AVERAGE RECIPROCALs OF ORDER OF $a$ MODULO $p$

KIM, SUNGJIN

Abstract. Let $a > 1$ be an integer. Denote by $l_a(p)$, $l_a(n)$ the multiplicative order of $a$ modulo primes $p$, and general integers $n$ respectively. We prove that
\[ \sum_{p < x} \frac{1}{l_a(p)} \leq \left( \frac{2}{\pi} \sqrt{6 \log a + o(1)} \right) \sqrt{x} / \log x, \]
which is an improvement over a statement in [MS]. Then for $l_a(n)$, we prove that
\[ \sum_{n \leq x : (n, a) = 1} \frac{1}{l_a(n)} = O_a \left( \log x \exp \left( - \left( \frac{1}{2} + o(1) \right) \log \frac{\log \log \log x}{\log \log x} \right) \right), \]
which is an improvement over [Z, Theorem 5].

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

1. Introduction

Let $a > 1$ be an integer. If $p$ be a prime not dividing $a$, then there the multiplicative order of $a$ modulo $p$ exists, say $l_a(p)$. Artin’s Conjecture on Primitive Roots (AC) states that $l_a(p) = p - 1$ for infinitely many primes $p$. Assuming the Generalized Riemann Hypothesis (GRH), Hooley [Ho] proved that $l_a(p) = p - 1$ for positive proportion of primes $p \leq x$. It is expected that $l_a(p)$ is large for majority of primes $p \leq x$. In [EM], Erdos and Murty showed that $l_a(p) \geq p^{1/2 + o(p)}$ for all but $O(\pi(x))$ primes $p \leq x$ where $\epsilon(p) \to 0$. With much simpler method, they showed a weaker result $l_a(p) > \frac{\sqrt{p}}{\log p}$ for all but $O(x / \log^3 x) \leq x$. Kurlberg and Pomerance [KP] applied Fouvry [Fo] to show that there is $\gamma > 0$ such that $l_a(p) > p^{1/2 + \gamma}$ for positive proportion of primes $p \leq x$. The reciprocal of $l_a(p)$ also has a significance. Murty and Srinivasan [MS] showed that
\[ \sum_{p < x} \frac{1}{l_a(p)} = O(\sqrt{x}) \]
and that
\[ \sum_{p < x} \frac{1}{l_a(p)} = O(x^{1/4}) \]
implies AC for $a$. On average, Felix [Fe] proved the following:
If $\frac{x}{\log x} = o(y)$, then

$$\frac{1}{y} \sum_{a \leq y} \sum_{p \leq x} \frac{1}{l_a(p)} = \log x + O(\log \log x) + O\left(\frac{x}{y}\right).$$

We apply an idea of Engberg [E, Lemma 5] to improve on [MS]:

**Lemma 1.1.**

$$\sum_{l_a(p) = d} \frac{1}{l_a(p)} \leq \frac{\varphi(d) \log a}{2 \log d} + O\left(\frac{d \log \log d}{(\log d)^2}\right).$$

As in [MS], we take the sum over $d < t$. Then by partial summation,

$$\sum_{d < t, l_a(p) = d} \frac{1}{l_a(p)} \leq \frac{3 \log a}{2 \pi^2} \frac{t^2}{\log t} + O\left(\frac{t^2 \log \log t}{(\log t)^2}\right).$$

Then again by partial summation,

$$\sum_{l_a(p) < y} \frac{1}{l_a(p)} \leq \frac{3 \log a}{\pi^2} \frac{y}{\log y} + O\left(\frac{y \log \log y}{(\log y)^2}\right).$$

Therefore, by considering sums over $l_a(p) < y$ and $l_a(p) \geq y$,

$$\sum_{p \leq x} \frac{1}{l_a(p)} \leq \frac{3 \log a}{\pi^2} \frac{y}{\log y} + O\left(\frac{y \log \log y}{(\log y)^2}\right) + \frac{\pi(x)}{y}.$$

Taking $y = \sqrt{x}/\sqrt{2C}$ where $C = (3 \log a)/\pi^2$, we have the following:

**Theorem 1.1.** Let $a > 1$. Denote by $l_a(p)$ the multiplicative order of $a$ modulo $p$. Then we have

$$\sum_{p < x} \frac{1}{l_a(p)} \leq \left(\frac{2}{\pi} \sqrt{6 \log a} + o(1)\right) \frac{\sqrt{x}}{\log x}.$$

The $l_a(p)$ can be extended to any positive integer $n$ coprime to $a$, just by defining $l_a(n)$ the multiplicative order of $a$ modulo $n$. In [KR], 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 $n \leq x$. In [KP], Kurlberg and Pomerance obtained the following result by applying Fouvry’s result. For some $\gamma > 0$, $l_a(n) \gg n^{1/2 + \gamma}$ for positive proportion of $n \leq x$.

On the other hand, Zelinsky [Z] proved that

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

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

$$\sum_{n \leq x, (n, a) = 1} \frac{1}{l_a(n)} = O_a\left(\frac{x}{\log^alpha x}\right)$$
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. For integral ideal $I$, denote by $NI$ the norm of $I$, and $\varphi(I)$ the Euler’s totient function of $I$. Denote by $U_K(I)$ the subgroup of $U_K$ formed by elements which are 1 modulo $I$. He obtained that

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

This also can be interpreted as

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

In the author’s work [K, 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 $O(x \exp(-\frac{2}{5} (\log x)^{3/5}))$ integral ideals $NI \leq x$. This implies that

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

The same idea also applies to

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

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

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

also

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

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

**Theorem 1.2.** Let $l_a(n)$ be multiplicative order of $a$ modulo $n$. Then

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

Furthermore, let $K$ be a number field, and assume that $U_K$ 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 $I$. Then

$$\sum_{NI \leq x} \frac{1}{[U_K : U_K(I)]} = O_K \left( x \exp \left( -\left( \frac{1}{2} + o(1) \right) \log x \frac{\log \log \log x}{\log x} \right) \right).$$
It is possible to apply this to improve on [K, Theorem 1.8].

**Theorem 1.3.** 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

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

**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 [B]):

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

From the upper bound of de Bruijn [B], and lower bound of Hildebrand [Hi], we have

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

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

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

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

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 $Np \leq y$ for any prime ideal $p|I$. Then the above theorem and corollary have their analogue (see [G, Section 1.3]):

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

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

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

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 \( O_a(x/cz^2) \). Therefore, by taking \( z = \exp(c/\sqrt{\log x \log \log x}) \), 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 \( O_a \left( x \exp(-c_a \sqrt{\log x \log \log x}) \right) \) integers \( n \leq x \).

Using the lower bound \( \exp(c_a \sqrt{\log x \log \log x}) \) for most \( n \leq x \), and the trivial lower bound 1 for the exceptional set of \( n \leq x \), it follows that
\[
\sum_{n \leq x, (n, a)=1} 1 \leq O_a \left( x \exp \left( -c_a \sqrt{\log x \log \log x} \right) \right)
\]
for some positive constant \( c_a \).

Furthermore, let \( K \) be a number field, and assume that \( U_K \) 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
\[
[U_K : U_K(I)] \geq l_a(I).
\]
The same idea as above applies, and we obtain for some \( c_K > 0 \),
\[
\sum_{N I \leq x} \frac{1}{[U_K : U_K(I)]} = O_K \left( x \exp \left( -c_K \sqrt{\log x \log \log x} \right) \right),
\]
To prove Theorem 1.2, we adopt an idea of Pomerance [P, Theorem 1]:

Theorem 2.3. Let \( a > 1 \) be an integer. There is an \( x_0(a) \) such that if \( x \geq x_0(a) \), then
\[
\sum_{m \leq x, l_a(m)=n} 1 \leq x \exp \left( -\left( \frac{1}{2} + o(1) \right) \log x / \log \log x \right).
\]

We may assume that \( n < x \). Similarly as in [B, Section 3], Pomerance applies Rankin’s method. Then for any \( c > 0 \),
\[
\sum_{m \leq x, l_a(m)=n} 1 \leq x^c \sum_{l_a(m)=n} m^{-c} \leq x^c \sum_{p \mid m} m^{-c} = x^c \prod_{l_a(p)=n} (1-p^{-c})^{-1} = x^c A.
\]
Then the optimal choice for \( c \) is \( c = 1 - (4 + \log \log x)/(2 \log \log x) \) with a requirement \( \log A = o(\log x / \log \log x) \).
Taking the sum of the LHS of Theorem 2.3 for \( n < z = \text{exp} \left( \frac{1}{4} \log x \frac{\log \log \log x}{\log \log x} \right) \), 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
\[
l_a(n) \geq \text{exp} \left( - \left( \frac{1}{2} + o(1) \right) \log x \frac{\log \log \log x}{\log \log x} \right)
\]
for all but \( O_a \left( x \exp \left( - \left( \frac{1}{2} + o(1) \right) \log x \frac{\log \log \log x}{\log \log x} \right) \right) \) integers \( n \leq x \).

However, we do not use the lemma to prove Theorem 1.2. Instead, observe the following:
\[
\sum_{m \leq x} 1 \leq \sum_{n < x} 1 \leq \sum_{m \leq x, l_a(m) = n} 1.
\]
Applying Theorem 2.3 directly, we obtain that
\[
\sum_{n < x} 1 \leq \sum_{n < x} 1 \leq x \exp \left( - \left( \frac{1}{2} + o(1) \right) \log x \frac{\log \log \log x}{\log \log x} \right) = O_a \left( x \exp \left( - \left( \frac{1}{2} + o(1) \right) \log x \frac{\log \log \log x}{\log \log x} \right) \right).
\]
This proves the first part of Theorem 1.2. The statement for the number field 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
\[
\sum_{N I \leq x, l_a(I) = n} 1 \leq x \exp \left( - \left( \frac{1}{2} + o(1) \right) \log x \frac{\log \log \log x}{\log \log x} \right).
\]

The proof is almost identical, with only difference in the Euler product:
\[
\sum_{N I \leq x, l_a(I) = n} 1 \leq x \exp \left( - \left( \frac{1}{2} + o(1) \right) \log x \frac{\log \log \log x}{\log \log x} \right) = O \left( \sum_{d \mid N I} (1 - N p^{-c})^{-1} = x^c A. \right)
\]
As in the proof of [P, 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
\[
\log A = \sum_{l_a(p) \mid n} N p^{-c} + O([K : \mathbb{Q}]) = \sum_{d \mid n} \sum_{l_a(p) = d} N p^{-c} + O([K : \mathbb{Q}]).
\]
The prime ideals \( p \) with \( l_a(p) = d \) all divide the principal ideal \((a^d - 1)\). Then the number of prime ideals \( p \) dividing \((a^d - 1)\) is \( O \left( [K : \mathbb{Q}] \frac{\log |a'|}{\log (d + 1)} \right) \) where \( a' \) is a conjugate of \( a \) with maximal \(|a'|\). Let \( q_1, \ldots, q_t \) 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 $q_i$ of $(a^d - 1)$ satisfies $Nq_i \equiv 1 \pmod{d}$. Then we have

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

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 1.2.

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 [P, 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 $q_1, \ldots, q_t$ 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 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

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

In this one, the Euler product behaves like \( R \)th power of the previous one. In fact,

\[
\sum_{m \leq x, \lambda_a((m)) = n} R^{w(m)} \leq x^c \sum_{l_a((m)) = n} R^{w(m)} \leq x^c \sum_{p | m = \lambda_a((p))} R^{w(m)} m^{-c} = x^c \prod_{l_a((p)) | n} (1 + Rp^{-c} + Rp^{-2c} + \cdots) = x^c A.
\]

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

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

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

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

This is an easy consequence of Theorem 2.6. We write

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

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 [Sh], also [L]. The CM theory for elliptic curves (see [Si], [Ru], also [Si2]) 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 2.7. Let \( A \) be an abelian variety. Then the center \( K \) of \( \text{End}_Q A := \text{End} A \otimes Q \) 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 \( 2 \dim A \).

Proposition 2.1. Let \( A \) be an abelian variety of dimension \( g \) and \( \mathcal{S} \) a commutative semi-simple subalgebra of \( \text{End}_Q A \). Then we have
\[
[\mathcal{S} : Q] \leq 2g.
\]
In particular, \( K \subset \mathcal{S} \), which gives \( [K : Q] \leq [\mathcal{S} : Q] \leq 2g \). We are interested in the case that \( [K : Q] = 2g \), 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 2.8. Let \( A \) be an abelian variety of dimension \( g \). Suppose that the center of \( \text{End}_Q A \) is \( K \), and \( K \) is a CM field of degree \( 2g \) over \( Q \). We say that \( A \) 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 \( (K, \Phi) \) the CM-type. Furthermore, there exists a lattice \( a \) in \( K \) such that there is an analytic isomorphism \( \theta : \mathbb{C}^g/\Phi(a) \rightarrow A(C) \). We write \( (K, \Phi, a) \) to indicate \( a \) is a lattice in \( K \) with respect to \( \theta \). Under the inclusion \( i : K \rightarrow \text{End}_Q A \), we have that
\[
\mathcal{O} = \{ \tau \in K | i(\tau) \in \text{End} A \} = \{ \tau \in K | \tau a \subset a \}
\]
is an order in \( K \).

This gives rise to the following composition:

Corollary 2.4. Let \( A \) be an abelian variety of dimension \( g \) with CM-type \( (K, \Phi, a) \) with respect to \( \theta \). Then \( \theta \circ \Phi \) maps \( K/a \) to \( A_{tor} \), i.e.
\[
K/a \xrightarrow{\Phi} \mathbb{C}^g/\Phi(a) \xrightarrow{\theta} A_{tor}.
\]
Proof. This is clear from noticing that \( a \otimes Q = K \). Also, \( \Phi \) is \( Q \)-linear, and \( \Phi(a) \otimes Q \) is a torsion subgroup of \( \mathbb{C}^g/\Phi(a) \). \( \square \)

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 \( (K, \Phi) \) 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 \( \rho \) be an element of \( G \) that induces complex conjugation on \( K \). Let \( S \) be the set of all elements of \( G \) that induce \( \phi_i \) 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 $(K, \Phi)$ be a CM-type. Let $L, G, \rho, S$ as above, and $H_1$ the subgroup of $G$ corresponding to $K$. Put

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

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

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

Proposition 2.3. Let $L, G, \rho, S$ 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 $(K', \Phi')$ is a primitive CM-type.

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

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

Then this map allows an extension to $N_{(K', \Phi')} : A_K^\times \rightarrow A_K^\times$. This extension is called the type norm. It can be seen that $N_{(K', \Phi')}$ is a continuous homomorphism on $A_K^\times$. (see [Sh, p124]) The field of definition $k$ of an abelian variety $A$ with CM-type $(K, \Phi)$ 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 [M, p 162, Lemma 4] can be obtained from applying the Main Theorem of Complex Multiplication (see [L, Theorem 1.1, p84]). 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. Let $A, (K, \Phi), (K', \Phi'), k$ be the same notations as before. Let $m \geq 2$ be an integer. Then there exists a nonzero rational integer $f$ such that

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

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

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

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

\[ ab^{-1} \in P^m_K = \{ (\alpha) : \alpha \equiv 1 \pmod{m} \}. \]

The \( m \)-ideal class group coincides with our definition \( C_m(K) = J^m_K / P^m_K \) in the previous chapter. Denote by \( h(m) \) the cardinality of \( J^m_K / P^m_K \), and \( h \) by the class number of \( K \). We have a formula that relates \( h(m) \) and the class number \( h \) of \( K \). This follows from an exact sequence:

\[ U(K) \longrightarrow (O_K/mO_K)^{\times} \oplus \{ \pm 1 \}^{r_1} \longrightarrow C_m(K) \longrightarrow C(K) \longrightarrow 1. \]

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

\[ h(m) = \frac{2^{r_1} h(\varphi(m))}{T(m)} \]

where \( \varphi(m) = |(O_K/mO_K)^{\times}|. \)

A direct corollary of Lemma 2.3 is the following:

**Lemma 2.4.** Let \( \mathcal{A}, (K, \Phi), (K', \Phi'), k \) be the same notations as before. Suppose also that \( p \subset k \) is a prime of good reduction for \( \mathcal{A} \), and \( p \nmid m \). 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

\( p \) splits completely in \( k(\mathcal{A}[m]) \) if and only if \( p \sim a_1, \ldots, p \sim a_{t(m)} \).

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

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

By Lemma 2.3 below, there is an absolute positive constant \( R \) depending only on \( \mathcal{A} \) such that

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

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

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 [Ri, Theorem 1.1], also [N])

**Lemma 2.5.** Let \( \mathcal{A} \) be an abelian variety of CM type \( (K, \Phi, a) \) 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 \( m \), \( \nu \) is an integer defined by \( \text{Rank}(\Phi, K) \), and \( 2 + \log_2 g \leq \nu \leq g + 1 \) if \( \mathcal{A} \) is absolutely simple. Since the reflex type \( (\Phi', K') \) is always simple and \( \text{Rank}(\Phi, K) = \)

\textit{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 1.3, \(g = 2\) 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,
\[
\sum_{m \leq \sqrt{x}} t(m) \ll_K \sqrt{x} \sum_{m \leq \sqrt{x}} \frac{R^w(m)}{T((mf))} \ll_K \sqrt{x} \sqrt{x} \exp \left( - \left( \frac{1}{4} + o(1) \right) \log x \frac{\log \log \log x}{\log \log x} \right).
\]
This completes the proof of Theorem 1.3.

\section*{References}


[K] S. Kim, \textit{Average of the First Invariant Factor of the Reductions of Abelian Varieties of CM Type}, accepted for publication.


