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

KIM, SUNGJIN

ABSTRACT. 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:

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

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 $1 \le i < g$.

We are interested in finding an asymptotic formula for the number of prime ideals $\mathfrak{p}$ with $N\mathfrak{p} < x$, $\mathcal{A}$ has a good reduction at $\mathfrak{p}$, $d_1(\mathfrak{p}) = 1$. We succeed in proving this under the assumption of the Generalized Riemann Hypothesis (GRH). Unconditionally, we achieve a short range asymptotic for abelian varieties of CM type, and the full cyclicity theorem for elliptic curves over a number field containing the CM field.

1. INTRODUCTION

Let E be an elliptic curve over $\mathbb{Q}$. If p is a prime of good reduction for E, then the structure of the reduction modulo p is well-known:

$$\mathbb{Z}/d_p\mathbb{Z} \oplus \mathbb{Z}/e_p\mathbb{Z}$$

where $d_p|e_p$. The cyclicity problem was originally proposed by J. P. Serre and proved under the Generalized Riemann Hypothesis (GRH). Let N be the conductor of elliptic curve E and denote by $\mathfrak{f}(x, E)$ the number of primes $p \le x$ of good reduction for E such that $d_p = 1$. A. Cojocaru and M. R. Murty obtained that if E does not have a complex multiplication (non-CM), then

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

under the GRH for the Dedekind zeta functions of division fields. If E has a complex multiplication (CM), they obtained

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

under the GRH for the Dedekind zeta functions of division fields. Unconditional error term in CM case is $O(x \log^{-A} x)$ for any positive A. In fact, R. Murty [M] obtained an asymptotic formula with that error term, and it was reformulated by A. Akbary and V. K. Murty [AM]:

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

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

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

Theorem 1.1. *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*

$$\mathfrak{f}(x, E) = C_E Li(x) + O_A\left(\frac{x}{\log^A x}\right) \tag{2}$$

where

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

We are interested in extending this to abelian varieties. Let $\mathcal{A}$ be a g-dimensional ($g \geq 2$) abelian variety defined over a number field k. Let $\mathfrak{p}$ be a prime in k such that $\mathcal{A}$ has a good reduction at $\mathfrak{p}$, and denote by $\mathcal{A}(\mathbb{F}_{\mathfrak{p}})$ the reduction of $\mathcal{A}$ modulo $\mathfrak{p}$. 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 focus on investigating $d_1(\mathfrak{p})$, especially the density of prime ideals $\mathfrak{p}$ such that $d_1(\mathfrak{p}) = 1$.

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 the GRH. Then R. Murty gave a general framework for various problems of this type. (see [M]) Upon generalization of cyclicity problem to higher dimensional abelian varieties, we have a huge technical difficulty 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: Let $\mathcal{A}$ be an abelian variety defined over $\mathbb{Q}$, and assume that the 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

$$\sum_{m=1}^{\infty} \frac{\mu(m)}{[\mathbb{Q}(\mathcal{A}[m]) : \mathbb{Q}]} \mathrm{Li}(x) + o\left(\frac{x}{\log x}\right). \tag{3}$$

We are able to 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

$$\sum_{m=1}^{\infty} \frac{\mu(m)}{[k(\mathcal{A}[m]) : k]} \mathrm{Li}(x) + o\left(\frac{x}{\log x}\right), \tag{4}$$

under the GRH for the extension $k(\mathcal{A}[m])$ over k. Our interest is obtaining similar theorems unconditionally with additional assumption on the abelian variety $\mathcal{A}$, especially abelian varieties of CM type. The following conjecture is what we expect:

Conjecture 1.1. *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 $B > 0$,*

$$\sum_{\substack{N\mathfrak{p} \leq x \\ d_1(\mathfrak{p})=1}} 1 = c_{\mathcal{A}} Li(x) + O_{\mathcal{A},B}\left(\frac{x}{\log^B x}\right), \tag{5}$$

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 (see [HL, Theorem 4]), we obtain a bound for $\pi_A(x; m)$.

$$\pi_{\mathcal{A}}(x; m) \ll \frac{x}{[k(\mathcal{A}[m]) : k]}, \tag{6}$$

provided that $2N(mf) < x$, and the implied constant depends on $\mathcal{A}$. The nonzero integer f is the integer from Lemma 2.1.

Thus, this bound is only applicable for small values of m. As A. Akbary and D. Ghioca pointed out in [AG], 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 the 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 formula in a short range instead of Conjecture 1.1:

Theorem 1.2. *Let $\mathcal{A}$ be an absolutely simple abelian variety of CM type $(K, \Phi, \mathfrak{a})$ of dimension $g \geq 2$ 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* $B > 0$,

$$\sum_{m<cx^{\frac{1}{2l}}} \mu(m)\pi_{\mathcal{A}}(x;m) = c_{\mathcal{A}}Li(x) + O_{\mathcal{A},B}\left(\frac{x}{\log^B x}\right), \tag{7}$$

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

$$\pi_{\mathcal{A}}(x;m) \ll \frac{x^g}{m^{2g}}, \tag{8}$$

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 the 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 1.1 is true under the GRH for Dedekind zeta functions of division fields with better error terms.

We turn our interest to the average behavior of $d_1(\mathfrak{p})$. Now, we consider the case $g \geq 2$. By Lemma 2.3, we have the convergence of

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

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). As before, we conjecture an upper bound result, and prove unconditional upper bound of a short range sum, and finally unconditional lower bound:

Conjecture 1.2. *Let* $\mathcal{A}, (K, \Phi), (K', \Phi'), k$ *be the same notations as above. Under the same hypotheses as in Theorem 1.2, for any positive* B,

$$\sum_{N\mathfrak{p}\leq x} d_1(\mathfrak{p}) = C_{\mathcal{A}}Li(x) + O_{\mathcal{A},B}\left(\frac{x}{\log^B x}\right). \tag{9}$$

Theorem 1.3. *Let* $\mathcal{A}, (K, \Phi), (K', \Phi'), k, g, g', l$ *be the same notations as above. Under the same hypotheses as in Theorem 1.2, for any positive* B, *there exists a positive constant* c *depending on* $\mathcal{A}$, *such that for any* $B > 0$,

$$\sum_{m\leq cx^{\frac{1}{2l}}} \varphi(m)\pi_{\mathcal{A}}(x;m) = C_{\mathcal{A}}Li(x) + O_{\mathcal{A},B}\left(\frac{x}{\log^B x}\right). \tag{10}$$

Theorem 1.4. *Let* $\mathcal{A}, (K, \Phi), (K', \Phi'), k$ *be the same notations as above. Under the same hypotheses as in Theorem 1.2, for any positive* B,

$$\sum_{N\mathfrak{p}\leq x} d_1(\mathfrak{p}) \geq C_{\mathcal{A}}Li(x) + O_{\mathcal{A},B}\left(\frac{x}{\log^B x}\right). \tag{11}$$

This is a direct consequence of Theorem 1.3:

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

We remark that the Conjectures 1.1 and 1.2 are true with a stronger error term under GRH for the Dedekind zeta function of division fields, and it can be generalized to:

Theorem 1.5. *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

$$\sum_{m\leq\sqrt{x}+1} f(m)\pi_{\mathcal{A}}(x;m) = c_{f,\mathcal{A}}Li(x) + O_{\mathcal{A},\epsilon}(x^{\frac{4g+2g\alpha-\alpha-1}{4g}+\epsilon}). \tag{12}$$

where

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

We also remark that the Theorems 1.2, 1.3, and 1.5 can be generalized to the following:

Theorem 1.6. *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 $B>0$,

$$\sum_{m<cx^{\frac{1}{2l}}} f(m)\pi_{\mathcal{A}}(x;m) = c_{f,\mathcal{A}}Li(x) + O_{\mathcal{A},B}\left(\frac{x}{\log^B x}\right), \tag{13}$$

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_1 be a finite extension of the field of definition k. Assume also GRH for the division fields $k_1(\mathcal{A}[m])$ over k_1 and let $c_{\mathcal{A},k_1} = \sum_{m=1}^{\infty} \frac{\mu(m)}{[k_1(\mathcal{A}[m]):k_1]}$. Then the constants $c_{\mathcal{A},k}$ and $c_{\mathcal{A},k_1}$ are related by an inequality $c_{\mathcal{A},k} \geq \frac{1}{[k_1:k]} c_{\mathcal{A},k_1}$. We prove this using (4). 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_1, then the number of primes $\mathcal{P}$ in k_1 with $N\mathcal{P} \leq x$ and $d_1(\mathcal{P}) = 1$ is

$$\sum_{m=1}^{\infty} \frac{\mu(m)}{[k_1(\mathcal{A}[m]) : k_1]} \mathrm{Li}(x) + o\left(\frac{x}{\log x}\right)$$

Consider a prime $\mathfrak{p}$ in k that lies below $\mathcal{P}$. Since $\mathcal{A}(\mathcal{O}_k/\mathfrak{p})$ forms a subgroup of $\mathcal{A}(\mathcal{O}_{k_1}/\mathcal{P})$ which is fixed by the 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 $[k_1 : k]$)-to-one" mapping. Hence the set $\{N\mathfrak{p} \leq x \mid d_1(\mathfrak{p}) = 1\}$ contains a subset of size at least

$$\frac{1}{[k_1 : k]} \sum_{m=1}^{\infty} \frac{\mu(m)}{[k_1(\mathcal{A}[m]) : k_1]} \mathrm{Li}(x) + o\left(\frac{x}{\log x}\right).$$

This proves the following theorem:

Theorem 1.7. *Let $\mathcal{A}, (K, \Phi), (K', \Phi'), k$ be the same notations as above, and k_1 be a finite extension of k. Assume the GRH for Dedekind zeta functions of division fields $k(\mathcal{A}[m])$ over k, and $k_1(\mathcal{A}[m])$ over k_1. Then we have*

$$\sum_{m=1}^{\infty} \frac{\mu(m)}{[k(\mathcal{A}[m]) : k]} \geq \frac{1}{[k_1 : k]} \sum_{m=1}^{\infty} \frac{\mu(m)}{[k_1(\mathcal{A}[m]) : k_1]}.$$

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

A difficulty in achieving Conjectures 1.1, and 1.2 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 2.2 on average in special cases:

Theorem 1.8. *Let $\mathcal{A}$ be an absolutely simple abelian variety of dimension 2 defined over a degree 4 CM-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 1.1 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 1.1 under the hypotheses of Theorem 1.8.

2. Preliminaries

2.1. **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 2.1. *A CM-field is a totally imaginary quadratic extension of a totally real number field.*

Theorem 2.1. *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 2.1. *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 2.2. *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 2.1. *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 a 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 2.2. *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. *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 $K = K'$.

Denote by $\mathbb{A}_k^\times$, $\mathbb{A}_K^\times$ the group of ideles of number fields k and K respectively. The following theorem is a version of the Main Theorem of Complex Multiplication for abelian varieties: (see [L, Theorem 1.1, p84])

Proposition 2.4 (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 2.1. *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 by $\mathcal{R}_K$ the subset of $\mathbb{A}_K^\times$ such that every component is integral with respect to each place (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. 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

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

□

A direct corollary of Lemma 2.1 is the following:

Lemma 2.2. *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 2.1. 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 below, 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 $\mathcal{A}$.

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

Lemma 2.3. *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(Φ, 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

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

2.2. **Analytic Background.** 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 $v_\mathfrak{p}(\mathfrak{m}) \leq v_\mathfrak{p}(\alpha - \beta)$ for all primes $\mathfrak{p}$ and $\alpha\beta^{-1}$ is totally positive. Then we can rewrite the equivalence relation $\sim$ by

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

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

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

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

Lemma 2.4 (Zelinsky)**.** *Let K be a number field such that $\mathcal{O}_K$ has infinitely many units. Then there is a constant $c > 1$ depending only on K such that*

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

uniformly on $\mathfrak{m}$.

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 $N\mathfrak{m} \le N(a^k - 1)$. There is a constant $C > 1$ depending only on a such that $|N(a^k - 1)| \le C^k$. Thus, $k \ge \log_C N\mathfrak{m}$ and this completes the proof. □

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

Theorem 2.3. *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 $1 \le m < x$, 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 2.5. *Let $\psi(x, y)$ be the number of all positive integers composed of primes $\le y$. If $y = (\log x)^a$ and $1 \le a \le (\log x)^{1/2}/(2 \log\log x)$, then*

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

Another big idea in proving Theorem 2.3 is from P. Erdos and R. Murty [EM]. They show in their introduction that for integer $a \ge 2$, there are at most $O(x/(\log x)^3)$ primes $p \le x$ 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 $p \le x$ such that $f(p) < \sqrt{x}/(\log x)$.

Proof of Theorem 2.3. 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 2.3 can be generalized to integral ideals. We want a lower bound of $T(\mathfrak{m})$ similar to Theorem 2.3 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 2.3. Note that $N((m)) = m^{[K:\mathbb{Q}]}$, thus we cannot require $m < x$. We need the following analogous proposition to Proposition 2.5:

Proposition 2.6. *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:

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

Theorem 2.4. *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 are arranged in 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 2.5 by inserting extra factor $R^{\omega(n)}$.

Proposition 2.7. *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 2.5. 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 2.5. Again with $z = (\log x)^{\frac{1}{2}(\log x)^{2/5}}$, we obtain the upper bound by the above proposition:

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

3. Proof of the theorems

3.1. **Proof of Conditional Theorems.**

Proof of Theorem 1.5. We begin with:

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

where y will be determined later.

To treat S_1, we use the Chebotarev density theorem:

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

S_2 can be bounded by [K, Lemma 5.2]:

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

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

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

□

3.2. **Proof of Unconditional Theorems.**

Proof of Theorem 1.1. We have the following:

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

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

Let $S_1 = \sum_{m\le\log^{B_1}x}$, 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

$$\pi_E(x;m) \ll \frac{x}{m^2} \tag{14}$$

by [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. In fact,

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

where $t(m) \le m^N/T(mf)$ as in Lemma 2.3. 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,

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

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. □

Proof of Theorem 1.6. 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 the Brun-Titchmarsh inequality, and Lemma 2.2. For S_1, by Lemma 2.3, we write

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

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

We substitute this into the sum S_1, then by the Bombieri-Vinogradov theorem, and by Lemma 2.2 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 $c_{f,\mathcal{A}}$. □

Proof of Theorem 1.8. 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 2.2 and ν is the integer as in Lemma 2.3. 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. 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 2.3, 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 2.7, 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 1.8 now follows. □

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

[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 36, 2004

[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)

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

[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

[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

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

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

[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