AVERAGE RECIPROCALS OF THE ORDER OF a MODULO n

KIM, SUNGJIN

Abstract. Let $a > 1$ be an integer. Denote by $l_a(n)$ the multiplicative order of a modulo integers n . We prove that

$$\sum_{n\le x,(n,a)=1} \frac{1}{l_a(n)} = O_a\left(x \exp\left(-\left(\frac{1}{2}+o(1)\right)\log x \frac{\log\log\log x}{\log\log x}\right)\right),$$

which is an improvement over [19, Theorem 5].

Further, we obtain several applications toward number fields and 2-dimensional abelian varieties of CM-type.

1. Introduction

Define $l_a(n)$ by the multiplicative order of a modulo n. In [7], Kurlberg and Rudnick showed that there exist a $\delta > 0$ such that $l_a(n) \gg \sqrt{n}\exp(\log n)^{\delta}$ for all but $o(x)$ integers $n \le x$. In [8], Kurlberg and Pomerance obtained the following result by applying Fouvry's result (see [2]). For some $\gamma > 0$, $l_a(n) \gg n^{1/2+\gamma}$ for positive proportion of $n \le x$.

On the other hand, Zelinsky [19] proved that

$$\sum_{n\le x,(n,a)=1} \frac{\varphi(n)}{l_a(n)} = O_a\left(\frac{x^2}{\log^{\alpha} x}\right)$$

for any $0 < \alpha < 3$. Indeed, this result can be interpreted as

$$\sum_{n\le x,(n,a)=1} \frac{1}{l_a(n)} = O_a\left(\frac{x}{\log^{\alpha} x}\right)$$

for any $0 < \alpha < 3$. Furthermore, he was able to generalize to number fields. Let K be a number field, and assume that U_K its group of units is infinite. Let R_K be the ring of integers in K. For integral ideal I, denote by NI the norm of I, and $\varphi(I)$ the Euler's totient function of I, which is defined by:

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

Denote by $U_K(I)$ the subgroup of U_K formed by elements which are 1 modulo I. He obtained that

$$\sum_{NI\le x} \frac{\varphi(I)}{[U_K : U_K(I)]} = O_K\left(\frac{x^2}{\log^{\alpha} x}\right)$$

This also can be interpreted as

$$\sum_{NI\le x} \frac{1}{[U_K : U_K(I)]} = O_K\left(\frac{x}{\log^{\alpha} x}\right).$$

In the author's work [6, Theorem 2.3], it is shown that

$$[U_K : U_K(I)] \gg (\log x)^{\frac{1}{2}(\log x)^{2/5}}$$

for all but $O(x\exp(-\frac{2}{5}(\log x)^{3/5}))$ integal ideals $NI \le x$. This implies that

$$\sum_{NI\le x} \frac{1}{[U_K : U_K(I)]} = O_K\left(x\exp\left(-\frac{2}{5}(\log x)^{2/5}\right)\right).$$

The same idea as in [6, Theorem 2.3] also applies to

$$\sum_{n\le x,(n,a)=1}\frac{1}{l_a(n)}=O_a\left(x\exp\left(-\frac{2}{5}(\log x)^{2/5}\right)\right).$$

We show that the same idea in [6, Theorem 2.3] further leads to

$$\sum_{NI\le x}\frac{1}{[U_K:U_K(I)]}=O_K\left(x\exp\left(-c\sqrt{\log x\log\log x}\right)\right),$$

also

$$\sum_{n\le x,(n,a)=1}\frac{1}{l_a(n)}=O_a\left(x\exp\left(-c\sqrt{\log x\log\log x}\right)\right)$$

for some positive constant c. Adopting an idea from Pomerance [13], we further improve these:

Theorem 1.1. *Let $l_a(n)$ be the multiplicative order of a modulo n. Then*

$$\sum_{n\le x,(n,a)=1}\frac{1}{l_a(n)}=O_a\left(x\exp\left(-\left(\frac{1}{2}+o(1)\right)\log x\frac{\log\log\log x}{\log\log x}\right)\right).$$

Furthermore, let K be a number field, and assume that U_K its group of units is infinite. For an integral ideal I, denote by $U_K(I)$ the subgroup of U_K formed by elements which are 1 modulo I. Then

$$\sum_{NI\le x}\frac{1}{[U_K:U_K(I)]}=O_K\left(x\exp\left(-\left(\frac{1}{2}+o(1)\right)\log x\frac{\log\log\log x}{\log\log x}\right)\right).$$

It is possible to apply this to improve on [6, Theorem 1.8]. Let $\mathcal{A}$ be a g-dimensional ($g\ge 2$) 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 $1\le i<g$. For the definition of $t(m)$, we refer to Lemma 2.3.

Theorem 1.2. *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*

$$\sum_{m<\sqrt{x}}t(m)=O_K\left(x\exp\left(-\left(\frac{1}{4}+o(1)\right)\log x\frac{\log\log\log x}{\log\log x}\right)\right).$$

The significance in this theorem is that this opens up a possibility of proving a special case $g=2$ of the author's Conjecture 1.1 in [6] 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 probably help in bounding the number of prime ideals with $N\mathfrak{p}\le x$ in each $t(m)$ residue classes $\mathfrak{a}_i$ modulo (mf). Then the following conjecture (see [6, Conjecture 1.1]) would follow by counting the number of prime ideals splitting completely in the division field $k(\mathcal{A}[m])$ by considering residue classes (see also Lemma 2.3):

Conjecture 1.1. *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*

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

where

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

In fact, this conjecture was made in an effort to generalize a theorem by Freiberg and Pollack [3, Theorem 1.1] to abelian varieties.

2. Backgrounds and Proofs

2.1. **Smooth Numbers.** Let $\psi(x, y)$ be the number of positive integers $n \leq x$ whose prime divisors $p \leq y$. For any $U > 0$, it is well known that

$$\psi(x, x^{1/u}) = x\rho(u) + O\left(\frac{x}{\log x}\right)$$

uniformly for $1 \leq u \leq U$. The function $\rho(u)$ is called the Dickman function, and it satisfies

$$\rho(u) = 1 \quad \text{for } 0 < u \leq 1,$$

$$-u\rho'(u) = \rho(u-1) \quad \text{for } u > 1.$$

This function also satisfies the following asymptotic formula (see [1]):

$$\rho(u) = \exp\left(-u\left(\log u + \log\log u - 1 + \frac{\log\log u}{\log u} - \frac{1}{\log u} + O\left(\frac{(\log\log u)^2}{(\log u)^2}\right)\right)\right).$$

From the upper bound of de Bruijn [1], and lower bound of Hildebrand [5], we have

Theorem 2.1. *Let $\epsilon > 0$, we have*

$$\psi(x, x^{1/u}) = x\rho(u)\exp\left(O_\epsilon(u\exp(-(\log u)^{3/5-\epsilon}))\right)$$

uniformly for $1 \leq u \leq (1-\epsilon)\log x/\log\log x$.

For a fixed positive c, let $u = \frac{\sqrt{\log x}}{c\sqrt{\log\log x}}$. Then we have

Corollary 2.1. *For $x \geq x_0(c)$, we have*

$$\psi\left(x, \exp\left(c\sqrt{\log x \log\log x}\right)\right) = x\exp\left(\left(-\frac{1}{2c} + o(1)\right)\sqrt{\log x\log\log x}\right).$$

For a given number field K, define $\psi_K(x, y)$ to be the number of integral ideals I with $NI \leq x$ such that $N\mathfrak{p} \leq y$ for any prime ideal $\mathfrak{p}|I$. Then the above theorem and corollary have their analogue (see [4, Section 1.3]):

Theorem 2.2. *Let $\epsilon > 0$, we have*

$$\psi_K(x, x^{1/u}) = \psi_K(x, x)\rho(u)\exp\left(O_\epsilon(u\exp(-(\log u)^{3/5-\epsilon}))\right)$$

uniformly for $1 \leq u \leq (1-\epsilon)\log x/\log\log x$.

As before, for a fixed positive c, let $u = \frac{\sqrt{\log x}}{c\sqrt{\log\log x}}$. Then we have

Corollary 2.2. *For $x \geq x_0(c)$, we have*

$$\psi_K\left(x, \exp\left(c\sqrt{\log x\log\log x}\right)\right) = \psi_K(x, x)\exp\left(\left(-\frac{1}{2c} + o(1)\right)\sqrt{\log x\log\log x}\right).$$

Let $a > 1$ be an integer. For some $z > 0$, it is clear that $l_a(n) < z$ implies $n | \prod_{i<z}(a^i - 1)$. Since the number of prime factors of $\prod_{i<z}(a^i - 1)$ is $O_a(z^2/\log z)$, the number of integers $n \leq x$ such that $l_a(n) < z$ is $O_a(\psi(x, c_a z^2))$. This is due to the fact that n is consisted of prime divisors of $\prod_{i<z}(a^i - 1)$. Therefore, by taking $z = \exp\left(c\sqrt{\log x\log\log x}\right)$, we establish the following:

Lemma 2.1. *Let $a > 1$ be an integer. Then there is $c_a > 0$ such that*

$$l_a(n) \geq \exp\left(c_a\sqrt{\log x\log\log x}\right)$$

for all but $O_a\left(x\exp\left(-c_a\sqrt{\log x\log\log x}\right)\right)$ *integers* $n \leq x$.

Using the lower bound $\exp\left(c_a\sqrt{\log x\log\log x}\right)$ for most $n\le x$, and the trivial lower bound 1 for the exceptional set of $n\le x$, it follows that

$$\sum_{n\le x,(n,a)=1}\frac{1}{l_a(n)}=O_a\left(x\exp\left(-c_a\sqrt{\log x\log\log x}\right)\right)$$

for some positive constant c_a.

Furthermore, let K be a number field, and assume that $U_K=(\mathcal{O}_K)^*$ its group of units is infinite. For integral ideal I, denote by NI the norm of I. Denote by $U_K(I)$ the subgroup of U_K formed by elements which are 1 modulo I. Let $a\in U_K$ be a unit of infinite order. We use the notation $l_a(I)$ for the order of a modulo I. Then we have

$$[U_K:U_K(I)]\ge l_a(I).$$

The same idea as above applies, and we obtain for some $c_K>0$,

$$\sum_{NI\le x}\frac{1}{[U_K:U_K(I)]}=O_K\left(x\exp\left(-c_K\sqrt{\log x\log\log x}\right)\right),$$

To prove Theorem 1.1, we adopt an idea of Pomerance [13, Theorem 1]:

Theorem 2.3. *Let $a>1$ be an integer. There is an $x_0(a)$ such that if $x\ge x_0(a)$, then*

$$\sum_{m\le x,l_a(m)=n}1\le x\exp\left(-\left(\frac{1}{2}+o(1)\right)\log x\frac{\log\log\log x}{\log\log x}\right).$$

We may assume that $n<x$. Similarly as in [1, Section 3], Pomerance applies Rankin's method. Then for any $c>0$,

$$\sum_{m\le x,l_a(m)=n}1\le x^c\sum_{l_a(m)=n}m^{-c}\le x^c\sum_{p|m\Rightarrow l_a(p)|n}m^{-c}=x^c\prod_{l_a(p)|n}(1-p^{-c})^{-1}=x^cA.$$

Then the optimal choice for c is $c=1-(4+\log\log\log x)/(2\log\log x)$ with a requirement $\log A=o(\log x/\log\log x)$. Here, A is the Euler product

$$\prod_{l_a(p)|n}(1-p^{-c})^{-1}$$

which depends on both a and n. Taking the sum of the LHS of Theorem 2.3 for $n<z=\exp\left(\frac{1}{4}\log x\frac{\log\log\log x}{\log\log x}\right)$, we obtain a strengthened version of Lemma 2.1.

Lemma 2.2. *Let $a>1$ be an integer. Then there is $c_a>0$ such that*

$$l_a(n)\ge\exp\left(\frac{1}{4}\log x\frac{\log\log\log x}{\log\log x}\right)$$

for all but $O_a\left(x\exp\left(-\left(\frac{1}{4}+o(1)\right)\log x\frac{\log\log\log x}{\log\log x}\right)\right)$ integers $n\le x$.

However, we do not use the lemma to prove Theorem 1.2. Instead, observe the following:

$$\sum_{m\le x}\frac{1}{l_a(m)}=\sum_{n<x}\frac{1}{n}\sum_{m\le x,l_a(m)=n}1.$$

Applying Theorem 2.3 directly, we obtain that

$$\begin{aligned}\sum_{n<x}\frac{1}{n}\sum_{m\le x,l_a(m)=n}1&\le\sum_{n<x}\frac{1}{n}x\exp\left(-\left(\frac{1}{2}+o(1)\right)\log x\frac{\log\log\log x}{\log\log x}\right)\\&=O_a\left(x\exp\left(-\left(\frac{1}{2}+o(1)\right)\log x\frac{\log\log\log x}{\log\log x}\right)\right).\end{aligned}$$

This proves the first part of Theorem 1.1. The statement for the number fields follows from a modified version of Theorem 2.3.

Theorem 2.4. *Let a be an integral element of K which is not a root of unity. There is an $x_0(K,a)$ such that if $x \geq x_0(K,a)$, then*

$$\sum_{NI \leq x, l_a(I)=n} 1 \leq x \exp\left(-\left(\frac{1}{2}+o(1)\right)\log x \frac{\log\log\log x}{\log\log x}\right).$$

The proof is almost identical, with only difference in the Euler product:

$$\sum_{NI \leq x, l_a(I)=n} 1 \leq x^c \sum_{l_a(I)=n} NI^{-c} \leq x^c \sum_{\mathfrak{p}|I \Rightarrow l_a(\mathfrak{p})|n} NI^{-c} = x^c \prod_{l_a(\mathfrak{p})|n} (1-N\mathfrak{p}^{-c})^{-1} = x^c A.$$

As in the proof of [13, Theorem 1], we may assume that $x > n$ otherwise there are no I satisfying $NI \leq x$ together with $l_a(I) = n$. The Euler product A is treated by

$$\log A = \sum_{l_a(\mathfrak{p})|n} N\mathfrak{p}^{-c} + O([K:\mathbb{Q}]) = \sum_{d|n}\sum_{l_a(\mathfrak{p})=d} N\mathfrak{p}^{-c} + O([K:\mathbb{Q}]).$$

The prime ideals $\mathfrak{p}$ with $l_a(\mathfrak{p}) = d$ all divide the principal ideal (a^d-1). Then the number of prime ideals $\mathfrak{p}$ dividing (a^d-1) is $O\left([K:\mathbb{Q}]\frac{d\log|a'|}{\log(d+1)}\right)$ where a' is a conjugate of a with maximal $|a'|$. Let $\mathfrak{q}_1, \cdots, \mathfrak{q}_t$ be all prime divisors of (a^d-1). Note that for a given norm, there are at most $[K:\mathbb{Q}]$ prime ideals of the same norm. Each prime divisor $\mathfrak{q}_i$ of (a^d-1) satisfies $N\mathfrak{q}_i \equiv 1 \pmod d$. This is because $(\mathcal{O}_K/\mathfrak{q}_i)^*$ is a cyclic group of order $N\mathfrak{q}_i - 1$. Then we have

$$\sum_{l_a(\mathfrak{p})=d} N\mathfrak{p}^{-c} = \sum_{i=1}^{t} N\mathfrak{q}_i^{-c} \leq [K:\mathbb{Q}] \sum_{j \leq d\log|a'|} (dj+1)^{-c} \leq [K:\mathbb{Q}] d^{-c}(1-c)^{-1}(d\log|a'|)^{1-c}$$

Following the rest of the proof, we obtain that

$$\log A \leq [K:\mathbb{Q}]\log|a'|\frac{2\log\log x}{4+\log\log\log x}(\log x)^{1/2} + O([K:\mathbb{Q}]),$$

which yields $\log A = o(\log x/\log\log x)$. This completes the proof. Applying Theorem 2.4, we obtain the second part of Theorem 1.1.

We need a principal ideal version of Theorem 2.4 to prove corresponding result on 2-dimensional abelian varieties with CM type.

Theorem 2.5. *Let a be an integral element of K which is not a root of unity. There is an $x_0(K,a)$ such that if $x \geq x_0(K,a)$, then*

$$\sum_{m \leq x, l_a((m))=n} 1 \leq x \exp\left(-\left(\frac{1}{2}+o(1)\right)\log x \frac{\log\log\log x}{\log\log x}\right).$$

The proof is almost identical, with only difference in the Euler product:

$$\sum_{m \leq x, l_a((m))=n} 1 \leq x^c \sum_{l_a((m))=n} m^{-c} \leq x^c \sum_{p|m \Rightarrow l_a((p))|n} m^{-c} = x^c \prod_{l_a((p))|n} (1-p^{-c})^{-1} = x^c A.$$

As in the proof of [13, Theorem 1], we may assume that $x^{[K:\mathbb{Q}]} > n$ otherwise there are no m satisfying $m \leq x$ together with $l_a((m)) = n$. The Euler product A is treated by

$$\log A = \sum_{l_a((p))|n} p^{-c} + O(1) = \sum_{d|n}\sum_{l_a((p))=d} p^{-c} + O(1).$$

The primes p with $l_a((p)) = d$ all divide the principal ideal (a^d-1). Then prime p dividing (a^d-1) also divides the integer $N(a^d-1)$. The number of such p is $O\left([K:\mathbb{Q}]\frac{d\log|a'|}{\log(d+1)}\right)$ where a' is a conjugate of a with maximal $|a'|$. Let $q_1, \cdots, q_t$ be all prime divisors of $N(a^d-1)$. Each prime divisor q_i of $N(a^d-1)$ satisfies $q_i \equiv 1 \pmod d$. Then we have

$$\sum_{l_a((p))=d} p^{-c} = \sum_{i=1}^{t} q_i^{-c} \leq \sum_{j \leq [K:\mathbb{Q}]d\log|a'|} (dj+1)^{-c} \leq d^{-c}(1-c)^{-1}([K:\mathbb{Q}]d\log|a'|)^{1-c}$$

Following the rest of the proof, we obtain that

$$\log A \leq [K:\mathbb{Q}]\log|a'|\frac{2\log\log x}{4+\log\log\log x}(\log x)^{1/2}+O(1),$$

which yields $\log A = o(\log x/\log\log x)$. This completes the proof.

We may insert an extra factor $R^{w(m)}$ where $w(m)$ is the number of distinct prime divisors of m, yet the upper bound still holds.

Theorem 2.6. *Let a be an integral element of K which is not a root of unity. Let $R>0$. There is an $x_0(K,a,R)$ such that if $x \geq x_0(K,a,R)$, then*

$$\sum_{m\leq x, l_a((m))=n} R^{w(m)} \leq x\exp\left(-\left(\frac{1}{2}+o(1)\right)\log x\frac{\log\log\log x}{\log\log x}\right).$$

In this one, the Euler product behaves likes Rth power of the previous one. In fact,

$$\begin{aligned}\sum_{m\leq x, l_a((m))=n} R^{w(m)} &\leq x^c \sum_{l_a((m))=n} R^{w(m)}m^{-c} \leq x^c \sum_{p|m\Rightarrow l_a((p))|n} R^{w(m)}m^{-c}\\ &= x^c\prod_{l_a((p))|n}(1+Rp^{-c}+Rp^{-2c}+\cdots) = x^cA.\end{aligned}$$

the Euler product A is treated by

$$\log A = \sum_{l_a((p))|n} Rp^{-c}+O(R) = \sum_{d|n}\sum_{l_a((p))=d} Rp^{-c}+O(R).$$

Following the rest of the proof, we obtain that

$$\log A \leq R[K:\mathbb{Q}]\log|a'|\frac{2\log\log x}{4+\log\log\log x}(\log x)^{1/2}+O(R),$$

which yields $\log A = o(\log x/\log\log x)$. This completes the proof.

Corollary 2.3. *Let a be an integral element of K which is not a root of unity. Let $R>0$. Then*

$$\sum_{m\leq x}\frac{R^{w(m)}}{l_a((m))} \leq x\exp\left(-\left(\frac{1}{2}+o(1)\right)\log x\frac{\log\log\log x}{\log\log x}\right).$$

This is an easy consequence of Theorem 2.6. We write

$$\begin{aligned}\sum_{m\leq x}\frac{R^{w(m)}}{l_a((m))} &= \sum_{n<x^{[K:\mathbb{Q}]}}\frac{1}{n}\sum_{m\leq x, l_a((m))=n} R^{w(m)}\\ &\leq \sum_{n<x^{[K:\mathbb{Q}]}}\frac{1}{n}x\exp\left(-\left(\frac{1}{2}+o(1)\right)\log x\frac{\log\log\log x}{\log\log x}\right)\\ &= x\exp\left(-\left(\frac{1}{2}+o(1)\right)\log x\frac{\log\log\log x}{\log\log x}\right).\end{aligned}$$

2.2. **Abelian Varieties with CM-type.** We give necessary definitions and theorems that are required to state Theorem 1.3. For more details, one can refer to [16], also [9]. The Definition 2.1 to Lemma 2.5 are also required and present in [6]. Many of those are stated and proved in detail in [17], [15], also in [18]). We present them for this paper to be self-contained. 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-fields.

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

The following theorem is [9, p6, Theorem 1.3]:

Theorem 2.7. *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 [16, 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 [16, p41, Theorem 2], also [9, p72])

Theorem 2.8. *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 that $\mathfrak{a}$ 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 2.4. *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 [16, 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 [16, 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 [16, 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 $K'^{\times}$:

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

Let $\mathbb{A}_K^\times$, $\mathbb{A}_{K'}^\times$ be the K-ideles and K'-ideles respectively. 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 [16, 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 $K = K'$.

An analogue of [10, p 162, Lemma 4] can be obtained from applying the Main Theorem of Complex Multiplication (See [9, Theorem 1.1, p84]). The idea of the proof is the same as in [10, p 162, Lemma 4], but we need a modification due to type norm factor in the Main Theorem of Complex Multiplication.

Lemma 2.3. *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 $(mf) \subset k$.

For the proof of this, we refer to [6, Lemma 2.1].

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 $\alpha \equiv \beta$ (mod* $\mathfrak{m}$) 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

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

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 $\varphi(\mathfrak{m}) = |(\mathcal{O}_K/\mathfrak{m}\mathcal{O}_K)^\times|$.

The following lemma is a direct corollary of Lemma 2.3:

Lemma 2.4. *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. 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 2.5 below, there is an absolute positive constant R depending only on $\mathcal{A}$ such that

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

The last inequality can be obtained from applying the following theorem on extension degree of division fields along with a formula for $h((mf))$. (See [14, Theorem 1.1], also [12])

Lemma 2.5. *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, $\nu = Rank(\Phi, K)$, 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 $Rank(\Phi, K) = Rank(\Phi', K')$, we also have that $2 + \log_2 g' \leq \nu \leq g' + 1$ if $[K' : \mathbb{Q}] = g'$. Thus, we have

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

On the assumptions for Theorem 1.2, $g = 2$ gives the only choice for $\nu = g + 1 = 3$. Then Lemma 2.4 gives

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

Taking the sum over $m \leq \sqrt{x}$ above, we have by Corollary 2.3 in section 2.1,

$$\sum_{m \leq \sqrt{x}} t(m) \ll_K \sqrt{x} \sum_{m \leq \sqrt{x}} \frac{R^{w(m)}}{T((mf))} \ll_K \sqrt{x}\sqrt{x} \exp\left(-\left(\frac{1}{4} + o(1)\right) \log x \frac{\log\log\log x}{\log\log x}\right).$$

This completes the proof of Theorem 1.2.

References

[1] N. G. de Bruijn, *On the number of positive integers $\leq x$ and free of prime factors $> y$*, Nederl. Akad. Wetensch. Proc. Ser. A 69=Indag. Math. 28 (1966), pp. 239-247.

[2] E. Fouvry, *Theoreme de Brun-Titchmarsh; application au theoreme de Fermat*, Invent. Math., 79, (1985) pp. 383-407

[3] T. Freiberg, P. Pollack, *The average of the first invariant factor for reductions of CM elliptic curves mod p*, Int. Math. Res. Notices, to appear

[4] A. Granville, *Smooth numbers: computational number theory and beyond*, Algorithmic Number Theory, MSRI Publications, Volume 44, (2008)

[5] A. J. Hildebrand, *On the Number of Positive Integers $\leq x$ and Free of Prime Factors $> y$*, Journal of Number Theory 22, (1986) pp. 289-307

[6] S. Kim, *Average of the First Invariant Factor of the Reductions of Abelian Varieties of CM Type*, accepted for publication.

[7] P. Kurlberg, Z. Rudnick, *On Quantum Ergodicity for Linear Maps of the Torus*, Comm. Math. Phys., 222(1):201-227, 2001

[8] P. Kurlberg, C. Pomerance, *On the period of linear congruential and power generators*, Acta Arith. 119 (2005), pp. 305-335.

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

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

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

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

[13] C. Pomerance, *On the distribution of pseudoprimes*, Math. Comp. 37 (1981), pp. 537-593.

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

[15] 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

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

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

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

[19] 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