AVERAGE BEHAVIORS OF INVARIANT FACTORS IN MORDELL-WEIL GROUPS OF CM ELLIPTIC CURVES MODULO p

KIM, SUNGJIN
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF CALIFORNIA, LOS ANGELES
MATH SCIENCE BUILDING 6160
E-MAIL: 707107@GMAIL.COM
TEL: 213) 393-5507

Abstract. Let E be an elliptic curve defined over $\mathbb{Q}$ and with complex multiplication by $\mathcal{O}_K$, the ring of integers in an imaginary quadratic field K. Let p be a prime of good reduction for E. It is known that $E(\mathbb{F}_p)$ has a structure

$$E(\mathbb{F}_p) \simeq \mathbb{Z}/d_p\mathbb{Z} \oplus \mathbb{Z}/e_p\mathbb{Z} \tag{1}$$

with uniquely determined $d_p|e_p$. We give an asymptotic formula for the average order of e_p over primes $p \le x$ of good reduction, with improved error term $O(x^2/\log^A x)$ for any positive number A, which previously $O(x^2/\log^{1/8} x)$ by [W]. Further, we obtain an upper bound estimate for the average of d_p, and a lower bound estimate conditionally on nonexistence of Siegel-zeros for Hecke L-functions.

1. Introduction

Let E be an elliptic curve over $\mathbb{Q}$, and p be a prime of good reduction. Denote by $E(\mathbb{F}_p)$ the group of $\mathbb{F}_p$-rational points of E. It is known that $E(\mathbb{F}_p)$ has a structure

$$E(\mathbb{F}_p) \simeq \mathbb{Z}/d_p\mathbb{Z} \oplus \mathbb{Z}/e_p\mathbb{Z} \tag{2}$$

with uniquely determined $d_p|e_p$. By Hasse's bound, we have

$$|E(\mathbb{F}_p)| = p + 1 - a_p \tag{3}$$

with $|a_p| < 2\sqrt{p}$. We fix some notation before stating results. Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$. Let $E[k]$ be the k-torsion points of the group $E(\overline{\mathbb{Q}})$. Denote by $\mathbb{Q}(E[k])$ the k-th division field of E, which is obtained by adjoining the coordinates of $E[k]$ to $\mathbb{Q}$. Denote by n_k the field extension degree $[\mathbb{Q}(E[k]) : \mathbb{Q}]$. Let $\mathrm{Li}(x)$ be the logarithmic integral defined by $\int_2^x \frac{1}{\log t} dt$. We use the notation $F = O(G)$ if $F(x) \le CG(x)$ holds for sufficiently large x and a positive constant C.

Recently, T. Freiberg and P. Kurlberg [FK] started investigating the average order of e_p. They obtained that for any $x \ge 2$, there exists a constant $c_E \in (0, 1)$ such that

$$\sum_{p \le x} e_p = c_E \mathrm{Li}(x^2) + O(x^{19/10}(\log x)^{6/5}) \tag{4}$$

under the Generalized Riemann Hypothesis(GRH), and

$$\sum_{p \le x} e_p = c_E \mathrm{Li}(x^2) \left(1 + O\left(\frac{\log\log x}{\log^{1/8} x}\right)\right) \tag{5}$$

unconditionally when E has a complex multiplication(CM). Here, the implied constants depend at most on E, and the GRH is for the Dedekind zeta functions of the field extensions $\mathbb{Q}(E[k])$ over $\mathbb{Q}$. (In the summation, we take 0 in place of e_p when E has a bad reduction at p.) More recently, J.

Wu [W] improved their error terms in both cases

$$\sum_{p\le x} e_p = c_E \mathrm{Li}(x^2) + O(x^{11/6}(\log x)^{1/3}) \tag{6}$$

under GRH, and

$$\sum_{p\le x} e_p = c_E \mathrm{Li}(x^2) + O(x^2/(\log x)^{9/8}) \tag{7}$$

unconditionally when E has CM.

In this paper, we improve the unconditional error term in the CM case by using a number field analogue of the Bombieri-Vinogradov theorem due to [H, Theorem 1]. Also, the result is uniform in the conductor of the elliptic curves under consideration.

Theorem 1.1. *Let E be an elliptic curve defined over $\mathbb{Q}$ and with complex multiplication by $\mathcal{O}_K$, the ring of integers in an imaginary quadratic field K. Let N be the conductor of E. Let $A, B > 0$, and $N \le (\log x)^A$. Then we have*

$$\sum_{p\le x, p\nmid N} e_p = c_E Li(x^2) + O_{A,B}(x^2/(\log x)^B)$$

where

$$c_E = \sum_{k=1}^{\infty} \frac{1}{n_k} \sum_{dm=k} \frac{\mu(d)}{m}.$$

We are also interested in the average behavior of d_p. In [K, Corollary 5.33], E. Kowalski proposed several problems concerning the structure of Mordell-Weil groups of elliptic curve over finite fields, and obtained

$$\sum_{p\le x} d_p \ll_E x\sqrt{\log x} \tag{8}$$

by applying the number field analogue of the Brun-Titchmarsh inequality(see [HL, Theorem 4]). (In the summation, we take 0 in place of d_p when E has a bad reduction at p.) In fact, this is true for any CM elliptic curve over any field containing its CM field. In this paper, we improve this upper bound.

Theorem 1.2. *Let E be an elliptic curve defined over $\mathbb{Q}$ and with complex multiplication by $\mathcal{O}_K$, the ring of integers in an imaginary quadratic field K. Let N be the conductor of E. Let $A > 0$, and $N \le (\log x)^A$. Then we have*

$$\sum_{p\le x, p\nmid N} d_p \ll x \log\log x$$

where the implied constant depends at most on K and A.

Again, if we only consider a fixed CM elliptic curve over a field containing its CM field. The result is also uniform in the conductor of the elliptic curves under consideration.

Getting a lower bound for the average of d_p is much more difficult than getting an upper bound. Thus, we present those in a separate section. (see section 5.)

2. Preliminaries

We use the same notations $d_p, e_p, E[k]$, and $\mathbb{Q}(E[k])$ as in the previous section, and let $K(E[k])$ be the field extension obtained by adjoining coordinates of $E[k]$ to K. Here, K is an imaginary quadratic field otherwise stated, and $\mathcal{O}_K$ is the ring of integers of K.

Lemma 2.1. *Let E be an elliptic curve defined over $\mathbb{Q}$ and with complex multiplication by the ring of integers $\mathcal{O}_K$ of an imaginary quadratic field K. Then for $k > 2$,*

$$\phi(k)^2 \ll n_k \ll k^2$$

where ϕ is the Euler's totient function, and the implied constants depend only on K.

Proof. One way is to use the Kronecker's Jugendtraum. The proof is outlined in [CM, page 611, Proposition 3.8]. Another way is to use Deuring's theorem on the Galois representation for the CM elliptic curves over $\mathbb{Q}$. (see [Se, Section 4.5].) □

Lemma 2.2. *Let E be an elliptic curve over $\mathbb{Q}$, and p be a prime of good reduction. Then*

$$k | d_p \Leftrightarrow p \text{ splits completely in } \mathbb{Q}(E[k]).$$

Proof. This is done by considering Galois theory on residue fields of the division fields $\mathbb{Q}(E[k])$ over $\mathbb{Q}$. The proof is given in detail in [M, page 159, Lemma 2]. □

Let N be the conductor of E, and let

$$\pi_E(x; k) = \#\{p \le x : p \nmid N, \quad p \text{ splits completely in } \mathbb{Q}(E[k])\}.$$

Lemma 2.3. *For $2 \le k \le 2\sqrt{x}$, we have*

$$\pi_E(x; k) \ll \frac{x}{k^2}$$

where the implied constant is absolute.

Proof. The main idea is to identify each endomorphisms of a CM elliptic curve as a member of the ring of integers $\mathcal{O}_K$ of K. The proof is given in detail in [M, page 163, Lemma 5], and note that there are only nine possibilities for K. (as known as the class number 1 problem for imaginary quadratic fields, see [S].) □

We state some results from the class field theory. For the proofs, see [AM, Lemma 2.6, 2.7].

Lemma 2.4. *If $k \ge 3$ then $\mathbb{Q}(E[k]) = K(E[k])$.*

Lemma 2.5. *Let $E/\mathbb{Q}$ have CM by $\mathcal{O}_K$ and $k \geq 1$ be an integer. Then there is an ideal $\mathfrak{f}$ of $\mathcal{O}_K$ and $t(k)$ ideal classes mod $k\mathfrak{f}$ with the following property:*

If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ with $\mathfrak{p} \nmid k\mathfrak{f}$, then

$\mathfrak{p}$ *splits completely in* $K(E[k]) \Leftrightarrow \mathfrak{p} \sim \mathfrak{m}_1$, *or* $\mathfrak{m}_2$, *or* $\cdots$, *or* $\mathfrak{m}_{t(k)}$ *mod* $k\mathfrak{f}$.

Moreover

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

where

$$t(k) \leq c\phi(\mathfrak{f}) \prod_{\mathfrak{p}|\mathfrak{f}} \left(1 + \frac{1}{N(\mathfrak{p}) - 1}\right).$$

Here c is an absolute constant and $\phi(\mathfrak{f})$ is the number field analogue of the Euler function.

Denote by $\pi_K(x; \mathfrak{q}, \mathfrak{a}) = \#\{\mathfrak{p} :$ prime ideal of $\mathcal{O}_K$; $N(\mathfrak{p}) \leq x$, and $\mathfrak{p} \sim \mathfrak{a} \bmod \mathfrak{q}\}$. Let $\mathfrak{q}$ be an integral ideal of K. Define a $\mathfrak{q}$-ideal class group by an abelian group of equivalence classes of ideals in the following relation:

$$\mathfrak{a} \sim \mathfrak{b} \pmod{\mathfrak{q}},$$

if $\mathfrak{a}\mathfrak{b}^{-1} = (\alpha)$, $\alpha \in K$, $\alpha \equiv 1 \pmod{\mathfrak{q}}$, and α is totally positive. Let $\alpha, \beta \in K$. Denote by $\alpha \equiv \beta$ (mod* $\mathfrak{q}$) if $v_{\mathfrak{p}}(\mathfrak{q}) \leq v_{\mathfrak{p}}(\alpha - \beta)$ for all primes $\mathfrak{p}$ and $\alpha\beta^{-1}$ is totally positive. Then we can rewrite the equivalence relation $\sim$ by

$$\mathfrak{a}\mathfrak{b}^{-1} \in P_K^{\mathfrak{q}} = \{(\alpha) : \alpha \equiv 1 \ (\text{mod}^* \ \mathfrak{q})\}.$$

Denote by $h(\mathfrak{q})$ the number of the equivalence classes for this equivalence relation $\sim$. Denote by $T(\mathfrak{q})$ the cardinality of the image of the unit group $U(K)$ of K in $(\mathcal{O}_K/\mathfrak{q}\mathcal{O}_K)^{\times}$. Thus, $T(\mathfrak{q}) \leq 6$ for imaginary quadratic fields, since there are at most 6 units in them. We will use the following is a number field analogue of the Bombieri-Vinogradov theorem due to Huxley [H, Theorem 1].

Lemma 2.6. *For each positive constant B, there is a positive constant $C = C(B)$ such that*

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

where $Q = x^{1/2}(\log x)^{-C}$. The implied constant depends only on B and on the field K.

We will also use a number field analogue of the Brun-Titchmarsh inequality due to J. Hinz and M. Lodemann [HL, Theorem 4].

Lemma 2.7. *Let $\mathfrak{H}$ denote any of the $h(\mathfrak{q})$ elements of the group of ideal-classes mod $\mathfrak{q}$ in the narrow sense. If $1 \leq N\mathfrak{q} < X$, then*

$$\sum_{\substack{N\mathfrak{p} < X \\ \mathfrak{p} \in \mathfrak{H}}} 1 \leq 2 \frac{X}{h(\mathfrak{q}) \log \frac{X}{N\mathfrak{q}}} \left\{ 1 + O\left(\frac{\log\log 3 \frac{X}{N\mathfrak{q}}}{\log \frac{X}{N\mathfrak{q}}} \right) \right\}.$$

We are now ready to prove Theorem 1.1. From now on, E is an elliptic curve over $\mathbb{Q}$ that has CM by $\mathcal{O}_K$, where K is one of the nine imaginary quadratic fields with class number 1. Let N be the conductor of E.

3. Proof of the theorem 1.1

By Hasse's bound, we have

$$\sum_{p\le x, p\nmid N} e_p = \sum_{p\le x, p\nmid N} \frac{p}{d_p} + O\left(\sum_{p\le x}\sqrt{p}\right), \tag{9}$$

where the error term is $O(\sqrt{x}\sum_{n\le x}1) = O(x^{3/2})$. As done in both [FK] and [W], we use the following elementary identity

$$\frac{1}{k} = \sum_{dm|k}\frac{\mu(d)}{m}. \tag{10}$$

Thus we obtain

$$\begin{aligned}\sum_{p\le x, p\nmid N}\frac{p}{d_p} &= \sum_{p\le x, p\nmid N} p\sum_{dm|d_p}\frac{\mu(d)}{m}\\ &= \sum_{k\le\sqrt{x}+1}\sum_{dm=k}\frac{\mu(d)}{m}\sum_{p\le x, p\nmid N, k|d_p} p.\end{aligned}$$

We split the sum into two parts as in [W]:

$$\begin{aligned}S_1 &= \sum_{k\le y}\sum_{dm=k}\frac{\mu(d)}{m}\sum_{p\le x, p\nmid N, k|d_p} p,\\ S_2 &= \sum_{y<k\le\sqrt{x}+1}\sum_{dm=k}\frac{\mu(d)}{m}\sum_{p\le x, p\nmid N, k|d_p} p.\end{aligned}$$

Here y is a parameter satisfying $3\le y\le 2\sqrt{x}$, and which will be chosen optimally later. We treat S_2 using trivial estimate

$$\left|\sum_{dm=k}\frac{\mu(d)}{m}\right| \le 1 \tag{11}$$

and Lemma 2.3, obtaining

$$|S_2| \ll \sum_{y<k\le\sqrt{x}+1} x\cdot\frac{x}{k^2} \ll \frac{x^2}{y}. \tag{12}$$

Let $E_k(x)$ be defined by the relation $\pi_E(x;k) = \frac{\mathrm{Li}(x)}{n_k} + E_k(x)$. Our goal for treating S_1 is making use of Lemma 2.6. First, we take care of the inner sum by partial summation. Thus,

$$\sum_{p\le x, p\nmid N, k|d_p} p = \int_{2-}^{x} t d\pi_E(t;k)$$
$$= \frac{1}{n_k}\mathrm{Li}(x^2) + O\left(x \max_{t\le x}|E_k(t)|\right).$$

Next, we combine this with the trivial estimate (11) and Lemma 2.1, obtaining
(13)

$$S_1 = c_E \mathrm{Li}(x^2) + O\left(x\max_{t\le x}|E_2(t)|\right) + O\left(\frac{x^2}{y\log x} + \sum_{3\le k\le y} x\max_{t\le x}|E_k(t)|\right)$$

where

$$c_E = \sum_{k=1}^{\infty}\frac{1}{n_k}\sum_{dm=k}\frac{\mu(d)}{m}.$$

The series defining c_E is convergent by (11) and Lemma 2.1, and positive due to [FK]. Here, Lemma 2.1 is used in bounding $\sum_{y<k}\frac{1}{n_k}\mathrm{Li}(x^2)$.

Let $\mathfrak{f}$ be a nonzero integral ideal of K which appears in Lemma 2.5. Let $\widetilde{\pi_E}(x;k) = \#\{\mathfrak{p} : N(\mathfrak{p}) \le x, \mathfrak{p}\nmid k\mathfrak{f}, \mathfrak{p} \text{ splits completely in } K(E[k])\}$. By Lemma 2.4 and [AM, (3.2)], we have

$$(14)\quad \pi_E(x;k) = \frac{1}{2}\widetilde{\pi_E}(x;k) + O\left(\frac{x^{1/2}}{\log x}\right) + O(\log N) \text{ uniformly for } k\ge 3.$$

The factor $1/2$ comes from rational prime p which splits in K, and the first error term comes from counting rational primes $p\le x$ of degree 2 in K, while the second error term comes from possible primes dividing N. For a detailed explanation, we refer to [AM, page 9]. By Lemma 2.5, we have

$$(15)\qquad \widetilde{\pi_E}(x;k) - \frac{\mathrm{Li}(x)}{[K(E[k]):K]} = \sum_{i=1}^{t(k)}\left(\pi_K(x,k\mathfrak{f},\mathfrak{m}_i) - \frac{\mathrm{Li}(x)}{h(k\mathfrak{f})}\right)$$

for a fixed nonzero integral ideal $\mathfrak{f}$ of K. Again using Lemma 2.5 to bound $t(k)$ and applying Lemma 2.6 as in [AM, page 10],
(16)

$$\sum_{3\le k\le \frac{x^{1/4}}{N(\mathfrak{f})(\log x)^{C/2}}} \max_{t\le x}\left|\widetilde{\pi_E}(t;k) - \frac{\mathrm{Li}(t)}{[K(E[k]):K]}\right| \ll_{A,B} N\log N\frac{x}{(\log x)^{A+B+1}},$$

where $C=C(A,B)$ is the corresponding positive constant in Lemma 2.6 for the positive constant $A+B+1$.
Note that $T(\mathfrak{q})\le 6$. Writing $\widetilde{E_k}(x) = \widetilde{\pi_E}(x;k) - \frac{\mathrm{Li}(x)}{[K(E[k]):K]}$, and using a

bound $\max_{t\le x}|E_2(t)| \ll x/\log^B x$ (see [AM, Lemma 2.3]), we have
(17)

$$S_1 = c_E \mathrm{Li}(x^2) + O_{A,B}\left(\frac{x^2}{(\log x)^B}\right) + O\left(\frac{x^2}{y\log x} + \sum_{3\le k\le y} x\max_{t\le x}|\widetilde{E_k}(t)| + \frac{x^{3/2}y\log N}{\log x}\right)$$

Now, taking $y = \frac{x^{1/4}}{N(\mathfrak{f})(\log x)^{C/2}}$, we obtain
(18)

$$S_1 = c_E \mathrm{Li}(x^2) + O_{A,B}\left(\frac{x^2}{(\log x)^B} + x^{7/4}N(\mathfrak{f})(\log x)^{C/2-1} + \frac{x^2 N\log N}{(\log x)^{A+B+1}} + \frac{x^{7/4}\log N}{N(\mathfrak{f})(\log x)^{1+C/2}}\right).$$

Note that $N = N(\mathfrak{f})|d_K|$ as in [AM, AM, page 7, Remark 2.8], where d_K is the discriminant of K. Combining with the estimate of $|S_2|$ in (12), it follows that
(19)

$$\sum_{p\le x, p\nmid N} \frac{p}{d_p} = c_E \mathrm{Li}(x^2) + O_{A,B}\left(\frac{x^2}{(\log x)^B} + \frac{x^2 N\log N}{(\log x)^{A+B+1}} + x^{7/4}N(\log x)^C\right).$$

Theorem 1.1 now follows.

4. Proof of Theorem 1.2

Let N be the conductor of a CM elliptic curve E satisfying $N \le (\log x)^A$. We use the following elementary identity

$$k = \sum_{dm|k} m\mu(d).$$

We unfold the sum similarly as in the proof of Theorem 1.1:

$$\begin{aligned}\sum_{p\le x, p\nmid N} d_p &= \sum_{p\le x, p\nmid N}\sum_{dm|d_p} m\mu(d)\\ &= \sum_{k\le\sqrt{x}+1}\sum_{dm=k} m\mu(d) \sum_{p\le x, p\nmid N, k|d_p} 1.\end{aligned}$$

We introduce a variable y and split the sum as shown in the proof of Theorem 1.1:

$$\begin{aligned}\sum_{p\le x, p\nmid N} d_p &= \pi_E(x;2) + \sum_{3\le k\le\sqrt{x}+1}\phi(k)\pi_E(x;k)\\ &\le \frac{2x}{\log x} + \sum_{3\le k\le y}\phi(k)\frac{1}{2}\widetilde{\pi_E}(x;k) + \sum_{y<k\le\sqrt{x}+1}\phi(k)\pi_E(x;k).\end{aligned}$$

The inequality in the last line is due to the primes $\mathfrak{p}$ in K which lie above primes p in $\mathbb{Q}$ that split completely in K. For each rational prime p that splits completely in $\mathbb{Q}(E[k]) = K(E[k])$, corresponds to two primes $\mathfrak{p}, \mathfrak{p}'$ in

K that lie above p. Let S_1, S_2 denote the second sum and the third term respectively:

$$S_1 = \sum_{3\le k\le y} \phi(k)\frac{1}{2}\widetilde{\pi_E}(x;k),$$
$$S_2 = \sum_{y<k\le\sqrt{x}+1} \phi(k)\pi_E(x;k).$$

Now, we use Lemma 2.5, and 2.7 to give an upper bound for each $\widetilde{\pi_E}(x;k)$:

$$\widetilde{\pi_E}(x;k) \le 2\frac{t(k)x}{h(k\mathfrak{f})\log\frac{x}{N(k\mathfrak{f})}}\left\{1+O\left(\frac{\log\log 3\frac{x}{N(k\mathfrak{f})}}{\log\frac{x}{N(k\mathfrak{f})}}\right)\right\}. \tag{20}$$

Then we treat S_1 by (19), and S_2 by the trivial bound ($\pi_E(x;k) \ll \frac{x}{k^2}$) in Lemma 2.3. As a result, we obtain

$$S_1 \ll x\sum_{3\le k\le y}\frac{\phi(k)}{n_k\log\frac{x}{k^2N(\mathfrak{f})}},$$
$$S_2 \ll x\sum_{y<k\le\sqrt{x}+1}\phi(k)\frac{1}{k^2} \ll x\log\frac{\sqrt{x}}{y},$$

where the implied constants are absolute. We apply partial summation to S_1 with $\phi(k)^2 \ll n_k$, and $\sum_{k\le t}\frac{1}{\phi(k)} = A_1\log t + O(1)$. Note that, we have $3 \le y \le 2\sqrt{x}$. Let $M = N(\mathfrak{f})$. We use $a_k = \frac{1}{\phi(k)}$, $A(t) = \sum_{k\le t} a_k = A_1\log t + O(1)$, and $f(t) = \frac{1}{\log\frac{x}{t^2M}}$.
Thus

$$f'(t) = -\frac{1}{\log^2\frac{x}{t^2M}}\frac{1}{\frac{x}{t^2M}}(-2)\frac{x}{M}t^{-3} = 2\frac{1}{t\log^2\frac{x}{t^2M}}.$$

We also restrict y with $3 \le \frac{x}{y^2M}$. By the way, we have

$$\frac{d}{dt}\left(\log\log\frac{x}{t^2M}\right) = \frac{1}{\log\frac{x}{t^2M}}\frac{1}{\frac{x}{t^2M}}\frac{x}{M}(-2)t^{-3} = -2\frac{1}{t\log\frac{x}{t^2M}}.$$

This yields $\frac{f(t)}{t} = -\frac{1}{2}\frac{d}{dt}\left(\log\log\frac{x}{t^2M}\right)$.

$$\begin{aligned}\sum_{3\le k\le y}\frac{1}{\phi(k)\log\frac{x}{k^2M}} &= \sum_{3\le k\le y} a_kf(k) = \int_{3-}^{y} f(t)dA(t)\\ &= A(t)f(t)|_{3-}^{y} - \int_3^y A(t)f'(t)dt\\ &= \frac{1}{2}A_1\left(\log\log\frac{x}{9M} - \log\log\frac{x}{y^2M}\right) + O(1).\end{aligned}$$

Hence, it follows that

$$S_1 \ll x\log\log\frac{x}{N(\mathfrak{f})} \ll x\log\log x, \tag{21}$$

provided that $3 \leq \frac{x}{y^2 N(\mathfrak{f})}$.

Choosing $y = \sqrt{\frac{x}{3N(\mathfrak{f})}}$, it follows that

$$S_1 + S_2 \ll_A x \log\log x \tag{22}$$

Therefore, Theorem 1.2 now follows.

Note that the trivial bound in Theorem 1.2 given by Lemma 2.3 is $\ll x \log x$. The number field analogue of Brun-Titchmarsh inequality(Lemma 2.7) contributed to the saving.

5. Lower Bound Results

Let E be a CM elliptic curve over $\mathbb{Q}$ with CM field K, and d_p, e_p as before. Recall that

$$\sum_{p \leq x, p \nmid N} d_p = \sum_{k \leq \sqrt{x}+1} \phi(k) \pi_E(x; k) \tag{23}$$

as in the previous section.

In [K], E. Kowalski gives the following unconditional result.

$$\sum_{p \leq x} d_p \gg_E \frac{x \log\log x}{\log x}.$$

A. T. Felix, and M. R. Murty(see [FM]) provided a detailed proof of a slightly stronger version than this,

$$\left(\sum_{p \leq x} d_p \right) / \left(\frac{x \log\log x}{\log x} \right) \to \infty$$

as $x \to \infty$. They also provided a result which is conditional on GRH for Dedekind zeta functions,

$$\sum_{p \leq x} d_p \gg_E x.$$

E. Kowalski(see [K, Theorem 3.8]) provided an asymptotic formula for shorter range of k in the sum (23) conditionally on GRH,

$$\sum_{k \leq \frac{x^{1/4}}{\log x}} \phi(k) \pi_E(x; k) = cx + O_E\left(\frac{x}{\log x} \right).$$

In this section, we derive a stronger lower bound than the unconditional result, but weaker than the GRH-conditional result, by assuming a weaker hypotheses than GRH. To this end, we use a classical zero-free region result for Hecke L-functions. (see [F])

Lemma 5.1. *(Fogels, 1962) Let K be a number field, χ be a Grossencharacter of K defined modulo its conductor $\mathfrak{f}$. Denote by $L(s,\chi)$ the associated L-function. Let $D = |\Delta| N\mathfrak{f} = D_0 > 1$ where Δ denotes the discriminant of* *the field, and* $N\mathfrak{f}$ *the norm of* $\mathfrak{f}$*. Then there is a positive constant* c*(which depends only on* $[K:\mathbb{Q}]$*) such that in the region*

$$\sigma \geq 1 - \frac{c}{\log D(1+|t|)} \geq \frac{3}{4} \quad (\sigma = Re\ s,\ t = Im\ s) \tag{24}$$

there is no zero of $L(s,\chi)$ *in the case of a complex* χ*. For at most one real* χ *there may be in (24) a simple zero* β *of* $L(s,\chi)$*(which we call Siegel-zero).*

Here, we use the prime ideal theorem in the following form.

Lemma 5.2. *Let* K *be a number field,* $\mathfrak{m}$ *be a nonzero integral ideal , and* $\mathfrak{a}$ *be an integral ideal prime to* $\mathfrak{m}$*. Let*

$$\psi(x,\mathfrak{m},\mathfrak{a}) := \sum_{\substack{N\mathfrak{b}\leq x \\ \mathfrak{b}\sim\mathfrak{a}\ mod\ \mathfrak{m}}} \Lambda(\mathfrak{b}).$$

Then

$$\psi(x,\mathfrak{m},\mathfrak{a}) = \frac{x}{h(\mathfrak{m})} - \frac{\overline{\chi_1}(\mathfrak{a})}{h(\mathfrak{m})}\frac{x^{\beta_1}}{\beta_1} + O\left(xe^{-c\sqrt{\log x}}\right) \tag{25}$$

for some positive constant c depending only on K*. The term involving Siegal-zero only occurs if it exists.*

A direct consequence of this lemma is as follows

$$\pi(x,\mathfrak{m},\mathfrak{a}) := \#\{N\mathfrak{p} \leq x \mid \mathfrak{p}\sim\mathfrak{a} \text{ mod } \mathfrak{m}\} = \frac{\mathrm{Li}(x)}{h(\mathfrak{m})} - \frac{\overline{\chi_1}(\mathfrak{a})}{h(\mathfrak{m})}\mathrm{Li}(x^{\beta_1}) + O\left(xe^{-c'\sqrt{\log x}}\right) \tag{26}$$

for some positive constants c, c' depending only on K. Here, χ_1 is a real character having a Siegel-zero β_1, and the implied O-constant depends only on K. The term involving Siegel-zero only occurs if it exists.

Theorem 5.1. *Let* E *be a CM elliptic curve over* $\mathbb{Q}$ *with quadratic imaginary CM field* K*. Let* χ *be a Grossencharacter of* K *defined modulo its conductor* $\mathfrak{f}$*. Suppose that there is no zero of* $L(s,\chi)$ *in the region (24)(which we will abbreviate it as NSZC-nonexistence of Siegel-zero condition). Then*

$$\sum_{p\leq x} d_p \gg_E \frac{x}{\sqrt{\log x}}. \tag{27}$$

Proof. We begin with the same method as in [FM, page 23], and use (14), (15):

$$\begin{aligned}\sum_{p\le x} d_p &= \sum_{k\le\sqrt{x}+1} \phi(k)\pi_E(x;k)\\ &\gg \sum_{3\le k\le y} \phi(k)\left(\frac{\mathrm{Li}(x)}{[K(E[k]):K]} + \widetilde{\pi_E}(x;k) - \frac{\mathrm{Li}(x)}{[K(E[k]):K]}\right) + O\left(\frac{y^2\sqrt{x}}{\log x}\right)\\ &\gg \frac{x\log y}{\log x} + \sum_{3\le k\le y} \phi(k)\left(\widetilde{\pi_E}(x;k) - \frac{\mathrm{Li}(x)}{[K(E[k]):K]}\right) + O\left(\frac{y^2\sqrt{x}}{\log x}\right)\\ &= \frac{x\log y}{\log x} + \sum_{3\le k\le y} \phi(k)\sum_{i=1}^{t(k)}\left(\pi_K(x,k\mathfrak{f},\mathfrak{m}_i) - \frac{\mathrm{Li}(x)}{h(k\mathfrak{f})}\right) + O\left(\frac{y^2\sqrt{x}}{\log x}\right).\end{aligned}$$

Here, an important point is that the O-term in Lemma 5.2 does not depend on $\mathfrak{m}$.

Applying this to our lower bound, and using the bound of $t(k)$ (see Lemma 2.5), we deduce under NSZC,

$$\sum_{p\le x} d_p \gg_E \frac{x\log y}{\log x} + O\left(xy^2e^{-c'\sqrt{\log x}}\right) + O\left(\frac{y^2\sqrt{x}}{\log x}\right). \tag{28}$$

Choosing $y = e^{c''\sqrt{\log x}}$ where $2c'' < c'$, the lower bound becomes

$$\sum_{p\le x} d_p \gg_E \frac{x}{\sqrt{\log x}} + O\left(xe^{(2c''-c')\sqrt{\log x}}\right).$$

Theorem 5.1 now follows. □

6. Remarks

The author investigated a possibility of obtaining Theorem 5.1 unconditionally. However, Siegel-zero can occur for some modulus $\mathfrak{q}_1$ satisfying $N\mathfrak{q}_1 < \sqrt{x}+1$ and multiples of $\mathfrak{q}_1$. Although Siegel-zero only occur for sparse set of modulus, the set of exceptional modulus indeed consists of the modulus giving primitive characters. Thus, this was a barrier in removing NSZC.

Acknowledgements The author thanks William Duke for helpful comments and guidance. The author also thanks Tristan Freiberg and Jie Wu for helpful discussions.

References

[AM] A. Akbary, K. Murty, *Cyclicity of CM Elliptic Curves Mod p*, Indian Journal of Pure and Applied Mathematics, 41 (1) (2010), 25-37

[C] A. Cojocaru, *Cyclicity of CM Elliptic Curves Modulo p*, Transaction of Americal Mathematical Society, volume 355, number 7

[CM] A. Cojocaru, M. R. Murty, *Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linniks problem*, Math. Ann. 330, 601.625 (2004)

[F] E. Fogels, *On the zeros of Hecke's L-functions I*, Acta Arithmetica VII, 87-106

[FK] T. Freiberg, P. Kurlberg, *On the Average Exponent of Elliptic Curves Modulo p*, Int Math Res Notices 2013 : rns280v1-29

[FM] A. T. Felix, M. R. Murty, *On the asymptotic nature of elliptic curves modulo p*, J. Ramanujan Math. Soc. 28, No.3 (2013) 271-298

[H] M. Huxley, *The Large Sieve Inequality for Algebraic Number Fields III*, J. London Math. Soc. 3 (1971), 233-240

[HL] J. Hintz, M. Lodemann, *On Siegel Zeros of Hecke-Landau Zeta-Functions*, Monashefte für Mathematik, Springer-Verlag 1994

[K] E. Kowalski, *Analytic problems for elliptic curves*, J. Ramanujan Math. Soc. 21 (2006), 19-114.

[M] R. Murty, *On Artin's Conjecture*, Journal of Number Theory, Vol 16, no.2, April 1983

[S] H. Stark, *A complete determination of the complex quadratic fields of class number one*, Michigan Mathematics Journal (1967), 1-27.

[Se] J-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques.*, Inventiones mathematicae volume 15; pp. 259 - 331

[W] J. Wu, *The Average Exponent of Ellptic Curves Modulo p*, Journal of Number Theory, Volume 135, February 2014, 28-35