Title
AVERAGE OF THE FIRST INVARIANT FACTOR OF THE REDUCTIONS OF ABELIAN VARIETIES OF CM TYPE

Author
Kim, Sungjin

Publication Date
2014

Peer reviewed|Thesis/dissertation

University of California
Los Angeles

Average of the First Invariant Factor of the Reductions of Abelian Varieties of CM Type

A dissertation submitted in partial satisfaction
of the requirements for the degree
Doctor of Philosophy in Mathematics

by

Sungjin Kim

2014

Abstract of the Dissertation

Average of the First Invariant Factor of the Reductions of Abelian Varieties of CM Type

by

Sungjin Kim

Doctor of Philosophy in Mathematics

University of California, Los Angeles, 2014

Professor William Duke, Chair

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

$$E(\mathbb{F}_p) \simeq \mathbb{Z}/d_p\mathbb{Z} \oplus \mathbb{Z}/e_p\mathbb{Z} \tag{0.1}$$

with uniquely determined $d_p|e_p$. We give an asymptotic formula for the average order of e_p over primes $p \leq x$ 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 [Wu]. 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.

Then we extend the methods to abelian varieties of CM type. For a field of definition k of an abelian variety $\mathcal{A}$ and prime ideal $\mathfrak{p}$ of k which is of a good reduction for $\mathcal{A}$, the structure of $\mathcal{A}(\mathbb{F}_\mathfrak{p})$ as abelian group is:

$$\mathcal{A}(\mathbb{F}_\mathfrak{p}) \simeq \mathbb{Z}/d_1(\mathfrak{p})\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_g(\mathfrak{p})\mathbb{Z} \oplus \mathbb{Z}/e_1(\mathfrak{p})\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/e_g(\mathfrak{p})\mathbb{Z}, \tag{0.2}$$

where $d_i(\mathfrak{p})|d_{i+1}(\mathfrak{p})$, $d_g(\mathfrak{p})|e_1(\mathfrak{p})$, and $e_i(\mathfrak{p})|e_{i+1}(\mathfrak{p})$ for $1 \leq i < g$.

We use the class field theory and the main theorem of complex multiplication to obtain the average behaviors of $d_1(\mathfrak{p})$ when averaged over primes $\mathfrak{p}$ in k with $N\mathfrak{p} < x$. Due to technical difficulties, some unconditional theorems for elliptic curves are not generalized to abelian varieties with CM. However, those allow us to prove the asymptotic formula for the average order of $e_{\mathfrak{p}}$ for elliptic curves over number fields containing the CM-field.

Finally, for elliptic curves E over $\mathbb{Q}$, the asymptotic density $C_{E,j}$ of primes $p \leq x$ with $d_p = j$ which is given by [C2]:

$$C_{E,j} = \sum_{k=1}^{\infty} \frac{\mu(k)}{[\mathbb{Q}(E[jk]) : \mathbb{Q}]}. \tag{0.3}$$

We prove under an appropriate conditions that these constants are positive.

The dissertation of Sungjin Kim is approved.

Eli Gafni

Chandrashekhar Khare

William Duke, Committee Chair

University of California, Los Angeles

2014

To my wife Michelle Kim.

Table of Contents

Acknowledgments

I would like to thank my wife Michelle Kim for all her support and encouragement. Although she was busy working on her doctor of pharmacy degree, she did not hesitate in cooking and giving emotional support for me. She is the best companion in my life and forever will be the one. I also am grateful to all support from family members. I also would like to thank my advisor Professor William Duke for helpful discussions on my thesis. He gave me numerous insightful comments and gave me directions in my research. He was very patient with me even when I have hard time expressing my thought. I further appreciates committee members Professor Eli Gafni, Professor Terence Tao, and Professor Chandrashekhar Khare. They showed great interests in my thesis and gave their insights and further suggestions on my thesis. I also thank University of California Mathematics Department for securing me financially with numerous teaching opportunities.

Vita

2001–2008	Yonsei University
2007	B.S. (Mathematics) Yonsei University.
2008–present	University of California, Los Angeles.

Publications

Average Behaviors of Invariant Factors in Mordell-Weil Groups of CM Elliptic Curves modulo p, accepted for publication in Finite Field and Their Applications

CHAPTER 1

Introduction

1.1 Average order of e_p

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

$$E(\mathbb{F}_p) \simeq \mathbb{Z}/d_p\mathbb{Z} \oplus \mathbb{Z}/e_p\mathbb{Z} \tag{1.1}$$

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

$$|E(\mathbb{F}_p)| = p + 1 - a_p \tag{1.2}$$

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 $F(x) \leq CG(x)$ 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 $x \geq 2$, there exists a constant $c_E \in (0, 1)$ such that

$$\sum_{p \leq x} e_p = c_E \mathrm{Li}(x^2) + O(x^{19/10}(\log x)^{6/5}) \tag{1.3}$$

under Generalized Riemann Hypothesis(GRH) for the Dedekind zeta functions of the field extensions $\mathbb{Q}(E[k])$ over $\mathbb{Q}$, and

$$\sum_{p\leq x} e_p = c_E \mathrm{Li}(x^2)\left(1+O\left(\frac{\log\log x}{\log^{1/8} x}\right)\right) \tag{1.4}$$

unconditionally when E has complex multiplication(CM). Here, implied constants depends at most on E. (In the summation, we take 0 in place of e_p when E has a bad reduction at p.) More recently, J. Wu [Wu] improved their error terms in both cases

$$\sum_{p\leq x} e_p = c_E \mathrm{Li}(x^2) + O(x^{11/6}(\log x)^{1/3}) \tag{1.5}$$

under GRH, and

$$\sum_{p\leq x} e_p = c_E \mathrm{Li}(x^2) + O(x^2/(\log x)^{9/8}) \tag{1.6}$$

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 [Hu, Theorem 1]. Also, the result is uniform in the conductors of the elliptic curves under consideration.

Theorem 1.1.1. *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 $N \leq (\log x)^A$. Then we have*

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

where

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

1.2 Bounds on the sum of d_p

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

$$\sum_{p\leq x} d_p \ll_E x\sqrt{\log x} \tag{1.7}$$

by applying the number field analogue of Brun-Titchmarsh inequality. (see [HL, Theorem 4]) 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 by applying partial summation.

Theorem 1.2.1. *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 $A > 0$, 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.

Again, if we only consider a fixed CM elliptic curve over a field containing its CM field (in this case, we do not have the conductor restriction), the above formula holds true with implied constant depending on E.

For the lower bound direction, E. Kowalski (see [K]) gives the following unconditional result.

$$\sum_{N\mathfrak{p}\leq x} d_{\mathfrak{p}} \gg_E \frac{x\log\log x}{\log x}.$$

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

$$\frac{x\log\log x}{\log x} = o\left(\sum_{N\mathfrak{p}\leq x} d_{\mathfrak{p}}\right).$$

They also provided a result which is conditional on GRH for Dedekind Zeta functions of

division fields,

$$\sum_{N\mathfrak{p}\leq x} d_{\mathfrak{p}} \gg_E x.$$

On a weaker hypothesis, we have

Theorem 1.2.2. *Let E be a CM elliptic curve over a number field L containing the CM field K. Let χ be any Grossencharacter of L defined modulo a nonzero integral ideal in L. Suppose that there is no zero of $L(s,\chi)$ in the region (3.1) (which we will abbreviate it as NSZC-nonexistence of Siegel-zero condition). Then*

$$\sum_{N\mathfrak{p}\leq x} d_{\mathfrak{p}} \gg_E \frac{x}{\sqrt{\log x}}. \tag{1.8}$$

1.3 Cyclicity Problem in larger number fields

The cyclicity problem asks for the density of primes p of good reduction for E such that $d_p = 1$. Let N be the conductor of elliptic curve E and $\mathfrak{f}(x,E)$ denotes the number of primes $p \leq x$ of good reduction for E such that $d_p = 1$. A. Cojocaru and M. R. Murty obtained that if E is non-CM curve, then

$$\mathfrak{f}(x,E) = C_E \mathrm{Li}(x) + O_N(x^{5/6}(\log x)^{2/3}),$$

under GRH for the Dedekind zeta functions of division fields. For CM curves, they obtained

$$\mathfrak{f}(x,E) = C_E \mathrm{Li}(x) + O_N(x^{3/4}(\log Nx)^{1/2}),$$

under GRH. Unconditional error term in CM case is $O(x\log x)^{-A}$ for any positive A. Precisely, A. Akbary and V. K. Murty obtained

$$\mathfrak{f}(x,E) = C_E \mathrm{Li}(x) + O_{A,B}(x(\log x)^{-A}),$$

for any positive constant A, B, and the $O_{A,B}$ is uniform for $N \leq (\log x)^B$. Here, $C_E = \sum_{k=1}^{\infty} \frac{\mu(k)}{[\mathbb{Q}(E[k]):\mathbb{Q}]}$.

We are able to generalize to CM elliptic curves defined over a number field L containing the CM field K. We state it as a theorem as well. Here, $\mathfrak{f}(x, E)$ is the number of $\mathcal{O}_L$-prime ideals $\mathfrak{p} \leq x$ of good reduction for E such that $d_{\mathfrak{p}} = 1$.

Theorem 1.3.1. *Let E be a CM elliptic curve over a number field L containing the CM field K. Let $A > 0$ be any positive number. Then we have*

$$\mathfrak{f}(x, E) = C_E Li(x) + O_A\left(\frac{x}{\log^A x}\right) \tag{1.9}$$

where

$$C_E = \sum_{k=1}^{\infty} \frac{\mu(k)}{[L(E[k]) : L]}.$$

A difficulty in achieving this theorem is the extra factor that comes from main theorem of complex multiplication. We resolve this issue by using the ray class fields.

1.4 Analogous theorems for abelian varieties of CM type

We are interested in extending previous theorems to abelian variety setting. Let $\mathcal{A}$ be a g-dimensional abelian variety defined over a number field k, and $\mathfrak{p}$ be a prime in k such that $\mathcal{A}$ has a good reduction at $\mathfrak{p}$, and denote the reduction by $\mathcal{A}(\mathbb{F}_{\mathfrak{p}})$. It is known that $\mathcal{A}(\mathbb{F}_{\mathfrak{p}})$ has an abelian group structure

$$\mathcal{A}(\mathbb{F}_{\mathfrak{p}}) \simeq \mathbb{Z}/d_1(\mathfrak{p})\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_g(\mathfrak{p})\mathbb{Z} \oplus \mathbb{Z}/e_1(\mathfrak{p})\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/e_g(\mathfrak{p})\mathbb{Z},$$

where $d_i(\mathfrak{p})|d_{i+1}(\mathfrak{p})$, $d_g(\mathfrak{p})|e_1(\mathfrak{p})$, and $e_i(\mathfrak{p})|e_{i+1}(\mathfrak{p})$ for $1 \leq i < g$. We are interested in finding the statistics of these numbers $d_i(\mathfrak{p})$, and $e_i(\mathfrak{p})$. However, obtaining any general information regarding $d_2(\mathfrak{p})$ through $e_g(\mathfrak{p})$ is out of reach within current methods. We are focused on investigating $d_1(\mathfrak{p})$. By Weil's Riemann Hypothesis for abelian varieties (see [W]), we have

the following upper bound for $d_1(\mathfrak{p})$:

$$d_1(\mathfrak{p})^{2g} \leq |\mathcal{A}(\mathbb{F}_q)| \leq (\sqrt{q}+1)^{2g},$$

where $q = N\mathfrak{p}$.

The cyclicity problem for elliptic curves, concerns about the density of primes p that the reduction of the curve modulo p is cyclic (see [C], [AM]). This is originally proposed by J. P. Serre, and proved under GRH by himself. Then R. Murty gave a general framework for this type of problems. Upon generalization of cyclicity problem to higher dimensional abelian varieties, we have a huge technical difficulties in requiring $\mathcal{A}(\mathbb{F}_q)$ to be cyclic. This could be done by requiring $d_{\mathfrak{p}} = 1$ in $g = 1$ case, but for higher dimensional case, it is clearly not enough to give cyclicity. Instead, we look for the density of primes $\mathfrak{p}$ which $\mathcal{A}(\mathbb{F}_{\mathfrak{p}})$ have $d_1(\mathfrak{p}) = 1$. Applying R. Murty's framework for abelian varieties, A. Akbary and D. Ghioca (see [AG, Theorem 1.4]) obtained the analogous theorem for abelian varieties.

Theorem 1.4.1. *(A. Akbary, D. Ghioca) Let $\mathcal{A}$ be an abelian variety defined over $\mathbb{Q}$, and assume GRH holds for each extension $\mathbb{Q}(\mathcal{A}[m])/\mathbb{Q}$. Then the number of primes $p \leq x$ such that $d_1(p) = 1$ satisfies the asymptotic formula*

$$\sum_{m=1}^{\infty} \frac{\mu(m)}{[\mathbb{Q}(\mathcal{A}[m]) : \mathbb{Q}]} Li(x) + o\left(\frac{x}{\log x}\right). \tag{1.10}$$

We can formulate the obvious analogue for abelian variety defined over a number field k:

The number of prime ideals $\mathfrak{p}$ with $N\mathfrak{p} \leq x$ and $d_1(\mathfrak{p}) = 1$ satisfies

$$\sum_{m=1}^{\infty} \frac{\mu(m)}{[k(\mathcal{A}[m]) : k]} \mathrm{Li}(x) + o\left(\frac{x}{\log x}\right), \tag{1.11}$$

under the assumption of GRH for the extension $k(\mathcal{A}[m])$ over k.

In fact, this can be done by applying [M, page 153, Theorem 1]:

Let K be a number field. Let S be the set of all rational primes. For each $q \in S$, the

extension L_q is normal over K. For square free k, define $L_k = \prod_{q|k} L_q$, $d_k = \mathrm{disc}(L_k/\mathbb{Q})$. Set $L_1 = K$ and $n_k = [L_k : K]$. The [M, page 153, Theorem 1]: states that

Theorem 1.4.2 (Murty)**.** *Suppose that*

$$\sum_{k=1}^{\infty} \frac{\mu^2(k)}{n_k} < \infty,$$

and

(i) we have $\frac{\log |d_k|}{n_k} = O(\log k)$

(ii) the number of prime ideals $\mathfrak{p}$ *in* K*,* $N\mathfrak{p} < x$*, which split completely in some* L_q*,* $q > x^{1/2}/\log x$ *is* $o(x/\log x)$*.*

Suppose further that the Generalized Riemann Hypothesis (GRH) is true for each of the Dedekind zeta functions $\zeta(s, L_k)$*. Then the number* $f(x, K)$ *of prime ideals* $\mathfrak{p}$ *with* $N\mathfrak{p} < x$ *which does not split completely in any* L_q*,* $q \in S$ *satisfies*

$$f(x, K) = C(K)x/\log x + o(x/\log x)$$

as $x \to \infty$*. The constant* $C(K)$ *satisfies*

$$C(K) = \sum_{k=1}^{\infty} \frac{\mu(k)}{n_k}.$$

For a justification of (1.11), we have (i) by Proposition 3.2.1, and GRH is assumed. Thus, we need to check (ii) for the prime ideals under consideration. By (2.4), we have $q < \sqrt{x}+1$. Since $\mathfrak{p}$ split completely in some L_q with $q > x^{1/2}/\log x$. Let $p^{f_p} = N\mathfrak{p}$ where p is the rational prime lying under $\mathfrak{p}$. Since we have $N\mathfrak{p} < x$, rational primes with inertia degree ≥ 2 contribute to $O(x^{1/2})$ which is $o(x/\log x)$. Thus, it is enough to consider primes in K of inertial degree 1 that lie above rational prime p. Let $\mathfrak{b}$ be a prime ideal in L_q lying above $\mathfrak{p}$. Then the inertia degree of $\mathfrak{b}/p$ is 1 since $\mathfrak{p}$ splits completely in L_q. Then the rational prime p has inertia degree 1 in $\mathbb{Q}(\zeta_q)$ as well. Since $L_q \supseteq \mathbb{Q}(\zeta_q)$, it follows that $p \equiv 1 \pmod{q}$. By

the Brun-Titchmarch theorem, we obtain (ii) with bound of $O(x \log\log x/\log^2 x)$.

To avoid notational complication, every summation over prime ideals $\mathfrak{p}$ that we write will be the summation over only primes of good reduction for the abelian variety $\mathcal{A}$. Necessary notations such as CM-type or $(K, \Phi, \mathfrak{a})$ are introduced in the chapter 2. As in the elliptic curve cases, we expect the unconditional result in CM case. (see [AM, Theorem 1.1]):

Conjecture 1.4.1. *Let $\mathcal{A}$ be an abelian variety of CM type $(K, \Phi, \mathfrak{a})$ of dimension g defined over a number field k. Then for any $B > 0$,*

$$\sum_{\substack{N\mathfrak{p}\leq x \\ d_1(\mathfrak{p})=1}} 1 = c_{\mathcal{A}} Li(x) + O_{\mathcal{A},B}\left(\frac{x}{\log^B x}\right), \tag{1.12}$$

where

$$c_{\mathcal{A}} = \sum_{m=1}^{\infty} \frac{\mu(m)}{[k(\mathcal{A}[m]) : k]}.$$

A motivation of this conjecture is the change of order of summation:

$$\begin{aligned}\sum_{N\mathfrak{p}\leq x} \sum_{m|d_1(\mathfrak{p})} \mu(m) &= \sum_{m\leq\sqrt{x}+1} \mu(m) \sum_{\substack{N\mathfrak{p}\leq x \\ m|d_1(\mathfrak{p})}} 1 \\ &= \sum_{m\leq\sqrt{x}+1} \mu(m)\pi_{\mathcal{A}}(x; m).\end{aligned}$$

Applying the number field analogue of Brun-Titchmarsh inequality due to J. Hinz and M. Lodemann [HL, Theorem 4], we obtain a bound for $\pi_A(x; m)$.

$$\pi_{\mathcal{A}}(x; m) \ll \frac{x}{[k(\mathcal{A}[m]) : k]}, \tag{1.13}$$

provided that $2N(mf) < x$, and the implied constant depends on $\mathcal{A}$.

Thus, this bound is only applicable for small values of m. As [AG] pointed out, the main difficulty is to deal with large values of m, in which we do not know how to obtain such bound when m is close to $\sqrt{x}$. Even when we assume GRH for Dedekind zeta functions of

division fields, we do not have a uniform bound that controls the case $m \sim \sqrt{x}$. What we obtain an asymptotic in short range instead of Conjecture 1.0.1:

Theorem 1.4.3. *Let $\mathcal{A}$ be an absolutely simple abelian variety of CM type $(K, \Phi, \mathfrak{a})$ of dimension g defined over a number field k, and (K', Φ') be its reflex type with $[K' : \mathbb{Q}] = 2g'$. Let $[k : \mathbb{Q}] = 2l \geq 2g'$. Then there exists a constant c depending only on $\mathcal{A}$ such that for any $B > 0$,*

$$\sum_{m<cx^{\frac{1}{2l}}} \mu(m)\pi_{\mathcal{A}}(x;m) = c_{\mathcal{A}} Li(x) + O_{\mathcal{A},B}\left(\frac{x}{\log^B x}\right), \tag{1.14}$$

where

$$c_{\mathcal{A}} = \sum_{m=1}^{\infty} \frac{\mu(m)}{[k(\mathcal{A}[m]) : k]}.$$

Since $\mathcal{A}$ is of CM-type, we actually have

$$\pi_{\mathcal{A}}(x;m) \ll \frac{x^g}{m^{2g}}, \tag{1.15}$$

for all $m \leq \sqrt{x}+1$. As it was pointed out by [AG, (4.5)], we are able to use the above when $m > x^{\frac{g}{2g+1}} \log^{\frac{1}{2g+1}} x$. Under GRH for Dedekind zeta functions of division fields, we can deal with the sum over $m \leq x^{\frac{g}{2g+1}} \log^{\frac{1}{2g+1}} x$ easily. Thus, we see that Conjecture 1.4.1 and 1.4.2 are true under GRH for Dedekind zeta functions of division fields with better error terms. The proof is outlined also in [V].

Similarly for the averaging problem, we expect that

Conjecture 1.4.2. *Let $\mathcal{A}, (K, \Phi), (K', \Phi'), k$ be the same notations as above. Under the same hypotheses as in Theorem 1.0.7, for any positive B, we have*

$$\sum_{N\mathfrak{p}\leq x} \frac{1}{d_1(\mathfrak{p})} = \sum_{m=1}^{\infty} \frac{1}{[k(\mathcal{A}[m]) : k]} \sum_{de=m} \frac{\mu(d)}{e} Li(x) + O_{\mathcal{A},B}\left(\frac{x}{\log^B x}\right).$$

A motivation of this conjecture is as before, the change of order of summation:

$$\sum_{N\mathfrak{p}\leq x}\frac{1}{d_1(\mathfrak{p})}=\sum_{N\mathfrak{p}\leq x}\sum_{de|d_1(\mathfrak{p})}\frac{\mu(d)}{e}$$
$$=\sum_{m\leq\sqrt{x}+1}\sum_{de=m}\frac{\mu(d)}{e}\sum_{\substack{N\mathfrak{p}\leq x\\ m|d_1(\mathfrak{p})}}1=\sum_{m\leq\sqrt{x}+1}\sum_{de=m}\frac{\mu(d)}{e}\pi_{\mathcal{A}}(x;m).$$

Here, we are able to only obtain short range summation:

Theorem 1.4.4. *Let $\mathcal{A},(K,\Phi),(K',\Phi'),k,g,g',l$ be the same notations as above. Under the same hypotheses as in Theorem 1.4.3, for any positive B, there is a positive constant c depending only on $\mathcal{A}$ such that*

$$\sum_{m<cx^{\frac{1}{2l}}}\sum_{de=m}\frac{\mu(d)}{e}\pi_{\mathcal{A}}(x;m)=\sum_{m=1}^{\infty}\frac{1}{[k(\mathcal{A}[m]):k]}\sum_{de=m}\frac{\mu(d)}{e}Li(x)+O_{\mathcal{A},B}\left(\frac{x}{\log^B x}\right).$$

We turn our interest to the average behavior of $d_{\mathfrak{p}}$. Now, we consider the case $g\geq 2$. By Lemma 2.3.5, we have the convergence of

$$C_{\mathcal{A}}=\sum_{m=1}^{\infty}\frac{\phi(m)}{[k(\mathcal{A}[m]):k]}.$$

In fact, the convergence of this constant is the major difference between $g=1$ (CM elliptic curves) and $g\geq 2$. (abelian varieties of CM type) Since we do not have the estimate (1.13), obtaining similar bound as in Theorem 1.1.2 is still out of reach with current method. The strength of further hypothesis such as GRH or NSZC, is very little here(does not affect the main estimates), compared to $g=1$ case where we had stronger lower bounds with bigger order of magnitude. As before, we conjecture an upper bound result, and prove unconditional upper bound of shorter range sum, and finally unconditional lower bound:

Conjecture 1.4.3. *Let $\mathcal{A},(K,\Phi),(K',\Phi'),k$ be the same notations as above. Under the*

same hypotheses as in Theorem 1.0.7, for any positive B,

$$\sum_{N\mathfrak{p}\leq x} d_1(\mathfrak{p}) = C_{\mathcal{A}} Li(x) + O_{\mathcal{A},B}\left(\frac{x}{\log^B x}\right). \tag{1.16}$$

Theorem 1.4.5. *Let $\mathcal{A}, (K,\Phi), (K',\Phi'), k, g, g', l$ be the same notations as above. Under the same hypotheses as in Theorem 1.4.3, for any positive B, there exists a positive constant c depending on $\mathcal{A}$, such that for any $B > 0$,*

$$\sum_{m\leq cx^{\frac{1}{2l}}} \phi(m)\pi_{\mathcal{A}}(x;m) = C_{\mathcal{A}} Li(x) + O_{\mathcal{A},B}\left(\frac{x}{\log^B x}\right). \tag{1.17}$$

Theorem 1.4.6. *Let $\mathcal{A}, (K,\Phi), (K',\Phi'), k$ be the same notations as above. Under the same hypotheses as in Theorem 1.4.3, for any positive B,*

$$\sum_{N\mathfrak{p}\leq x} d_1(\mathfrak{p}) \geq C_{\mathcal{A}} Li(x) + O_{\mathcal{A},B}\left(\frac{x}{\log^B x}\right). \tag{1.18}$$

This is a direct consequence of Theorem 1.4.5:

$$\sum_{N\mathfrak{p}\leq x} d_1(\mathfrak{p}) = \sum_{m<\sqrt{x}+1} \phi(m)\pi_{\mathcal{A}}(x;m) \geq \sum_{m\leq cx^{\frac{1}{2l}}} \phi(m)\pi_{\mathcal{A}}(x;m) = C_{\mathcal{A}}\mathrm{Li}(x) + O_{\mathcal{A},B}\left(\frac{x}{\log^B x}\right).$$

We remark that the Conjecture 1.4.1, 1.4.2 are true with stronger error term under GRH for the Dedekind zeta function of division fields, and it can be generalized to:

Theorem 1.4.7. *Let $\mathcal{A}$ be an absolutely simple abelian variety of CM type $(K,\Phi,\mathfrak{a})$ of dimension g defined over a number field k, and (K',Φ') be its reflex type with $[K':\mathbb{Q}] = 2g'$. Let $[k:\mathbb{Q}] = 2l \geq 2g'$. Let $f : \mathbb{N} \longrightarrow \mathbb{C}$ be an arithmetic function satisfying*

$$f(m) = O(m^{\alpha}),$$

with $0 < \alpha < \frac{1}{2g-1}$. *Assume GRH for the Dedekind zeta function of division fields, then*

$$\sum_{m \leq \sqrt{x}+1} f(m)\pi_{\mathcal{A}}(x;m) = c_{f,\mathcal{A}} Li(x) + O_{\mathcal{A},\epsilon}(x^{\frac{4g+2g\alpha-\alpha-1}{4g}} + \epsilon). \tag{1.19}$$

where

$$c_{f,\mathcal{A}} = \sum_{m=1}^{\infty} \frac{f(m)}{[k(\mathcal{A}[m]) : k]}.$$

We also remark that the theorems 1.4.3, 1.4.4, and 1.4.5 can be generalized to the following:

Theorem 1.4.8. *Let* $\mathcal{A}$ *be an absolutely simple abelian variety,*$(K, \Phi), (K', \Phi'), k$ *be the its CM-type, reflex type, and field of definition respectively. Let* $[K : \mathbb{Q}] = 2g$, $[K' : \mathbb{Q}] = 2g'$, *and* $[k : \mathbb{Q}] = 2l \geq 2g'$. *Let* $f : \mathbb{N} \longrightarrow \mathbb{C}$ *be an arithmetic function satisfying the growth condition:*

$$f(m) = O(m^{\alpha}),$$

for some $\alpha < 2$. *Then there exists a constant* $c > 0$ *depending only on* $\mathcal{A}$ *such that for any* $B > 0$,

$$\sum_{m < cx^{\frac{1}{2l}}} f(m)\pi_{\mathcal{A}}(x;m) = c_{f,\mathcal{A}} Li(x) + O_{\mathcal{A},B}\left(\frac{x}{\log^B x}\right), \tag{1.20}$$

where

$$c_{f,\mathcal{A}} = \sum_{m=1}^{\infty} \frac{f(m)}{[k(\mathcal{A}[m]) : k]}.$$

A natural question on the constant $c_{\mathcal{A},k} = \sum_{m=1}^{\infty} \frac{\mu(m)}{[k(\mathcal{A}[m]):k]}$ is whether we can determine the sign of it. In general, this is a very difficult problem because of $\mu(m)$. Assume GRH for the division fields $k(\mathcal{A}[m])$ over k. Let k_0 be a finite extension of the field of definition k. Assume also GRH for the division fields $k_0(\mathcal{A}[m])$ over k_0 and let $c_{\mathcal{A},k_0} = \sum_{m=1}^{\infty} \frac{\mu(m)}{[k_0(\mathcal{A}[m]):k_0]}$. Then the constants $c_{\mathcal{A},k}$ and $c_{\mathcal{A},k_0}$ are related by an inequality $c_{\mathcal{A},k} \geq \frac{1}{[k_0:k]} c_{\mathcal{A},k_0}$. We prove

this using (1.11). The number of primes $\mathfrak{p}$ in k with $N\mathfrak{p} \leq x$ and $d_1(\mathfrak{p}) = 1$ is

$$\sum_{m=1}^{\infty} \frac{\mu(m)}{[k(\mathcal{A}[m]) : k]} \mathrm{Li}(x) + o\left(\frac{x}{\log x}\right).$$

We provide a subset of those primes which has positive density. Consider the finite extension k_0, then the number of primes $\mathcal{P}$ in k_0 with $N\mathcal{P} \leq x$ and $d_1(\mathcal{P}) = 1$ is

$$\sum_{m=1}^{\infty} \frac{\mu(m)}{[k_0(\mathcal{A}[m]) : k_0]} \mathrm{Li}(x) + o\left(\frac{x}{\log x}\right)$$

Consider a prime $\mathfrak{p}$ in k that lies below $\mathcal{P}$. Since $\mathcal{A}(\mathcal{O}_k/\mathfrak{p})$ forms a subgroup of $\mathcal{A}(\mathcal{O}_{k_0}/\mathcal{P})$ which is fixed by Frobenious automorphism, it follows that

$$d_1(\mathcal{P}) = 1 \text{ implies } d_1(\mathfrak{p}) = 1.$$

Therefore, the correspondence $\mathcal{P} \mapsto \mathfrak{p}$ gives "(at most $[k_0 : k]$)-to-one" mapping. Hence the set $\{N\mathfrak{p} \leq x \mid d_1(\mathfrak{p}) = 1\}$ contains a subset of size at least

$$\frac{1}{[k_0 : k]} \sum_{m=1}^{\infty} \frac{\mu(m)}{[k_0(\mathcal{A}[m]) : k_0]} \mathrm{Li}(x) + o\left(\frac{x}{\log x}\right).$$

This proves the following theorem:

Theorem 1.4.9. *Let $\mathcal{A}, (K, \Phi), (K', \Phi'), k$ be the same notations as above, and k_0 be a finite extension of k. Assume GRH for Dedekind zeta functions of division fields $k(\mathcal{A}[m])$ over k, and $k_0(\mathcal{A}[m])$ over k_0. Then we have*

$$\sum_{m=1}^{\infty} \frac{\mu(m)}{[k(\mathcal{A}[m]) : k]} \geq \frac{1}{[k_0 : k]} \sum_{m=1}^{\infty} \frac{\mu(m)}{[k_0(\mathcal{A}[m]) : k_0]}.$$

It will be an interesting problem to look for unconditional proof of this.

A difficulty in achieving Conjectures 1.4.1, 1.4.2, and 1.4.3 is an insufficient information on $\pi_{\mathcal{A}}(x; (mf), \mathfrak{a}_i)$ where $N(mf) > x/2$. However, it is possible to achieve some information

on the numbers $t(m)$ in Lemma 2.3.7 on average in special cases:

Theorem 1.4.10. *Let $\mathcal{A}$ be an absolutely simple abelian variety of dimension 2 defined over a degree 4 CM-field (which is a quadratic extension of an imaginary quadratic field), with CM-type $(K, \Phi, \mathfrak{a})$. Suppose that the reflex type $(K', \Phi', \mathfrak{a}')$ satisfies $K = K'$. Then we have*

$$\sum_{m<\sqrt{x}} t(m) \ll_K x \exp(-\frac{1}{6}(\log x)^{2/5}).$$

The significance in this theorem is that this opens up a possibility of proving a special case $g = 2$ of Conjecture 1.4.1 unconditionally. If we are able to prove

$$\pi_{\mathcal{A}}(x; (mf), \mathfrak{a}_i) \ll_K (\log x)^B$$

for some positive absolute constant B in the case $N(mf) > x/2$, then this would provide an unconditional proof of Conjecture 1.4.1 under the hypotheses of Theorem 1.4.10.

1.5 Positivity Conditions for Rational Elliptic Curves

A. Cojocaru obtained the density of primes p of good reduction for E such that $d_p = j$ for $j > 1$. (see [C2]) It is

$$C_{E,j} = \sum_{k=1}^{\infty} \frac{\mu(k)}{[\mathbb{Q}(E[jk]) : \mathbb{Q}]},$$

under GRH for the Dedekind zeta functions of division fields. For CM curves, it can be shown unconditionally. The positivity of $C_E = \sum \frac{\mu(k)}{[\mathbb{Q}(E[k]):\mathbb{Q}]}$ in non-CM case is achievable under GRH, and it can be done unconditionally in CM case.

However, it was not known whether $C_{E,j} > 0$ for some $j > 1$. In this note, we obtain the positivity under appropriate conditions.

Theorem 1.5.1. *Let E be a non-CM elliptic curve over $\mathbb{Q}$, and N the conductor of E. Let $A(E)$ be the associated Serre's constant. Suppose also that $\mathbb{Q}(E[2]) \neq \mathbb{Q}$. Let $j > 1$ and*

$(j, 2NA(E)) = 1$. *If we assume GRH for division fields, we have* $C_{E,j} > 0$.

The prime 2 requires a special care, for an elliptic curve $y^2 = x^3 + ax + b$ defined over $\mathbb{Q}$, let K_2 be a quadratic or cubic subfield of $\mathbb{Q}(E[2])$. Precisely, K_2 is defined as follows,

$$K_2 = \begin{cases} \mathbb{Q}(\sqrt{-4a^3 - 27b^3}) & \text{if } [\mathbb{Q}(E[2]) : \mathbb{Q}] = 2, \text{ or } 6 \\ \mathbb{Q}(\alpha) & \text{if } [\mathbb{Q}(E[2]) : \mathbb{Q}] = 3. \end{cases}$$

where α is a root of $x^3 + ax + b = 0$ in $\overline{\mathbb{Q}}$.

Theorem 1.5.2. *Let* E *be an elliptic curve over* $\mathbb{Q}$ *which has CM by the full ring of integers* $\mathcal{O}_K$ *in an imaginary quadratic field* K. *Let* N *be the conductor of* E. *Suppose that* $K_2 \neq K$. *Let* $(j, 6N) = 1$. *Then* $C_{E,j} > 0$.

CHAPTER 2

Algebraic Background

2.1 Elliptic Curves

2.1.1 Structure of Reductions modulo $\mathfrak{p}$

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

$$E(\mathbb{F}_p) \simeq \mathbb{Z}/d_p\mathbb{Z} \oplus \mathbb{Z}/e_p\mathbb{Z}. \tag{2.1}$$

with $d_p | e_p$.

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 $[\mathbb{Q}(E[k]) : \mathbb{Q}]$. To prove (2.1), we consider the structure of $E[k]$ (see [Si, p86, Corollary 6.4]).

Proposition 2.1.1. *Let E be an elliptic curve over a field K and let $m \in \mathbb{Z}$ with $m \neq 0$.*

(a) If $m \neq 0$ in K, i.e. , if either $char(K) = 0$ or $p = char(K) > 0$ and $p \nmid m$, then

$$E[m] = \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}.$$

(b) If $char(K) = p > 0$, then one of the following is true:

(i) $E[p^e] = \{O\}$ for all $e = 1, 2, 3 \cdots$.

(ii) $E[p^e] = \mathbb{Z}/p^e\mathbb{Z}$ for all $e = 1, 2, 3 \cdots$.

The case that we are interested is (a). Together with the fact that $E(\mathbb{F}_p)$ is finite, we see that the following is true

$$E(\mathbb{F}_p) \subset E[m] = \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z},$$

which proves (2.1).

Analogous statement for (2.1) for abelian varieties is as follows. Let $\mathcal{A}$ be a g-dimensional abelian variety defined over a number field k, and $\mathfrak{p}$ be a prime in k such that $\mathcal{A}$ has a good reduction at $\mathfrak{p}$, and denote the reduction by $\mathcal{A}(\mathbb{F}_\mathfrak{p})$. Then $\mathcal{A}(\mathbb{F}_\mathfrak{p})$ has an abelian group structure

$$\mathcal{A}(\mathbb{F}_\mathfrak{p}) \simeq \mathbb{Z}/d_1(\mathfrak{p})\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_g(\mathfrak{p})\mathbb{Z} \oplus \mathbb{Z}/e_1(\mathfrak{p})\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/e_g(\mathfrak{p})\mathbb{Z}, \tag{2.2}$$

where $d_i(\mathfrak{p})|d_{i+1}(\mathfrak{p})$, $d_g(\mathfrak{p})|e_1(\mathfrak{p})$, and $e_i(\mathfrak{p})|e_{i+1}(\mathfrak{p})$ for $1 \leq i < g$

Another useful fact about primes of good reduction for abelian varieties is given in the following proposition. (see [ST, Theorem 1])

Proposition 2.1.2 (Neron-Ogg-Shafarevic)**.** *Let $\mathcal{A}$ be an abelian variety over K. Suppose that the residue field k of v is perfect. Then the following properties are equivalent:*

(a) $\mathcal{A}$ has a good reduction at v.

(b) $A_m = Hom(\mathbb{Z}/m\mathbb{Z}, A(K_s))$ is unramified at v for all m prime to $char(k)$.

Let $\mathcal{A}$ be an abelian variety over a number field k. Denote $\mathcal{A}[m]$ the m-torsion points of $\mathcal{A}(\overline{k})$. Then we have the following corollary which can be obtained from (b) of the above proposition:

Corollary 2.1.1. *If $\mathfrak{p} \subset k$ is a prime of good reduction for $\mathcal{A}$, and $(m, N\mathfrak{p}) = 1$. Then $\mathfrak{p}$ is unramified in the division field $k(\mathcal{A}[m])$.*

An elliptic curve E over $\mathbb{Q}$ has its reduction modulo p for each rational prime p. By the Riemann Hypothesis for varieties (also known as Weil's Conjectures, see [W], also [Si, p142,

Theorem 2.3.1]). Then we have

$$|E(\mathbb{F}_p)| = p + 1 - a_p \tag{2.3}$$

with $|a_p| < 2\sqrt{p}$.

For abelian varieties, the Riemann Hypothesis for varieties gives

$$(\sqrt{q} - 1)^{2g} \leq |\mathcal{A}(\mathbb{F}_q)| \leq (\sqrt{q} + 1)^{2g}, \tag{2.4}$$

where $q = N\mathfrak{p}$.

The following lemma shows the relation between residue field extension and division fields (see [AGP, Lemma 2.3]):

Lemma 2.1.1. *Let (K, v) be a discrete valued field, A/K an abelian extension with good reduction at v, n an integer coprime to the residue characteristic of v, $L = K(\mathcal{A}[n])$ and w an extension of v to L. Denote the residue field of v (resp. w) by $k(v)$ (resp. $k(w)$). Let $\mathcal{A}_v/k(v)$ be the reduction of A at v. Then $k(w) = k(v)(\mathcal{A}_v[n])$.*

Proof. The result is also valid when K is a number field, since we can replace K by K_v. This lemma is an another interpretation of [ST, Lemma 2], since v is unramified in $K(\mathcal{A}[n])$ by Neron-Ogg-Shafarevic. Thus, L equals the fixed field of inertia group $I(w/v)$, and the reduction map $r : \mathcal{A}(L) \longrightarrow \mathcal{A}_w(k(w))$ defines a homomorphism

$$\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathcal{A}(L)) \longrightarrow \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathcal{A}_w(k(w))),$$

which is proven to be an isomorphism by [ST, Lemma 2]. Furthermore, this isomorphism commutes with the decomposition group $D(w/v) = G_{k(w)/k(v)}$. This completes the proof of this lemma. □

The following lemma can be deduced from above, and it will be used frequently. (see [M, p. 159, Lemma 2])

Lemma 2.1.2. *Let $\mathcal{A}$ be an abelian variety defined over a number field k, and $\mathfrak{p} \subset k$ be a prime of good reduction for $\mathcal{A}$, and $\mathfrak{p} \nmid m$. Then*

$$m \mid d_1(\mathfrak{p}) \Leftrightarrow \mathfrak{p} \text{ splits completely in } k(\mathcal{A}[m]).$$

Proof. We look at the reduced variety $\mathcal{A}_\mathfrak{p}$ over $\mathbb{F}_\mathfrak{p}$. Let $\pi_\mathfrak{p}$ be the Frobenious endomorphism of $\mathbb{F}_\mathfrak{p}$ given by $\pi_\mathfrak{p}(x) = x^{N\mathfrak{p}}$, then $\pi_\mathfrak{p} : \mathcal{A}_\mathfrak{p} \longrightarrow \mathcal{A}_\mathfrak{p}$ is a homomorphism and $\ker(\pi_\mathfrak{p} - 1) = \mathcal{A}_\mathfrak{p}$. Hence, $\mathcal{A}_\mathfrak{p}$ contains $\mathbb{Z}/m\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m\mathbb{Z}(2g \text{ summands})$ if and only if $\pi_\mathfrak{p}$ is trivial on $\mathcal{A}_\mathfrak{p}[m]$. By Lemma 2.1.1, the decomposition group $D(\mathfrak{q}/\mathfrak{p})$ for prime $\mathfrak{q} \subset k(\mathcal{A}[m])$ lying over $\mathfrak{p}$ is identical to the cyclic group generated by the generator $\pi_\mathfrak{p}$ of $G_{\mathbb{F}_\mathfrak{p}(\mathcal{A}_\mathfrak{p}[m])/\mathbb{F}_\mathfrak{p}}$. Then $\mathcal{A}_\mathfrak{p}$ contains $\mathbb{Z}/m\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m\mathbb{Z}$ if and only if $D(\mathfrak{q}/\mathfrak{p})$ is trivial. □

2.1.2 Weil Paring

Let E/K be an elliptic curve. Let $m \geq 2$ be an integer coprime to $\mathrm{char}(K)$. Then by Proposition 2.1.1,

$$E[m] \simeq \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}.$$

Choosing a basis $\{T_1, T_2\}$ for $E[m]$, a determinant paring for $P, Q \in E[m]$ can be defined:

$$E[m] \longrightarrow \mathbb{Z}/m\mathbb{Z}, \quad (P, Q) \mapsto \det(P, Q) = \det \begin{pmatrix} a & c \\ b & d \end{pmatrix},$$

where $P = aT_1 + bT_2$, and $Q = cT_1 + dT_2$. However, this is not Galois invariant.

Using a primitive m-th root of unity ζ_m, and define

$$e_m : E[m] \times E[m] \longrightarrow \mu_m, \quad (P, Q) \mapsto \zeta_m^{\det(P,Q)}.$$

This non-degenerate paring e_m is called Weil paring. (see [Si, p. 94]) An important property of e_m is Galois invariance:

$$e_m(P^\sigma, Q^\sigma) = e_m(P, Q)^\sigma,$$

for any $\sigma \in G_{\overline{K}/K}$.

On abelian variety $\mathcal{A}$ of dimension g, Weil paring is similarly defined:

$$e_{\mathcal{A},m} : \mathcal{A}[m]^{2g} \longrightarrow \mu_m, \quad (P_1, P_2, \cdots, P_{2g}) \mapsto \zeta_m^{\det(P_1, P_2, \cdots, P_{2g})}.$$

Also, this is non-degenerate and Galois invariant. This allows a proof of the following lemma:

Lemma 2.1.3. *(An Extension of [GM, Lemma 2]) Let k be a number field. Let $\mathcal{A}/k$ be an abelian variety of dimension g, and $m \geq 2$ be an integer. Then*

$$k(\zeta_m) \subset k(\mathcal{A}[m]).$$

Proof. Let $\sigma \in G_{\overline{k}/k(\mathcal{A}[m])}$, and $P_1, \cdots, P_{2g} \in \mathcal{A}[m]$ such that $e_{\mathcal{A},m}(P_1, \cdots, P_{2g}) = \zeta_m$ (This is possible because $e_{\mathcal{A},m}$ is non-degenerate). Then

$$e_{\mathcal{A},m}(P_1^\sigma, \cdots, P_{2g}^\sigma) = e_{\mathcal{A},m}(P_1, \cdots, P_{2g})^\sigma$$

by Galois invariance. We see that $P_i^\sigma = P_i$ for each i. Thus,

$$e_{\mathcal{A},m}(P_1, \cdots, P_{2g})^\sigma = e_{\mathcal{A},m}(P_1, \cdots, P_{2g}).$$

This yields $\zeta_m^\sigma = \zeta_m$. Therefore, we have $G_{\overline{k}/k(\mathcal{A}[m])} \subset G_{\overline{k}/k(\zeta_m)}$. Equivalently, by Galois theory, $k(\zeta_m) \subset k(\mathcal{A}[m])$. □

2.2 Class Field Theory

2.2.1 Main Theorem

We use the main theorem of global class field theory. Before stating the theorem, we list notations for basic objects. (We follow some notations in Neukirch [N])

$\mathbb{A}_k^\times$ The group of ideles over k.

$C_k = \mathbb{A}_k^\times / k^\times$ The idele class group over k.

J_k The group of fractional ideals of k

$$U_{k,\mathfrak{p}}^{(n_\mathfrak{p})} = \begin{cases} 1 + \mathfrak{p}^{n_\mathfrak{p}} & \text{if } \mathfrak{p} \text{ is finite,} \\ \mathbb{R}_+^\times \subset \mathbb{R}^\times & \text{if } \mathfrak{p} \text{ is real,} \\ \mathbb{C}^\times & \text{if } \mathfrak{p} \text{ is complex.} \end{cases} \quad \text{The basic open sets in } \mathbb{A}_k^\times$$

Let $\mathfrak{m} = \mathfrak{m}_{\text{fin}}\mathfrak{m}_\infty$ be a modulus, where $\mathfrak{m}_{\text{fin}}$ is a proper fractional ideal of k, and $\mathfrak{m}_\infty$ is a product of real embeddings of k.

$U_{k,\mathfrak{m}} = \{s \in \mathbb{A}_k^\times | s_\mathfrak{p} \equiv 1 \pmod{\mathfrak{m}_{\text{fin}}} \text{ for all finite } \mathfrak{p}, \text{ and } s_\nu > 0 \text{ for real embeddings } \nu | \mathfrak{m}_\infty\}$

Given $\alpha_\mathfrak{p} \in k_\mathfrak{p}^\times$ we write

$$\alpha_\mathfrak{p} \equiv 1 \pmod{\mathfrak{p}^{n_\mathfrak{p}}} \Leftrightarrow \alpha_\mathfrak{p} \in U_{k,\mathfrak{p}}^{(n_\mathfrak{p})}.$$

$C_k^\mathfrak{m} = I_k^\mathfrak{m} k^\times / k^\times$, where $I_k^\mathfrak{m} = \prod_\mathfrak{p} U_{k,\mathfrak{p}}^{(n_\mathfrak{p})}$, and $\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{p}^{n_\mathfrak{p}}$.

The $C_k^\mathfrak{m}$ is called the congruence subgroup, and $C_k / C_k^\mathfrak{m}$ is called the ray class group modulo $\mathfrak{m}$.

$J_k^\mathfrak{m}$ The group of fractional ideals prime to $\mathfrak{m}$.

$P_k^\mathfrak{m}$ The group of principal ideals (a) such that $a \equiv 1 \pmod{\mathfrak{m}}$, and a is totally positive.

$C_\mathfrak{m}(k) = J_k^\mathfrak{m} / P_k^\mathfrak{m}$ The $\mathfrak{m}$-ideal class group.

Then the following proposition binds the ideal theoretic and idele theoretic view points together.

Proposition 2.2.1. *The homomorphism*

$$() : \mathbb{A}_k^\times \longrightarrow J_k, \quad \alpha \mapsto (\alpha) = \prod_{\mathfrak{p} \nmid \infty} \mathfrak{p}^{\nu_\mathfrak{p}(\alpha_\mathfrak{p})}$$

induces an isomorphism

$$C_k / C_k^\mathfrak{m} \simeq J_k^\mathfrak{m} / P_k^\mathfrak{m}$$

The following theorem is considered as the main theorem of class field theory, it corresponds all finite abelian extension of a number field k to closed subgroups of finite index in C_k.

Theorem 2.2.1 (Main Theorem of Class Field Theory)**.** *Let k be a number field. Then the following mapping gives an inclusion reversing one-to-one correspondence between finite abelian extensions L/k and the closed subgroups of finite index in C_k:*

$$L \mapsto N_{L|k}C_L,$$

where $N_{L|k} : \mathbb{A}_L^\times \longrightarrow \mathbb{A}_k^\times$ is the norm map.

This correspondence also gives an isomorphism:

$$\mathrm{Gal}(L/k) \simeq C_k/N_{L|k}C_L.$$

For any closed subgroup $\mathcal{N}$ of C_k which has finite index in it, the above correspondence gives a finite abelian extension L/k such that $N_{L|k}C_L = \mathcal{N}$. In particular, there is a finite abelian extension $k_\mathfrak{m}/k$ corresponding to the congruence group $C_k^\mathfrak{m}$. This $k_\mathfrak{m}$ is called the ray class field modulo $\mathfrak{m}$.

To understand finite abelian extension of a number field k, it is enough to investigate the ray class fields via the following lemma.

Lemma 2.2.1. *Let k be a number field and L be a finite abelian extension of k. Then the corresponding group $N_{L|k}C_L$ contains a congruence group $C_k^\mathfrak{m}$ for some fractional ideal $\mathfrak{m} \subset k$. Consequently, it follows by the correspondence theorem that*

$$L \subset k_\mathfrak{m}.$$

This lemma works for general finite abelian extensions of k, but it is difficult to find $\mathfrak{m}$ explicitly in terms of L. However, we will do this for $L = k(\mathcal{A}[m])$ where $\mathcal{A}$ is an abelian

variety defined over k and admits a complex multiplication. See Section 2.3.2 for details.

Another important theorem in class field theory is Artin's reciprocity law, we state an idelic version of this. (see [Si2, p120, Theorem 3.5])

Theorem 2.2.2. *Let k be a number field, and let k^{ab} be the maximal abelian extension of K. There exists a unique continuous homomophism*

$$\mathbb{A}_k^\times \longrightarrow Gal(k^{ab}/k), \quad s \mapsto [s,k],$$

with the following property:

- *If L is a finite abelian extension of k, then*

$$[s,k]|_L = ((s), L/k).$$

Here $(\cdot, L/k)$ is the Artin map, and $Gal(k^{ab}/k)$ is given the profinite topology.

- *$k^\times$ is contained in its kernel.*
- *The reciprocity map is compatible with norm map:*

$$[s,L]|_{k^{ab}} = [N_k^L s, k] \quad \textit{for all } s \in \mathbb{A}_L^\times.$$

The correspondence theorem is compatible with Artin map by the following relations:

Theorem 2.2.3. *Let $\mathcal{F}$ be the set of all finite abelian extension of k inside $\overline{k}$, $\mathcal{G}$ be the set of all closed subgroups of finite index in $\mathbb{A}_k^\times/k^\times$, and $\mathcal{H}$ be the set of all closed subgroups of finite index in $Gal(k^{ab}/k)$. Then we have the following:*

$$\mathcal{F} \xrightarrow{\textit{Correspondence}} \mathcal{G} \xrightarrow{\textit{Artin's Reciprocity Law}} \mathcal{H} \xrightarrow{\textit{fixed field}} \mathcal{F},$$

via

$$L \longmapsto N_{L|k}C_L \longmapsto [N_{L|k}C_L, k] \longmapsto L.$$

We now say that an idele fixes an element if the corresponding element in Galois group fixes the element. Then $s \in \mathbb{A}_k^\times$ fixes $x \in k^{ab}$ means that $\sigma = [s, k] \in \mathrm{Gal}(k^{ab}/k)$ fixes x. Also, we say that $L \subset k^{ab}$ is a fixed field of a subgroup H of $\mathbb{A}_k^\times$ if L is a fixed field of $[H, k] \subset \mathrm{Gal}(k^{ab}/k)$.

Note that the third isomorphism theorem gives a correspondence between subgoups $Hk^\times$ of $\mathbb{A}_k^\times$ containing $k^\times$ and subgroups H of C_k, also we have

$$\mathbb{A}_k^\times / Hk^\times \simeq C_k/H.$$

Thus, we have the identical subgroup index $[\mathbb{A}_k^\times : Hk^\times] = [C_k : H]$. Hence, if one of them is finite, then the other is also finite.

The following lemma is a basic fact from topological group theory.

Lemma 2.2.2. *Let $f : \mathbb{A}_K^\times \longrightarrow \mathbb{A}_k^\times$ be a continuous homomorphism. Suppose that $H \subset \mathbb{A}_k^\times$ be a closed subgroup of finite index in $\mathbb{A}_k^\times$, then $f^{-1}(H) \subset \mathbb{A}_K^\times$ is a closed subgroup of finite index in $\mathbb{A}_K^\times$. Furthermore, $[\mathbb{A}_K^\times : f^{-1}(H)] \leq [\mathbb{A}_k^\times : H]$.*

Proof. First, $f^{-1}(H)$ is clearly a closed subgroup of $\mathbb{A}_K^\times$ by continuity of f. Since H is of finite index in $\mathbb{A}_k^\times$, we have a coset decomposion of $\mathbb{A}_k^\times$ into finite union of cosets, say $\mathbb{A}_k^\times = \cup_i H a_i$ with a finite set of representatives $\{a_i\}_i$. Let $\{b_j\}_j \subset \mathbb{A}_K^\times$ have properties:

(1) $f(b_j) \in \{a_i\}_i$ for all j.

(2) If $f(b_{j_1}) = a_{i_1}$ and $f(b_{j_2}) = a_{i_2}$ for $b_{j_1} \neq b_{j_2}$, then $a_{i_1} \neq a_{i_2}$.

Then, we claim that $\mathbb{A}_K^\times$ has a coset decomposition $\mathbb{A}_K^\times = \cup_j f^{-1}(H) b_j$. We need to establish for any j, $f^{-1}(H)b_j = f^{-1}(Ha_i)$ for some i. Suppose $x \in f^{-1}(H)b_j$, then $f(x) \in Hf(b_j) = Ha_i$, so $x \in f^{-1}(Ha_i)$. On the other hand, if $y \in f^{-1}(Ha_i)$, then $y = yb_j^{-1}b_j$. Also, $f(yb_j^{-1}) = f(y)f(b_j)^{-1} = f(y)a_i^{-1} \in Ha_i a_i^{-1} = H$. Thus, $y \in f^{-1}(H)b_j$. Hence, our claim is proved. The last inequality follows from $|\{b_j\}_j| \leq |\{a_i\}_i|$. □

2.2.2 Imaginary Quadratic Case-Kronecker's Jugendtraum

Kronecker's Jugendtraum stems in an attempt to classifying finite abelian over K. This was successful by classifying ray class field over K instead. To this end, Weber function is introduced:

Definition 2.2.1. *For any point $P \in E$, Weber function $h : E \longrightarrow \mathbb{C}$ is defined by:*

$$h(x,y) = \begin{cases} x & \text{if } g_2 g_3 \neq 0 \\ x^2 & \text{if } g_3 = 0 \\ x^3 & \text{if } g_2 = 0. \end{cases}$$

For any nonzero fractional ideal $\mathfrak{m}$ in K, the classification of ray class field is as follows:

Theorem 2.2.4. *Let $E : y^2 = 4x^3 - g_2 x - g_3$ be an elliptic curve over $\mathbb{C}$ that admits CM by the full ring of integers an imaginary quadratic field K. The ray class field $K_{\mathfrak{m}}$ is the finite extension obtained by*

$$K_{\mathfrak{m}} = K(j(E), h(E[\mathfrak{m}])),$$

where $E[\mathfrak{m}]$ denotes $\mathfrak{m}$-torsion points on E.

Here, $j(E)$ is the j-invariant of elliptic curve E. (Definition is given in Section 2.3)

Corollary 2.2.1. *Let L be a finite abelian extension of imaginary quadratic field K. Then there is a fractional ideal $\mathfrak{m}$ such that*

$$L \subset K(j(E), h(E[\mathfrak{m}])).$$

2.3 Complex Multiplication (CM)

2.3.1 Elliptic Curves with CM

Let E be an elliptic curve over $\mathbb{C}$ which corresponds to a complex lattice Λ. To see a clear exposition of this correspondence, we introduce Weierstrass $\wp$-function. (see [Co])

Definition 2.3.1. *Weierstrass $\wp$-function associated to a complex lattice $\Lambda = [\omega_1, \omega_2]$ is defined by:*

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{w\in\Lambda-\{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right). \tag{2.5}$$

We simply write $\wp(z) = \wp(z;\Lambda)$. Note that $\wp(z+w) = \wp(z)$ for all $w \in \Lambda$.

Lemma 2.3.1. *Let $G_k(\Lambda) = \sum_{w\in\Lambda-\{0\}} w^{-k}$ for $k > 2$. Then, Weierstrass $\wp$-function for a lattice Λ has Laurent expansion*

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1) G_{2n+2}(\Lambda) z^{2n}. \tag{2.6}$$

Proof. We have the series expansion

$$\frac{1}{(1-x)^2} = 1 + \sum_{n=1}^{\infty} (n+1)x^n$$

for $|x| < 1$. Thus, if $|z| < |w|$, we have

$$\frac{1}{(z-w)^2} - \frac{1}{w^2} = \sum_{n=1}^{\infty} \frac{n+1}{w^{n+2}} z^n.$$

Summing over $w \in \Lambda - \{0\}$, we obtain

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (n+1) G_{n+2}(\Lambda) z^n.$$

Since $\wp$ is an even function, the odd coefficients must vanish and (2) follows. □

Lemma 2.3.2. *$\wp$-function for a lattice Λ satisfies the differential equation*

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3 \tag{2.7}$$

where $g_2 = 60G_4$, and $g_3 = 140G_6$.

Proof. Let $F(z) = \wp'(z)^2 - 4\wp(z)^3 + g_2\wp(z) + g_3$, then F has possible poles at $z = w \in \Lambda$, is holomorphic on $\mathbb{C} - \Lambda$, and $F(z + w) = F(z)$ for all $w \in \Lambda$. But, Laurent series expansions

$$\wp(z)^3 = \frac{1}{z^6} + \frac{9G_4}{z^2} + 15G_6 + O(z),$$

and

$$\wp'(z)^2 = \frac{4}{z^6} - \frac{24G_4}{z^2} - 80G_6 + O(z)$$

imply that F is holomorphic at 0, and $F(0) = 0$. By Liouville's theorem, we have $F(z) = 0$ for all $z \in \mathbb{C}$. □

Then the correspondence is given by

$$[\text{An elliptic curve } y^2 = 4x^3 - g_2x - g_3] \quad \longleftrightarrow \quad [\text{A lattice } \Lambda \text{ with } g_2(\Lambda)^3 - 27g_3(\Lambda)^2 \neq 0].$$

Then the endomorphism ring of E can be viewed as

$$\{\alpha \in \mathbb{C} | \alpha\Lambda \subset \Lambda\}.$$

This gives two possibilities, namely non-CM case (or we say that E does not have a complex multiplication):

$$\{\alpha \in \mathbb{C} | \alpha\Lambda \subset \Lambda\} = \mathbb{Z},$$

and CM case (or we say that E admits a complex multiplication):

$$\{\alpha \in \mathbb{C} | \alpha\Lambda \subset \Lambda\} = \mathcal{O}$$

In CM case, $\mathcal{O}$ turns out to be an order in an imaginary quadratic field K. In particular $\mathcal{O} \otimes \mathbb{Q} = K$, and K is called the CM-field.

Definition 2.3.2. *The j-invariant $j(\Lambda)$ of a lattice Λ is defined to be the complex number*

$$j(\Lambda) = 1728\frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3(\Lambda)^2} = 1728\frac{g_2(\Lambda)^3}{\Delta(\Lambda)}. \tag{2.8}$$

The j-invariant $j(\Lambda)$ characterizes the lattice Λ up to homothety, thus it characterizes the elliptic curve up to isomorphism. It is convenient to have the lattice Λ embedded in K. This is possible by replacing Λ by a lattice $\Lambda' = [1, \tau]$ which is homothetic to Λ. This also holds for abelian varieties with complex multiplication. (see Section 2.3.2)

If an elliptic curve E over $\mathbb{Q}$ admits CM by an order of imaginary quadratic field K, then its j-invariant is rational. The we have $[K(j(E)) : K] = 1$. This shows that the class number of K must be 1. H. Stark [St] proved that there are only nine imaginary quadratic field of class number one, namely $\mathbb{Q}(-d)$, $d = 3, 4, 7, 8, 11, 19, 43, 67, 163$.

In addition, such elliptic curves yields a useful property for division fields. The following lemma is from [M, p165, Lemma 6].

Lemma 2.3.3. *Let E be an elliptic curve over $\mathbb{Q}$ with complex multiplication by an order $\mathcal{O}$ of imaginary quadratic field K. Then for $m \geq 3$, we have*

$$\mathbb{Q}(E[m]) = K(E[m]).$$

Proof. It is enough to show that $K \subset \mathbb{Q}(E[m])$. To do this, consider $\tau \in G_{\overline{\mathbb{Q}}/\mathbb{Q}}$ that fixes $\mathbb{Q}(E[m])$. Then we claim that τ also fixes K. Suppose not, then τ is the complex conjugation on K. Let $\lambda \in \mathrm{End}(E)$. Then we have for any $x \in E[m]$,

$$\tau(\lambda(x)) = \lambda(x),$$

since τ fixes $E[m]$. On the other hand,

$$\tau(\lambda(x)) = \tau(\lambda)\tau(x) = \tau(\lambda)x = \overline{\lambda}(x).$$

Thus, $\lambda - \overline{\lambda} \in m\mathcal{O}$ and this forces $m|2$. The result now follows. □

2.3.2 Abelian Varieties of CM type

The CM theory can be generalized to abelian varieties. The endomorphism rings of abelian varieties are far more complex than those of elliptic curves. However, their center (as an algebra) can be described via CM-field (see [L, p6, Theorem 1.3]):

Definition 2.3.3. *A CM-field is a totally imaginary quadratic extension of a totally real number field.*

Theorem 2.3.1. *Let $\mathcal{A}$ be an abelian variety. Then the center K of $End_{\mathbb{Q}}\mathcal{A} := End\mathcal{A} \otimes \mathbb{Q}$ is either a totally real field or a CM field.*

Furthermore, we have by the following proposition (see [Sh, p36, Proposition 1]) that the degree of K in above theorem is bounded by $2\dim\mathcal{A}$.

Proposition 2.3.1. *Let $\mathcal{A}$ be an abelian variety of dimension g and $\mathfrak{S}$ a commutative semi-simple subalgebra of $End_{\mathbb{Q}}\mathcal{A}$. Then we have*

$$[\mathfrak{S} : \mathbb{Q}] \leq 2g.$$

In particular, $K \subset \mathfrak{S}$, which gives $[K : \mathbb{Q}] \leq [\mathfrak{S} : \mathbb{Q}] \leq 2g$. We are interested in the case that $[K : \mathbb{Q}] = 2g$, and K is a CM field. The following definition generalizes complex multiplication of elliptic curves to abelian varieties. (see [Sh, p41, Theorem 2], also [L, p72])

Theorem 2.3.2. *Let $\mathcal{A}$ be an abelian variety of dimension g. Suppose that the center of $End_{\mathbb{Q}}\mathcal{A}$ is K, and K is a CM field of degree $2g$ over $\mathbb{Q}$. We say that $\mathcal{A}$ admits complex*

multiplication. In this case, there is an ordered set $\Phi = \{\phi_1, \cdots, \phi_g\}$ *of* g *distinct isomorphisms of* K *into* $\mathbb{C}$ *such that no two of them is conjugate. We call this pair* (K, Φ) *the CM-type. Furthermore, there exists a lattice* $\mathfrak{a}$ *in* K *such that there is an analytic isomorphism* $\theta : \mathbb{C}^g/\Phi(\mathfrak{a}) \longrightarrow A(\mathbb{C})$. *We write* $(K, \Phi, \mathfrak{a})$ *to indicate* $\mathfrak{a}$ *is a lattice in* K *with respect to* θ. *In short, we say that* $\mathcal{A}$ *is of type(CM-type)* $(K, \Phi, \mathfrak{a})$ *with respect to* θ. *Under the inclusion* $i : K \longrightarrow End_{\mathbb{Q}}\mathcal{A}$, *we have that*

$$\mathcal{O} = \{\tau \in K | i(\tau) \in End\mathcal{A}\} = \{\tau \in K | \tau\mathfrak{a} \subset \mathfrak{a}\}$$

is an order in K.

This gives rise to the following composition:

Corollary 2.3.1. *Let* $\mathcal{A}$ *be an abelian variety of dimension* g *with CM-type* $(K, \Phi, \mathfrak{a})$ *with respect to* θ. *Then* $\theta \circ \Phi$ *maps* $K/\mathfrak{a}$ *to* $\mathcal{A}_{tor}$, *i. e.*

$$K/\mathfrak{a} \xrightarrow{\Phi} \mathbb{C}^g/\Phi(\mathfrak{a}) \xrightarrow{\theta} \mathcal{A}_{tor}.$$

Proof. This is clear from noticing that $\mathfrak{a} \otimes \mathbb{Q} = K$. Also, Φ is $\mathbb{Q}$-linear, and $\Phi(\mathfrak{a}) \otimes \mathbb{Q}$ is torsion subgroup of $\mathbb{C}^g/\Phi(\mathfrak{a})$. □

We define a reflex-type of a given CM-type. (see [Sh, p59-62])

Let K be a CM-field of degree $2g$, $\Phi = \{\phi_1, \cdots, \phi_g\}$ a set of g embeddings of K into $\mathbb{C}$ so that (K, Φ) is a CM-type. Let L be a Galois extension of $\mathbb{Q}$ containing K, and G the Galois group of L over $\mathbb{Q}$. Let ρ be an element of G that induces complex conjugation on K. Let S be the set of all elements of G that induce ϕ_i for some $i = 1, \cdots, g$.

A CM-type is called primitive if any abelian variety with the type is simple. The following proposition gives a criterion for primitiveness of CM-type. (see [Sh, p61, Proposition 26])

Proposition 2.3.2. *Let* (K, Φ) *be a CM-type. Let* L, G, ρ, S *as above, and* H_1 *the subgroup*

of G corresponding to K. Put

$$H_S = \{\gamma \in G | \gamma S = S\}.$$

Then (K, Φ) is primitive if and only if $H_1 = H_S$.

The following proposition relates a CM-type (K, Φ) and a primitive CM-type (K', Φ'). (see [Sh, p62, Proposition 28])

Proposition 2.3.3. *Let L, G, ρ, S as above. Put*

$$S' = \{\sigma^{-1} | \sigma \in S\}, \quad H_{S'} = \{\gamma \in G | \gamma S' = S'\}.$$

Let K' be the subfield of L corresponding to $H_{S'}$, and let $\Phi' = \{\psi_1, \cdots, \psi_{g'}\}$ be a set of g' embeddings of K' to $\mathbb{C}$ so that no two of them are conjugate. Then (K', Φ') is a primitive CM-type.

We call (K', Φ') the reflex of CM-type (K, Φ). We define a type norm for a given CM-type. The following map is well defined on $K'^{\times}$:

$$N_{(K',\Phi')} : K'^{\times} \longrightarrow K^{\times}, \quad x \mapsto \prod_{\sigma \in \Phi'} \sigma(x).$$

Then this map allows an extension to $N_{(K',\Phi')} : \mathbb{A}_{K'}^{\times} \longrightarrow \mathbb{A}_K^{\times}$. This extension is called the type norm. It can be seen that $N_{(K',\Phi')}$ is a continuous homomorphism on $\mathbb{A}_{K'}^{\times}$. (see [Sh, p124]) The field of definition k of an abelian variety $\mathcal{A}$ with CM-type (K, Φ) contains the reflex K'. In brief, $k \supset K'$. Thus, we can also define the type norm on the field of definition:

$$N_{\Phi'_k} = N_{(K',\Phi')} N_{k|K'}$$

where $N_{k|K'}$ is the standard norm map of ideles. Note that if $g = 1$ (elliptic curves) then $K = K'$.

The following theorem is a version of the Main Theorem of Complex Multiplication for abelian varieties: (see [L, Theorem 1.1, p84])

Proposition 2.3.4 (Main Theorem of Complex Multiplication)**.** *Let $\mathcal{A}$ be an abelian variety of dimension g with CM type $(K, \Phi, \mathfrak{a})$ with respect to θ, and defined over a number field k. Then:*

(i) The extension $k(\mathcal{A}_{tor}) : k$ is abelian.

(ii) There exists a unique character

$$\alpha : \mathbb{A}_k^\times \to K^\times$$

having the following property. If we define

$$\psi_{\mathcal{A}}(s) = \alpha(s) N_{\Phi'_k}(s^{-1}), \text{ for } s \in \mathbb{A}_k^\times,$$

then the diagram is commutative:

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\theta\cdot\Phi} & \mathcal{A}_{tor} \\ \Big\downarrow{\scriptstyle \psi_{\mathcal{A}}(s)} & \circlearrowleft & \Big\downarrow{\scriptstyle [s,k]} \\ K/\mathfrak{a} & \xrightarrow{\theta\cdot\Phi} & \mathcal{A}_{tor} \end{array}$$

(iii) This character α satisfies $\alpha(s)\overline{\alpha(s)} = N(s)$ and $\alpha(s)\mathfrak{a} = N_{\Phi'_k}(s)\mathfrak{a}$.

Here, the map $\psi_{\mathcal{A}}(s)$ on the downward arrow on the left side acts as the multiplication by an idele, and the map $[s, k]$ on the right side acts as the element of $\mathrm{Gal}(\overline{k}/k)$ corresponding to the idele s by Artin's reciprocity law. Now, we are ready to state the analogue of [M, p 162, Lemma 4]. The idea of the proof is the same as in [M], but we need a modification due to type norm factor in the Main Theorem of Complex Multiplication.

Lemma 2.3.4. *Let $\mathcal{A}, (K, \Phi), (K', \Phi'), k$ be the same notations as before. Let $m \geq 2$ be an*

integer. Then there exists a nonzero rational integer f such that

$$k(\mathcal{A}[m]) \subset k_{(mf)},$$

where $k_{(mf)}$ is the ray class field corresponding to the principal ideal $(mf) \subset k$.

Proof. By class field theory and Artin's reciprocity, we need to find a subgroup H of $\mathbb{A}_k^\times$ such that $k(\mathcal{A}[m])$ is a fixed field of H. Let $\xi = \theta \circ \Phi$. Then $\xi(x)$ is fixed by elements $[s, k]$ for all $s \in H$ and for all $x \in \frac{1}{m}\mathfrak{a}/\mathfrak{a}$. By the Main Theorem of Complex Multiplication, the following condition should hold:

$$\xi(\psi_{\mathcal{A}}(s)x) = \xi(x) \quad \text{for all } x \in \frac{1}{m}\mathfrak{a}/\mathfrak{a}.$$

Thus, $\psi_{\mathcal{A}}(s)x = x$ for all $x \in \frac{1}{m}\mathfrak{a}/\mathfrak{a}$. This is equivalent to

$$\psi_{\mathcal{A}}(s)x \equiv x \pmod{\mathfrak{a}} \quad \text{for all } x \in \frac{1}{m}\mathfrak{a}$$

Then we have

$$(\psi_{\mathcal{A}}(s) - 1)\frac{1}{m}\mathfrak{a} \subset \mathfrak{a}.$$

We see that $x = \frac{\psi_{\mathcal{A}}(s)-1}{m}$ belongs to the set:

$$X_{\mathfrak{a}} := \{x \in \mathbb{A}_K^\times | x\mathfrak{a} \subset \mathfrak{a}\}.$$

Denote by $\mathfrak{a} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ the $\mathfrak{a}_p$, a lattice in $K \otimes_{\mathbb{Q}} \mathbb{Q}_p$. Denote $\mathcal{R}_K$ by the subset of $\mathbb{A}_K^\times$ such that every component is integral with respect to each places (infinite places included). If $x \in X_{\mathfrak{a}}$, then $x_p\mathfrak{a}_p \subset \mathfrak{a}_p$. Therefore,

$$H = \{s \in \mathbb{A}_k^\times \mid \frac{\psi_{\mathcal{A}}(s) - 1}{m} \in X_{\mathfrak{a}}\},$$

Since any order in K contains a nonzero integral ideal, there exists a nonzero rational integer

f independent of m such that:

$$f\mathcal{R}_K \subset X_{\mathfrak{a}} \subset \mathcal{R}_K.$$

and

$$\{s \in \mathbb{A}_k^\times \mid \frac{\psi_{\mathcal{A}}(s)-1}{m} \in f\mathcal{R}_K\} \subset H \subset \{s \in \mathbb{A}_k^\times \mid \frac{\psi_{\mathcal{A}}(s)-1}{m} \in \mathcal{R}_K\}.$$

This can be rewritten as

$$\{s \in \mathbb{A}_k^\times \mid \psi_{\mathcal{A}}(s) \in U_{K,(fm)}\} \subset H \subset \{s \in \mathbb{A}_k^\times \mid \psi_{\mathcal{A}}(s) \in U_{K,(m)}\},$$

where (fm) and (m) are principal ideals generated by fm and m respectively, and we consider product of all real embeddings is included in both modulus. Simply, we have

$$\{s \in \mathbb{A}_k^\times \mid N_{\Phi'_k}(s^{-1}) \in K^\times U_{K,(fm)}\} \subset H \subset \{s \in \mathbb{A}_k^\times \mid N_{\Phi'_k}(s^{-1}) \in K^\times U_{K,(m)}\}.$$

Equivalently,

$$\{s \in \mathbb{A}_k^\times \mid N_{\Phi'_k}(s) \in K^\times U_{K,(fm)}\} \subset H \subset \{s \in \mathbb{A}_k^\times \mid N_{\Phi'_k}(s) \in K^\times U_{K,(m)}\}.$$

Then the conclusion follows since we have

$$U_{k,(fm)} \subset \{s \in \mathbb{A}_k^\times \mid N_{\Phi'_k}(s) \in K^\times U_{K,(fm)}\}.$$

□

We also have a bound on extension degree of division fields. (see [Ri, Theorem 1.1])

Lemma 2.3.5. *Let $\mathcal{A}$ be an abelian variety of CM type $(K, \Phi, \mathfrak{a})$ of dimension g defined over a number field k. Then for some $c_1, c_2 > 0$, $n_m = [k(\mathcal{A}[m]) : k]$ satisfies*

$$m^\nu c_1^{w(m)} \leq n_m \leq m^\nu c_2^{w(m)},$$

where $w(m)$ is the number of distinct prime factors of m, ν is an integer defined by Rank(Φ, K), and $2 + \log_2 g \leq \nu \leq g + 1$ if $\mathcal{A}$ is absolutely simple. Since the reflex type (Φ', K') is always simple and Rank$(\Phi, K) =$ Rank(Φ', K'), we also have that $2 + \log_2 g' \leq \nu \leq g' + 1$ if $[K' : \mathbb{Q}] = g'$. Thus, we have

$$max(2 + \log_2 g, 2 + \log_2 g') \leq \nu \leq min(g + 1, g' + 1).$$

A special case of this when $g = 1$ is:

Lemma 2.3.6. *Let E be a CM elliptic curve defined over $\mathbb{Q}$ and with complex multiplication by $\mathcal{O}_K$. Then for $k > 2$,*

$$\phi(k)^2 \ll [\mathbb{Q}(E[k]) : \mathbb{Q}] \ll k^2$$

where ϕ is the Euler function.

The Theorem 1.1 of [Ri] covers more general case when $\mathrm{End}_{\mathbb{Q}}\mathcal{A}$ contains commutative semisimple algebra of degree $2g$ over $\mathbb{Q}$. The proof of this is followed from considering l-adic Tate module of $\mathcal{A}$. (Definition is given in Section 2.4, see also [ST])

A direct corollary of Lemma 2.3.4 is the following:

Lemma 2.3.7. *Let $\mathcal{A}, (K, \Phi), (K', \Phi'), k$ be the same notations as before. Suppose also that $\mathfrak{p} \subset k$ is a prime of good reduction for $\mathcal{A}$, and $\mathfrak{p} \nmid m$. Let f be the nonzero integer as in Lemma 2.3.4. Given $m \geq 1$, there are $t(m)$ ideal classes modulo $(mf) \subset k$ such that*

$$\mathfrak{p} \text{ splits completely in } k(\mathcal{A}[m]) \text{ if and only if } \mathfrak{p} \sim \mathfrak{a}_1, \cdots, \mathfrak{p} \sim \mathfrak{a}_{t(m)}.$$

Furthermore, $t(m)$ satisfies the following identity by class field theory,

$$\frac{t(m)}{h(mf)} = \frac{1}{[k(\mathcal{A}[m]) : k]}.$$

By Lemma 2.3.5, there is an absolute positive constant c depending only on $\mathcal{A}$ such that

$$t(m) = \frac{h(mf)}{[k(\mathcal{A}[m]) : k]} \leq \frac{m^{2l-\nu}}{T(mf)} c^{w(m)} \leq \frac{m^N}{T(mf)},$$

where $N = N(\mathcal{A})$ is an integer depending only on $\mathcal{A}$.

In a special case $g = 1$, we have $t(m) = O(1)$ where implied constant depends only on the imaginary quadratic field K.

2.4 Image of Galois Representation

2.4.1 Serre's Open Image Theorem

Let E be an elliptic curve over $\mathbb{Q}$, p a prime of good reduction for E. We have the Galois representation:

$$\rho : G_{\overline{\mathbb{Q}}/\mathbb{Q}} \longrightarrow \mathrm{Aut}(E[p]).$$

Since $E[p] \simeq \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$, we have $\mathrm{Aut}(E[p]) \simeq \mathrm{GL}(2, \mathbb{F}_p)$. The above representation has kernel $G_{\overline{\mathbb{Q}}/\mathbb{Q}(E[p])}$, thus it follows by Galois theory that the representation

$$\rho : G_{\mathbb{Q}(E[p])/\mathbb{Q}} \longrightarrow \mathrm{Aut}(E[p])$$

has the same image as above. We are interested in how large this image can be inside $\mathrm{GL}(2, \mathbb{F}_p)$. An answer is given by Serre in more general statement on Tate modules. We introduce Tate module here, since it is often convenient to combine p-power torsion data together.

Definition 2.4.1. *Let E be an elliptic curve over a number field K. A l-adic Tate-module is defined by:*

$$T_l(E) = \varprojlim E[l^n]$$

where the inverse limit is taken along the inverse system composed of projections π_{ji} :

$E[l^j] \longrightarrow E[l^i]$ for $i \leq j$. The l-adic Tate module $T_l(\mathcal{A}) = \varprojlim \mathcal{A}[l^n]$ for an abelian variety $\mathcal{A}$ can be defined similarly.

Note that $T_l(E)$ is a $\mathbb{Z}_l$-module of rank 2. (for abelian variety $\mathcal{A}$ of dimension g, $T_l(\mathcal{A})$ is a $\mathbb{Z}_l$-module of rank $2g$.) Then we see that $\mathrm{Aut}(T_l(E)) \simeq \mathrm{GL}(2, \mathbb{Z}_l)$. The image of Galois representation inside the automorphism group of l-adic Tate module has the following properties (see [Si, p. 92, Theorem 7.9]):

Theorem 2.4.1 (Serre)**.** *Let K be a number field and let E/K be an elliptic curve without complex multiplication.*

(a) $\rho_l(G_{\overline{K}/K})$ is of finite index in $Aut(T_l(E))$ for all primes $l \neq char(K)$.

(b) $\rho_l(G_{\overline{K}/K}) = Aut(T_l(E))$ for all but finitely many primes l.

This theorem is called the open image theorem due to the following equivalent formulation:

Theorem 2.4.2 (Serre)**.** *Let P be the set of all rational primes, and E be an elliptic curve defined over K without complex multiplication. Let G be the absolute Galois group of K. Then the image $\rho(G)$ under the following homomorphism is open subgroup of $\prod_{l \in P} GL(2, \mathbb{Z}_l)$.*

$$\rho : G \longrightarrow \prod_{l \in P} Aut(T_l(E)) \simeq \prod_{l \in P} GL(2, \mathbb{Z}_l).$$

Since $\prod_{l \in P} \mathrm{GL}(2, \mathbb{Z}_l)$ is compact, $\rho(G)$ is an open subgroup of finite index in $\mathrm{GL}(2, \mathbb{Z}_l)$. In general, for a subgroup H of a compact topological group G, the following are equivalent:

- H is open.
- H is an open subgroup of finite index in G.
- H is a closed subgroup of finite index in G.

The theorem can be rephrased as:

Corollary 2.4.1. *If E is non-CM curve, then there exists a positive integer $A(E)$ depending only on E such that*

$$Gal(\mathbb{Q}(E[k])/\mathbb{Q}) \simeq GL(2, \mathbb{Z}/k\mathbb{Z}),$$

where $(k, A(E)) = 1$.

The integer $A(E)$ is called the Serre's constant for E. This version had been used in [CM], and it will also be frequently used in this paper.

2.4.2 Deuring's Open Image Theorem

Unlike the non-CM case, the image of Galois representation is small. The following theorem is proved by Deuring: (see [D], also [Se])

Theorem 2.4.3. *Let E be an elliptic curve over its quadratic imaginary CM-field K, and $\mathcal{O} = End(E)$ an order in K. Let G be the absolute Galois group of K, and $\mathcal{O}_l = \mathcal{O} \otimes \mathbb{Z}_l$. Then the image $\rho(G)$ of under the following Galois representation is an open subgroup of $\prod_{l \in P} \mathcal{O}_l^\times$:*

$$\rho : G \longrightarrow \prod_{l \in P} \mathcal{O}_l^\times.$$

Since $\mathcal{O}_l^\times$ is compact, $\rho(G)$ is a closed subgroup of finite index in $\mathcal{O}_l^\times$. A corollary in a special case $\mathcal{O} = \mathcal{O}_K$ is mentioned in [Ru, Corollary 5.20]

Corollary 2.4.2. *If E has CM by the full ring of integers $\mathcal{O}_K$ of an imaginary quadratic field K and N be the conductor of E, then*

$$Gal(K(E[k])/K) \simeq (\mathcal{O}_K/k\mathcal{O}_K)^\times,$$

where $(k, 6N) = 1$.

We are interested in the arithmetic function:

$$n \mapsto [\mathbb{Q}(E[n]) : \mathbb{Q}].$$

We will see in section 2.6 that its value is the same as some multiplicative function up to finite many factors.

2.5 Frobenious Endomorphism

Let $\mathcal{A}$ be an absolutely simple abelian variety of dimension g which is of type $(K, \Phi, \mathfrak{a})$. Let k be the field of definition of $\mathcal{A}$. Let $\mathfrak{p}$ be a prime ideal in k of a good reduction for $\mathcal{A}$, and l be a rational prime which is coprime to $\mathfrak{p}$. By [T, Theorem 2], the characteristic polynomial $f_{\mathcal{A},\mathfrak{p}}$ for Frobenious endomorphism $\pi_{\mathcal{A},\mathfrak{p},l} : T_l(\mathcal{A}) \longrightarrow T_l(\mathcal{A})$ is independent of l, hence $f_{\mathcal{A},\mathfrak{p}}$ is indeed a rational polynomial. Thus, we drop the dependence on l and just write $\pi_{\mathcal{A},\mathfrak{p}}$ for Frobenious endomorphism associated with $\mathcal{A}(\mathbb{F}_\mathfrak{p})$. Then $\mathbb{Q}[\pi_{\mathcal{A},\mathfrak{p}}]$ is the center of $\mathbb{Q} \otimes \mathrm{End}_{\mathbb{F}_\mathfrak{p}}\mathcal{A}(\mathbb{F}_\mathfrak{p})$, in our case for abelian variety with CM, both are isomorphic to K. Furthermore, we have the following:

Proposition 2.5.1. *Let $\mathcal{A}$, g, $(K, \Phi, \mathfrak{a})$, k, $\mathfrak{p}$, l, $f_{\mathcal{A},\mathfrak{p}}$, and $\pi_{\mathcal{A},\mathfrak{p}}$ be as above. Then all conjugates of $f_{\mathcal{A},\mathfrak{p}}$ have the absolute value $\sqrt{q} = \sqrt{N\mathfrak{p}}$, and they can be listed as:*

$$\pi_{\mathcal{A},\mathfrak{p}} := \pi_{\mathcal{A},\mathfrak{p},1}, \pi_{\mathcal{A},\mathfrak{p},2}, \cdots, \pi_{\mathcal{A},\mathfrak{p},g}, \pi'_{\mathcal{A},\mathfrak{p},1}, \pi'_{\mathcal{A},\mathfrak{p},2}, \cdots, \pi'_{\mathcal{A},\mathfrak{p},g}$$

where

$$\pi'_{\mathcal{A},\mathfrak{p},i} = \overline{\pi_{\mathcal{A},\mathfrak{p},i}} \text{ for all } 1 \leq i \leq g.$$

Let $m \geq 1$ be an integer and $x \geq 2$. Denote by $\pi_\mathcal{A}(x; m)$ the number of prime ideals $\mathfrak{p}$ in k which split completely in $k(\mathcal{A}[m])$ and satisfying $N\mathfrak{p} < x$ and have good reductions for $\mathcal{A}$. Let $\sigma_1, \cdots, \sigma_g, \sigma'_1, \cdots, \sigma'_g$ be distinct embeddings of K to $\mathbb{C}$ with $\sigma'_i = \overline{\sigma_i}$ for each $1 \leq i \leq g$. Denote by $\sigma := (\mathrm{Re}\sigma_1, \mathrm{Im}\sigma_1, \cdots, \mathrm{Re}\sigma_g, \mathrm{Im}\sigma_g)$ be a canonical embedding of K in $\mathbb{R}^{2g}$.

For such prime ideal $\mathfrak{p}$ in k, we have $\pi_{\mathcal{A},\mathfrak{p}} \equiv 1 \pmod{m}$. Consider the following association:

$$\mathrm{Spec}k \xrightarrow{\text{Frobenious}} \mathbb{Q} \otimes \mathrm{End}_K\mathcal{A} \xrightarrow{\sigma} \mathbb{R}^{2g},$$

via

$$\mathfrak{p} \longmapsto \pi_{\mathcal{A},\mathfrak{p}} \longmapsto (\pi_{\mathcal{A},\mathfrak{p},1}, \cdots \pi_{\mathcal{A},\mathfrak{p},g}).$$

Thus, each such prime ideal is associated to an algebraic integer α satisfying $\alpha \equiv 1 \pmod{m}$

and $|\alpha| < \sqrt{x}$. It is well known that σ maps $\mathcal{O}_K$ to a $\mathbb{Z}$-lattice L_K in $\mathbb{R}^{2g}$. Then the number of such α is $O(x^g/m^{2g})$ where implied constant depends only on K. Furthermore, for a fixed α, there are at most $2g$ prime ideals which corresponds to α. Hence, we have:

Lemma 2.5.1. *Let $\mathcal{A}$, g, $(K, \Phi, \mathfrak{a})$, k, and $\pi_{\mathcal{A}}(x; m)$ be as above. Then*

$$\pi_{\mathcal{A}}(x; m) \ll_k \frac{x^g}{m^{2g}}.$$

2.6 Multiplicative Functions

2.6.1 Elementary Identities

A multiplicative function f is an arithmetic function that satisfies

$$f(mn) = f(m)f(n),$$

for all m, n with $(m, n) = 1$. If f satisfies $f(mn) = f(m)f(n)$ for all m, n without any condition, then we call f a completely multiplicative function. For example, the functions $\mu(n)$(Möbius function), $\phi(n)$(Euler totient function), $\Lambda(n)$(von-Mangoldt function) are multiplicative functions but not completely multiplicative. The functions n^α, $\chi_d(n)$(Dirichlet character) are completely multiplicative functions.

Thus, if we know that f is multiplicative, then the values at prime power $f(p^k)$ for $k \geq 0$ determine the function. If we know that f is completely multiplicative, then the values at prime numbers $f(p)$ determine the function.

We state a basic lemma about multiplicative functions:

Lemma 2.6.1. *Let f and g be multiplicative functions, then the Dirichlet convolution $h = f * g$ defined by:*

$$h(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right)$$

is also multiplicative.

Applying this lemma multiple times, we obtain:

Corollary 2.6.1. *Let f and g be multiplicative functions, then we have*

$$\mathcal{H}(n) = \sum_{dk|n} f(d)g(k)$$

is also multiplicative.

Proof. We can see this directly from $\mathcal{H} = (f*g)*1$, where 1 denotes the constant function. □

Here, we prove the following elementary identity involving Möbius function:

Corollary 2.6.2. *Let $j \in \mathbb{C}$ be fixed. Then for any $n \in \mathbb{N}$:*

$$\frac{1}{n^j} = \sum_{dk|n} \frac{\mu(d)}{k^j}.$$

Proof. By Corollary 2.5.1, we know that both sides are multiplicative. Thus, we establish the identity by evaluating at prime powers, say $n = p^a$. The sum gives

$$1 + \sum_{m=1}^{a} \left(\frac{1}{p^{mj}} - \frac{1}{p^{(m-1)j}} \right) = \frac{1}{p^{aj}}.$$

This proves the identity. □

This identity is used in [FM], and $j = 1$ case in [FK].

2.6.2 A Generalization to Euler's Totient Function

We generalize a certain property of Euler Totient function ϕ.

Definition 2.6.1. *We call a function $f : \mathbb{N} \longrightarrow \mathbb{C}$ multiplicative function of ϕ-type if there is a fixed arithmetic function g and a number $N > 0$ such that*

$$f(n) = n^N \prod_{p|n} g(p).$$

We present a few examples of multiplicative functions of ϕ-type.

Example 2.6.1. *Euler Totient function*

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

with $N = 1$ *and* $g(p) = 1 - \frac{1}{p}$.

Example 2.6.2. *The cardinality of* $GL(2, \mathbb{Z}/n\mathbb{Z})$

$$\psi(n) = n^4 \prod_{p|n} \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p^2}\right),$$

with $N = 4$ *and* $g(p) = \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p^2}\right)$.

Example 2.6.3. *The analogue of Euler Totient function for a quadratic field* K

$$\Phi(n) = \left|(\mathcal{O}_K/n\mathcal{O}_K)^\times\right| = n^2 \prod_{p|n} g(p),$$

where

$$g(p) = \begin{cases} 1 - \frac{1}{p^2} & \text{if } p \text{ is inert in } K \\ \left(1 - \frac{1}{p}\right)^2 & \text{if } p \text{ splits in } K \\ 1 - \frac{1}{p} & \text{if } p \text{ ramifies in } K \end{cases},$$

with $N = 2$.

This follows from considering prime splitting in quadratic field. Note that $\mathcal{O}_K/n\mathcal{O}_K$ factors as $\mathcal{O}_K/\left(\prod {p_i}^{e_i}\right)\mathcal{O}_K$ where $n = \prod {p_i}^{e_i}$ is the prime factorization of n. Then by Chinese remainder theorem, we have

$$\mathcal{O}_K/\left(\prod {p_i}^{e_i}\right)\mathcal{O}_K \simeq \prod \left(\mathcal{O}_K/{p_i}^{e_i}\mathcal{O}_K\right).$$

By taking unit groups of both sides,

$$\left(\mathcal{O}_K/\left(\prod {p_i}^{e_i}\right)\mathcal{O}_K\right)^{\times} \simeq \prod \left(\mathcal{O}_K/{p_i}^{e_i}\mathcal{O}_K\right)^{\times}.$$

For each prime ideals $\mathfrak{p}$ lying above a rational prime p, we see that

$$\left|\left(\mathcal{O}_K/\mathfrak{p}^e\mathcal{O}_K\right)^{\times}\right| = (N\mathfrak{p})^e - (N\mathfrak{p})^{e-1} = (N\mathfrak{p})^e\left(1-\frac{1}{N\mathfrak{p}}\right).$$

The characterization now follows by:

$$N\mathfrak{p} = \begin{cases} p^2 & \text{if } p \text{ is inert in } K \\ p & \text{if } p \text{ splits or ramified in } K. \end{cases}$$

Furthermore, the splitting of primes can be written in terms of Kronecker's symbol:

Let D be the discriminant of K. Then

$$\text{A rational prime } p \begin{cases} \text{splits} & \text{if } \left(\frac{D}{p}\right) = 1 \\ \text{is inert} & \text{if } \left(\frac{D}{p}\right) = -1 \\ \text{is ramified} & \text{if } \left(\frac{D}{p}\right) = 0. \end{cases}$$

Let $[m,n]$ be the least common multiple of m and n, (m,n) be the greatest common divisor ot them. If f is a multiplicative function of ϕ-type, then it satisfies

$$f([m,n])f((m,n)) = f(m)f(n).$$

This is easy to see from our definition. In fact, if $p^a||m$ and $p^b||n$, then $p^{\min(a,b)}||(m,n)$ and $p^{\max(a,b)}||[m,n]$. Thus, we have the well known identity

$$[m,n](m,n) = mn,$$

and by definition

$$f([m,n]) = [m,n]^N \prod_{p|[m,n]} g(p), \quad f((m,n)) = (m,n)^N \prod_{p|(m,n)} g(p)$$

$$f(m) = m^N \prod_{p|m} g(p), \quad f(n) = n^N \prod_{p|n} g(p).$$

Since $g(p)$ for $p|(m,n)$ on both sides get multiplied two times, we obtain the identity $f([m,n])f((m,n)) = f(m)f(n)$.

Denote by $\langle n \rangle := \{h : p|h \Rightarrow p|n\}$, the set of integers whose prime divisors are those of n, and $G_k := \mathrm{Gal}(\mathbb{Q}(E[k])/\mathbb{Q})$.

By the argument given in [FK, Chapter 7], together with open image theorem by Serre, we have the following proposition with some $m \in \langle 2A(E) \rangle$ when E does not have CM.

Proposition 2.6.1. *Let $k = hj$ with $h \in \langle m \rangle$, and $(j,m) = 1$. Then $|G_k| = |G_h||G_j|$, and with $h_1 = (h,m)$, we have*

$$|G_h| = |G_{h_1}| \prod_{\substack{p^{\nu_p}||h \\ \nu_p > m_p}} p^{4(\nu_p - m_p)}.$$

Further, $|G_j| = \psi(j)$, and hence

$$|G_k| = |G_{h_1}|\psi(j) \prod_{\substack{p^{\nu_p}||h \\ \nu_p > m_p}} p^{4(\nu_p - m_p)}.$$

If E is an elliptic curve over its CM-field K with CM by the full ring of integers $\mathcal{O}_K$, then the image of Galois representation is small. Let $[K(E[k]) : K] = |G_k|$ where G_k is the image under the following Galois representation,

$$\mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{Aut}(E[k]) \simeq (\mathcal{O}_K/k\mathcal{O}_K)^*$$

As in [FK, Chapter 7], we adopt the same idea in the CM case. We have a homomorphism

of groups

$$\rho : \mathrm{Gal}(\overline{K}/K) \longrightarrow G := \prod_{l:\text{primes in } K} (\mathcal{O}_{K,l})^*$$

There is natural projection $\pi_k : G \longrightarrow (\mathcal{O}_K/k\mathcal{O}_K)^*$ for each k.

Let $\Gamma_k = \mathrm{Ker}(\pi_k)$. Then $H := \rho(\mathrm{Gal}(\overline{K}/K))$ has a finite index in G by Serre's open image theorem. The image of the composition $\pi_k \circ \rho$ is isomorphic to G_k, hence by the first isomorphism theorem,

$$H/H \cap \Gamma_k \simeq G_k.$$

The claim in [FK, Chapter 7, page 19], in the CM case, is as follows.

They take m to be the smallest positive integer that $\Gamma_m < H$, but there is no significance that m has to be the smallest. We can take $m \in \langle 6N \rangle := \{h : p|h \Rightarrow p|6N\}$. Write $m = \prod_{p|m} p^{m_p}$, $k = \prod_{p|k} p^{k_p}$.

Claim: If $k_p \geq m_p$ for some p and $a \geq 1$, then

$$|H/H \cap \Gamma_{p^a k}| = |H/H \cap \Gamma_k| \cdot |\Gamma_{p^{k_p}}/\Gamma_{p^{a+k_p}}|$$

Moreover, if $k_p = 0$, we have $|\Gamma_{p^{k_p}}/\Gamma_{p^{a+k_p}}| = |\Gamma_1/\Gamma_{p^a}| = \Phi(p^a)$, and if $k_p > 0$, then

$$|\Gamma_{p^{k_p}}/\Gamma_{p^{a+k_p}}| = |\Gamma_p/\Gamma_{p^2}|^a = p^{2a}.$$

From this claim, we obtain that

Proposition 2.6.2. *Let $k = hj$ with $h \in \langle m \rangle := \{h : p|h \Rightarrow p|m\}$, and $(j, m) = 1$. Then $|G_k| = |G_h||G_j|$, and with $h_1 = (h, m)$, we have*

$$|G_h| = |G_{h_1}| \prod_{\substack{p^{\nu_p}||h \\ \nu_p > m_p}} p^{2(\nu_p - m_p)}.$$

Further, $|G_j| = \Phi(j)$*, and hence*

$$|G_k| = |G_{h_1}|\Phi(j) \prod_{\substack{p^{\nu_p}||h \\ \nu_p > m_p}} p^{2(\nu_p - m_p)}.$$

CHAPTER 3

Analytic Backbround

3.1 Number Field Analogue of Classical Theorems

3.1.1 Bombieri-Vinogradov Theorem

The classical Bombieri-Vinogradov Theorem gives an error bound on average in primes in arithmetic progression. Define the Von-Mangoldt function by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \\ 0 & \text{otherwise,} \end{cases}$$

and a sum of $\Lambda(n)$ over $n \leq x$ over an arithmetic progression $n \equiv a \bmod q$:

$$\psi(x; q, a) = \sum_{\substack{n \leq x \\ n \equiv a \bmod q}} \Lambda(n).$$

Each of these sums are approximated by $x/\phi(q)$ by Siegel-Walfisz theorem. The error terms emerging from this approximation for $q \leq \log^A x$ with $A > 0$ fixed is bounded by $O(x \exp(-c\sqrt{\log x}))$ for some constant $c > 0$. This is a strong upper bound, but the strength is weak in terms of the range of q. On average, the error bound becomes $O(x/\log^A x)$ which is weaker than $x \exp(-c\sqrt{\log x})$, but the strength on the range of q is stronger. In fact, we have

Theorem 3.1.1 (Bombieri-Vinogradov)**.** *Let $q > 1$ be an integer, and $A > 0$ be a fixed*

positive number. Then there is $B = B(A) > 0$ *such that*

$$\sum_{q \le Q} \max_{(a,q)=1} \max_{y \le x} \left| \psi(x; q, a) - \frac{x}{\phi(q)} \right| = O_A \left(\frac{x}{\log^A x} \right),$$

where $Q = x^{1/2} (\log x)^{-B}$.

The following form is obtained by partial summation:

Theorem 3.1.2. *Let* $\pi(x; q, a) = \#\{p \le x : p \text{ is prime, }, p \equiv a \pmod q\}$. *Then*

$$\sum_{q \le Q} \max_{(a,q)=1} \max_{y \le x} \left| \pi(x; q, a) - \frac{Li(x)}{\phi(q)} \right| = O_A \left(\frac{x}{\log^A x} \right),$$

where $Q = x^{1/2} (\log x)^{-B}$.

This result first generalized by R. Wilson(See [Wi]) who proved an analogous theorem with $Q = x^{1/(n+1)} (\log x)^{-B}$. Then Huxley [Hu] announced an improved version with $Q = x^{1/2} (\log x)^{-B}$.

Let K be a number field of degree $n = r_1 + 2r_2$ with ring of integers $\mathcal{O}_K$ and r_1 the number of distinct real embeddings of K, and let $\mathfrak{m}$ be an integral ideal of K. Define a $\mathfrak{m}$-ideal class group by an abelian group of equivalence classes of ideals in the following relation:

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

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

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

The $\mathfrak{m}$-ideal class group coincides with our definition $C_{\mathfrak{m}}(K) = J_K^{\mathfrak{m}} / P_K^{\mathfrak{m}}$ in the previous chapter. Denote by $h(\mathfrak{m})$ the cardinality of $J_K^{\mathfrak{m}} / P_K^{\mathfrak{m}}$, and h by the class number of K. We

have a formula that relates $h(\mathfrak{m})$ and the class number h of K. This follows from an exact sequence:

$$U(K) \longrightarrow (\mathcal{O}_K/\mathfrak{m}\mathcal{O}_K)^\times \oplus \{\pm 1\}^{r_1} \longrightarrow C_{\mathfrak{m}}(K) \longrightarrow C(K) \longrightarrow 1.$$

Denote by $T(\mathfrak{m})$ the cardinality of the image of the unit group $U(K)$ in $(\mathcal{O}_K/\mathfrak{m}\mathcal{O}_K)^\times \oplus \{\pm 1\}^{r_1}$. Then we have

$$h(\mathfrak{m}) = \frac{2^{r_1} h\phi(\mathfrak{m})}{T(\mathfrak{m})}$$

where $\phi(\mathfrak{m}) = |(\mathcal{O}_K/\mathfrak{m}\mathcal{O}_K)^\times|$. J. Zelinsky [Z, Corollary 12] gave a lower bound of $T(\mathfrak{m})$ for nonzero integral ideals $\mathfrak{m} \subset K$:

Lemma 3.1.1 (Zelinsky)**.** *Let K be a number field such that $\mathcal{O}_K$ has infinitely many units. Then there is a constant $c > 1$ such that*

$$T(\mathfrak{m}) \gg \log_c N\mathfrak{m}.$$

Proof. The proof of this follows by considering a unit a with infinite order in $(\mathcal{O}_K)^\times$. Assume that $\mathfrak{m}|(a^k - 1)$ then $N\mathfrak{m} \leq N(a^k - 1)$. There is a constant $C > 1$ depending only on a such that $|N(a^k - 1)| \leq C^k$. Thus, $k \geq \log_C N\mathfrak{m}$ and this completes the proof. □

Let $1 \leq m < x$ be an integer, then we can improve this result on principal ideals (m) for almost all m:

Theorem 3.1.3. *Let K be a number field such that $\mathcal{O}_K$ has infinitely many units. Then we have*

$$T((m)) \gg (\log x)^{\frac{1}{2}(\log x)^{2/5}}$$

for almost all integer $1 \leq m < x$, and the number of exceptional m's is $O(x \exp(-\frac{2}{5}(\log x)^{3/5}))$. The implied constants depend only on K.

A crucial point in measuring the size of exceptional set of m's, we need the following classical result on number of integers composed of small primes. (see [MV, Corollary 7.9]):

Proposition 3.1.1. *Let $\psi(x,y)$ be the number of all positive integers composed of primes $\leq y$. If $y = (\log x)^a$ and $1 \leq a \leq (\log x)^{1/2}/(2\log\log x)$, then*

$$\psi(x,y) < x^{1-1/a} \exp\left(\frac{(\log a + O(1))\log x}{a \log\log x}\right).$$

In particular, if $a = (\log x)^{2/5}$, then

$$\begin{aligned}\psi(x,y) &< x^{1-1/(\log x)^{2/5}} \exp\left(\frac{((2/5)\log\log x + O(1))\log x}{(\log x)^{2/5}\log\log x}\right) \\ &= x\exp\{-(\log x)^{3/5} + (2/5)(\log x)^{3/5} + O(1)(\log x)^{3/5}/\log\log x\} \\ &< x\exp\{-(3/5)(\log x)^{3/5} + (1/5)(\log x)^{3/5}\} \\ &= x\exp(-(2/5)(\log x)^{3/5}).\end{aligned}$$

Rankin's proof of this proposition begins with the following basic estimate:

$$\psi(x,y) \leq \sum_{\substack{n\leq x \\ p|n\Rightarrow p\leq y}} \left(\frac{x}{n}\right)^\sigma \leq x^\sigma \sum_{p|n\Rightarrow p\leq y} \frac{1}{n^\sigma} = x^\sigma \prod_{p\leq y}\left(1 - \frac{1}{p^\sigma}\right)^{-1}.$$

Then for an obtimal choice of σ to estimate the Euler product, the upper bound follows. A combinatorial argument is used in proving the lower bound.

Another big idea in proving Theorem 3.1.3 is from P. Erdos and R. Murty [EM]. They show in their introduction that for integer $a \geq 2$, there are at most $O(x/(\log x)^3)$ primes $p \leq x$ such that the order $f(p)$ of a modulo p is less than $\sqrt{p}/\log p$. The proof goes as follows:

If $f(p) < z$ then p divides $V = \prod_{t<z}(a^t - 1)$. Let $\omega(V)$ be the number of prime divisors of V. Then we have

$$\omega(V) \ll \sum_{t<z} \frac{t}{\log t} \ll \frac{z^2}{\log z}.$$

For $z = \sqrt{x}/(\log x)$, it follows that $\omega(V) \ll x/(\log x)^3$. Thus there are at most $O(x/(\log x)^3)$ primes $p \leq x$ such that $f(p) < \sqrt{x}/(\log x)$.

Proof of Theorem 3.1.3. Let u be a unit in $\mathcal{O}_K$ having infinite order. Consider

$$V = \prod_{t<z}(u^t - 1).$$

Let $f(m)$ be the order of u in $(\mathcal{O}_K/m\mathcal{O}_K)^\times$. Suppose that $f(m) < z$, then we see that $f(p) < z$ for all primes $p|m$, and $m|V$. Since u has infinite order in $(\mathcal{O}_K)^\times$, V is nonzero. Thus, its norm $NV = N_{\mathbb{Q}}^K V$ is a nonzero integer. Since $m|V$, it is clear that $m|NV$. By the previous argument, we have

$$\omega(|NV|) \ll_K \sum_{t<z} \frac{t}{\log t} \ll_K \frac{z^2}{\log z}.$$

Thus, m is consisted of at most $\frac{z^2}{\log z}$ primes. Moreover, the prime divisors of m are contained in the prime divisors of $|NV|$. The number of all $1 \le m < x$ composed in this way is bounded by the number of m composed of the first $\omega(|NV|)$ primes. Thus, it is $\ll \psi(x, cz^2)$ where c depends only on K. Take $z = (\log x)^{\frac{1}{2}(\log x)^{2/5}}$, then the number of $1 \le m < x$ such that $f(m) < z$ is $\ll x \exp\left(-\frac{2}{5}(\log x)^{3/5}\right)$. This completes the proof. □

Theorem 3.1.3 can be generalized to integral ideals. We want a lower bound of $T(\mathfrak{m})$ similar to Theorem 3.1.3 for integral ideal $\mathfrak{m} \subset K$ such that $N\mathfrak{m} < x$. There is a limitation to the following theorem since this cannot imply Theorem 3.1.3. Note that $N((m)) = m^{[K:\mathbb{Q}]}$, thus we cannot require $m < x$. We need the following analogous proposition to Proposition 3.1.1:

Proposition 3.1.2. *Let K be a number field. Denote by $\Psi(x, y)$ the number of all integral ideals $\mathfrak{m}$ in K with $N\mathfrak{m} \le x$ composed of prime ideals $\mathfrak{p}$ with $N\mathfrak{p} \le y$. If $y = (\log x)^a$ and $1 \le a \le (\log x)^{1/2}/(2\log\log x)$, then*

$$\Psi(x, y) < x^{1-1/a} \exp\left(\frac{(\log a + O(1))\log x}{a \log\log x}\right),$$

where the implied constant depends only on K.

To prove this, we use the Euler product for the Dedekind zeta function of K:

$$\Psi(x,y) \leq \sum_{\substack{N\mathfrak{m}\leq x \\ \mathfrak{p}|\mathfrak{m}\Rightarrow N\mathfrak{p}\leq y}} \left(\frac{x}{N\mathfrak{m}}\right)^{\sigma} \leq x^{\sigma} \sum_{\mathfrak{p}|\mathfrak{m}\Rightarrow N\mathfrak{p}\leq y} \frac{1}{N\mathfrak{m}^{\sigma}} = x^{\sigma} \prod_{N\mathfrak{p}\leq y} \left(1-\frac{1}{N\mathfrak{p}^{\sigma}}\right)^{-1}.$$

Theorem 3.1.4. *Let K be a number field with infinite $(\mathcal{O}_K)^{\times}$. Let $\mathfrak{m}$ be a nonzero integral ideal of K, and let $T(\mathfrak{m})$ defined as above. Then we have*

$$T(\mathfrak{m}) \gg (\log x)^{\frac{1}{2}(\log x)^{2/5}}$$

for almost all $\mathfrak{m}$ with $N\mathfrak{m} < x$, and the number of exceptional $\mathfrak{m}$'s is $O(x\exp(-\frac{2}{5}(\log x)^{3/5}))$. The implied constants depend only on K.

Proof. Similarly as before, let u be a unit of infinite order. Let $V = \prod_{t<z}(u^t - 1)$. Denote by $f(\mathfrak{m})$ the order of u modulo $\mathfrak{m}$. Suppose that $f(\mathfrak{m}) < z$ for some $\mathfrak{m}$ with $N\mathfrak{m} < x$. Then $\mathfrak{m}|V$. We define $\omega_K(\mathfrak{b})$ for integral ideals $\mathfrak{b}$ by the number of distinct prime divisors of $\mathfrak{b}$. Taking norms, we obtain $N\mathfrak{m}|NV$. As before, we have

$$\omega_K(|NV|) \ll_K \frac{z^2}{\log z}.$$

Take $z = (\log x)^{\frac{1}{2}(\log x)^{2/5}}$. We see that $N\mathfrak{m}$ is an integer composed of prime ideal divisors of $|NV|$. Consider

$$B = \{N\mathfrak{m} < x | \mathfrak{m} \text{ is an integral ideal of } K \text{ composed of prime ideal divisors of } |NV|\}.$$

Let F be the set of all integral ideals with $N\mathfrak{m} < x$ composed of the first $\omega_K(|NV|)$ prime ideals (where prime ideals arranged norm-ascending order), then the above sum is bounded by the cardinality of F. This set has cardinality $\ll x\exp\left(-\frac{2}{5}(\log x)^{3/5}\right)$, thereby proving the theorem. □

We improve Proposition 3.1.1 by inserting extra factor $R^{\omega(n)}$.

Proposition 3.1.3. *Let $R > 1$ be fixed. Let $\psi_2(x, y)$ be a sum over numbers composed of primes $\leq y$ defined by:*

$$\psi_2(x, y) = \sum_{\substack{m<x \\ p|m \Rightarrow p \leq y}} R^{\omega(m)}.$$

If $y = (\log x)^a$ and $1 \leq a \leq (\log x)^{1/2}/(2 \log\log x)$, then

$$\psi_2(x, y) < x^{1-1/a} \exp\left(\frac{(\log a + O(R)) \log x}{a \log\log x}\right).$$

The proof of this proposition parallels with Proposition 3.1.1. For,

$$\psi_2(x, y) \leq \sum_{\substack{n \leq x \\ p|n \Rightarrow p \leq y}} \left(\frac{x}{n}\right)^{\sigma} R^{\omega(n)} \leq x^{\sigma} \sum_{p|n \Rightarrow p \leq y} \frac{R^{\omega(n)}}{n^{\sigma}} = x^{\sigma} \prod_{p \leq y} \left(1 + \frac{R}{p^{\sigma}} + \frac{R}{p^{2\sigma}} + \cdots\right).$$

We see that the Dirichlet series part behaves like R-th power of the previous one in Proposition 3.1.1. Again with $z = (\log x)^{\frac{1}{2}(\log x)^{2/5}}$, we obtain the upper bound by the above proposition:

$$\sum_{m \in F} R^{\omega(m)} \ll_{K,R} x \exp(-\frac{2}{5}(\log x)^{3/5}).$$

Let $\pi_K(x; \mathfrak{m}, \mathfrak{a}) = \#\{\mathfrak{p} : \text{ prime ideal; } N(\mathfrak{p}) \leq x, \text{ and } \mathfrak{p} \sim \mathfrak{a} \bmod \mathfrak{m}\}$.

The following is a number field analogue of the Bombieri-Vinogradov theorem due to Huxley [Hu, Theorem 1].

Theorem 3.1.5 (Huxley)**.** *For each positive constant B, there is a positive constant $C = C(B)$ such that*

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

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

3.1.2 Brun-Titchmarsh Inequality

The classical Brun-Titchmarsh inequality concerns about an upper bound of the number of primes in arithmetic progression:

Theorem 3.1.6 (Brun-Titchmarsh). *Let a, q be integers with $(a, q) = 1$. Let $\pi(x; q, a)$ as above, and x, y be positive real numbers with $y \geq 2q$. Then*

$$\pi(x + y; q, a) - \pi(x; q, a) \leq \frac{2y}{\phi(q) \log(y/q)} \left(1 + O\left(\frac{1}{\log(y/q)}\right)\right).$$

There is a number field analogue of Brun-Titchmarsh inequality due to J. Hinz and M. Lodemann [HL, Theorem 4].

Theorem 3.1.7 (Hinz-Lodemann). *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*

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

3.2 Zero-Free Regions of L-functions

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

Theorem 3.2.1. *(Fogels, 1962) Let K be a number field, χ be any Grossencharacter of K defined modulo its conductor $\mathfrak{f}$. We denote by $L(s, \chi)$ the associated L-function. Let further $D = |\Delta| N\mathfrak{f} = D_0 > 1$ 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*

$$\sigma \geq 1 - \frac{c}{\log D(1 + |t|)} \geq \frac{3}{4} \quad (\sigma = Re\ s,\ t = Im\ s) \tag{3.1}$$

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 (3.1) a simple zero β of $L(s,\chi)$(which we call Siegel-zero).

Here, we use an analogous lemma, which generalizes Dirichlet's Theorem on arithmetic progressions. (see [F])

Lemma 3.2.1. *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*

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

Then

$$\psi(x,\mathfrak{m},\mathfrak{a}) = \frac{x}{h(\mathfrak{m})} - \frac{\overline{\chi_1}(\mathfrak{a})}{h(\mathfrak{m})}\frac{x^{\beta_1}}{\beta_1} + O\left(xe^{-c\sqrt{\log x}}\right). \tag{3.2}$$

Applying partial summation, we have

$$\pi(x,\mathfrak{m},\mathfrak{a}) := \#\{N\mathfrak{p}\le x \mid \mathfrak{p}\sim\mathfrak{a}\ mod\ \mathfrak{m}\} = \frac{Li(x)}{h(\mathfrak{m})} - \frac{\overline{\chi_1}(\mathfrak{a})}{h(\mathfrak{m})}Li(x^{\beta_1}) + O\left(xe^{-c_1\sqrt{\log x}}\right) \tag{3.3}$$

for some positive constants c, c_1 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.

3.2.1 Chebotarev Density Theorem

Let K be a number field and L a normal extension of K with Galois group $G = G(L/K)$. Let d_L and d_K denote the absolute values of discriminants of L and K. Let $n_L = [L:\mathbb{Q}]$, $n_K = [K:\mathbb{Q}]$. For each conjugacy class C of G, define

$$\pi(x, L/K) = |\{\mathfrak{p} : \mathfrak{p} \text{ unramified in } L, [\mathfrak{p}, L/K] = C, N_{K/\mathbb{Q}}\mathfrak{p} \le x\}|.$$

The Chebotarev density theorem gives an asymptotic density of primes whose Artin symbol lie in a conjugacy class C. Indeed,

$$\pi_C(x, L/K) \sim \frac{|C|}{|G|}\mathrm{Li}(x) \quad \text{as } x \to \infty.$$

For practical applications, it is often useful to have the above in quantitative form. J.C. Lagarias and A.M. Odlyzko. (see [LO]) Their version include both conditional theorem on GRH and unconditional theorem. The conditional theorem states that

Theorem 3.2.2. *There exists an effectively computable positive absolute constant c_1 such that if the GRH holds for the Dedekind zeta function of L, then for every $x > 2$,*

$$|\pi_C(x, L/K) - \frac{|C|}{|G|}Li(x)| \leq c_1\{\frac{|C|}{|G|}x^{1/2}\log(d_L x^{n_L}) + \log d_L\}.$$

Furthermore, for practical use, we use a bound of discriminant of number field given by Serre [Se2, Proposition 6]:

Proposition 3.2.1. *Let K be a number field of degree n over $\mathbb{Q}$, $P(K)$ be the set of primes dividing d_K. Then we have*

$$\log d_K \leq (n-1)\sum_{p \in P(K)} \log p + n|P(K)|\log n.$$

An unconditional density theorem depends on Siegel-zero β_0 (real and simple) of Dedekind zeta function which satisfies:

Theorem 3.2.3. *If $n_K > 1$ then $\zeta_K(s)$ has at most one zero β_0 in the region defined by $s = \sigma + it$ with*

$$1 - (4\log d_K)^{-1} \leq \sigma \leq 1, \quad |t| \leq (4\log d_K)^{-1}.$$

We state the unconditional Chebotarev density theorem:

Theorem 3.2.4. *Let K be a Galois extension of $\mathbb{Q}$. Let β_0 as above. Then there exist effec-*

tively computable positive absolute constants c_3 and c_4 such that if $x \geq \exp(10n_K(\log d_K)^2)$, then

$$|\pi_C(x) - \frac{|C|}{|G|}Li(x)| \leq \frac{|C|}{|G|}Li(x^{\beta_0}) + c_3 x \exp(-c_4 n_K^{-1/2}(\log x)^{1/2}),$$

where the β_0 term is present only when β_0 exists.

3.3 Sieve Methods

The use of sieve theory in elliptic curves originates from [GM]. They use their [GM, Lemma 3] to prove that any elliptic curve E over $\mathbb{Q}$ with an irrational 2-division point, has infinitely many reduction $E(\mathbb{F}_p)$ modulo p such that $E(\mathbb{F}_p)$ is cyclic. The prime 2 requires a special care, for an elliptic curve $y^2 = x^3 + ax + b$ defined over $\mathbb{Q}$, let K_2 be a quadratic or cubic subfield of $\mathbb{Q}(E[2])$. Precisely, K_2 is defined as follows,

$$K_2 = \begin{cases} \mathbb{Q}(\sqrt{-4a^3 - 27b^3}) & \text{if } [\mathbb{Q}(E[2]) : \mathbb{Q}] = 2, \text{ or } 6 \\ \mathbb{Q}(\alpha) & \text{if } [\mathbb{Q}(E[2]) : \mathbb{Q}] = 3. \end{cases}$$

where α is a root of $x^3+ax+b = 0$ in $\overline{\mathbb{Q}}$. We want to impose that p does not split completely in K_2. We will see that this condition can be implemented as a congruence relation. Now, [GM, Lemma 3] states that

Lemma 3.3.1 (Gupta, Murty)**.** *Let $S_\epsilon(x)$ be the set of primes $p \leq x$ such that all odd prime divisors of $p-1$ are distinct and $\geq x^{\frac{1}{4}+\epsilon}$, p does not split completely in the field K_2, and E has good reduction at p. Then if $K_2 \neq \mathbb{Q}$ there is an $\epsilon > 0$ such that $|S_\epsilon(x)| \gg x/\log^2 x$.*

On the other hand, for E an elliptic curve over $\mathbb{Q}$ with CM by the full ring of integers $\mathcal{O}_K$, which necessarily have a quadratic CM-field K, we impose additional congruence relation. Then we have:

Lemma 3.3.2. *Let $S_\epsilon(x)$ be the set of primes $p \leq x$ such that all odd prime divisors of $p-1$ are distinct and $\geq x^{\frac{1}{4}+\epsilon}$, p does not split completely in the field K_2, p splits completely in the*

imaginary quadratic CM field K, and E has good reduction at p. Then if $K_2 \neq \mathbb{Q}$ there is an $\epsilon > 0$ such that $|S_\epsilon(x)| \gg x/\log^2 x$.

In order to justify the insertion of congruence conditions, we use the following generalized version of sieve lemma by Heath-Brown (see [He, Lemma 1]):

Lemma 3.3.3 (Heath-Brown)**.** *Let $k = 1, 2, 3$, and put $K = 2^k$. Let u, v be coprime integers such that $K|u-1$, $16|v$ and $\left(\frac{u-1}{K}, v\right) = 1$. Then there exists $\alpha \in (\frac{1}{4}, \frac{1}{2}]$, possibly depending on k, u, v such that*

$$|\{p \leq x | p \equiv u(\ mod\ v), \frac{p-1}{K} = P_2(\alpha)\}| \gg \frac{x}{(\log x)^2}.$$

Here $n \in P_2(\alpha)$ means that n is a product of at most 2 primes and each prime divisors of n is at least n^α. Note that contribution of primes $\ll \sqrt{x}$ is at most $O(\sqrt{x}/\log x)$. Thus, we may have in Lemma 3.3.2 that $\frac{p-1}{K} = P_2(\alpha)$ with each odd prime divisor of $\frac{p-1}{K}$ is $\geq x^\alpha$. Heath-Brown modified the proof of [BFI, Theorem 10] to include congruence conditions. [BFI, Theorem 10] states that:

Theorem 3.3.1 (Bombieri, Friedlander, Iwaniec)**.** *An arithmetic function $\lambda(q)$ is called well factorable of level Q if for any $Q_1, Q_2 \geq 1$ such that $Q_1 Q_2 = Q$ there exist two functions $\lambda_1(q_1)$, $\lambda_2(q_2)$ supported in $[1, Q_1]$ and $[1, Q_2]$ respectively such that*

$$|\lambda_1| \leq 1, \quad |\lambda_2| \leq 1 \quad \text{and} \quad \lambda = \lambda_1 * \lambda_2.$$

Let $a \neq 0$, $\epsilon > 0$ and $Q = x^{4/7-\epsilon}$. For any well factorable function $\lambda(q)$ of level Q and any $A > 0$ we have

$$\sum_{(q,a)=1} \lambda(q) \left(\psi(x; q, a) - \frac{x}{\varphi(q)}\right) \ll \frac{x}{(\log x)^A};$$

the implied constants depends at most on ϵ, a and A.

We will now show that the conditions in Lemma 3.3.1 can fit into the conditions in Lemma 3.3.2, hence proving Lemma 3.3.1.

Case 1) Quadratic case:

Let $\Delta = d_{K_2}$ be the discriminant of K_2. For prime p to be inert in K_2, we need $\left(\frac{\Delta}{p}\right) = -1$. We establish this by requiring p to satisfy the congruences: Let $p_0 \neq 3$ be a prime which divides Δ if exists.

$$\left(\frac{q}{p}\right) = 1 \text{ if } 3|\Delta,\ q \neq 3$$

$$\left(\frac{3}{p}\right) = -1.$$

$$\left(\frac{q}{p}\right) = 1 \text{ if } 3 \nmid \Delta,\ q \neq p_0|\Delta$$

$$\left(\frac{p_0}{p}\right) = -1.$$

Then by the Chinese Remainder Theorem(CRT), we have a congruence $p \equiv u_0 \pmod{v}$ such that p does not split completely in K_2 and $16|v$. Now, we modify our choice of u_0 by finding another prime q_0 and letting $u_1 = u_0 q_0^2$. Another requirement on u is $\left(\frac{u-1}{K}, v\right) = 1$ where K is the largest power of 2 dividing $u - 1$.

We see that $u_1 = u_0(q_0^2 - 1) + u_0$. Let $\rho|(u_0 - 1, v)$ be a prime. Then $\rho \neq 3$ from our definition of u_0. For $\rho \geq 5$, we require

$$q_0^2 - 1 \equiv 3 \pmod{\rho}$$

This is achievable by $q_0 \equiv 2 \pmod{\rho}$. For $\rho|v$, but $\rho \nmid u_0 - 1$, we set $u \equiv 2 \pmod{\rho}$. Let $q_0 \equiv 3$ (mod 16) so that $q_0^2 - 1 \equiv 8 \pmod{16}$. Find prime q_0 by CRT and Dirichlet's theorem on primes in arithmetic progression, and let $u \pmod{v}$ be the congruence satisfying

$$u \equiv u_1 \pmod{\rho} \text{ where } \rho|(u_0 - 1, v) \text{ is an odd prime}$$

$$u \equiv 2 \pmod{\rho} \text{ where } \rho \nmid u_0 - 1, \text{ but } \rho|v.$$

Then $p \equiv u \pmod{v}$ satisfies all conditions in [He, Lemma 1].

Case 2) Cubic case:

This is when $\mathbb{Q}(E[2]) = K_2$ is a cubic field over $\mathbb{Q}$. By Kronecker-Weber theorem, $K_2 \subset \mathbb{Q}(\zeta_n)$ for some n. Then we can establish a congruence modulo n such that p does not split completely in K_2. Let $v = 16n$, and denote the resulting congruence modulo v as $u_0 \pmod{v}$. For odd primes $\rho|(u_0 - 1, v)$, we set $u_1 = u_0(q_0^3 - 1) + u_0$. Let $q_0 \equiv 2 \pmod{\rho}$ if $\rho \neq 7$, and $q_0 \equiv 3 \pmod{7}$ if $\rho = 7$. For $\rho|v$, but $\rho \nmid u_0 - 1$, we set $u \equiv 2 \pmod{\rho}$. Finally, let $q_0 \equiv 5 \pmod{8}$. Find prime q_0 satisfying above congruences by CRT and Diricchlet's theorem on primes in arithmetic progression, and let $u \pmod{v}$ be the congruence satisfying

$$u \equiv u_1 \pmod{\rho} \text{ where } \rho|(u_0 - 1, v) \text{ is an odd prime}$$

$$u \equiv 2 \pmod{\rho} \text{ where } \rho \nmid u_0 - 1, \text{ but } \rho|v.$$

CHAPTER 4

Proof of Theorems

4.1 Average order of e_p

4.1.1 Proof of Theorem 1.1.1

Throughout this section, let E be 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. By Hasse's bound, we have

$$\sum_{p\leq x, p\nmid N} e_p = \sum_{p\leq x, p\nmid N} \frac{p}{d_p} + O\left(\sum_{p\leq x}\sqrt{p}\right), \tag{4.1}$$

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

$$\frac{1}{k} = \sum_{dm|k} \frac{\mu(d)}{m}. \tag{4.2}$$

Thus we obtain

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

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

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

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

$$\left|\sum_{dm=k}\frac{\mu(d)}{m}\right| \le 1 \tag{4.3}$$

and Lemma 2.5.1, obtaining

$$|S_2| \ll \sum_{y<k\le\sqrt{x}+1} x\cdot\frac{x}{k^2} \ll \frac{x^2}{y}. \tag{4.4}$$

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 Theorem 3.1.5. First, we take care of the inner sum by partial summation. Thus,

$$\begin{aligned}\sum_{p\le x, p\nmid N, k|d_p} p &= \int_{2-}^{x} t d\pi_E(t;k)\\ &= x\pi_E(x;k) - \int_2^x \pi_E(t;k)dt\\ &= \frac{x\mathrm{Li}(x)}{n_k} - \int_2^x \frac{\mathrm{Li}(t)}{n_k}dt + O\left(x|E_k(x)| + \int_2^x |E_k(t)|dt\right)\\ &= \frac{1}{n_k}\mathrm{Li}(x^2) + O\left(x\max_{t\le x}|E_k(t)| + 1\right).\end{aligned}$$

Next, we combine this with the trivial estimate $\pi_E(x;k) \ll x/k^2$ and Lemma 2.3.6, obtaining

$$S_1 = c_E\mathrm{Li}(x^2) + O\left(x\max_{t\le x}|E_2(t)|\right) + O\left(\frac{x^2}{y\log x} + \sum_{3\le k\le y} x\max_{t\le x}|E_k(t)| + \sqrt{x}\right) \tag{4.5}$$

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 Lemma 2.3.6, and positive due to [FK]. Here, Lemma 2.3.6 is used in bounding $\sum_{y<k} \frac{1}{n_k} \mathrm{Li}(x^2)$.

Let $\mathfrak{f} = (f)$ be a nonzero principal ideal of K which appears in Lemma 2.3.7. Let $\widetilde{\pi_E}(x;k) = \#\{\mathfrak{p} : N(\mathfrak{p}) \leq x, \mathfrak{p} \nmid k\mathfrak{f}, \mathfrak{p} \text{ splits completely in } K(E[k])\}$. By [AM, (3.2)], we have

$$\pi_E(x;k) = \frac{1}{2}\widetilde{\pi_E}(x;k) + O\left(\frac{x^{1/2}}{\log x}\right) + O(\log N) \text{ uniformly for } k \geq 3. \tag{4.6}$$

The factor $1/2$ comes from rational prime p which splits in K, and the first error term comes from counting rational primes $p \leq x$ 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 2.3.7 and $t(k) = O(1)$, we have

$$\widetilde{\pi_E}(x;k) - \frac{\mathrm{Li}(x)}{[K(E[k]) : K]} = \sum_{i=1}^{t(k)} \left(\pi_K(x, k\mathfrak{f}, \mathfrak{m}_i) - \frac{\mathrm{Li}(x)}{h(k\mathfrak{f})}\right) \tag{4.7}$$

for a fixed nonzero integral ideal $\mathfrak{f}$ of K. Again by $t(k) = O(1)$ and applying Lemma 3.1.5 as in [AM, page 10],

$$\sum_{3 \leq k \leq \frac{x^{1/4}}{N(\mathfrak{f})(\log x)^{C/2}}} \max_{t \leq x} \left|\widetilde{\pi_E}(t;k) - \frac{\mathrm{Li}(t)}{[K(E[k]) : K]}\right| \ll_{A,B} N \log N \frac{x}{(\log x)^{A+B+1}}, \tag{4.8}$$

where $C = C(A,B)$ is the corresponding positive constant in Lemma 3.1.5 for the positive constant $A + B + 1$.

Note that $T(\mathfrak{q}) \leq 6$ since there are at most 6 units in imaginary quadratic fields. Writing $\widetilde{E_k}(x) = \widetilde{\pi_E}(x;k) - \frac{\mathrm{Li}(x)}{[K(E[k]):K]}$, and using a bound $\max_{t \leq x} |E_2(t)| \ll x/\log^B x$ (see [AM,

Lemma 2.3]), we have

$$S_1 = c_E \mathrm{Li}(x^2) + O_{A,B}\left(\frac{x^2}{(\log x)^B}\right) + O\left(\frac{x^2}{y\log x} + \sum_{3\le k\le y} x \max_{t\le x} |\widetilde{E_k}(t)| + \frac{x^{3/2} y \log N}{\log x}\right) \quad (4.9)$$

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

$$S_1 = c_E \mathrm{Li}(x^2) + O_{A,B}\left(\frac{x^2}{(\log x)^B} + x^{7/4} N(\mathfrak{f})(\log x)^{C/2-1} + \frac{x^2 N \log N}{(\log x)^{A+B+1}} + \frac{x^{7/4}\log N}{N(\mathfrak{f})(\log x)^{1+C/2}}\right). \quad (4.10)$$

Note that $N = N(\mathfrak{f})|d_K|$ as in [AM, page 7, Remark 2.8], where d_K is the discriminant of K. Combining with the estimate of $|S_2|$ in (4.4), it follows that

$$\sum_{p\le x, p\nmid N} \frac{p}{d_p} = c_E \mathrm{Li}(x^2) + O_{A,B}\left(\frac{x^2}{(\log x)^B} + \frac{x^2 N \log N}{(\log x)^{A+B+1}} + x^{7/4} N (\log x)^C\right). \quad (4.11)$$

Theorem 1.1.1 now follows.

4.2 Bounds on the sum of d_p

4.2.1 Proof of Theorem 1.2.1

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 1.1.1:

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

We introduce a variable y and split the sum as shown in the proof of Theorem 1.1.1:

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

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:

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

Now, we use Lemma 3.1.7 to give an upper bound for each $\widetilde{\pi_E}(x;k)$:

$$\widetilde{\pi_E}(x;k) \le 2\frac{t(k)x}{h(k\mathfrak{f})\log\frac{x}{N(k\mathfrak{f})}}\left\{1 + O\left(\frac{\log\log 3\frac{x}{N(k\mathfrak{f})}}{\log\frac{x}{N(k\mathfrak{f})}}\right)\right\}. \tag{4.12}$$

Then we treat S_1 by (4.12), 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

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

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 $f(t) = \frac{1}{\log \frac{x}{t^2 M}}$.
Thus

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

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

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

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

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

Hence, it follows that

$$S_1 \ll x \log \log \frac{x}{N(\mathfrak{f})} \ll x \log \log x, \tag{4.13}$$

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

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

$$S_1 + S_2 \ll_A x \log \log x \tag{4.14}$$

Therefore, Theorem 1.2.1 now follows.

Note that the trivial bound in Theorem 1.2.1 given by Lemma 2.5.1 is $\ll x \log x$. The

number field analogue of Brun-Titchmarsh inequality (Lemma 3.1.7) contributed to the saving.

4.2.2 Proof of Theorem 1.2.2

We begin with the same method as in [FM, page 23], and use (4.6), (4.7):

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

Here, an important point is that the O-term in Lemma 3.2.1 does not depend on $\mathfrak{m}$.

Applying this to our lower bound, and using $t(k) = O(1)$, we deduce under NSZC,

$$\sum_{p\le x} d_p \gg_E \frac{x\log y}{\log x} + O\left(xy^2e^{-c'\sqrt{\log x}}\right) + O\left(\frac{y^2\sqrt{x}}{\log x}\right). \tag{4.15}$$

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 1.2.2 now follows.

4.3 Cyclicity Problem in larger number fields

4.3.1 Proof of Theorem 1.3.1

We have the following:

$$\sum_{N\mathfrak{p}\leq x}\sum_{m|d_1(\mathfrak{p})}\mu(m) = \sum_{m\leq\sqrt{x}+1}\mu(m)\sum_{\substack{N\mathfrak{p}\leq x\\ m|d_1(\mathfrak{p})}}1$$
$$= \sum_{m\leq\sqrt{x}+1}\mu(m)\pi_E(x;m)$$

where $\pi_E(x;m) = \#\{N\mathfrak{p} < x : \mathfrak{p} \text{ splits completely in } L(E[m])\}$.

Let $S_1 = \sum_{m\leq\log^{B_1}x}$, and $S_2 = \sum_{\log^{B_1}x<m<\sqrt{x}+1}$ where B_1 will be chosen optimally later. For elliptic curves, we have

$$\pi_E(x;m) \ll \frac{x}{m^2} \tag{4.16}$$

by Lemma 2.5.1 (see also [K, Lemma 5.2]). Thus, we obtain $S_2 \ll x/\log^{B_1}x$. Here and after, all implied constants will depend at most on L.

We treat S_1 by Lemma 2.3.7. In fact,

$$\pi_E(x;m) = \sum_{i=1}^{t(m)}\pi(x;mf,\mathfrak{a}_i),$$

where $t(m) \leq m^N/T(mf)$ as in Lemma 2.3.7. Here, N depends only on E. We write

$$\pi(x;mf,\mathfrak{a}_i) = \frac{\mathrm{Li}(x)}{h(mf)} + E_i(x,(mf)).$$

Then

$$\pi_E(x;m) = \sum_{i=1}^{t(m)} \left(\frac{1}{h(mf)} \mathrm{Li}(x) + E_i(x,(mf)) \right)$$
$$= \frac{1}{[L(E[m]):L]} \mathrm{Li}(x) + \sum_{i=1}^{t(m)} E_i(x,(mf)).$$

Therefore,

$$S_1 = \sum_{m \leq \log^{B_1} x} \left(\frac{\mu(m)}{[L(E[m]):L]} \mathrm{Li}(x) + \mu(m) \sum_{i=1}^{t(m)} E_i(x,(mf)) \right)$$
$$= c_E \mathrm{Li}(x) + O_E\left(\frac{x}{\log^{B_1} x} \right) + O_E\left(\sum_{m \leq \log^{B_1} x} t(m) \max |E_i(x,(mf))| \right)$$
$$= c_E \mathrm{Li}(x) + O_E\left(\frac{x}{\log^{B_1} x} \right) + O_{E,B_2}\left(\frac{x}{\log^{B_2} x} \right)$$

with

$$c_E = \sum_{m=1}^{\infty} \frac{\mu(m)}{[L(E[m]):L]}.$$

Therefore, the constant c_E is nonnegative since it is the asymptotic density of a certain set of prime ideals.

4.4 Analogous theorems for abelian varieties of CM type

4.4.1 Proof of Theorem 1.4.7

We begin with:

$$\sum_{m \leq \sqrt{x}+1} f(m)\pi_{\mathcal{A}}(x;m) = \sum_{m \leq y} f(m)\pi_{\mathcal{A}}(x;m) + \sum_{y < m \leq \sqrt{x}+1} f(m)\pi_{\mathcal{A}}(x;m)$$
$$= S_1 + S_2,$$

where y will be determined later.

To treat S_1, we use Chebotarev density theorem. (see Theorem 3.2.2):

$$\begin{aligned} S_1 &= \sum_{m<y} f(m) \left(\frac{1}{[k(\mathcal{A}[m]) : k]} \mathrm{Li}(x) + O(x^{1/2} \log mx) \right) \\ &= \sum \frac{f(m)}{[k(\mathcal{A}[m]) : k]} \mathrm{Li}(x) + O\left(\sum_{m>y} \frac{f(m)}{[k(\mathcal{A}[m]) : k]} \frac{x}{\log x} \right) + O\left(\sum_{m<y} x^{1/2} |f(m)| \log x \right) \end{aligned}$$

S_2 can be bounded by Lemma 2.5.1:

$$S_2 \ll \sum_{m>y} m^{\alpha} \frac{x^g}{m^{2g}} \ll \frac{x^g}{y^{2g-\alpha-1}}.$$

By Lemma 2.3.5, the error terms can be simplified to:

$$O\left(\frac{x}{y \log x} + x^{1/2} y^{\alpha+1} \log x + \frac{x^g}{y^{2g-\alpha-1}} \right).$$

Choosing $y = x^{\beta}$ with $\beta = (g - 1/2)/(2g)$, the error terms become

$$O_{\mathcal{A},\epsilon}(x^{\frac{4g+2g\alpha-\alpha-1}{4g}+\epsilon}).$$

4.4.2 Proof of Theorem 1.4.8

We split the range of sum into two parts $S_1 = \sum_{m \le \log^{B_1} x}$, and $S_2 = \sum_{\log^{B_1} x < m < cx^{\frac{1}{2l}}}$. It is easier to bound S_2 as before. We have $S_2 \ll \frac{x}{\log^{B_1} x}$ by Theorem 3.1.6 (Brun-Titchmarsh

inequality), and Lemma 2.3.5. For S_1, by Lemma 2.3.7, we write

$$\begin{aligned}\pi_{\mathcal{A}}(x;m) &= \sum_{i=1}^{t(m)} \pi_{\mathcal{A}}(x;(mf),\mathfrak{a}_i) \\ &= \sum_{i=1}^{t(m)} \left(\frac{1}{h(mf)} \mathrm{Li}(x) + E_i(x,(mf)) \right) \\ &= \frac{1}{[k(\mathcal{A}[m]):k]} \mathrm{Li}(x) + \sum_{i=1}^{t(m)} E_i(x,(mf))\end{aligned}$$

where $\pi_{\mathcal{A}}(x;(mf),\mathfrak{a}_i) = \#\{N\mathfrak{p} \leq x \mid \mathfrak{p} \sim \mathfrak{a}_i\}$.

We substitute this into the sum S_1, then by Lemma 3.1.6 (Bombieri-Vinogradov theorem), and Lemma 2.3.5 we have

$$\begin{aligned}S_1 &= \sum_{m \leq \log^{B_1} x} \left(\frac{f(m)}{[k(\mathcal{A}[m]):k]} \mathrm{Li}(x) + f(m) \sum_{i=1}^{t(m)} E_i(x,(mf)) \right) \\ &= c_{f,\mathcal{A}} \mathrm{Li}(x) + O_{\mathcal{A}}\left(\frac{x}{\log^{B_1} x} \right) + O_{\mathcal{A}}\left(\sum_{m \leq \log^{B_1} x} m^{\alpha} t(m) \max |E_i(x,(mf))| \right) \\ &= c_{f,\mathcal{A}} \mathrm{Li}(x) + O_{\mathcal{A}}\left(\frac{x}{\log^{B_1} x} \right) + O_{\mathcal{A},B_2}\left(\frac{x}{\log^{B_2} x} \right)\end{aligned}$$

where

$$c_{f,\mathcal{A}} = \sum_{m=1}^{\infty} \frac{f(m)}{[k(\mathcal{A}[m]):k]}.$$

Combining the estimates for S_1 and S_2 finishes the proof. Note that the assumption $\alpha < 2$ guarantees the convergence of the series defining $c_{f,\mathcal{A}}$.

4.4.3 Proof of Theorem 1.4.10

Recall that

$$t(m) = \frac{h(mf)}{[K(\mathcal{A}[m]):K]} \leq \frac{m^{2g-\nu}}{T(mf)} c^{w(m)}$$

where f is the integer as in Lemma 2.3.4 and ν is the integer as in Lemma 2.3.5. Also, note that the field of definition is assumed to be the CM field K. Since we have $g = 2$ in our case, the number $\nu = 3$ is the only possibility by Lemma 2.3.5. Thus, we have

$$t(m) \leq \frac{m}{T(mf)} c^{w(m)}.$$

By Dirichlet's unit theorem, K has infinitely many units. Then by Theorem 3.1.3, the for almost all m within $1 \leq m < \sqrt{x}$, such that $T(mf) \gg \exp(\frac{1}{5}(\log x)^{2/5})$. The exceptional m's contribute to $O(\sqrt{x}\exp(-\frac{1}{5}(\log x)^{3/5}))$. Denote by B the set of these exceptional m's. Then the summation is bounded above by:

$$\sum_{m<\sqrt{x}} t(m) \ll_K \sum_{m<\sqrt{x}} \frac{mc^{w(m)}}{\exp(\frac{1}{5}(\log x)^{2/5})} + \sum_{m\in B} mc^{w(m)}.$$

The first sum on the right is bounded above by:

$$\frac{\sqrt{x}}{\exp(\frac{1}{5}(\log x)^{2/5})} \sum_{m<\sqrt{x}} c^{w(m)} \ll_K \sqrt{x}\exp(-\frac{1}{5}(\log x)^{2/5})\sqrt{x}(\log x)^{c-1} \ll x\exp(-\frac{1}{6}(\log x)^{2/5}).$$

On the second sum, we have the following upper bound:

$$\sqrt{x}\sum_{m\in B} c^{w(m)}.$$

Then by Proposition 3.1.3, the above is bounded by:

$$\sqrt{x}\sqrt{x}\exp(-\frac{1}{6}(\log x)^{3/5}) = x\exp(-\frac{1}{6}(\log x)^{3/5}).$$

Therefore, Theorem 1.4.10 now follows.

4.5 Positivity Conditions for Rational Elliptic Curves

4.5.1 Proof of Theorem 1.5.1

By Proposition 2.6.1, it follows that

Corollary 4.5.1. *Let E be a non-CM elliptic curve. Then we have*

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{[\mathbb{Q}(E[k]) : \mathbb{Q}]} = \left(\sum_{k \in \langle 2NA(E) \rangle} \frac{\mu(k)}{[\mathbb{Q}(E[k]) : \mathbb{Q}]} \right) \prod_{p \nmid 2NA(E)} \left(1 - \frac{1}{\psi(p)} \right).$$

For $j > 1$ with $(j, 2NA(E)) = 1$, similar formula holds true,

Corollary 4.5.2. *Let E be a non-CM elliptic curve. Then we have*

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{[\mathbb{Q}(E[jk]) : \mathbb{Q}(E[j])]} = \left(\sum_{k \in \langle 2NA(E) \rangle} \frac{\mu(k)}{[\mathbb{Q}(E[k]) : \mathbb{Q}]} \right) \prod_{p \nmid 2NA(E)} \left(1 - \frac{\psi(j)}{\psi(jp)} \right).$$

Thus, positivity of $\sum \frac{\mu(k)}{[\mathbb{Q}(E[k]):\mathbb{Q}]}$ is equivalent to positivity of $\sum \frac{\mu(k)}{[\mathbb{Q}(E[jk]):\mathbb{Q}]}$ in $(j, 2NA(E)) = 1$. On the other hand, positivity of former one follows from [CM, Theorem 1.1]. Therefore, we have Theorem 1.5.1.

4.5.2 Proof of Theorem 1.5.2

First, notice that

$$C_{E,j} = \sum_{k=1}^{\infty} \frac{\mu(k)}{[\mathbb{Q}(E[jk]) : \mathbb{Q}(E[j])][\mathbb{Q}(E[j]) : \mathbb{Q}]}.$$

We prove positivity of $C_{E,j}[\mathbb{Q}(E[j]) : \mathbb{Q}]$.

Since $(j, 6N) = 1$, we know that $\mathbb{Q}(E[j])$ contains K. Proving positivity of $C_{E,j}[\mathbb{Q}(E[j]) : \mathbb{Q}]$ is equivalent to proving that of

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{[K(E[jk]) : K(E[j])]}.$$

Note that the number of primes $\mathfrak{p}$ in K with $N\mathfrak{p} \leq x$ that lie above p, and p is inert in K, is $O(\frac{\sqrt{x}}{\log x})$. We are now ready to prove Theorem 1.5.2.

Hence, we see that

$$|\{N\mathfrak{p} \leq x : E \text{ has a good reduction at } \mathfrak{p}, d_1(\mathfrak{p}) = 1\}| \gg \frac{x}{\log^2 x}. \tag{4.17}$$

The following proposition is proved in [CM].

Proposition 4.5.1. *Let E be an elliptic curve over $\mathbb{Q}$ which has CM by $\mathcal{O}_K$. Then we have*

$$C_E \geq \frac{1}{2}$$

if $K \subseteq \mathbb{Q}(E[2])$. On the other hand,

$$C_E \geq \frac{1}{4}$$

if $K \nsubseteq \mathbb{Q}(E[2])$.

We provide an alternative proof of this proposition based on our theory. In fact, we have

$$C_E = \frac{1}{2} + \frac{1}{2}\sum_{k=1}^{\infty} \frac{\mu(k)}{[K(E[k]) : K]}$$

if $K \subseteq \mathbb{Q}(E[2])$. On the other hand,

$$C_E = \frac{1}{2} - \frac{1}{2[K(E[2]) : K]} + \frac{1}{2}\sum_{k=1}^{\infty} \frac{\mu(k)}{[K(E[k]) : K]}$$

if $K \nsubseteq \mathbb{Q}(E[2])$. Since $E[2]$ is not rational over $\mathbb{Q}$, we see that $[K(E[2]) : K] = [\mathbb{Q}(E[2]) : \mathbb{Q}] \geq 2$ in the second case. Moreover,

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{[K(E[k]) : K]} \geq 0$$

because this is the density of prime ideals $\mathfrak{p}$ such that $N\mathfrak{p} \leq x$, $d_1(\mathfrak{p}) = 1$, and E has a good

reduction at $\mathfrak{p}$. (see Theorem 1.3.1)

Applying methods shown in [FK, Chapter 7] (see Proposition 2.6.2) to CM case, we have

Corollary 4.5.3. *Let E be an elliptic curve that has CM by $\mathcal{O}_K$. Then we have*

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{|G_k|} = \left(\sum_{k \in \langle 6N \rangle} \frac{\mu(k)}{|G_k|} \right) \prod_{p \nmid 6N} \left(1 - \frac{1}{\Phi(p)} \right).$$

For $j > 1$ with $(j, 6N) = 1$, similar formula holds true,

Corollary 4.5.4. *Let E be an elliptic curve that has CM by $\mathcal{O}_K$. Then we have*

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{[K(E[jk]) : K(E[j])]} = \left(\sum_{k \in \langle 6N \rangle} \frac{\mu(k)}{|G_k|} \right) \prod_{p \nmid 6N} \left(1 - \frac{\Phi(j)}{\Phi(jp)} \right).$$

If $k \in \langle 6N \rangle$ and $(6N, m) = 1$, then $|G_{jkm}| = |G_k||G_{jm}|$. Thus, $|G_{jkm}|/|G_j| = |G_k||G_{jm}|/|G_j|$. Since Φ is a multiplicative function of ϕ-type, we have $m \mapsto |G_{jm}|/|G_j|$ is a multiplicative function from positive integers coprime to $6N$.

These corollaries show that positivity of any one of the constants mentioned, would provide positivity of the other. The LHS of Corollary 4.5.3 represents the density of prime ideals $\mathfrak{p}$ such that $N\mathfrak{p} \leq x$, E has a good reduction at $\mathfrak{p}$, and $d_1(\mathfrak{p}) = 1$. This density must be positive because of (4.17), otherwise the number of the prime ideals above would be $O(\frac{x}{\log^3 x})$ which contradicts (4.17).

References

[AG] A. Akbary, D. Ghioca, *A Geometric Variant of Titchmarsh Divisor Problem*, International Journal of Number Theory Vol. 8, No. 1 (2012) 53.69

[AGP] S. Arias-de-Reyna, W. Gajda, S. Petersen, *Abelian varieties over finitely generated fields and the conjecture of Geyer and Jarden on torsion*, arXiv:1010.2444v1, available at http://arxiv.org/pdf/1010.2444v1.pdf

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

[BFI] E. Bombieri, J. Friedlander, H. Iwaniec, *Primes in Arithmetic Progression to Large Moduli*, Acta Mathematica, Volume 156, Issue 1, p 203-251

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

[C2] A. Cojocaru, *Questions About the Reductions Modulo Primes of an Elliptic Curve*, Centre de Recherches Mathematiques CRM Proceedings and Lecture Notes Volume ??, 2004

[Co] D. Cox, *Primes of the form* $x^2 + ny^2$, John Wiley & Sons. Inc.

[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)

[D] M. Deuring, *Die KlassenKörper der Komplexen Multiplikation*, Enz. Math. Wiss., Band 1-2, Heft 10, Teil II. Stuttgart: Teubner 1958.

[EM] P. Erdos, R. Murty, *On the Order of a mod p*, CRM Proceedings and Lecture Notes, Volume 19, (1999) pp. 87-97.

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

[FI] E. Fouvry, H. Iwaniec, *Primes in arithmetic progression*, Acta Arith. 42, 197-218, (1983)

[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

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

[He] D. R. Heath-Brown, *Artin's Conjecture for primitive roots*, Q. J. Math, Oxford. II. Ser. 37, 27-38, (1986)

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

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

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

[L] S. Lang, *Complex Multiplication*, Springer-Verlag, 1983

[LO] J. Lagarias, A. Odlyzko, *Effective Versions of the Chebotarev Density Theorem*, Algebraic Number Fields(L-functions and Galois properties), Edited by A. Fröhlich, Academic Press London: New York: San Francisco

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

[MV] H. Montgomery, R. Vaughan, *Multiplicative Number Theory I, Classical Theory*, Cambridge Studies in Advanced Mathematics, Cambridge University Press 2007.

[N] J. Neukirch, *Algebraic Number Theory*, Springer 1999

[Ri] K. Ribet, *Division Fields of Abelian Varieties with Complex Multiplication*, Memoires de la S. M. F. 2e serie, tome 2 (1980), p. 75-94

[Ru] K. Rubin, *Elliptic Curves with Complex Multiplication and the Conjecture of Birch and Swinnerton-Dyer*, available at http://wstein.org/swc/aws/notes/files/99RubinCM.pdf

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

[Se2] J-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Publications mathématiques de l'I.H.É.S., tome 54(1981), p. 123-201.

[Sh] G. Shimura, *Abelian Varieties with Complex Multiplications and Modular Functions*, Princeton University Press, 1998

[Si] J. Silverman, *The Arithmetic of Elliptic Curves*, 2nd Edition, Graduate Texts in Mathematics 106, Springer

[Si2] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Springer

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

[ST] J-P. Serre, J. Tate, *Good Reduction of Abelian Varieties*, The Annals of Mathematics, Second Series, Volume 88, Issue 3(Nov ., 1968), p. 492-517

[T] J. Tate, *Endomorphisms of Abelian Varieties over Finite Fields*, Inventiones Mathematicae, Volume 2, p. 134-144

[V] C. Virdol, *Cyclicity of Abelian Varieties*, http://www2.math.kyushu-u.ac.jp/∼virdol/

[W] A. Weil, *Varietes abeliennes et courbes algebriques*, Paris: Hermann, OCLC 826112 (1948).

[Wi] R. Wilson, *The Large Sieve in Algebraic Number Fields*,

[Wu] J. Wu, *The Average Exponent of Ellptic Curves Modulo p*, arXiv preprint arXiv:1206.5929 (2012)

[Z] J. Zelinsky, *Upper bounds for the number of primitive ray class characters with conductor below a given bound*, arXiv preprint arXiv:http://arxiv.org/abs/1307.2319