes mod $\mathfrak{q}$. $N\mathfrak{q}$ is called the

norm of $\mathfrak{q}$. The residue classes relatively prime to $\mathfrak{q}$ forms a group under multiplication. We denote the order of this group by $\varphi(\mathfrak{q})$, which is the number field analogue of the Euler function. We have

$$\varphi(\mathfrak{q}) = N\mathfrak{q} \prod_{\mathfrak{p}|\mathfrak{q}} \left(1 - \frac{1}{N\mathfrak{p}}\right).$$

If all real conjugates of an algebraic number α (if any) are positive, we write $\alpha \succ 0$. We say that $\alpha \equiv \beta \pmod^* \mathfrak{q}$ if $\alpha \equiv \beta \pmod{\mathfrak{q}}$, $\alpha \succ 0$, and $\beta \succ 0$. We denote by $T(\mathfrak{q})$ the number of residue classes $(\mathrm{mod}^*\ \mathfrak{q})$ that contain a unit. If K is an imaginary quadratic field we have $T(\mathfrak{q}) \leq w_K$, where w_K is the number of roots of unity in K. It is known that $w_K = 2$, 4, or 6.

We define an equivalence relation on the set of ideals of $\mathfrak{O}_K$ as follows. We say two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent, written $\mathfrak{a} \sim \mathfrak{b}$, if there exists $\alpha, \beta \in \mathfrak{O}_K$ such that $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$, where (α) (resp. (β)) denotes the ideal generated by α (resp. β). This relation gives us h equivalence classes, where h is called the class number of K (or $\mathfrak{O}_K$). We also say that two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent $\mathrm{mod}^*\ \mathfrak{q}$, denoted $\mathfrak{a} \sim \mathfrak{b} \pmod^* \mathfrak{q}$, if they are relatively prime to $\mathfrak{q}$ and there exists $\alpha, \beta \in \mathfrak{O}_K$, such that $\alpha \equiv \beta \equiv 1 \pmod^* \mathfrak{q}$, and $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$. Again this is an equivalence relation and we have $h(\mathfrak{q})$ classes where

$$h(\mathfrak{q}) = \frac{h2^{r_1}\varphi(\mathfrak{q})}{T(\mathfrak{q})}.$$

For $(\mathfrak{a}, \mathfrak{q}) = 1$, let

$$\pi_K(x; \mathfrak{q}, \mathfrak{a}) = \#\{\mathfrak{p} :\ \text{prime ideal};\ N\mathfrak{p} \leq x,\ \text{and}\ \mathfrak{p} \sim \mathfrak{a} \pmod^* \mathfrak{q}\}.$$

Finding good estimations for $\pi_K(x; \mathfrak{q}, \mathfrak{a})$ has fundamental importance in the analytic theory of number fields. Here we mention two important estimations of $\pi_K(x; \mathfrak{q}, \mathfrak{a})$. The first one can be considered as a Brun-Titchmarsh type inequality for number fields.

Theorem 2.1 (Hinz and Lodemann) *If $1 \leq N\mathfrak{q} < x$, then*

$$\pi_K(x; \mathfrak{q}, \mathfrak{a}) \leq 2\, \frac{x}{h(\mathfrak{q}) \log \frac{x}{N\mathfrak{q}}} \left\{1 + O\left(\frac{\log\log 3\frac{x}{N\mathfrak{q}}}{\log \frac{x}{N\mathfrak{q}}}\right)\right\},$$

where the O-constant depends only on K.

Proof See [HL], Theorem 4. □

The following is an extension of the Bombieri-Vinogradov theorem to K.

Theorem 2.2 (Huxley) *For each positive constant A, there is a positive constant $B = B(A)$ such that*

$$\sum_{N\mathfrak{q} \leq Q} \max_{(\mathfrak{a},\mathfrak{q})=1} \frac{1}{T(\mathfrak{q})} \left|\pi_K(x; \mathfrak{q}, \mathfrak{a}) - \frac{\mathrm{li}(x)}{h(\mathfrak{q})}\right| \ll \frac{x}{\log^A x},$$

where $Q = x^{\frac{1}{2}}(\log x)^{-B}$. The implied constant depends only on A and on the field K. Here $\mathrm{li}(x) = \int_2^x \frac{dy}{\log y}$, and $x \geq 2$.

Proof See [H], Theorem 1. □

Let E be an elliptic curve defined over $\mathbb{Q}$. This means that E is a non-singular curve defined by an equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with a_1, a_2, a_3, a_4, $a_6 \in \mathbb{Z}$ together with a point at infinity $\mathcal{O}$ given in projective coordinates by $[0, 1, 0]$. The discriminant Δ of E is a polynomial in the a_i which is non-zero if and only if E is non-singular. Let $E(\mathbb{Q})$ be the set of rational points on E together with $\mathcal{O}$. One can show that $E(\mathbb{Q})$ with an appropriate addition law has a group structure.

Let $\mathrm{End}_{\overline{\mathbb{Q}}}E$ be the ring of endomorphisms of E defined over $\overline{\mathbb{Q}}$ (the algebraic closure of $\mathbb{Q}$). It is known that $\mathrm{End}_{\overline{\mathbb{Q}}}E$ is either $\mathbb{Z}$ or is an order in an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$. If $\mathrm{End}_{\overline{\mathbb{Q}}}E \neq \mathbb{Z}$, then E is said to have CM (i.e. complex multiplication by an order in an imaginary quadratic field K). The class number of an order R in K is defined as the cardinality of the group of projective modules of rank 1 over R. One can show that in the case $R = \mathfrak{O}_K$, this definition of class number coincides with the definition in terms of ideal classes. It is known that if E has CM, then its corresponding order has class number 1, and so it is one of the thirteen rings, $\mathbb{Z}[\sqrt{-d}]$ ($d = 1, 2, 3, 7$), $\mathbb{Z}[\frac{1+\sqrt{-d}}{2}]$ ($d = 3, 7, 11, 19, 43, 67, 163$), $\mathbb{Z}[2\sqrt{-1}]$, $\mathbb{Z}[\frac{1+3\sqrt{-3}}{2}]$. Up to isomorphism over $\overline{\mathbb{Q}}$, there are exactly thirteen elliptic curves with CM. Each class is determined by the so-called j-invariant and contains infinitely many curves. For example, all the curves $y^2 = x^3 + Dx$ have $j = 1728$.

Next we assume that E is given by an equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, $a_i \in \mathbb{Z}$, such that the valuation of the discriminant Δ of this equation is minimal in the set of valuations of all equations for E with coefficients in $\mathbb{Z}$. We call such an equation a minimal Weierstrass equation. Then the reduction E_p of E modulo prime p is defined by

$$y^2 + \bar{a}_1xy + \bar{a}_3y = x^3 + \bar{a}_2x^2 + \bar{a}_4x + \bar{a}_6$$

where $\bar{a}_i \in \mathbb{F}_p$ is the reduction of a, b mod p. If E_p is an elliptic curve over $\mathbb{F}_p$ (i.e. E_p is non-singular), we say that E has good reduction at p, and we call p a good prime. p is a good prime if and only if $(p, \Delta) = 1$. If E has good reduction at p, then $E_p(\mathbb{F}_p)$ forms a group, we let $N_p = \#E_p(\mathbb{F}_p)$. We have the following important estimation for N_p.

Hasse's bound: $p + 1 - 2\sqrt{p} \leq N_p \leq p + 1 + 2\sqrt{p}$.

So if $p \leq x$, then $N_p \leq x^+$.

A point $Q \in E_p(\overline{\mathbb{F}_p})$ is called a p-division point, if $pQ = \mathcal{O}$. We denote the set of all p-division points of E_p by $E_p[p]$. A good prime p is called supersingular if $\#E_p[p] = 1$, and it is called ordinary if $\#E_p[p] = p$. One can show that, for $p \geq 5$, a good prime p is supersingular if and only if $N_p = p+1$.

As part of Deuring's results regarding CM curves, we have the following theorem which gives a complete characterization of supersingular primes and ordinary primes for a CM elliptic curve.

Theorem 2.3 *Let E be an elliptic curve defined over $\mathbb{Q}$ with good reduction at p. Suppose that E has* CM *by an order in an imaginary quadratic field K. Then p is supersingular if and only if p has only one prime of K above it (i.e p ramifies or p is inert in K).*

Proof See [L], p. 182, Theorem 12. □

So we have

$$p \text{ is ordinary } \iff (p, \Delta) = 1,\ (p) = \mathfrak{p}_1\mathfrak{p}_2 \text{ in } K\ \ (\mathfrak{p}_1 \neq \mathfrak{p}_2) \iff (p, \Delta) = 1,\ p \text{ splits completely in } K.$$

From this observation and the Chebotarev density theorem we have

$$\#\{p \leq x,\ p \text{ ordinary}\} \sim \frac{1}{2}\ \frac{x}{\log x}, \tag{1}$$

as $x \to \infty$. This is in contrast with the non-CM case, where one can prove that

$$\#\{p \leq x,\ p \text{ ordinary}\} \sim \frac{x}{\log x},$$

as $x \to \infty$. Another striking difference between the CM and non-CM cases is the following. In general, we know that the reduction map

$$r_p : \mathrm{End}_{\overline{\mathbb{Q}}}(E) \otimes_{\mathbb{Z}} \mathbb{Q} \to \mathrm{End}_{\overline{\mathbb{F}}_p}(E_p) \otimes_{\mathbb{Z}} \mathbb{Q}$$

is injective. Also if p is an ordinary prime then $\mathrm{End}_{\overline{\mathbb{F}}_p}(E_p) \otimes_{\mathbb{Z}} \mathbb{Q}$ is an imaginary quadratic field. So if E has CM by an order in an imaginary quadratic field K, the above injection implies that $\mathrm{End}_{\overline{\mathbb{F}}_p}(E_p) \otimes_{\mathbb{Z}} \mathbb{Q} = K$. On the other hand the p-th power Frobenius morphism $(x, y) \to (x^p, y^p)$ is an endomorphism of E_p that can be identified with an imaginary quadratic number π_p. So

$$\mathbb{Q}(\pi_p) \subseteq \mathrm{End}_{\overline{\mathbb{F}}_p}(E_p) \otimes_{\mathbb{Z}} \mathbb{Q} = K,$$

which implies $K = \mathbb{Q}(\pi_p)$. In summary, in the CM case, for any ordinary prime p there is a unique choice of an element $\pi_p \in \mathfrak{O}_K$ such that π_p represents the p-power Frobenius morphism, $p = \pi_p \bar{\pi}_p$, (π_p) is a prime ideal of $\mathfrak{O}_K$, and $K = \mathbb{Q}(\pi_p)$. Moreover in this case $N_p = N(\pi_p - 1) = p + 1 - (\pi_p + \bar{\pi}_p)$, where $N(\pi_p - 1)$ denote the norm of the ideal $(\pi_p - 1)$.

The next statement plays an important role in the study of the ordinary primes p whose N_p is divisible by a fixed prime power.

Lemma 2.4 *Let $E/\mathbb{Q}$ have* CM *by $\mathfrak{O}_K$. Let p be a prime of ordinary reduction for E. Then we have the following.*

1. *Assume that ℓ is inert in K (i.e. (ℓ) is a prime ideal of $\mathfrak{O}_K$ with $N(\ell) = \ell^2$). We have*

(i) If k is odd,

$$\ell^k \mid N_p \iff \pi_p \equiv 1 \pmod{(\ell)^{\frac{k+1}{2}}}.$$

(ii) If k is even,

$$\ell^k \mid N_p \iff \pi_p \equiv 1 \pmod{(\ell)^{\frac{k}{2}}}.$$

2. *Assume that ℓ splits completely in K (i.e. $(\ell) = \mathfrak{l}_1\mathfrak{l}_2$, $\mathfrak{l}_1 \neq \mathfrak{l}_2$, and $N\mathfrak{l}_1 = N\mathfrak{l}_2 = \ell$). Then*

$$\ell^k \mid N_p \iff \pi_p \equiv 1 \pmod{\mathfrak{l}_1^i \mathfrak{l}_2^{k-i}},\ \textit{for some } 0 \leq i \leq k.$$

3. *Assume that ℓ ramifies in K (i.e. $(\ell) = \mathfrak{l}^2$ and $N\mathfrak{l} = \ell$). Then*

$$\ell^k \mid N_p \iff \pi_p \equiv 1 \pmod{\mathfrak{l}^k}.$$

Proof See [C], Lemma 14. □

Definition *For prime ℓ and integer $k \geq 1$, we define*

$$N^*(\ell)^k = \begin{cases} \ell^{k+1} & \text{if } \ell \textit{ is inert in } K, \textit{ and } k \textit{ is odd} \\ \ell^k & \textit{otherwise} \end{cases}.$$

We end this section by giving two estimations for

$$\pi_E^{\mathrm{o}}(x; \ell^k) = \sum_{\substack{p \leq x,\ p \text{ ordinary} \\ \ell^k | N_p}} 1,$$

which counts the number of ordinary primes $p \leq x$ whose N_p is divisible by a fixed prime power.

Proposition 2.5 *Let $E/\mathbb{Q}$ have* CM *by $\mathfrak{O}_K$. Let ℓ be prime, $k \geq 1$ and $1 \leq N^*(\ell)^k \leq \frac{x}{\log x}$. Then*

$$\pi_E^{\mathrm{o}}(x; \ell^k) \ll_K \frac{x}{\psi(\ell^k) \log \frac{x}{N^*(\ell)^k}},$$

where

$$\psi(\ell^k) = \begin{cases} \ell^{k+1} - \ell^{k-1} & \textit{if} \quad \ell \textit{ is inert in } K, \textit{ and } k \textit{ is odd}, \\ \ell^k - \ell^{k-2} & \textit{if} \quad \ell \textit{ is inert in } K, \textit{ and } k \textit{ is even}, \\ \frac{\ell^k - \ell^{k-1}}{k+1} & \textit{if} \quad \ell \textit{ splits in } K, \\ \ell^k - \ell^{k-1} & \textit{if} \quad \ell \textit{ ramifies in } K. \end{cases}$$

The implied constant depends only on K.

Proof We prove this in the case that ℓ is inert in K, and k is odd. The proof in the other cases is similar. From Lemma 2.4, and Theorem 2.1 we have

$$\begin{aligned} \pi_E^{\mathrm{o}}(x; \ell^k) &\leq \pi_K(x; (\ell)^{\frac{k+1}{2}}, (1)) \\ &\leq 2T((\ell)^{\frac{k+1}{2}}) \frac{x}{\varphi((\ell)^{\frac{k+1}{2}}) \log \frac{x}{N(\ell)^{\frac{k+1}{2}}}} \left\{ 1 + O\left(\frac{\log\log 3\frac{x}{N(\ell)^{\frac{k+1}{2}}}}{\log \frac{x}{N(\ell)^{\frac{k+1}{2}}}} \right) \right\}. \end{aligned}$$

The result follows, since $T((\ell)^{\frac{k+1}{2}}) \leq 6$ and $N^*(\ell)^k \leq \frac{x}{\log x}$. □

Proposition 2.6 *Let $E/\mathbb{Q}$ have* CM *by $\mathfrak{O}_K$. Let ℓ be prime, $k \geq 1$, and $1 \leq N^*(\ell)^k \leq x^+$. Then*

$$\pi_E^{\mathrm{o}}(x; \ell^k) \ll_K \delta(\ell^k) \frac{x}{N^*(\ell)^k},$$

where $\delta(\ell^k) = k+1$ if ℓ splits in K, and $\delta(\ell^k) = 1$ otherwise. The implied constant depends only on K.

Proof We first prove that if K is an imaginary quadratic field of class number 1, then

$$\pi_K(x; \mathfrak{q}, (1)) \ll_K \frac{x}{N\mathfrak{q}}.$$

This is true since

$$\begin{aligned} \pi_K(x; \mathfrak{q}, (1)) &\leq \#\{\omega \in \mathfrak{O}_K;\ N(\omega) \leq x,\ \omega \equiv 1 \pmod{\mathfrak{q}}\} \\ &\leq \#\{\gamma \in \mathfrak{O}_K;\ N(\gamma) \leq \frac{x^+}{N\mathfrak{q}}\} \\ &\ll_K \frac{x}{N\mathfrak{q}}. \end{aligned}$$

The result follows from this observation and Lemma 2.4. We prove this for the case that ℓ splits in K. Proof of the other cases are similar.

If ℓ splits, from part (ii) of Lemma 2.4 we have

$$\begin{aligned}\pi_E^{\mathrm{o}}(x;\ell^k) &\leq \sum_{i=0}^{k}\pi_K(x;\mathfrak{l}_1^i\mathfrak{l}_2^{k-i},(1))\\ &\ll_K (k+1)\frac{x}{\ell^k}.\end{aligned}$$

□

Finally we can also consider

$$\pi_E^{\mathrm{s}}(x;\ell^k)=\sum_{\substack{p\leq x,\ p\ \text{supersingular}\\ \ell^k\mid N_p}} 1.$$

In this case, since for $p\geq 5$, $N_p=p+1$, the problem of finding upper bounds for $\pi_E^{\mathrm{s}}(x;\ell^k)$ basically reduces to the classical estimations for $\pi(x;\ell^k,-1)=\#\{p\leq x;\ p\equiv -1\pmod{\ell^k}\}$. Also the problem of finding lower bounds for $P(N_p)$ for supersingular p's is essentially the same as the classical problem of finding lower bounds for $P(p+1)$. From now on we only consider the case of ordinary primes. By employing Bombieri-Vinogradov theorem over $\mathbb{Q}$ and the classical Brun-Titchmarsh inequality, one can easily write the analogous arguments for supersingular primes.

3 The field of $\mathfrak{a}$-division points

We first review some facts from class field theory. Let $K\subset L$ be a finite Abelian extension of number fields. Let $\mathfrak{p}$ be an unramified prime of K in this extension, and $\mathfrak{P}$ be a prime above $\mathfrak{p}$. The Artin symbol

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

is the unique element of $\mathrm{Gal}(L/K)$ which maps to the generator of the Galois group of $\mathfrak{O}_L/\mathfrak{P}$ over $\mathfrak{O}_K/\mathfrak{p}$. This generator is the Frobenius automorphism $x\to x^{N_{\mathbb{Q}}^K\mathfrak{p}}$. Let $\mathfrak{m}$ be an ideal of K which contains all the ramified primes in the extension L/K. For prime $(\mathfrak{p},\mathfrak{m})=1$, we define

$$\Phi_{\{L/K,\ \mathfrak{m}\}}(\mathfrak{p})=\left(\frac{L/K}{\mathfrak{p}}\right).$$

This map extended over all (fractional) ideals of K relatively prime to $\mathfrak{m}$ is called the Artin map for L/K and $\mathfrak{m}$. Let

$$P(\mathfrak{m})=\{(\alpha):\ \alpha\in K^{\times},\ \alpha\equiv 1\ (\mathrm{mod}^*\ \mathfrak{m})\}$$

be the group of principal ideals of K congruent to 1 modulo $\mathfrak{m}$. We define the ray class field $K_{\mathfrak{m}}$ associated to $\mathfrak{m}$ as the Abelian extension $K_{\mathfrak{m}}$ of K such that

$$\mathrm{Ker}\ \Phi_{\{K_{\mathfrak{m}}/K,\ \mathfrak{m}\}}=P(\mathfrak{m}).$$

From class field theory we know that, for any $\mathfrak{m}$, $K_{\mathfrak{m}}$ exists and is unique. Moreover $K_{\mathfrak{m}}$ is characterized by the property that it is an Abelian extension of K and satisfies

$$\{\text{primes of } K \text{ that split completely in } K_{\mathfrak{m}}\}=\{\text{prime ideals in } P(\mathfrak{m})\}$$

(see [S2], Page 117, Theorem 3.2).

From now on K is an imaginary quadratic number field, and we assume that E has CM with the whole ring of integers $\mathfrak{O}_K$. We use the above information to study the field generated by the $\mathfrak{a}$-division points of a CM elliptic curve E defined over K. Also we fix an isomorphism $[\ ] : \mathfrak{O}_K \to \mathrm{End}_{\overline{\mathbb{Q}}}(E)$. For an ideal $\mathfrak{a}$ of K, we define

$$E[\mathfrak{a}] = \{P \in E : \ [\alpha]P = \mathcal{O} \text{ for all } \alpha \in \mathfrak{a}\}.$$

We call $E[\mathfrak{a}]$ the group of $\mathfrak{a}$-division points of E. If $\mathfrak{a} = (\alpha)$ then

$$E[\mathfrak{a}] = E[(\alpha)] = \mathrm{Ker}\ [\alpha].$$

It is clear that $E[(\alpha)]$ is independent of the choice of the generator of (α).

Let $K(E[\mathfrak{a}])$ be the field obtained by adjoining all the $\mathfrak{a}$-division points of E to K. Let $\mathfrak{f}$ be an ideal of K divisible by all primes of bad reduction of E over K. We are interested in studying the extension $K(E[\mathfrak{a}])/K$. First of all we know that this extension is Abelian ([R], Page 182, Corollary 5.5). Secondly if $\mathfrak{p}$ is a prime ideal of K with $(\mathfrak{p}, \mathfrak{f}\mathfrak{a}) = 1$, then $\mathfrak{p}$ is unramified in this extension ([S1], Page 184, Theorem 7.1).

The next statement describes the action of the Artin symbol of the extension $K(E[\mathfrak{a}])/K$ on the $\mathfrak{a}$-division points of E.

Lemma 3.1 *Let E/K have CM by $\mathfrak{O}_K$. Then there is a Hecke character (character of a generalized ideal class group of K) $\chi_{E/K}$ of conductor $\mathfrak{f}$ such that for a prime $\mathfrak{p}$ of K where $(\mathfrak{p}, \mathfrak{f}\mathfrak{a}) = 1$, the Artin symbol $\left(\frac{K(E[\mathfrak{a}])/K}{\mathfrak{p}}\right)$ acts on $E[\mathfrak{a}]$ by multiplication by $\chi_{E/K}(\mathfrak{p})$.*

Proof See [R], Page 186, Corollary 5.16 (ii). □

The next lemma can be considered as an analogue of the Kronecker-Weber theorem for the Abelian extension $K \subset K(E[\mathfrak{a}])$.

Lemma 3.2 *Let E/K have CM by $\mathfrak{O}_K$. For an ideal $\mathfrak{a}$ of K there is an ideal $\mathfrak{f}$ of K such that*

$$K(E[\mathfrak{a}]) \subseteq K_{\mathfrak{f}\mathfrak{a}},$$

where $K_{\mathfrak{f}\mathfrak{a}}$ is the ray class field associated to $\mathfrak{f}\mathfrak{a}$.

Proof We know that $K(E[\mathfrak{a}])$ is a finite Abelian extension of K whose ramified primes are among the prime divisors of $\mathfrak{f}\mathfrak{a}$. To prove the assertion we only need to prove that

$$\mathrm{Ker}\ \Phi_{\{K_{\mathfrak{f}\mathfrak{a}}/K,\ \mathfrak{f}\mathfrak{a}\}} \subseteq \mathrm{Ker}\ \Phi_{\{K(E[\mathfrak{a}])/K,\ \mathfrak{f}\mathfrak{a}\}} \tag{2}$$

(see [Co], Corollary 8.7). Now let $\mathfrak{p}$ be a prime of K in the kernel of the Artin map $\Phi_{\{K_{\mathfrak{f}\mathfrak{a}}/K,\ \mathfrak{f}\mathfrak{a}\}}$, and so $\left(\frac{K_{\mathfrak{f}\mathfrak{a}}/K}{\mathfrak{p}}\right) = 1$. More specifically this means that $\mathfrak{p}$ has a generator α such that $\alpha \equiv 1 \pmod{\mathfrak{f}\mathfrak{a}}$. So $\mathfrak{p}$ is unramified in $K(E[\mathfrak{a}])$ and by the previous lemma for a point $P \in E[\mathfrak{a}]$, we have

$$\left(\frac{K(E[\mathfrak{a}])/K}{\mathfrak{p}}\right) P = \chi_{E/K}(\mathfrak{p})P = \chi_{E/K}((\alpha))P = P.$$

Here we used the fact that any $\alpha \equiv 1 \pmod{\mathfrak{f}}$ is in the kernel of χ (see [N], Proposition 7.6 (ii)). So the kernel of the Artin map $\mathfrak{p} \mapsto \left(\frac{K_{\mathfrak{f}\mathfrak{a}}/K}{\mathfrak{p}}\right)$ is a subset of the kernel of the Artin map $\mathfrak{p} \mapsto \left(\frac{K(E[\mathfrak{a}])/K}{\mathfrak{p}}\right)$. This implies the result. □

Lemma 3.3 *Let E/K have CM by $\mathfrak{O}_K$, and $\mathfrak{p}$ be a prime ideal of K with $(\mathfrak{p}, \mathfrak{f}\mathfrak{a}) = 1$. Then, for some t, there are t ideal classes mod $\mathfrak{f}\mathfrak{a}$ represented by $\mathfrak{a}_1, \cdots, \mathfrak{a}_t$ such that*

$$\mathfrak{p} \text{ splits completely in } K(E[\mathfrak{a}]) \iff \mathfrak{p} \sim \mathfrak{a}_1, \text{ or } \mathfrak{a}_2, \text{ or } \cdots, \text{ or } \mathfrak{a}_t \pmod{\mathfrak{f}\mathfrak{a}}.$$

Moreover

$$t\,[K(E[\mathfrak{a}]) : K] = h(\mathfrak{f}\mathfrak{a}),$$

and if $(\mathfrak{a}, 6\mathfrak{f}) = 1$

$$t = \frac{h(\mathfrak{f}\mathfrak{a})}{\varphi(\mathfrak{a})} \leq h\varphi(\mathfrak{f}).$$

Proof Since the primes that split completely are in the kernel of the Artin map, the first assertion is clear from (2). Next let

$$\phi(x; K(E[\mathfrak{a}])/K) = \#\{\mathfrak{p} : \text{ prime ideal of } K;\ N\mathfrak{p} \leq x,\ (\mathfrak{p}, \mathfrak{f}\mathfrak{a}) = 1, \text{ and } \left(\frac{K(E[\mathfrak{a}])/K}{\mathfrak{p}}\right) = 1\}.$$

Then we have

$$\phi(x; K(E[\mathfrak{a}])/K) = \sum_{i=1}^{t} \pi_K(x; \mathfrak{f}\mathfrak{a}, \mathfrak{a}_i).$$

Now the second statement follows by employing the Chebotarev density theorem, the prime ideal theorem, and comparing the main terms of the two sides of the above identity. Finally the last assertion is true since by [R], Page 187, Corollary 5.20 (ii), we have $[K(E[\mathfrak{a}]) : K] = \varphi(\mathfrak{a})$ if $(\mathfrak{a}, 6\mathfrak{f}) = 1$. □

Lemma 3.4 *Let $E/\mathbb{Q}$ have CM by $\mathfrak{O}_K$, and $p = \pi_p\bar{\pi}_p$ be an ordinary prime. Let $\mathfrak{l} = (\lambda)$ be a degree 1 prime of K such that $(p, \mathfrak{l}) = 1$. Then*

$$\pi_p \equiv 1 \pmod{\mathfrak{l}} \iff (\pi_p) \textit{ splits completely in } K(E[\mathfrak{l}]).$$

Proof From [S1], Page 181, Proposition 5.4 (b) and [S2], Page 168, Theorem 9.2 (b) follows that E does not have good reduction over K at primes dividing $\mathfrak{f}$ and prime divisors of $\mathfrak{f} \mid \Delta$. Now since $(p, \Delta\mathfrak{l}) = 1$, then (π_p) is unramified in $K(E[\mathfrak{l}])$. Thus (π_p) splits completely in $K(E[\mathfrak{l}])$ if and only if the Artin symbol $\left(\frac{K(E[\mathfrak{l}])/K}{(\pi_p)}\right) = 1$. This means that the endomorphism $[\pi_p]$ corresponding to the p-power Frobenius morphism $(x, y) \to (x^p, y^p)$ acts trivially on $E[\mathfrak{l}]$. So $[\pi_p]P = P$ for all $P \in E[\mathfrak{l}]$. Thus (π_p) splits completely in $K(E[\mathfrak{l}])$ if and only if $\mathrm{Ker}\,[\lambda] \subseteq \mathrm{Ker}\,[\pi_p - 1]$. This is true if and only if there is an endomorphism ϕ of E such that $[\pi_p - 1] = \phi o[\lambda]$ (see [S1], Page 77, Corollary 4.11). The proof is complete. □

The following corollaries are direct consequences of the previous lemma and Lemma 2.4.

Corollary 3.5 *Suppose that the prime ℓ splits completely in K (i.e. $(\ell) = \mathfrak{l}\bar{\mathfrak{l}}$, $\mathfrak{l} \neq \bar{\mathfrak{l}}$), p is an ordinary prime, and $p \neq \ell$. Then*

$$\ell \mid N_p \iff (\pi_p) \textit{ splits completely in } K(E[\mathfrak{l}]) \textit{ or } (\pi_p) \textit{ splits completely in } K(E[\bar{\mathfrak{l}}]).$$

Corollary 3.6 *If a prime ℓ splits completely in K then we have*

$$\pi_E^{\circ}(x; \ell) = \frac{1}{2}\left(\sum_{\substack{\mathfrak{l} \\ N\mathfrak{l}=\ell}} \sum_{\substack{N(\mathfrak{p}) \leq x,\ (\mathfrak{p}, \mathfrak{f}\mathfrak{l})=1 \\ \mathfrak{p} \text{ degree } 1 \\ \mathfrak{p} \text{ splits completely in } K(E[\mathfrak{l}])}} 1 - \sum_{\substack{N(\mathfrak{p}) \leq x,\ (\mathfrak{p}, \mathfrak{f}(\ell))=1 \\ \mathfrak{p} \text{ degree } 1 \\ \mathfrak{p} \text{ splits completely in } K(E[(\ell)])}} 1\right) + O(1).$$

4 Lemmas

This section describes lemmas that will be used in the proof of Theorem 5.2. We assume that $E/\mathbb{Q}$ has CM by $\mathfrak{O}_K$. First of all observe that by interchanging the order of addition, we have

$$\sum_{\substack{p\le x\\ p \text{ ordinary}}}\sum_{\ell\mid N_p}\log\ell=\sum_{\ell\le x^+}(\log\ell)\pi_E^{\mathrm{o}}(x;\ell). \tag{3}$$

In our first lemma we evaluate the left-hand side of (3).

Lemma 4.1 *We have*

$$\sum_{\substack{p\le x\\ p \text{ ordinary}}}\sum_{\ell\mid N_p}\log\ell=\frac{x}{2}+O_E\left(\frac{x}{\log x}\right),$$

as $x\to\infty$.

Proof Let $\Lambda(n)$ be the von Mangoldt function. Then from the identity $\sum_{n\mid d}\Lambda(n)=\log d$, (1), and the prime number theorem we have

$$\begin{aligned}
\sum_{\substack{p\le x\\ p \text{ ordinary}}}\sum_{\ell\mid N_p}\log\ell &= \sum_{\substack{p\le x\\ p \text{ ordinary}}}\sum_{n\mid N_p}\Lambda(n)-\sum_{\substack{p\le x\\ p \text{ ordinary}}}\sum_{\substack{\ell^k\mid N_p\\ k\ge 2}}\log\ell\\
&= \sum_{\substack{p\le x\\ p \text{ ordinary}}}\log N_p-\sum_{\substack{p\le x\\ p \text{ ordinary}}}\sum_{\substack{\ell^k\mid N_p\\ k\ge 2}}\log\ell\\
&= \sum_{\substack{p\le x\\ p \text{ ordinary}}}\log p+\sum_{\substack{p\le x\\ p \text{ ordinary}}}\log\left(1+\frac{1-a_p}{p}\right)-\sum_{k\ge 2}\sum_{\ell^k\mid N_p}(\log\ell)\pi_E^{\mathrm{o}}(x;\ell^k)\\
&= \frac{x}{2}+O\left(\frac{x}{\log x}\right)+(\mathrm{I})+(\mathrm{II}),
\end{aligned} \tag{4}$$

where $a_p=p+1-N_p$. By applying Hasse's bound ($|a_p|\le 2\sqrt{p}$) we have

$$\begin{aligned}
(\mathrm{I}) &= \sum_{\substack{p\le 5\\ p \text{ ordinary}}}\log\left(1+\frac{1-a_p}{p}\right)+\sum_{\substack{5<p\le x\\ p \text{ ordinary}}}\log\left(1-\frac{a_p-1}{p}\right)\\
&\ll \sum_{\substack{p\le x\\ p \text{ ordinary}}}\frac{|a_p-1|}{p}\ll x^{1/2}.
\end{aligned}$$

Here we used the fact that

$$-\log(1-z)=\sum_{k=1}^{\infty}\frac{z^k}{k},$$

for $|z|<1$, and $\frac{|a_p-1|}{p}\le\frac{2\sqrt{p}+1}{p}<1$ for $p>5$.

To evaluate (II), we note that for inert ℓ and odd k if $\ell^k\mid N_p$ then $\ell^{k+1}\mid N_p$. This is true since $N_p=(\pi_p-1)(\bar{\pi}_p-1)$, so the multiplicity of ℓ in N_p is even. Therefore we have

$$\begin{aligned}(\mathrm{II}) &\le \sum_{k\ge 2}\sum_{\substack{\ell\le (x^+)^{\frac{1}{k}}\\ \ell \text{ non}-\text{inert}}}(\log\ell)\pi_E^{\mathrm{o}}(x;\ell^k)+\sum_{\substack{k\ge 2\\ k \text{ even}}}\sum_{\substack{\ell\le (x^+)^{\frac{1}{k}}\\ \ell \text{ inert}}}(\log\ell)\pi_E^{\mathrm{o}}(x;\ell^k)\\ &\quad+\sum_{\substack{k\ge 2\\ k \text{ odd}}}\sum_{\substack{\ell\le (x^+)^{\frac{1}{k+1}}\\ \ell \text{ inert}}}(\log\ell)\pi_E^{\mathrm{o}}(x;\ell^k)\\ &= \sum_{\text{non}-\text{inert}}+\sum_{\substack{\text{inert}\\ k \text{ even}}}+\sum_{\substack{\text{inert}\\ k \text{ odd}}}. \end{aligned}\tag{5}$$

Next we employ Propositions 2.5 and 2.6 to estimate these sums. We have

$$\begin{aligned}\sum_{\text{non}-\text{inert}} &= \sum_{k\ge 2}\sum_{\substack{\ell\le x^{\frac{3}{4k}}\\ \ell \text{ non}-\text{inert}}}(\log\ell)\pi_E^{\mathrm{o}}(x;\ell^k)+\sum_{k\ge 2}\sum_{\substack{x^{\frac{3}{4k}}<\ell\le (x^+)^{\frac{1}{k}}\\ \ell \text{ non}-\text{inert}}}(\log\ell)\pi_E^{\mathrm{o}}(x;\ell^k)\\ &\ll \frac{x}{\log x}\sum_{k\ge 2}\sum_{\ell\le x^{\frac{3}{4k}}}\frac{(k+1)\log\ell}{(\ell^k-\ell^{k-1})}+x^{\frac{1}{4}}\sum_{k\ge 2}\sum_{x^{\frac{3}{4k}}<\ell\le (x^+)^{\frac{1}{k}}}(k+1)\log\ell\\ &\ll \frac{x}{\log x}+x^{\frac{3}{4}}(\log x)^2. \end{aligned}$$

Here, we have used the fact that $k\ll \log x$. Similarly we have

$$\begin{aligned}\sum_{\substack{\text{inert}\\ k \text{ even}}} &= \sum_{\substack{k\ge 2\\ k \text{ even}}}\sum_{\substack{\ell\le x^{\frac{3}{4k}}\\ \ell \text{ inert}}}(\log\ell)\pi_E^{\mathrm{o}}(x;\ell^k)+\sum_{\substack{k\ge 2\\ k \text{ even}}}\sum_{\substack{x^{\frac{3}{4k}}<l\le (x^+)^{\frac{1}{k}}\\ \ell \text{ inert}}}(\log\ell)\pi_E^{\mathrm{o}}(x;\ell^k)\\ &\ll \frac{x}{\log x}\sum_{k\ge 2}\sum_{l\le x^{\frac{3}{4k}}}\frac{\log\ell}{(\ell^k-\ell^{k-2})}+x^{\frac{1}{4}}\sum_{k\ge 2}\sum_{x^{\frac{3}{4k}}<\ell\le (x^+)^{\frac{1}{k}}}\log\ell\\ &\ll \frac{x}{\log x}+x^{\frac{3}{4}}\log x, \end{aligned}$$

and

$$\begin{aligned}\sum_{\substack{\text{inert}\\ k \text{ odd}}} &= \sum_{\substack{k\ge 2\\ k \text{ odd}}}\sum_{\substack{\ell\le x^{\frac{3}{4(k+1)}}\\ \ell \text{ inert}}}(\log\ell)\pi_E^{\mathrm{o}}(x;\ell^k)+\sum_{\substack{k\ge 2\\ k \text{ odd}}}\sum_{\substack{x^{\frac{3}{4(k+1)}}<\ell\le (x^+)^{\frac{1}{k+1}}\\ \ell \text{ inert}}}(\log\ell)\pi_E^{\mathrm{o}}(x;\ell^k)\\ &\ll \frac{x}{\log x}\sum_{k\ge 3}\sum_{\ell\le x^{\frac{3}{4(k+1)}}}\frac{\log\ell}{(\ell^{k+1}-\ell^{k-1})}+x^{\frac{1}{4}}\sum_{k\ge 3}\sum_{x^{\frac{3}{4(k+1)}}<\ell\le (x^+)^{\frac{1}{k+1}}}\log\ell\\ &\ll \frac{x}{\log x}+x^{\frac{1}{2}}\log x, \end{aligned}$$

Applying the above three estimations in (5) yields

$$(\mathrm{II})\ll \frac{x}{\log x}+x^{\frac{3}{4}}(\log x)^2.$$

Finally replacing the above bounds for (I) and (II) in (4) implies the result. □

In the next two lemmas we consider the right-hand side of (3). We first show that the contribution of the inert primes ℓ to the right-hand side of (3) is negligible.

Lemma 4.2 *We have*

$$\sum_{\substack{\ell\le x^+\\ \ell \text{ inert}}} (\log\ell)\pi_E^{\circ}(x;\ell) = O_K\left(\frac{x}{\log x}\right).$$

Proof A calculation similar to the one used in treating $\sum_{\substack{\text{inert}\\ k \text{ odd}}}$ of (II) in the previous lemma yields

$$\begin{aligned}\sum_{\substack{\ell\le x^+\\ \ell \text{ inert}}} (\log\ell)\pi_E^{\circ}(x;\ell) &= \sum_{\substack{\ell\le x^{\frac{3}{8}}\\ \ell \text{ inert}}} (\log\ell)\pi_E^{\circ}(x;\ell) + \sum_{\substack{x^{\frac{3}{8}}<\ell\le (x^+)^{\frac{1}{2}}\\ \ell \text{ inert}}} (\log\ell)\pi_E^{\circ}(x;\ell)\\ &\ll \frac{x}{\log x}\sum_{\ell\le x^{\frac{3}{8}}}\frac{\log\ell}{(\ell^2-1)} + x^{\frac{1}{4}}\sum_{x^{\frac{3}{8}}<\ell\le (x^+)^{\frac{1}{2}}}\log\ell\\ &\ll \frac{x}{\log x} + x^{\frac{3}{4}}.\end{aligned}$$

□

In the following lemma we deduce an asymptotic formula for the non-inert terms $\ell < x^{\frac{1}{2}}$ in the right-hand side of (3).

Lemma 4.3 *Let $\mathcal{L} = \log x$ and let B be the constant given in Theorem* 2.2 *provided A is chosen ≥ 2. Then for non-inert primes ℓ, we have*

$$\sum_{\substack{\ell\le x^{\frac{1}{2}}\mathcal{L}^{-B}\\ \ell \text{ non}-\text{inert}}} (\log\ell)\pi_E^{\circ}(x;\ell) = \frac{1}{4}x + O_E\left(\frac{x\log\log x}{\log x}\right).$$

Proof First of all without loss of generality we assume that $B > 1$. Secondly by Corollary 3.6 and Lemma 3.3, for split prime ℓ, we have

$$\begin{aligned}\pi_E^{\circ}(x;\ell) &= \frac{1}{2}\left(\sum_{\substack{\mathfrak{l}\\ N\mathfrak{l}=\ell}}\sum_{\substack{N(\mathfrak{p})\le x,\ (\mathfrak{p},\mathfrak{f}\mathfrak{l})=1\\ \mathfrak{p}\text{ degree }1\\ \mathfrak{p}\text{ splits completely in }K(E[\mathfrak{l}])}} 1 - \sum_{\substack{N(\mathfrak{p})\le x,\ (\mathfrak{p},\mathfrak{f}(\ell))=1\\ \mathfrak{p}\text{ degree }1\\ \mathfrak{p}\text{ splits completely in }K(E[(\ell)])}} 1\right) + O(1)\\ &= \frac{1}{2}\left(\sum_{\substack{\mathfrak{l}\\ N\mathfrak{l}=\ell}}\sum_i \pi_K(x;\mathfrak{f}\mathfrak{l},\mathfrak{l}_i) - \sum_i \pi_K(x;\mathfrak{f}(\ell),(\ell)_i)\right) + O\left(\frac{x^{\frac{1}{2}}}{\log x}\right).\end{aligned}$$

(Here we used the fact that the number of inert prime ideals (ω) with $N(\omega)\le x$ in K is bounded by $x^{1/2}/\log x$.)

Let S be the set of rational primes that are ramified in K together with the prime divisors of $6\,N\mathfrak{f}$. Now by applications of the above expression for $\pi_E^{\circ}(x;\ell)$, we have

$$\begin{aligned}\sum_{\substack{\ell\le x^{\frac{1}{2}}\mathcal{L}^{-B}\\ \ell \text{ non}-\text{inert},\ \ell\notin S}} (\log\ell)\pi_E^{\circ}(x;\ell) &= \frac{1}{2}\sum_{\substack{N\mathfrak{l}=\ell\le x^{\frac{1}{2}}\mathcal{L}^{-B}\\ \ell \text{ split},\ell\notin S}} \log N\mathfrak{l}\sum_i \pi_K(x;\mathfrak{f}\mathfrak{l},\mathfrak{l}_i)\\ &\quad -\frac{1}{2}\sum_{\substack{\ell\le x^{\frac{1}{2}}\mathcal{L}^{-B}\\ \ell \text{ split},\ell\notin S}} \log\ell\sum_i \pi_K(x;\mathfrak{f}(\ell),(\ell)_i) + O\left(\frac{x}{\log^B x}\right).\end{aligned}$$

By Lemma 3.3 and Theorem 2.2, the last formula is

$$\begin{aligned}
&= \frac{1}{2} \sum_{\substack{N\mathfrak{l}=\ell\le x^{\frac12}\mathcal{L}^{-B} \\ \ell \text{ split}, \ell\notin S}} \log N\mathfrak{l} \left\{ \frac{\mathrm{li}(x)}{\varphi(\mathfrak{l})} + \left(\sum_i \pi_K(x; \mathfrak{fl}, \mathfrak{l}_i) - \frac{\mathrm{li}(x)}{\varphi(\mathfrak{l})} \right) \right\} \\
&\quad -\frac{1}{2} \sum_{\substack{\ell\le x^{\frac12}\mathcal{L}^{-B} \\ \ell \text{ split}, \ell\notin S}} \log \ell \left\{ \frac{\mathrm{li}(x)}{\varphi((\ell))} + \left(\sum_i \pi_K(x; \mathfrak{f}(\ell), (\ell)_i) - \frac{\mathrm{li}(x)}{\varphi((\ell))} \right) \right\} + O\left(\frac{x}{\log^B x} \right) \\
&= \frac{1}{2} \,.\, 2 \,.\, \mathrm{li}(x) \sum_{\substack{\ell\le x^{\frac12}\mathcal{L}^{-B} \\ \ell \text{ split},\ \ell\notin S}} \frac{\log \ell}{\ell - 1} - \frac{1}{2} \,.\, \mathrm{li}(x) \sum_{\substack{\ell\le x^{\frac12}\mathcal{L}^{-B} \\ \ell \text{ split},\ \ell\notin S}} \frac{\log \ell}{(\ell-1)^2} + O\left(\log x \frac{x}{\log^A x} \right) \\
&= \frac{1}{4} x + O\left(\frac{x \log\log x}{\log x} \right).
\end{aligned}$$

□

We also need the following straightforward estimation in the sequel.

Lemma 4.4 *Let $\frac12 \le \vartheta < 1$. We have*

$$\sum_{\substack{x^{\frac12}\mathcal{L}^{-B} < \ell \le x^{\vartheta} \\ \ell \text{ prime}}} \frac{\log \ell}{\ell \log \frac{x}{\ell}} = -\log\{2(1-\vartheta)\} + O_\vartheta\left(\frac{\log\log x}{\log x} \right).$$

Proof Let $y = x^{\frac12}\mathcal{L}^{-B}$, $z = x^{\vartheta}$, and $f(t) = (t \log \frac{x}{t})^{-1}$. Then by partial summation and the prime number theorem, we have

$$\begin{aligned}
\sum_{\substack{y<\ell\le z \\ \ell \text{ prime}}} \frac{\log \ell}{\ell \log \frac{x}{\ell}} &= \left(\sum_{\ell\le z} \log \ell \right) f(z) - \left(\sum_{\ell\le y} \log \ell \right) f(y) - \int_y^z \left(\sum_{\ell\le t} \log \ell \right) f'(t) dt \\
&= O\left(\frac{1}{\log x} \right) - \int_y^z t f'(t)\, dt + O\left\{ \frac{1}{\log x} \int_y^z t\, |f'(t)|\, dt \right\} \\
&= \int_y^z f(t)\, dt + O\left(\frac{1}{\log x} \right) \\
&= \log\log \frac{x}{y} - \log\log \frac{x}{z} + O\left(\frac{1}{\log x} \right) \\
&= -\log\{2(1-\vartheta)\} + O\left(\frac{\log\log x}{\log x} \right).
\end{aligned}$$

□

5 Proof of Theorems 5.2 and 5.4

We recall that by Lemma 4.1 the left-hand side of (3) is asymptotic to $x/2$ as $x \to \infty$. On the other hand, on the right-hand side of (3), by Lemma 4.2, the contribution of the inert summands is $O(x/\log x)$, and by Lemma 4.3 the sum of the non-inert summands ℓ corresponding to $\ell \le x^{\frac12}\mathcal{L}^{-B}$

are asymptotic to $x/4$. Now we use Theorem 2.1 together with Lemma 4.3 to find an upper bound for the contribution of non-inert summands ℓ to the right-hand side of (3) in the range $x^{\frac{1}{2}}\mathcal{L}^{-B} < \ell \le x^{\vartheta}$, and as a result we get the following.

Proposition 5.1 *Let* $\frac{1}{2} \le \vartheta < 1 - \frac{1}{2}e^{-\frac{1}{4}} = 0.6105\ldots$. *Then*

$$\sum_{\substack{x^{\vartheta} < \ell \le x^{+} \\ \ell \text{ non-inert}}} (\log \ell)\pi_E^{\mathrm{o}}(x;\ell) \ge \log\{2e^{\frac{1}{4}}(1-\vartheta)\}x + O_{E,\vartheta}\left(\frac{x\log\log x}{\log x}\right).$$

Proof First of all by Corollary 3.6 and Lemma 3.3, for split prime ℓ, we have

$$\begin{aligned}
\pi_E^{\mathrm{o}}(x;\ell) &= \frac{1}{2}\left(\sum_{\substack{\mathfrak{l} \\ N\mathfrak{l}=\ell}} \sum_{\substack{N(\mathfrak{p})\le x,\ (\mathfrak{p},\mathfrak{f}\mathfrak{l})=1 \\ \mathfrak{p} \text{ degree } 1 \\ \mathfrak{p} \text{ splits completely in } K(E[\mathfrak{l}])}} 1 - \sum_{\substack{N(\mathfrak{p})\le x,\ (\mathfrak{p},\mathfrak{f}(\ell))=1 \\ \mathfrak{p} \text{ degree } 1 \\ \mathfrak{p} \text{ splits completely in } K(E[(\ell)])}} 1\right) + O(1) \\
&\le \frac{1}{2}\sum_{\substack{\mathfrak{l} \\ N\mathfrak{l}=\ell}} \sum_{i} \pi_K(x;\mathfrak{f}\mathfrak{l},\mathfrak{l}_i) + O(1).
\end{aligned}$$

Let S be as defined in Lemma 4.3. Then by an application of the above inequality, Theorem 2.1, and Lemma 4.4 we have

$$\begin{aligned}
\sum_{\substack{x^{\frac{1}{2}}\mathcal{L}^{-B} < \ell \le x^{\vartheta} \\ \ell \text{ non-inert},\ \ell \notin S}} (\log \ell)\pi_E^{\mathrm{o}}(x;\ell) &\le \frac{1}{2}\sum_{\substack{x^{\frac{1}{2}}\mathcal{L}^{-B} < N\mathfrak{l} = \ell \le x^{\vartheta} \\ \ell \text{ split},\ \ell \notin S}} \log N\mathfrak{l} \sum_i \pi_K(x;\mathfrak{f}\mathfrak{l},\mathfrak{l}_i) + O(x^{\vartheta}\log x) \\
&\le \frac{1}{2}\sum_{\substack{x^{\frac{1}{2}}\mathcal{L}^{-B} < N\mathfrak{l} = \ell \le x^{\vartheta} \\ \ell \text{ split},\ \ell \notin S}} \log N\mathfrak{l}\, \frac{h(\mathfrak{f}\mathfrak{l})}{\varphi(\mathfrak{l})}\, \frac{2x}{h(\mathfrak{f}\mathfrak{l})\log\frac{x}{N\mathfrak{l}}}\left(1 + O\left(\frac{\log\log 3\frac{x}{N\mathfrak{l}}}{\log\frac{x}{N\mathfrak{l}}}\right)\right) \\
&\quad + O(x^{\vartheta}\log x) \\
&= \frac{1}{2}\,.\,2\,.\,x \sum_{\substack{x^{\frac{1}{2}}\mathcal{L}^{-B} < \ell \le x^{\vartheta} \\ \ell \text{ split},\ \ell \notin S}} \frac{2\log\ell}{\varphi(\ell)\log\frac{x}{\ell}} + O\left(\frac{x\log\log x}{(\log x)^2}\sum_{\ell \le x}\frac{\log\ell}{\ell}\right) \\
&= -\log\{2(1-\vartheta)\}x + O\left(\frac{x\log\log x}{\log x}\right),
\end{aligned}$$

as $x \to \infty$.

Finally the assertion of the proposition follows from applications of Lemmas 4.1, 4.2 and 4.3 in (3) and the fact that

$$\sum_{\substack{x^{\frac{1}{2}}\mathcal{L}^{-B} < \ell \le x^{\vartheta} \\ \ell \text{ non-inert}}} (\log \ell)\pi_E^{\mathrm{o}}(x;\ell) \le -\log\{2(1-\vartheta)\}x + O\left(\frac{x\log\log x}{\log x}\right).$$

□

We are ready to prove our first main result.

Theorem 5.2 *Let $E/\mathbb{Q}$ have CM by $\mathfrak{O}_K$, and let $\vartheta < \vartheta_0 = 1 - \frac{1}{2}e^{-\frac{1}{4}} = 0.6105\cdots$. Then there are positive constants $X_0(E,\vartheta)$, and $\eta(\vartheta) < 1/2$ such that for all large $x > X_0(E,\vartheta)$ we have*

$$\#\{p \le x,\ p \text{ ordinary and } P(N_p) > x^{\vartheta}\} > \eta(\vartheta)\frac{x}{\log x}.$$

Proof Without loss of generality we can assume that $\vartheta > \frac{1}{2}$. By the previous proposition we have

$$\begin{aligned}
\#\{p \le x,\ p \text{ ordinary and } P(N_p) > x^{\vartheta}\} &\ge \frac{1}{\log x^+} \sum_{\substack{p \le x \\ p \text{ ordinary}}} \sum_{\substack{\ell \mid N_p \\ \ell > x^{\vartheta}}} \log \ell \\
&= \frac{1}{\log x^+}\left(\sum_{\substack{x^{\vartheta} < \ell \le x^+ \\ \ell \text{ non-inert}}} (\log \ell)\pi_E^{\mathrm{o}}(x;\ell) + O\left(\frac{x}{\log x}\right)\right) \\
&\ge \log\{2e^{\frac{1}{4}}(1-\vartheta)\}\frac{x}{\log x^+} + O\left(\frac{x\log\log x}{\log^2 x}\right).
\end{aligned}$$

□

Corollary 5.3 *Under the assumptions of the previous theorem, for a positive proportion of primes $p \le x$,*

$$P(N_p) > p^{\vartheta}.$$

Proof This is clear from the previous theorem since

$$\#\{p \le x,\ p \text{ ordinary and } P(N_p) > p^{\vartheta}\} \ge \#\{p \le x,\ p \text{ ordinary and } P(N_p) > x^{\vartheta}\}.$$

□

In the above discussion ϑ was a real number, next we consider the case that $\vartheta(x)$ is a function of x. We observe that if $x^{\vartheta(x)} \ll x^{\frac{1}{2}}\mathcal{L}^{-B}$, where B is the constant given in Lemma 4.3, then an argument similar to the one given in the proof of Lemma 4.3 implies that

$$\sum_{\substack{\ell \le x^{\vartheta(x)} \\ \ell \text{ non-inert}}} (\log \ell)\pi_E^{\mathrm{o}}(x;\ell) = \frac{\vartheta(x)}{2}x + O\left(\{1+\vartheta(x)\}\frac{x}{\log x}\right).$$

Now applications of the above identity and Lemmas 4.1 and 4.2 in (3) yields

$$\sum_{\substack{x^{\vartheta(x)} < \ell \le x^+ \\ \ell \text{ non-inert}}} (\log \ell)\pi_E^{\mathrm{o}}(x;\ell) = \frac{1-\vartheta(x)}{2}x + O\left(\{1+\vartheta(x)\}\frac{x}{\log x}\right).$$

So, by an argument similar to Theorem 5.2, we have the following.

Theorem 5.4 *Let $E/\mathbb{Q}$ have CM by $\mathfrak{O}_K$ and let $\vartheta(x)$ be a function of x such that $x^{\vartheta(x)} \ll x^{\frac{1}{2}}\mathcal{L}^{-B}$, where B is the constant given in Theorem 2.2 provided A is chosen ≥ 2. Then*

$$\#\{p \le x,\ p \text{ ordinary and } P(N_p) > x^{\vartheta(x)}\} \ge \frac{1-\vartheta(x)}{2}\frac{x}{\log x^+} + O\left(\{1+\vartheta(x)\}\frac{x}{\log^2 x}\right).$$

Corollary 5.5 *In the previous theorem, let $\vartheta(x) \to 0$ as $x \to \infty$. Then*

$$\#\{p \le x,\ p \text{ ordinary and } P(N_p) > x^{\vartheta(x)}\} \sim \frac{1}{2}\,\frac{x}{\log x},$$

as $x \to \infty$. So for all but $o(x/\log x)$ of primes $p \le x$,

$$P(N_p) > p^{\vartheta(p)}.$$

Proof Since the density of ordinary primes in the set of primes is $1/2$, the first assertion is clear from the previous theorem. Next we note that for supersingular prime $p \ge 5$ we have $N_p = p + 1$, so repeating the above arguments for supersingular p results in

$$\#\{p \le x,\ p \text{ supersingular and } P(N_p) > x^{\vartheta(x)}\} \sim \frac{1}{2}\,\frac{x}{\log x},$$

as $x \to \infty$. So if $x^{\vartheta(x)}$ is a monotone increasing unbounded function, we have

$$\#\{p \le x, P(N_p) \le p^{\vartheta(p)}\} \le \#\{p \le x, P(N_p) \le x^{\vartheta(x)}\} = o\left(\frac{x}{\log x}\right).$$

Thus for almost all primes p, $P(N_p) > p^{\vartheta(p)}$. Finally we note that if $x^{\vartheta(x)}$ is not a monotone increasing unbounded function, we can always find a $\vartheta_1(x)$ such that $\vartheta(x) \le \vartheta_1(x)$, $\vartheta_1(x) \to 0$, and $x^{\vartheta_1(x)}$ is a monotone increasing unbounded function, so the result for $\vartheta(x)$ follows from the result for $\vartheta_1(x)$. □

6 Application

Let Γ be a free subgroup of rank r of $E(\mathbb{Q})$ and let Γ_p be the reduction of Γ mod p. We recall a known result on the number of primes p for which $|\Gamma_p|$ is bounded by a number z.

Lemma 6.1 $\#\{p :\ |\Gamma_p| \ll z\} = O\left(z^{1+\frac{2}{r}}/\log z\right).$

Proof See [GM], Lemma 14, or [AM], Proposition 1.2. □

Lemma 6.2 *Let $\vartheta > \frac{1}{2}$ be fixed and $r \ge 2$. Then*

$$\#\{p \le x,\ p \text{ ordinary};\ |\Gamma_p| \le x^{\vartheta} \text{ and } P(N_p) > x^{\vartheta}\} = o\left(\frac{x}{\log x}\right).$$

Proof It is clear that for a prime in this set $P(N_p) \nmid |\Gamma_p|$. Therefore $N_p = |\Gamma_p| P(N_p) k$ for some integer k and so

$$|\Gamma_p| = \frac{N_p}{P(N_p)k} \le \frac{N_p}{P(N_p)} \le \frac{x^+}{x^{\vartheta}} \ll x^{1-\vartheta}.$$

However from Lemma 6.1 we have

$$\#\{p;\ |\Gamma_p| \ll x^{1-\vartheta}\} \ll \frac{(x^{1-\vartheta})^{1+\frac{2}{r}}}{\log x} = o\left(\frac{x}{\log x}\right).$$

□

Theorem 6.3 *Let $E/\mathbb{Q}$ have CM by $\mathfrak{O}_K$. Let $r \geq 2$, $\epsilon > 0$ and $\vartheta_0 = 1 - \frac{1}{2}e^{-\frac{1}{4}} = 0.6105\cdots$. Then for a positive proportion of primes $p \leq x$,*

$$|\Gamma_p| > p^{\vartheta_0 - \epsilon}.$$

Proof By employing the previous lemma and Theorem 5.2, we have

$$\begin{aligned}
& \#\{p \leq x,\ p \text{ ordinary};\ |\Gamma_p| \leq p^{\vartheta_0-\epsilon}\} \\
\leq\ & \#\{p \leq x,\ p \text{ ordinary};\ |\Gamma_p| \leq x^{\vartheta_0-\epsilon}\} \\
=\ & \#\{p \leq x,\ p \text{ ordinary};\ |\Gamma_p| \leq x^{\vartheta_0-\epsilon},\ \text{and } P(N_p) \leq x^{\vartheta_0-\epsilon}\} \\
+\ & \#\{p \leq x,\ p \text{ ordinary};\ |\Gamma_p| \leq x^{\vartheta_0-\epsilon},\ \text{and } P(N_p) > x^{\vartheta_0-\epsilon}\} \\
\leq\ & \#\{p \leq x,\ p \text{ ordinary};\ P(N_p) \leq x^{\vartheta_0-\epsilon}\} + o\left(\frac{x}{\log x}\right) \\
\leq\ & \left(\frac{1}{2} - \eta(\vartheta_0 - \epsilon)\right)\frac{x}{\log x} + o\left(\frac{x}{\log x}\right).
\end{aligned}$$

□

ACKNOWLEDGMENT

The author would like to thank Professor Ram Murty for his suggestions and several helpful discussions related to this work.

References

[AKS] M. AGRAWAL, N. KAYAL, AND N. SAXENA, Primes is in P, *Ann. of Math.* **160** (2004), 781–793.

[AM] 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, 27 pages, to appear.

[BH] R. C. BAKER, G. HARMAN, Shifted primes without large prime factors, *Acta Arith.* **83** (1998), 331–361.

[C] A. C. COJOCARU, Reduction of an elliptic curve with almost prime orders, *Acta Arith.* **119** (2005), 265–289.

[Co] D. A. COX, *Primes of the form $x^2 + ny^2$, Fermat, class field theory, and complex multiplication*, John Wiley & Sons, 1989.

[G] M. GOLDFELD, On the number of primes p for which $p + a$ has a large prime factor, *Mathematika* **20** (1969), 119–134.

[GM] R. GUPTA AND M. R. MURTY, Primitive points on elliptic curves, *Compositio Math.* **58** (1986), 13–44.

[H] M. N. HUXLEY, The large sieve inequality for algebraic number fields III, *J. London Math. Soc.* **3** (1971), 233–240.

[HL] J. HINZ AND M. LODEMANN, On Siegel zeros of Hecke-Landau Zeta-functions, *Monatsh. Math.* **118** (1994), 231–248.

[L] S. LANG, *Elliptic Functions, second edition*, Springer-Verlag, New York, 1987.

[LT] S. LANG, H. TROTTER, Primitive points on elliptic curves, *Bull. Amer. Math. Soc.* **83** (1977), 289–292.

[M] Y. MOTOHASHI, A note on the least prime in an arithmetic progression with a prime difference, *Acta. Arith.* **17** (1970), 283–285.

[MMS] M. R. MURTY, V. K. MURTY AND N. SARADHA, Modular forms and the Chebotarev density theorem, *American J. Math.* **110** (1988), 253-281.

[N] W. NARKIEWICZ, *Elementary and analytic theory of algebraic numbers, third edition*, Springer-Verlag, Berlin Heidelberg, 2004.

[R] K. RUBIN, *Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer*, Lecture Notes in Mathematics, no. 1716, pp. 167–234, Springer-Verlag, Berlin Heidelberg, 1999.

[S1] J. H. SILVERMAN, *The arithmetic of elliptic curves*, GTM 106, Springer-Verlag, New York, 1986.

[S2] J. H. SILVERMAN, *Advanced topics in the arithmetic of elliptic curves*, GTM 151, Springer-Verlag, New York, 1994.

[S] C. L. STEWART, The greatest prime factor of $a^n - b^n$, *Acta Arith.* **26** (1975), 427–433.

Department of Mathematics and Computer Science, University of Lethbridge, 4401 University Drive West, Lethbridge, Alberta, T1K 3M4, CANADA
E–mail address: amir.akbary@uleth.ca