ON THE A VERAGE EXPONENT OF CM ELLIPTIC CURVES MODULO $p$

KIM, SUNGJIN

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

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

with $d_p | e_p$. We give an asymptotic formula for the average order of $e_p$, with improved error term, and upper bound estimate for the average of $d_p$.

1. Introduction

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

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

with $d_p | e_p$. By Weil’s bound, we have

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

with $|a_p| < 2\sqrt{p}$. We fix some notations before stating results. Let $E[k]$ be the $k$-torsion points of the group $E(\overline{\mathbb{Q}})$. Denote $\mathbb{Q}(E[k])$ the $k$-th division field, which is obtained by adjoining coordinates of $E[k]$. Denote $n_k$ the field extension degree $[\mathbb{Q}(E[k]) : \mathbb{Q}]$. Recently, T.Freiberg and P.Kurlberg [TP] started investigating the average order of $e_p$(In the summation, we take 0 in place of $e_p$ when $E$ has a bad reduction at $p$). They obtained that there exists a constant $c_E \in (0,1)$ such that

$$\sum_{p \leq x} e_p = c_E \text{Li}(x^2) + O(x^{19/10} (\log x)^{6/5})$$

under GRH, and

$$\sum_{p \leq x} e_p = c_E \text{Li}(x^2) + O(x^2 \log \log \log x / \log x \log \log x).$$

unconditionally when $E$ has CM. More recently, J.Wu [JW] improved their error terms in both cases

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

1
under GRH, and
\[
\sum_{p \leq x} e_p = c_E \text{Li}(x^2) + O(x^2/(\log x)^{9/8}).
\]
unconditionally when \( E \) has CM.

In this paper we improve the unconditional error term in CM case by using a number field analogue of Bombieri-Vinogradov theorem due to [H, Theorem 1].

**Theorem 1.1.** Let \( E \) be a CM 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 \( N \leq (\log x)^A \). Then we have
\[
\sum_{p \leq x, p \nmid N} e_p = c_E \text{Li}(x^2) + O_{A,B}(x^2/(\log x)^B).
\]
where
\[
c_E = \sum_{k=1}^{\infty} \frac{1}{n_k} \sum_{d \mid m} \frac{\mu(d)}{m}.
\]

We are also interested in the average behavior of \( d_p \). For the average of \( d_p \), we have an upper bound result. We apply the number field analogue of Brun-Titchmarsh inequality due to [HL, Theorem 4].

**Theorem 1.2.** Let \( E \) be a CM 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 \( N \leq (\log x)^A \). Then we have
\[
\sum_{p \leq x, p \nmid N} d_p \ll_A x \log \log x,
\]
where the implied constant is absolute.

Note that the upper bound is sharper than the trivial bound \( \ll x \log x \).

2. Preliminaries

**Lemma 2.1.** Let \( E \) be a CM elliptic curve defined over \( \mathbb{Q} \) and with complex multiplication by \( \mathcal{O}_K \). Then for \( k > 2 \),
\[
\phi(k)^2 \ll n_k \ll k^2
\]
where \( \phi \) is the Euler function.

**Lemma 2.2.** Let \( E \) be an elliptic curve over \( \mathbb{Q} \), and \( p \) be a prime of good reduction. Then
\[
k \mid d_p \iff p \text{ splits completely in } \mathbb{Q}(E[k]).
\]
**Proof.** See [M, page 159].
Let \( N \) be the conductor of \( E \), and denote
\[
\pi_E(x; k) = \#\{ p \leq x : p \nmid N, \ p \text{ splits completely in } \mathbb{Q}(E[k]) \}
\]

**Lemma 2.3.** For \( 2 \leq k \leq 2\sqrt{x} \), we have
\[
\pi_E(x; k) \ll \frac{x}{k^2}
\]
where the implied constant is absolute.

**Proof.** See A. Cojocaru [AC, Lemma 2.6], and note that there are only nine possibilities of \( K \). \( \square \)

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

**Lemma 2.4.** If \( k \geq 3 \) 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
\[
\mathfrak{p} \text{ splits completely in } K(E[k]) \iff \mathfrak{p} \sim m_1, \text{ or } m_2, \text{ or } \cdots, \text{ or } m_{t(k)} \mod k\mathfrak{f}.
\]
Moreover,
\[
t(k)[K(E[k]) : K] = h(k\mathfrak{f}),
\]
where
\[
t(k) \leq c\phi(f) \prod_{\mathfrak{p} \nmid \mathfrak{f}} \left( 1 + \frac{1}{N(p) - 1} \right).
\]

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

Let \( \pi_K(x; q, a) = \#\{ \mathfrak{p} : \text{prime ideal; } N(\mathfrak{p}) \leq x, \text{ and } \mathfrak{p} \sim a \mod q \} \). 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
\[
\sum_{N(q) \leq Q} \max_{(a, q) = 1} \max_{y \leq x} \frac{1}{T(q)} \left| \pi_K(y; q, a) - \frac{Li(y)}{h(q)} \right| \ll \frac{x}{(\log x)^B},
\]
where \( Q = x^{1/2}(\log x)^{-C} \). The implied constant depends only on \( B \) and on the field \( K \).

There is a number field analogue of Brun-Titchmarsh inequality due to J. Hinz and M. Lodemann [HL, Theorem 4].
Lemma 2.7. Let $H$ denote any of the $h(q)$ elements of the group of ideal-classes mod $q$ in the narrow sense. If $1 \leq Nq < X$, then

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

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 field with class number 1. Let $N$ be the conductor of $E$.

3. Proof of the theorem 1.1

By Weil’s bound, we have

$$
\sum_{p \leq x, p \nmid N} e_p = \sum_{p \leq x, p \nmid N} \frac{p}{d_p} + O\left( \frac{x^{3/2}}{\log x} \right).
$$

As shown in both [TP] and [JW], we use the following elementary identity

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

Thus we obtain

$$
\sum_{p \leq x, p \nmid N} \frac{p}{d_p} = \sum_{p \leq x, p \nmid N} p \sum_{dm | d_p} \mu(d) \frac{1}{m} = \sum_{k \leq 2\sqrt{x}} \sum_{dm = k} \mu(d) \frac{1}{m} \sum_{p \leq x, p \nmid N, k | d_p} p.
$$

Then we split the sum into two parts as in [JW].

$$
S_1 = \sum_{k \leq y} \sum_{dm = k} \mu(d) \frac{1}{m} \sum_{p \leq x, p \nmid N, k | d_p} p,
$$

$$
S_2 = \sum_{y < k \leq 2\sqrt{x}} \sum_{dm = k} \mu(d) \frac{1}{m} \sum_{p \leq x, p \nmid N, k | d_p} p.
$$

Here a variable $y$ is to be chosen later within $3 \leq y \leq 2\sqrt{x}$. We treat $S_2$ using trivial estimate

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

and Lemma 2.3, then we obtain

$$
|S_2| \ll \sum_{y < k \leq 2\sqrt{x}} x \cdot \frac{x}{k^2} \ll \frac{x^2}{y}.
$$
Let \( \pi_E(x; k) = \frac{\operatorname{Li}(x)}{n_k} + E_k(x) \). Our goal for treating \( S_1 \) is making use of Lemma 2.6. First, we take care of the inner sum by partial summation

\[
\sum_{p \leq x, p \nmid N, k \mid d_p} x \pi_E(x; k) = \int_{2^{-}}^{x} t d\pi_E(t; k) = x \pi_E(x; k) - \int_{2}^{x} \pi_E(t; k) dt
\]

\[
= x \frac{\operatorname{Li}(x)}{n_k} - \int_{2}^{x} \frac{\operatorname{Li}(t)}{n_k} dt + O \left( x |E_k(x)| + \int_{2}^{x} |E_k(t)| dt \right)
\]

\[
= \frac{1}{n_k} \operatorname{Li}(x^2) + O \left( x \max_{t \leq x} |E_k(t)| + 1 \right).
\]

Then we deal with \( S_1 \) using the trivial estimate (10) and Lemma 2.1, we have

\[
S_1 = c_E \operatorname{Li}(x^2) + O \left( x \max_{t \leq x} |E_2(t)| \right) + O \left( \frac{x^2}{y \log x} + \sum_{3 \leq k \leq y} x \max_{t \leq x} |E_k(t)| + \sqrt{x} \right)
\]

where

\[
c_E = \sum_{k=1}^{\infty} \frac{1}{n_k} \sum_{d \text{ such that } d \mid m_k} \mu(d) \frac{\mu(d)}{m}.
\]

Let \( \tilde{\pi}_E(x; k) = \# \{ p : N(p) \leq x, p \mid k, p \text{ splits completely in } K(E[k]) \} \).

By Lemma 2.4, we have

\[
\pi_E(x; k) = \frac{1}{2} \tilde{\pi}_E(x; k) + O \left( \frac{x^{1/2}}{\log x} \right) + O(\log N) \text{ uniformly for } k \geq 3.
\]

For the detailed explanation, we refer to [AM, page 9]. By Lemma 2.5, we have

\[
\tilde{\pi}_E(x; k) - \frac{\operatorname{Li}(x)}{[K(E[k]): K]} = \sum_{i=1}^{t(k)} \left( \pi_K(x, k; \bar{m}_i) - \frac{\operatorname{Li}(x)}{h(k)} \right).
\]

Again using Lemma 2.5 to bound \( t(m) \) and applying Lemma 2.6 as in [AM, page 10],

\[
\sum_{3 \leq k \leq \frac{x^{1/4}}{N(\log x)^{C/2}}} \max_{t \leq x} \left| \tilde{\pi}_E(t; k) - \frac{\operatorname{Li}(t)}{[K(E[k]): K]} \right| \ll_{A, B} N \log N \frac{x}{(\log x)^{A+B+1}},
\]

where \( C = C(A, B) \) is the corresponding positive constant in Lemma 2.6 for the positive constant \( A + B + 1 \).

Note that \( T(q) \leq 6 \). Writing \( \tilde{E}_k(x) = \tilde{\pi}_E(x; k) - \frac{\operatorname{Li}(x)}{[K(E[k]): K]} \), and using a
bound for \( \max_{t \leq x} |E_2(t)| \) (See [AM, Lemma 2.3]), we have
(16)
\[
S_1 = c_E \text{Li}(x^2) + O_{A,B} \left( \frac{x^2}{(\log x)^B} \right) + O \left( \frac{x^2}{y \log x} + \sum_{3 \leq k \leq y} x \max_{t \leq x} |\tilde{E}_k(t)| + \frac{x^{3/2} y \log N}{\log x} \right)
\]
Now, taking \( y = \frac{x^{1/4}}{N(f)(\log x)^{C/2}} \), we obtain
(17)
\[
S_1 = c_E \text{Li}(x^2) + O_{A,B} \left( \frac{x^2}{(\log x)^B} + x^{7/4} N(f)(\log x)^{C/2-1} + \frac{x^2 N \log N}{(\log x)^{A+B+1} + x^{7/4} \log N \log x} + \frac{x^{7/4} \log N}{N(f)(\log x)^{1+C/2}} \right).
\]
Note that \( N = N(f)|d_K| \), where \( d_K \) is the discriminant of \( K \). Combining with estimate of \( |S_2| \) in (12), it follows that
(18)
\[
\sum_{p \leq x, p \nmid N} \frac{p}{d_p} = c_E \text{Li}(x^2) + O_{A,B} \left( \frac{x^2}{(\log x)^B} + x^2 N \log N \log x + x^{7/4} N(\log x)^C \right).
\]

Theorem 1.1 now follows.

4. PROOF OF THEOREM 1.2

Let \( N \) be the conductor of a CM elliptic curve \( E \) satisfying \( N \leq (\log x)^A \).
We use the following elementary identity
\[
k = \sum_{d | m} \mu(d)
\]
We unfold the sum similarly as in the proof of Theorem 1.1.
\[
\sum_{p \leq x, p \nmid N} d_p = \sum_{p \leq x, p \nmid N} \sum_{d | p} \mu(d) = \sum_{k \leq 2 \sqrt{x}} \sum_{d | k} m(d) \sum_{p \leq x, p \nmid N, k | d_p} 1
\]
We introduce a variable \( y \) and split the sum as shown in the proof of Theorem 1.1. The inequality in the last line is due to the primes \( p \) in \( K \) which have degree 2 over \( \mathbb{Q} \) and split completely in \( K(E[k]) \).
\[
\sum_{p \leq x, p \nmid N} d_p = \pi_E(x; 2) + \sum_{3 \leq k \leq 2 \sqrt{x}} \phi(k) \pi_E(x; k) \\
\leq \frac{2x}{\log x} + \sum_{3 \leq k \leq y} \phi(k) \frac{1}{2} \pi_E(x; k) + \sum_{y < k \leq 2 \sqrt{x}} \phi(k) \pi_E(x; k).
\]
Let $S_1$, $S_2$ denote the second sum and the third sum respectively.

\[
\begin{align*}
S_1 &= \sum_{3 \leq k \leq y} \phi(k) \frac{1}{2} \tilde{\pi}_E(x; k), \\
S_2 &= \sum_{y < k \leq 2\sqrt{x}} \phi(k) \pi_E(x; k).
\end{align*}
\]

Now, we use Lemma 2.5, and 2.7 to give an upper bound for each $\tilde{\pi}_E(x; k)$.

\[
(19) \quad \tilde{\pi}_E(x; k) \leq 2 \frac{t(k)x}{h(kf)} \log \frac{x}{N(f)} \left\{ 1 + O \left( \frac{\log \log 3 \cdot \frac{x}{N(f)}}{\log \frac{x}{N(f)}} \right) \right\}
\]

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

\[
\begin{align*}
S_1 &\ll x \sum_{3 \leq k \leq y} \frac{\phi(k)}{n_k \log \frac{x}{N(f)}}, \\
S_2 &\ll x \sum_{y < k \leq 2\sqrt{x}} \phi(k) \frac{1}{k^2} \ll x \log \frac{\sqrt{x}}{y},
\end{align*}
\]

where the implied constants are absolute. Applying partial summation to $S_1$ with $\phi(k)^2 \ll n_k$, and $\sum_{k \leq t} \frac{1}{\phi(k)} = A_1 \log t + O(1)$, we obtain

\[
(20) \quad S_1 \ll x \log \log \frac{x}{N(f)} \ll A_1 x \log \log x,
\]

provided that $3 \leq \frac{x}{N(f)}$.

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

\[
(21) \quad S_1 + S_2 \ll A_1 x \log \log x
\]

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.

References

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

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

[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

[JW] J. Wu, The Average Exponent of Elliptic Curves Modulo $p$, arXiv preprint arXiv:1205.5929 (2012)

[M] R. Murty, On Artin’s Conjecture, Journal of Number Theory, Vol 16, no.2, April 1983
[TP] T. Freiberg, P. Kurlberg, *On the Average Exponent of Elliptic Curves Modulo $p$*, arXiv preprint [arXiv:1203.4382] (2012)