DISTRIBUTION OF ROOT NUMBERS OF HECKE CHARACTERS ATTACHED TO SOME ELLIPTIC CURVES

KEUNYOUNG JEONG, JIGU KIM, TAEKYUNG KIM

Abstract. In this paper, we show that an action on the set of elliptic curves with $j = 1728$ preserves a certain kind of symmetry on the local root number of Hecke characters attached to such elliptic curves. As a consequence, we give results on the distribution of the root numbers and their average of the aforementioned Hecke characters.

1. Introduction

Let $K$ be the number field $\mathbb{Q}(i)$ and $O$ its ring of integers. We fix an embedding $K \hookrightarrow \mathbb{C}$ once and for all. The main object of this paper is the root number of Hecke characters attached to elliptic curves with complex multiplication by $O$. Unlike the case of root numbers of elliptic curves, root numbers of Hecke characters associated with the curves need not have value $\pm 1$, and in general they have values in the complex unit circle. However, we will show that there is still a “symmetry” on these root numbers.

Before giving a formal definition of the symmetry, we define some basic notions. By the theory of complex multiplication, the elliptic curve with complex multiplication by $O$ is uniquely determined by an equation

$$E_d : y^2 = x^3 - dx$$

up to isomorphism defined over $K$ for the fourth-power-free element $d \in O$. Let $\mathcal{E}$ be the set of $K$-isomorphism classes of such elliptic curves. Then the group $K^\times/(K^\times)^4$ acts on $\mathcal{E}$ by $\mathcal{T}.E_d := E_{xd}$. By definition, an element $x$ of $K^\times$ gives an action of order dividing 4, i.e., $\mathcal{T}^4.E_d$ is isomorphic to $E_d$.

We say that an action induced by $\mathcal{T}$ preserves a symmetry on the (local) root numbers when the root numbers are changed only by a multiple of $(2\pi)/4$ via the action. Since every root number of elliptic curves is either 1 or $-1$, arbitrary actions induced by an element of $K^\times/(K^\times)^4$ preserve a symmetry on the root numbers of elliptic curves. However, in the case of Hecke characters attached to elliptic curves with complex multiplication, it is not true in general. Nevertheless, we will show that units and primes of degree two (cf. Subsection 2.1) preserve a symmetry on the root numbers of Hecke characters. More precisely, we will compute the ratio between the root numbers of Hecke character induced by $E_d$ and $\mathcal{T}.E_d$ where $x$ is a unit or a prime of degree two.

Intuitively, the existence of such a symmetry-preserving action shows that the local root numbers do not particularly prefer one quarter circle than others. By adapting this intuition, we can show that the set of local root numbers of Hecke character of elliptic curves with complex multiplication by $O$ at bad primes is dense in the unit circle.

Theorem 1.1. Let $S^1$ be the unit circle in $\mathbb{C}$. For arbitrary $\theta \in S^1$ and $\epsilon > 0$, there is an elliptic curve $E$ having CM by the ring $O$ and a prime $\mathfrak{p}$ of $K$ such that the root number $\mathfrak{w}_v(\chi_E) \in B_\theta(\epsilon)$ where $B_z(r)$ denotes the open ball having centre at $z \in \mathbb{C}$ and radius $r > 0$.

As primes of degree two preserves a symmetry, when we are given a local root number, there are certain powers of a prime of degree two that do not change the given root number when multiplied by the prime.

2010 Mathematics Subject Classification. Primary 11G15, Secondary 11N69.

Key words and phrases. Hecke characters, Complex multiplication, Distribution of root numbers.
Theorem 1.2. Let $\theta \in S^1$ be fixed. If there exists a single elliptic curve $E_0$ having CM by the ring $O$ and a prime $v$ of $K$ such that the root number $w_v(\chi_{E_0}) = \theta$, then there are infinitely many (isomorphism classes of) elliptic curves $E$ having CM by $O$ such that $w_v(\chi_E) = \theta$.

Local symmetry-preserving properties also lead us into the computation of the average value of the global root numbers. Given a suitable “base element” $d \in O$, we investigate the local root numbers of Hecke characters $\chi_{dQ}$, where $Q$ varies over the products of distinct primes of degree two. The symmetry-preserving property for these kinds of primes allows us to compare the local root numbers between $\chi_d$ and $\chi_{dQ}$. With a help from quartic reciprocity and the balanced distribution of quadratic residues, we can show that the average “global” root number (except for the 2-part) with such varying $Q$ is equal to zero.

Theorem 1.3. For a real number $X > 0$, let $Q(X)$ be the set of elements in $O$ which can be represented as the product of distinct primary primes of degree two (i.e. of the form $-q$ for rational primes $q$ with $q \equiv 3 \pmod{4}$), and which has absolute value less than $X$. Fix $d \in O$ of the form

$$d = \prod_{i \in I} \pi_i \cdot \prod_{j \in J} (-q_j)^{n_j},$$

where $\pi_i$ are primary primes of degree one and $-q_j$ are primary primes of degree two, for $i \in I$ and $j \in J$. For such a $d$, let us consider the elliptic curve $E_d$ defined as in (5) together with their twists $E_{dQ}$ and their corresponding Hecke characters $\chi_{dQ}$. Then,

$$\lim_{X \to \infty} \frac{1}{|Q(X)|} \sum_{Q \in Q(X)} \frac{w(\chi_{dQ})}{w_2(\chi_{dQ})} = 0.$$ 

The “ideal” statement in this direction would be

$$\lim_{X \to \infty} \frac{1}{|E_d(X)|} \sum_{E \in E_d(X)} w(\chi_E) = 0,$$

where $E_d(X)$ is the set of elliptic curves obtained by twisting $E_d$ with an element in $O$ whose absolute value is less than $X$. However, we have a trouble in computing the local root number at a prime above 2, and we only have a symmetry on primes of degree two. For these reasons, we use $Q(X)$ instead of $E_d$ and $w(\chi_E)/w_2(\chi_E)$ instead of $w(\chi_E)$.

This paper is organised as follows: in Section 2, we recall some basic facts about the Gaussian integers $O$, elliptic curves with complex multiplication by $O$, and Hecke characters associated by elliptic curves with complex multiplication by $O$. In Section 3 we give certain concrete computations on such Hecke characters, even though these topics are already studied by [RS09]. In Section 4 we will give a proof for the main results of this paper.

2. Preliminaries

2.1. Gaussian primes. Consider the number field $K = \mathbb{Q}(i)$ and its ring of integers $O = \mathbb{Z}[i]$. The elements of $O$ are called Gaussian integers. The unit elements amongst them are exactly 1, $-1$, $i$ and $-i$. A non-unit $a \in O$ is called to be primary if $a \equiv 1 \pmod{2(1 + i)}$. Such primary elements $a = a + bi$ are classified as the elements with $(a, b) \equiv (1, 0) \pmod{4}$ or $(a, b) \equiv (3, 2) \pmod{4}$. It is well-known that if $a$ is a non-unit element in $O$ with $(1 + i) \nmid a$, there is a unique unit $u$ such that $\bar{a} = ua$ is primary. Since $K$ has class number one, the ring $O$ is a unique factorisation domain, and thus for any non-zero $d \in O$, we have a unique primary prime decomposition

$$d = i^{n_u} \cdot (1 + i)^{n_2} \cdot \prod_{\pi: \text{primary primes}} \pi^{n_\pi},$$

(1)
with \( n_d \in \{0, 1, 2, 3\} \) and \( n_2, n_\pi \geq 0 \) being integers, where the product runs over all odd (elements not divisible by \((1 + i)\)) primary prime elements in \( \mathcal{O} \). We say that a prime ideal of \( \mathcal{O} \), or a prime element generating the ideal, or even the valuation corresponding the ideal, is of degree one (resp. of degree two) if its residual degree is equal to one (resp. two).

### 2.2. Quartic residue symbol and quartic reciprocity.

Suppose that \( \pi \) is an odd prime element of \( \mathcal{O} \) and \( \alpha \in \mathcal{O} \) is an element prime to \( \pi \). The quartic residue character of \( \alpha \mod \pi \) is the unique unit \( i^k \) \((k \in \{0, 1, 2, 3\})\) such that \( \alpha^{N\pi^{-1}} \equiv i^k \mod \pi \). Here \( N\pi \) is the absolute norm of \( \pi \) (i.e. the size of the residue field \( \mathcal{O}/\mathcal{O}\pi \)) and the existence of such unit is guaranteed by Fermat’s little theorem: \( \alpha^{N\pi-1} \equiv 1 \mod \pi \). The quartic residue character of \( \alpha \mod \pi \) is denoted by \( \left( \frac{\alpha}{\pi} \right)_4 \). We use the following well-known properties on the quartic residue character in the present paper.

**Proposition 2.1** (Properties of the quartic residue symbol). Let \( \pi = a + bi \) be an odd prime element in \( \mathcal{O} \) and \( \alpha, \beta \in \mathcal{O} \) Gaussian integers prime to \( \pi \). Then the following hold.

1. \( \left( \frac{\alpha \beta}{\pi} \right)_4 = \left( \frac{\alpha}{\pi} \right)_4 \left( \frac{\beta}{\pi} \right)_4 \).
2. \( \left( \frac{\alpha}{\pi} \right)_4 = \left( \frac{\bar{\alpha}}{\pi} \right)_4 \), where \( \bar{\cdot} \) denotes the complex conjugation.
3. If \( \pi' \) is an associate of \( \pi \), then \( \left( \frac{\alpha}{\pi} \right)_4 = \left( \frac{\alpha}{\pi'} \right)_4 \).
4. If \( \alpha \equiv \beta \mod \pi \), then \( \left( \frac{\alpha}{\pi} \right)_4 = \left( \frac{\beta}{\pi} \right)_4 \).
5. Let \( q \) be a rational prime congruent to \( 3 \) modulo \( 4 \). Then for any \( a \in \mathbb{Z} \) with \( a \neq 0 \) and \( q \nmid a \), we have \( \left( \frac{a}{q} \right)_4 = 1 \).

For future reference, here we also give the quartic reciprocity law.

**Theorem 2.2** (Quartic Reciprocity). Suppose that \( \alpha, \beta \in \mathcal{O} \) are primary (hence not even) relatively prime non-unit elements. Then

\[
\left( \frac{\alpha}{\beta} \right)_4 \left( \frac{\beta}{\alpha} \right)^{-1}_4 = (-1)^{\frac{N\alpha-1}{4} \frac{N\beta-1}{4}},
\]

or equivalently,

\[
\left( \frac{\beta}{\alpha} \right)_4 = \begin{cases} 
- \left( \frac{\alpha}{\beta} \right)_4 & \text{if both } \alpha \text{ and } \beta \equiv 3 + 2i \mod 4, \\
\left( \frac{\alpha}{\beta} \right)_4 & \text{otherwise.} 
\end{cases}
\]

Furthermore, we have the following auxiliary relations for a primary prime \( \pi = a + bi \):

\[
\left( \frac{i}{\pi} \right)_4 = i^{\frac{a-1}{2}} \quad \text{and} \quad \left( \frac{1 + i}{\pi} \right)_4 = i^{\frac{a^{2} + b^{2} - 2}{4}}.
\]

### 2.3. Elliptic curves having CM by \( \mathcal{O} \).

Let \( E \) be an elliptic curve defined over the algebraic closure of \( \mathbb{Q} \) having complex multiplication by \( \mathcal{O} \). From the classical theory of complex multiplication, such \( E \) is defined over the Hilbert class field of \( K \), which is \( K \) itself and its \( j \)-invariant is 1728. Furthermore, such elliptic curves are defined by the Weierstrass equation

\[
y^2 = x^3 - dx, \quad d \in \mathcal{O}
\]

where the discriminant of the equation \( \Delta = 2^6 d^3 \neq 0 \). The curve defined by the equation (5) is denoted by \( E_d \). Note that two such equations for \( d \) and \( d' \) define the isomorphic curve if and only if \( d' = x^4 d \) for some \( x \in \mathcal{O} \). For convenience, we therefore assume \( d \) is fourth-power-free.
For future reference, we also investigate the reduction type of $E$ modulo the prime $(1 + i)$. This can be easily verified by using Tate’s algorithm (e.g. see [Sil94, §IV.9]).

**Lemma 2.3.** Let $E/K$ be an elliptic curve defined by a Weierstrass equation (5) with fourth-power-free $d$. We write $\pi = 1 + i \in K$ and consider the power series expansion of $d$ in the completion $K_\pi$ of $K$ with respect to $\pi$:

$$d = \sum_{j=0}^\infty d_j \pi^j, \quad d_j \in \{0, 1\}.$$  \hspace{1cm} (6)

Then the reduction types of $E$ and corresponding conductor exponents are given in terms of the values of $d_j$ in the Table 1.

| $d_0$ | $d_1$ | $d_2$ | $d_3$ | $d_4$ | $d_5$ | Reduction Type | Conductor Exponent |
|-------|-------|-------|-------|-------|-------|----------------|-------------------|
| 0     | 0     | 0     | 1     | -     | -     | III             | 14                |
| 0     | 0     | 1     | 0     | -     | -     | $I_0^*$         | 10                |
| 0     | 0     | 1     | 1     | -     | -     | $I_2^*$         | 12                |
| 0     | 1     | -     | -     | -     | -     | III             | 14                |
| 1     | 0     | 0     | 0     | -     | -     | $I_2^*$         | 6                 |
| 1     | 0     | 0     | 1     | -     | -     | $I_0^*$         | 8                 |
| 1     | 0     | 1     | 0     | 0     | 0     | good            | 0                 |
| 1     | 0     | 1     | 0     | 0     | 1     | $II^*$          | 4                 |
| 1     | 0     | 1     | 0     | 1     | 0     | $II^*$          | 4                 |
| 1     | 0     | 1     | 0     | 1     | 1     | good            | 0                 |
| 1     | 0     | 1     | 1     | -     | -     | $I_0^*$         | 8                 |
| 1     | 1     | -     | -     | -     | -     | II              | 12                |

**Table 1.** Reduction types and conductor exponents of the elliptic curve $E_d$, in terms of the power series expansion of $d$ (cf. (6)). Here - means that the corresponding value is irrelevant.

2.4. **Hecke characters associated with CM elliptic curves and their root numbers.** For a non-zero ideal $\mathfrak{f}$ of $O$, we define:

$$K(\mathfrak{f}) = \{ \alpha \in K^\times : (\alpha O, \mathfrak{f}) = 1 \},$$

$$K_\mathfrak{f} = 1 + K(\mathfrak{f})\mathfrak{f} = \{ \alpha \in K^\times : \alpha \equiv 1 \text{ mod } K(\mathfrak{f}) \} \subset K(\mathfrak{f}),$$

$$I(\mathfrak{f}) = \{ \text{fractional ideals of } K \text{ coprime to } \mathfrak{f} \},$$

$$P(\mathfrak{f}) = \{ \text{principal fractional ideals } \alpha O \text{ of } K \text{ coprime to } \mathfrak{f} \},$$

$$P_\mathfrak{f} = \{ \text{principal fractional ideals } \alpha O \text{ of } K \text{ where } \alpha \equiv 1 \text{ mod } K(\mathfrak{f}) \}. $$

Let $E = E_d$ be an elliptic curve defined over $K$ with the same assumptions as in Subsection 2.3. From the theory of complex multiplication of elliptic curves, there is a Hecke character $\chi_A : A_K^\times / K^\times \rightarrow C^\times$ where $A_K^\times$ is the idèle group of $K$. In terms of ideal groups, this can be viewed as a pair $(\chi, \chi_\infty)$, where $\chi : I(\mathfrak{f}) \rightarrow C^\times$ is a character from the ideal group co-prime to a non-zero ideal $\mathfrak{f}$ of $O$, and $\chi_\infty : (R \otimes Q K)^\times = C^\times \rightarrow C^\times$ is a continuous character. Here the two characters $\chi$ and $\chi_\infty$ are related in the following way: for $\alpha \in K_\mathfrak{f}$, we have $\chi(\alpha O) = \chi_\infty^{-1}(1 \otimes \alpha)$. Furthermore, we have more refined relation giving the values of the character at $\alpha \in K(\mathfrak{f})$: we have a character $\epsilon : (O/\mathfrak{f})^\times \equiv K(\mathfrak{f})/K_\mathfrak{f} \rightarrow S^1 \subset C^\times$ such that $\chi(\alpha O) = \epsilon(\alpha K_\mathfrak{f})\chi_\infty^{-1}(1 \otimes \alpha)$ for each $\alpha \in K(\mathfrak{f})$. Such a Hecke character $\chi$ is now called a Hecke character with conductor $\mathfrak{f}$, $(O/\mathfrak{f})^\times$-type $\epsilon$ and infinity-type $\chi_\infty$. The non-zero ideal $\mathfrak{f}$ is called the conductor of the Hecke character $\chi$ and it is known that it has the same prime factors as the conductor of the curve $E$. 


3.1. Explicit computation of Hecke characters. From §2, we see that there is an element \( d \in O \) unique up to multiplication by a fourth-power in \( O \) such that \( E \) is isomorphic to \( E_d \) (cf. Equation (5)). We choose \( d \) itself to be fourth-power-free, i.e. in the unique primary prime decomposition (1) of \( d \), we have \( 0 \leq n_d, n_2, n_\pi \leq 3 \) for each odd prime \( \pi \) of \( K \). This means that Equation (5) defining \( E_d \) is minimal at each prime except \( (1 + i)O \). In particular, the curve \( E_d \) has good reduction modulo any odd prime not dividing \( d \).

Let \( \chi : I(\tilde{f}) \to \mathbb{C}^\times \) be the Hecke character associated with the curve \( E_d \). Here \( \tilde{f} \) is an integral ideal of \( O \) having the same primary ideal divisors as the conductor of the curve \( E_d \).

**Lemma 3.1.** Let \( \wp \) be a prime ideal of \( K \) such that \( \wp \nmid 2\tilde{f} \) with residue field \( k = k_{\wp} \). If \( E = E_d \) is the elliptic curve defined by the Weierstrass equation (5), then concerning the number of \( k \)-rational points on the reduction \( \tilde{E} \) of \( E \) modulo \( \wp \), we have the following results.

- If \( \wp \) is of degree one, i.e. \( k = \mathbb{F}_p \) for some rational prime \( p \equiv 1 \pmod{4} \), we have
  \[ \#\tilde{E}(k) = p + 1 - \left( \frac{d}{\pi} \right) \pi - \left( \frac{d}{\overline{\pi}} \right) \overline{\pi}, \]
  where \( p = \pi \overline{\pi} \) is the decomposition of \( p \) in \( K \) with primary prime elements \( \pi \) and \( \overline{\pi} \).

- If \( \wp \) is of degree two, i.e. \( k \) is a degree two extension of \( \mathbb{F}_p \) for some rational prime \( p \equiv 3 \pmod{4} \), we have
  \[ \#\tilde{E}(k) = \begin{cases} p^2 + 1 & d \text{ is not a square in } k, \\ p^2 + 1 - 2p & d \text{ is a square but not a fourth power in } k, \\ p^2 + 1 + 2p & d \text{ is a fourth power in } k. \end{cases} \]

**Proof.** Over the rationals \( \mathbb{Q} \), it is proved in [IR90, §18.4, Theorem 5]. We can prove the result similarly over \( K \). \( \square \)

**Proposition 3.2.** The Hecke character \( \chi : I(\tilde{f}) \to \mathbb{C}^\times \) associated with the curve \( E_d \) defined by the equation (5) is given by, for any prime ideal \( \wp \) of \( K \) co-prime to \( 2\tilde{f} \),

\[ \chi(\wp) = \left( \frac{d}{\wp} \right) \pi, \]

where \( \pi \) is the unique primary generator of \( \wp \).

**Proof.** This is due to Lemma 3.1, as explained in [Sil94, Example II.10.6]. \( \square \)

From this, we can identify the infinity type of the Hecke character \( \chi_{\infty} \).

**Lemma 3.3.** Let \( E = E_d \) be an elliptic curve over \( K \) with the same assumptions as in Subsection 2.3. Then the infinity type \( \chi_{\infty} : \mathbb{C}^\times \to \mathbb{C}^\times \) of the corresponding Hecke character \( \chi \) is given by \( z \mapsto z^{-1} \).

**Proof.** Since the Hecke characters attached to CM elliptic curves are of weight 1 (cf. [Sch88, §1.1]), the infinity type must be either of the form \( z \mapsto z^{-1} \) or of the form \( z \mapsto \bar{z}^{-1} \). In order to determine which one is the true infinity type for our case, we consider an element \( \alpha \in O \) such that \( \alpha \equiv 1 \pmod{\wp^n} \) where \( \wp \) is an odd prime with \( \wp^n \mid \tilde{f} \), \( n > 0 \), that \( \alpha \equiv 1 \pmod{(1 + i)^mO} \) where \( m \) is any integer \( \geq \max(\text{ord}_{(1+i)O} \tilde{f}, 3) \) and that \( \alpha O \) is a prime ideal of \( O \). The existence of such an element is guaranteed by Lemma 4.1. Now, since \( \alpha O \in \mathcal{P}_1 \) and since \( (\bar{d}/\alpha O)_4 = 1 \) due to the conditions of \( \alpha \), we see that \( \chi_{\infty}(\alpha) = \alpha^{-1} \). This implies that the infinity type is indeed \( z \mapsto z^{-1} \). \( \square \)
3.2. Root numbers of Hecke characters. Let $E$ be an elliptic curve defined over $K$ given by the Weierstrass equation (5) with fourth-power-free $d \in O$. The (global) root number of the associated Hecke character $\chi$ of $E$ can be represented by the product of local root numbers of $\chi$. In our case, for any place $v$ of $K$, we can compute the local root number $w_v(\chi)$ as follows with three cases (cf. [Roh11, Lecture 2], or [Wat11, §§3–5]):

1. If $v$ is archimedean, in other words, since our $K$ is imaginary quadratic, if $v$ is the unique complex place of $K$, then $w_v(\chi) = -1$.

2. If $\chi$ is unramified at $v$, in other words, if $E$ has good reduction at $v$, then $w_v(\chi) = \chi^v(b_v)/|\chi^v(b_v)|$, where $\chi^v$ is the local component of $\chi_K$, i.e., $\chi^v = \chi_K \circ \iota_v$, where $\iota_v : K_v^\times \to \mathbf{A}_K^\times / K^\times$ is induced by the natural inclusion and $b_v$ is the local different of the completion $K_v$ of $K$ with respect to $v$. In particular, if moreover $v$ is odd, then $w_v(\chi) = +1$. On the other hand, if $v$ is the unique place lying over the prime $2$, i.e. the place corresponds to the prime ideal $(1 + i)O$ of $K$ and if $E$ has good reduction at $v$, then $w_v(\chi) = \chi(b_v) = \chi((1 + i)^2O)$.

3. Suppose $\chi$ is ramified at $v$, i.e., $E$ has bad reduction at $v$. Let $\chi^v = \chi^v/|\chi^v|$. We have

$$w_v(\chi) = \chi^v(\beta) \cdot G(\chi^v),$$

where $\beta \in K^\times$ is any element satisfying $v(\beta) = a(\chi^v) + n$. Here $a(\chi^v)$ is the exponent of the conductor of $\chi^v$ (cf. [Roh11], pp. 28–29), and $n$ is the valuation of the local different ideal of $K_v$. Moreover, $G(\chi^v)$ is the normalised Gauss sum given by:

$$G(\chi^v) = q^{-a(\chi^v)/2} \cdot \sum_{x \in (O_v/(\chi^v))^\times} (\chi^v)^{-1}(x) \cdot e^{2\pi i \text{tr}_{K_v}(x/\beta)}.$$

Remark. (1) The local character $\chi^v : K_v^\times \to \mathbf{C}^\times$ is ramified if and only if the original curve $E$ has bad reduction at $v$. Moreover, the exponent of the conductor $a(\chi^v)$ of $\chi^v$ is exactly the half of the exponent of the conductor of $E$ at $v$ (cf. [ST68, Theorem 12]). In particular, if $v$ is odd and $E$ has bad reduction at $v$, then $a(\chi^v) = 1$.

(2) We can compute the values of $\chi^v$ using [Roh11, Proposition 2.1]. More precisely, suppose that $\mathfrak{p}$ is a prime ideal of $K$ with corresponding finite place $v$ and $\pi$ is a uniformiser for $K_v$. Then we have the following.

- If $\mathfrak{p} \nmid \mathfrak{f}$, then $\chi^\mathfrak{p}(\pi) = \chi(\mathfrak{p})$.
- If $\mathfrak{p} | \mathfrak{f}$ then $\chi^\mathfrak{p}[O_K^\times] = e_\mathfrak{p}^{-1}$.
- If $\beta \in O_K$ and $\beta O_K$ is a power of some prime ideal $\mathfrak{p}$ dividing $\mathfrak{f}$, then

$$\chi^\mathfrak{p} = \chi_\mathfrak{f}^{-1}(\beta) \cdot \prod_{q|\mathfrak{f}, \alpha \not\equiv \mathfrak{p}} e_q(\beta).$$

4. Proofs of the main results

The following result is a generalisation of Dirichlet’s theorem on arithmetic progression over the Gaussian field $K$.

Lemma 4.1. Let $m_1, \cdots, m_J$ be mutually relatively prime ideals of $O$ and $\alpha_j \in O$ for $j = 1, \cdots, J$ be given. Then, there are infinitely many prime elements $x \in O$ such that $x \equiv \alpha_j \pmod{m_j}$ for all $j = 1, \cdots, J$.

Let us consider the elliptic curve $E_d$ defined by the equation (5) with fourth-power-free $d \in O$ and the primary prime decomposition (cf. Subsection 2.1) of $d$:

$$d = \frac{i^{n_\mathfrak{p}} \cdot (1 + i)^{n_2}}{\prod_{\mathfrak{p} : \text{degree } 1} \pi_{\mathfrak{p}}^{n_\mathfrak{p}} \cdot \prod_{-q : \text{degree } 2} (-q)^{n_q}}.$$ (8)

Here, we have separated prime elements of $K$ into two kinds: those with absolute residual degree one or two. Note also that the primary generator of a prime of degree two is of the form $-q$ with $q$ being a rational prime congruent to 3 modulo 4. For primes of degree one, we denote by $\pi$ its
primary generator. Also note the range of the exponents \( n_* \) of the factors in (8): we have \( 0 \leq n_* < 4 \) since \( i^4 = 1 \) and \( d \) is assumed to be fourth-power-free.

**Lemma 4.2.** Suppose that \( v \) is a finite place of \( K \) with corresponding prime ideal \( p_v \) of \( O \), and assume that \( p_v \nmid 2 \) and that \( p_v \) is of degree one. Let \( d \) be a fourth-power-free element in \( O \). Then the local epsilon type \( \epsilon_v \) associated with \( E_d \) at \( v \) is completely determined by the value \( v(d) \). More precisely, \( \epsilon \) is of exact order 4 (resp. 2, resp. 1) if and only if \( v(d) \in \{ 1, 3 \} \) (resp. \( v(d) = 2 \), resp. \( v(d) = 0 \)).

**Proof.** Note that the residue field of \( p_v \) is \( \mathbb{F}_p \) for a rational prime \( p \equiv 1 \pmod{4} \). Fix an element \( g \) of \( O \) which generates the multiplicative group \( \mathbb{F}_p^* \) modulo \( p_v \). By Lemma 4.1, we can find a primary prime element \( x \in O \) and \( u \in O^* \) such that

\[
ux \equiv \begin{cases} 
g \pmod{p_v}, \\ 1 \pmod{p_v} \end{cases} \text{ for all } w \text{ with } w(d) > 0, w(2) = 0 \text{ and } w \neq v,
\]

Note that \( u = 1 \) because both \( x \) and \( ux \) are primary. Write \( x = a + bi \) with \( a, b \in \mathbb{Z}, a \equiv 1 \pmod{16} \) and \( b \equiv 0 \pmod{16} \). Expand \( d \) as the product of primary elements, i.e. \( d = i^{n_u} \cdot (1 + i)^{n_2} \cdot \prod_{l|d, \text{odd}} \pi_l^{n_l} \), with \( \pi_l \) being primary odd primes. Then,

\[
\epsilon_v(g) = \epsilon(x) = \chi(xO)x_\infty(x)
\]

\[
= \left( \frac{i}{x} \right)_4^{n_u} \cdot \left( \frac{1 + i}{x} \right)_4^{n_2} \cdot \prod_{l|d, \text{odd}} \left( \frac{\pi_l}{x} \right)_4^{n_l}
\]

\[
= \left( \frac{i^{-1}}{x} \right)_4^{n_u} \cdot \left( \frac{a-b-1}{x} \right)_4^{n_2} \cdot \left( \frac{g}{p_v} \right)_4^{n_{p_v}} = \left( \frac{g}{p_v} \right)_4^{n_{p_v}},
\]

by Proposition 3.2 and quartic reciprocity (Theorem 2.2). As \( \langle \cdot/p_v \rangle_4 \) is of exact order 4, so \( \epsilon \) is of exact order 4 (resp. 2, resp. 1) when \( n_{p_v} = v(d) \in \{ 1, 3 \} \) (resp. \( 2 \), resp. \( 0 \)). \( \square \)

**Proposition 4.3.** Let \( d \in O \) be a fourth-power-free element and \( E_d \) the elliptic curve defined by (5) with \( d \) and with corresponding Hecke character \( \chi \).

1. Suppose that \( \pi \) arbitrary primary prime of degree one dividing \( d \) with order \( n \in \{ 1, 2, 3 \} \), and \( v \) its corresponding valuation of \( K \). Then,

\[
w_\pi(\chi) = \eta^n \cdot \frac{\pi}{\pi_1} \cdot \frac{d/\pi^n}{\pi} \cdot \left( \frac{\pi^{-1}}{\pi} \right)_4^n \cdot G(\chi^v), \quad (9)
\]

where \( \eta \in \{ \pm 1 \} \). Here \( \eta = -1 \) if and only if \( \pi \equiv 3 + 2i \pmod{4} \).

2. Let \( q \) be a rational prime dividing \( d \) congruent to 3 modulo 4 and \( v \) the valuation corresponding to the prime \( qO \). Then,

\[
w_q(\chi) = -\left( \frac{d/(-q)^v}{-q} \right)_4 \cdot G(\chi^v). \quad (10)
\]

In this case, one has

\[
G(\chi^v) = \begin{cases} 
1 & \text{when } \chi^v \text{ has exact order 2}, \\
-1 & \text{when } \chi^v \text{ has exact order 4}.
\end{cases}
\]

**Proof.** (1) Let \( \mathfrak{f} \) be the conductor of the character \( \chi \). We compute \( w_\pi(\chi) \) following the formula (7) with picking \( \beta = p \) as follows.

\[
w_\pi(\chi) = \frac{\chi^v(p)}{[\chi^v(p)]} \cdot G(\chi^v) = \frac{\pi}{\pi} \cdot \chi^v(\pi) \cdot \prod_{w(f) > 0, w \neq v} \epsilon_w(\pi) \cdot G(\chi^v). \]

7
Let $\mathfrak{p}_w$ be the prime ideal corresponding to each valuation $w \neq v$ such that $w(f) > 0$, i.e. $\mathfrak{p}_w$’s are prime ideal factors of $f$. In order to compute the product of local epsilon factors in the above expression, we choose, by Lemma 4.1, a primary prime element $x \in \mathcal{O}$ and a unit $u \in \mathcal{O}^\times$ so that

$$ux \equiv \begin{cases} 
\pi \pmod{(1 + i)\beta} \\
\pi \pmod{p_w} \\
\pi^{-1} \pmod{p_v^n}.
\end{cases}$$

for odd $w \neq v$ and $w(f) > 0$,

Since $\pi$ is primary, the first condition ensures that $u = 1$, and all of the conditions above are arranged to imply

$$\chi^u(\pi) \prod_{w(f) > 0, w \neq v} \varepsilon_w(\pi) = \varepsilon(x) = \left(\frac{d}{x}\right)_4.$$  

Therefore,

$$w_v(\chi) = \frac{\pi}{\pi} \cdot \varepsilon(x) \cdot G(\chi^u) = \frac{\pi}{\pi} \cdot \left(\frac{d/\pi^n}{x}\right)_4 \cdot \left(\frac{\pi}{x}\right)_4 \cdot G(\chi^u)$$

$$= \frac{\pi}{\pi} \cdot \left(\frac{i^n}{x}\right)_4 \cdot \left(\frac{1+i}{x}\right)_4 \cdot \left(\frac{d/(i^n(1+i))}{x}\right)_4 \cdot \left(\frac{\pi}{x}\right)_4 \cdot G(\chi^u).$$

Now one can observe the following.

- It follows from Equation (4) that $(i/\pi)_4 = (i/\pi)_4$ and $((1+i)/x)_4 = (1+i)/\pi)_4$.
- Since $d/(i^n(1+i))\pi^n$ is the product of primary prime elements, by factoring it into primary primes and interchanging the “denominators” and the “numerators” in the quartic residue symbol by Equation (3), we get

$$\left(\frac{d/(i^n(1+i))\pi^n}{x}\right)_4 = \left(\frac{d/(i^n(1+i))\pi^n}{\pi}\right)_4.$$  

- Since $x \equiv \pi \pmod{\pi}$, we see $(\pi/\pi)_4 = \eta \cdot (x/\pi)_4 = \eta \cdot (\pi^{-1}/\pi)_4$.

Summarising, we obtain Equation (9).

(2) In this case, the normalised Gauss sum $G(\chi^u) = 1$ (resp. $-1$) if and only if $\chi^u$ has exact order 2 (resp. 4) (cf. [MvdV03], p. 383 and [Mbo98, Theorem 2.4]). This shows the last statement. Now, by Formula (7) with $\beta = q$,

$$w_\pi(\chi) = \frac{\chi^u(q)}{\chi^u(q)} \cdot G(\chi^u) = \prod_{w(f) > 0, w \neq v} \varepsilon_w(q) \cdot G(\chi^u).$$

Let $\mathfrak{p}_w$ be the prime ideal corresponding to each valuation $w \neq v$ such that $w(f) > 0$, i.e. $\mathfrak{p}_w$’s are prime ideal factors of $f$. As above, we choose a primary prime element $x \in \mathcal{O}$ and a unit $u \in \mathcal{O}^\times$ so that

$$ux \equiv \begin{cases} 
q \pmod{(1 + i)^{\max(\text{ord}_{1+i}, 4)}} \\
q \pmod{p_w} \\
1 \pmod{p_v^n}.
\end{cases}$$

for odd $w \neq v$ and $w(f) > 0$,

Since $-q$ is primary, the first condition ensures that $u = -1$, and all of the conditions above are arranged to imply

$$w_q(\chi) = \varepsilon(-x) \cdot G(\chi^u) = -\left(\frac{d}{x}\right)_4 \cdot G(\chi^u) = -\left(\frac{d/(-q)^n}{x}\right)_4 \cdot \left(\frac{(-q)^n}{x}\right)_4 \cdot G(\chi^u).$$
Now, in the same fashion as above, we can see
\[ \left( \frac{d}{(-q)^n} \frac{x}{q} \right)_4 = \left( \frac{d}{(-q)^n} \frac{x}{q} \right)_4, \quad \text{and} \quad \left( \frac{-q}{x} \right)_4 = \left( \frac{-1}{-q} \right)_4 = 1, \]
whence (10).

**Corollary 4.4.** Let \( \pi \) be a primary prime element of degree one of \( O \) such that \( \pi \equiv 3 + 2i \pmod{4} \) and \( v \) its corresponding valuation of \( K \). Consider the elliptic curve \( E_\pi \) defined by (5) with \( d = \pi \) and the corresponding Hecke character \( \chi_\pi \). Then the set \( \{ w_v(\chi_\pi) \} \) is identical to the set of the fourth roots of unity, \( \mu_4 \).

**Proof.** The defining equation for \( E \) is also given by Equation (5) with \( d = i^m \pi \) for some \( m = 0, 1, 2, 3 \). Then it follows from Lemma 4.2 and Proposition 4.3 (1), we see that \( w_v(\chi_\pi) = \left( \frac{i}{\pi} \right)_4 \). Since \( \pi \equiv 3 + 2i \pmod{4} \), by Formula (4) we have \( \left( \frac{i}{\pi} \right)_4 = \pm i \), whence the result follows.

Now we are ready to prove Theorem 1.1.

**Proof of Theorem 1.1.** Let \( E \) be the elliptic curve defined by the Weierstrass equation (5) with \( d = \pi \) being a primary Gaussian prime of degree one. Also, let \( v \) be the place of \( K \) corresponding to the prime \( \pi \) and \( \chi \) the corresponding Hecke character for \( E/K \). It follows from [Mat79, Theorem 2], that the Gauss sum \( G(\chi^v) \) in (7) is contained in \( \mu_4 \cdot \sqrt{\pi} \sqrt{\pi} \). Thus, \( w_v(\chi) \in \mu_4 \cdot \pi^{3/2} / |\pi|^{3/2} \). Thus, it is enough to show

1. that the set \( \{ \pi / |\pi| : \pi \text{ being primary Gaussian primes of degree one.} \} \) is dense in the unit circle \( S^1 \), and
2. that for each such prime \( \pi \) and a fourth root \( \zeta \), there is an elliptic curve \( E \) with Hecke character \( \chi \) such that \( w_v(\chi) = \zeta \cdot \pi^{3/2} / |\pi|^{3/2} \).

For (1), it can be shown by the Sato–Tate theory for CM elliptic curves. Let \( p \) be a rational prime congruent to 1 modulo 4. Then we may write \( p = l^2 + m^2 \) for \( l, m \in \mathbb{Z} \). In fact, there are 8 representations \( (l, m) \) satisfying this equation; if we further require \( l \equiv (-1)^{(p-1)/4} \pmod{4} \), then such \( l \) is unique with \( l = \frac{1}{2} a_p \), where \( a_p \) is the eigenvalue of the Hecke operator \( T_p \) on the modular form associated with the elliptic curve \( E : y^2 = x^3 - x \). For such choices of \( l \) and \( m \), we see that \( \pi = l + mi \) and \( \pi = l - mi \) are primary primes. Since \( E \) is a CM elliptic curve, it is well-known due to Hecke that \( a_p = 2 \sqrt{p} \cos \theta_p \) with \( \theta_p \in [0, \pi] \), and that for any interval \( I = [\alpha, \beta] \subset [0, \pi] \), we have
\[
\lim_{x \to \infty} \frac{\# \{ p \leq x : \theta_p \in I \}}{\# \{ p \leq x \}} = \frac{\delta I}{2} + \frac{\beta - \alpha}{2 \pi},
\]
where \( \delta I = 1 \) if \( \pi/2 \in I \) and \( \delta I = 0 \) otherwise. In particular, this implies that there are infinitely many primary Gaussian primes \( \pi \) such that \( \pi / |\pi| \) is contained in any ball centred at a point in \( S^1 \) and having arbitrary positive radius.

Now let us prove (2). By Corollary 4.4, given \( \zeta \in \mu_4 \) and \( \pi \), there is \( m \in \{0, 1, 2, 3\} \) such that \( w_v(\chi^{\pi}) = \zeta \cdot \pi^{3/2} / |\pi|^{3/2} \). This proves the Theorem. 

**Corollary 4.5.** Let \( q' \) be a rational prime congruent to 3 modulo 4, relatively prime to \( d \), and \( k \in \{1, 2, 3\} \).

1. Let \( \pi \) be a prime of degree one dividing \( d \). Then,
\[ w_\pi(\chi^{(-q')^k \pi}) = w_\pi(\chi^d) \cdot \left( \frac{-q'}{\pi} \right)_4^k. \]

2. Let \( q \) be a prime of degree two dividing \( d \). Then,
\[ w_q(\chi^{(-q')^k \pi}) = w_q(\chi^d). \]
Proof. (1) From Lemma 4.2, it follows that $G(\chi_{(\cdot,q)\mathcal{O}}) = G(\chi_\mathcal{O})$, and hence

$$w_\pi(\chi_{(\cdot,q)\mathcal{O}})/w_\pi(\chi_\mathcal{O}) = \left(\frac{-q}{\pi}\right)^k,$$

by Proposition 4.3. This gives the result.

(2) The proof is the same as in (1), once one notes that $\left(\frac{-q}{\pi}\right)^4 = 1$ (cf. Proposition 2.1 (5)).

Proof of Theorem 1.2. Given $\theta \in S^1$, let $E_d$ be the curve defined by (5) as usual and $v$ a valuation of $K$ such that $w_v(\chi_\mathcal{O}) = \theta$. Suppose first that $v$ corresponds to a prime ideal of $\mathcal{O}$ of degree two, i.e. there is a rational prime $q \equiv 3 \pmod{4}$ such that $q\mathcal{O}$ is the prime ideal corresponding to $v$. In this case, Corollary 4.5 (2) shows that $w_v(\chi_{(\cdot,q)\mathcal{O}}) = w_v(\chi_\mathcal{O})$ for any rational prime $q' \neq q$ with $q' \equiv 3 \pmod{4}$.

Suppose that $v$ corresponds to a prime ideal $p = \pi\mathcal{O}$ of degree one with primary prime generator $\pi \in \mathcal{O}$. Then by Lemma 4.1, there are infinitely many rational primes $q$ congruent to 3 modulo 4 such that $\left(\frac{-q}{\pi}\right)^4 = -1$, so $\left(\frac{-q}{\pi}\right)^4 = 1$. Then by Corollary 4.5 (1), for the curve $E_{(\cdot,q)\mathcal{O}}$ and for its corresponding Hecke character $\chi_{(\cdot,q)\mathcal{O}}$, we have $w_v(\chi_{(\cdot,q)\mathcal{O}}) = w_v(\chi_\mathcal{O})$. □

Now we turn our focus to Theorem 1.3. We recall some classical results of Wirsing.

Lemma 4.6 ([Wir61, Satz 1]). Let $f$ be a non-negative multiplicative function such that

- there exist constants $c_1$ and $c_2 < 2$ satisfying $f(p^v) \leq c_1c_2^v$ for all primes $p$ and $v \geq 2$,
- there exists a real number $\tau > 0$ satisfying
  \[
  \sum_{p \leq X} f(p) = (\tau + o(1))\frac{X}{\log X}.
  \]

Then, we have

\[
\sum_{n \leq X} f(n) = \left(\frac{1}{e^\gamma \Gamma(\tau)} + o(1)\right)\frac{X}{\log X} \prod_{p \leq X} \sum_{v=0}^{\infty} \frac{f(p^v)}{p^v}.
\]

Here $\Gamma$ is the gamma function and $\gamma$ is the Euler–Mascheroni constant.

Lemma 4.7 ([Wir67, Satz 1.2.2]). Let $f$ be a non-negative multiplicative function such that

- there exists a constant $c$ satisfying $f(p) \leq c$ for all primes $p$,
- there exists a real number $\tau > 0$ satisfying
  \[
  \sum_{p \leq X} f(p) = (\tau + o(1))\frac{X}{\log X}.
  \]

Then, for $g$ with $|g(n)| \leq f(n)$, we have

\[
\sum_{n \leq X} g(n) = \left(\prod_p \left(1 + \frac{g(p)}{p} + \frac{g(p^2)}{p^2} + \cdots \right) \left(1 + \frac{f(p)}{p} + \frac{f(p^2)}{p^2} + \cdots \right)^{-1} + o(1)\right)\left(\sum_{n \leq X} f(n)\right).
\]

The following lemma is a variant of [Wil74, Theorem 1].

Lemma 4.8. Let $\xi$ be an $n$-th root of unity for some positive integer $n$, and let $a$ and $m$ be positive integers satisfying $(n, m) = 1$ and $(a, m) = 1$. Then the product

\[
\prod_{p \leq X \atop p \equiv a \pmod{m}} \left(1 - \frac{\xi}{p}\right)^{-1}
\]
converges to non-zero constant as $X$ goes to infinity.
Proof. Let \( \psi \) be a non-principal Dirichlet character of order \( m \). There is a constant \( b_\psi \) such that 
\[
\sum_{p \leq X} \frac{\psi(p)}{p} = b_\psi + O_\psi \left( \frac{1}{\log X} \right).
\]

Then,
\[
- \sum_{p \leq X} \log \left( 1 - \frac{\xi \psi(p)}{p} \right) = \xi \sum_{p \leq X} \frac{\psi(p)}{p} + \sum_{p} \left( \sum_{k=2}^{\infty} \frac{\xi^k \psi(p)^k}{kp^k} \right) + O_\psi \left( \frac{1}{\log X} \right) = b'_\psi, \xi + O_\psi \left( \frac{1}{\log X} \right),
\]
for some constant \( b'_\psi, \xi \). Therefore, by taking exponential to the above equation, we see that there is a constant \( c_\psi, \xi \neq 0 \) such that
\[
\prod_{p \leq X} \left( 1 - \frac{\xi \psi(p)}{p} \right)^{-1} = c_\psi, \xi + O_\psi \left( \frac{1}{\log X} \right). \tag{11}
\]

Let \( k_{\psi, \xi} \) be a completely multiplicative function defined by
\[
k_{\psi, \xi}(p) := p \left( 1 - \left( 1 - \frac{\xi \psi(p)}{p} \right) \left( 1 - \frac{\xi}{p} \right)^{-\psi(p)} \right),
\]
for each prime \( p \). By following [Wil74], we have
\[
|k_{\psi, \xi}(p)| \leq \frac{1}{p} + \sum_{n=3}^{\infty} \frac{1}{p^{n-1}} \frac{n-1}{n} \leq \frac{1}{p-1}.
\]

Therefore,
\[
\sum_p \left| \sum_{n=1}^{\infty} \frac{k_{\psi, \xi}(p)}{p^n} \right|^n \leq \sum_p \sum_{n=1}^{\infty} \left( \frac{1}{(p-1)p^n} \right)^n = \sum_p \frac{1}{p^{\sigma+1} - p^{\sigma} - 1}
\]
is finite for \( \sigma > 0 \). In the same region,
\[
\prod_p \left( 1 - \frac{k_{\psi, \xi}(p)}{p^s} \right)^{-1} = \prod_p \left( 1 + \sum_{n=1}^{\infty} \frac{k_{\psi, \xi}(p)}{p^s} \right)^n
\]
converges absolutely. Hence,
\[
K_{\xi}(s, \psi) := \sum_{n=1}^{\infty} \frac{k_{\psi, \xi}(n)}{n^s}
\]
converges absolutely and has Euler product on \( \sigma > 0 \). Therefore, there exists \( c_\psi \neq 0 \) such that
\[
\prod_{p \leq X} \left( 1 - \frac{k_{\psi, \xi}(p)}{p} \right)^{-1} = c_\psi + O_\psi \left( \frac{1}{\log X} \right). \tag{12}
\]

By the orthogonality of characters,
\[
\prod_{p \leq X} \left( 1 - \frac{\xi}{p} \right)^{\phi(k)} = \prod_{\psi} \left( \prod_{p \leq X} \left( 1 - \frac{\xi}{p} \right)^{\psi(p)} \right)^{\psi(a)}.
\]
Then by Equations (11) and (12) and the definition of \( k_{\psi, \xi} \), we have

\[
\prod_{p \leq X} \left( 1 - \frac{\xi}{p} \right)^{\psi(p)} = \prod_{p \leq X} \left( 1 - \frac{\xi \psi(p)}{p} \right) \prod_{p \leq X} \left( 1 - k_{\psi, \xi}(p)^{-1} \right).
\]

\[
= \left( \psi + O \left( \frac{1}{\log X} \right) \right) \left( \psi + O \left( \frac{1}{\log X} \right) \right) = \psi \psi + O \left( \frac{1}{\log X} \right).
\]

Therefore,

\[
\prod_{p \equiv a \pmod{m}} \left( 1 - \frac{\xi}{p} \right) = \prod_{\psi} \left( \psi \psi c_{\psi, \xi} \right) + O \left( \frac{1}{\log X} \right),
\]

which proves the lemma. \( \square \)

**Proposition 4.9.** Let \( a, b, m \) and \( n \) be integers such that \((a, m) = (b, n) = (m, n) = 1\), \( \Omega(X) \) be the set of square-free positive integers \( x \) whose size is less than \( X \) and each prime divisor of \( x \) is congruent to \( b \) modulo \( n \). Then there is a constant \( c \neq 0 \) such that

\[
|\Omega(X)| = c \left[ 1 + o(1) \right] \frac{X}{(\log X)^{1 - \frac{1}{\phi(n)}}}.
\]

Let \( \Omega_{a,m}(X) \) be a set of elements of \( \Omega(X) \) which is equal to \( a \) modulo \( m \). Then

\[
\left| \Omega_{a,m}(X) \right| = \frac{1}{m} |\Omega(X)| + O \left( \frac{X}{\log X} \right).
\]

**Proof.** We recall [Wil74, Theorem 1], that is

\[
\prod_{p \leq X, p \equiv b} \left( 1 - \frac{1}{p} \right) = \left( e^{-\gamma} n \prod_{\psi \phi(n)} K(1, \psi) \bar{\psi(b)} \right) \frac{1}{(\log X)^{1 - \frac{1}{\phi(n)}}} + O \left( \frac{1}{(\log X)^{1 - \frac{1}{\phi(n)}}} \right). \tag{13}
\]

Following the proof of [BFL08, Lemma 11], define a multiplicative function \( f \) by, for each prime \( p \),

\[
f(p) = \begin{cases} 1 & p \equiv b \pmod{n}, \\ 0 & \text{otherwise.} \end{cases}
\]

and \( f(p^v) = 0 \) for all \( v \geq 2 \). Then, we have \( \sum_{k \leq X} f(k) = |\Omega(X)| \). By the prime number theorem for arithmetic progressions, this multiplicative function \( f \) satisfies the condition of Lemma 4.6 for \( c_2 = 0 \) and \( \tau = 1/\phi(n) \). Therefore,

\[
|\Omega(X)| = \left( \frac{1}{e^{\gamma} n} \Gamma(\phi(n)^{-1}) + o(1) \right) \frac{X}{\log X} \prod_{p \leq X, p \equiv b} \left( 1 + \frac{1}{p} \right).
\]

Since the product \( \prod_{p \leq X, p \equiv b (\mod n)} (1 - 1/p^2) \) is convergent to a non-zero constant as \( X \rightarrow \infty \), Equation (13) yields

\[
\prod_{p \leq X, p \equiv b} \left( 1 + \frac{1}{p} \right) = c_3 (1 + o(1)) (\log X)^{1 - \frac{1}{\phi(n)}},
\]

for some non-zero constant \( c_3 \). This gives the first part of Proposition.

By the orthogonality of characters, we have

\[
|\Omega_{a,m}(X)| = \frac{1}{\phi(m)} \sum_{k \leq X} \psi(a) \psi(k) f(k) = \frac{1}{\phi(m)} \sum_{\psi} \psi(a) \sum_{k \leq X} \psi(k) f(k),
\]

for some non-zero constant \( c_3 \). This gives the first part of Proposition.
where $\sum_\psi$ is taken over Dirichlet characters of modulus $m$. Therefore, it is enough to show that
\[
\sum_{k \leq X} f(k)\psi(k) = \begin{cases} (1 + o(1)) \cdot \frac{\phi(m)}{m} \cdot |\Omega(X)| & \text{if } \psi = \psi_0, \\
O \left( \frac{X}{\log X} \right) & \text{if } \psi \neq \psi_0,
\end{cases}
\]
where $\psi_0$ is the principal Dirichlet character of modulus $m$. We first consider $(\psi = \psi_0)$-case. We define
\[
m' = \prod_{p \mid m, \; p \equiv b \pmod{n}} p.
\]
Since the number of elements in $\Omega(X)$ which is divisible by $p$ is exactly $|\Omega(X/p)|$, by the inclusion-exclusion principle, we have
\[
\sum_{k \leq X} f(k)\psi_0(k) = \sum_{d \mid m'} \mu(d)|\Omega(\frac{X}{d})|.
\]
By the first part of this proposition, we have
\[
\sum_{k \leq X} f(k)\psi_0(k) = (1 + o(1)) \cdot \left( \sum_{d \mid m'} \mu(d) \right) \cdot |\Omega(X)| = (1 + o(1)) \cdot \frac{\phi(m')}{m'} \cdot |\Omega(X)|.
\]
Since $f(k)$ and $f(k)\psi(k)$ satisfy the condition of Lemma 4.7, we have
\[
\sum_{k \leq X} f(k)\psi(k) = \left( \sum_{p \leq X} \frac{f(p)\psi(p)}{p} \right) \left( \sum_{j=0}^{\infty} \frac{f(p^j)}{p^j} \right)^{-1} + o(1) \sum_{k \leq X} f(k). \tag{14}
\]
Now, we will show that
\[
\prod_{p \equiv b \pmod{n}} \left( 1 + \frac{\psi(p)}{p} \right) \tag{15}
\]
converges to a non-zero complex number as $X$ goes to infinity, for all non-principal characters $\psi$ of modulus $m$. Write
\[
\prod_{p \equiv b \pmod{n}} \left( 1 - \frac{\psi(p)}{p} \right)^{-1} = \prod_{i=0}^{m-1} \prod_{p \equiv b + in \pmod{mn}} \left( 1 - \frac{\psi(b + in)}{p} \right)^{-1}.
\]
Then by Lemma 4.8, each product converges to the non-zero complex number. Since
\[
\prod_{p \equiv b \pmod{n}} \left( 1 - \frac{\psi^2(p)}{p^2} \right)
\]
converges to a non-zero constant, the product (15) also converges to a non-zero constant. Then by (14) and the previous calculations, there is a non-zero constant $c_4$ such that
\[
\sum_{k \leq X} f(k)\psi(k) = c_4 \frac{1}{(\log X)^{\frac{1}{m}}} \sum_{k \leq X} f(k),
\]
which gives the cases with $(\psi \neq \psi_0)$. \hfill \square
Proof of Theorem 1.3. Recall for a real number \(X > 0\), \(Q(X)\) is the set of elements \(x \in O\) with \(|x| < X\), represented as the product of distinct primary primes of degree two. Write \(d\) as the product of primary primes (cf. Equation (8)):

\[
d = \prod_{i \in I} \pi_i \cdot \prod_{j \in J} (-q_j)^{n_j},
\]

and let

\[
d_1 = \prod_{i \in I} \pi_i, \quad d_2 = \prod_{j \in J} (-q_j)^{n_j}, \quad \widehat{d}_2 = \prod_{j \in J} (-q_j).
\]

For each function \(f : J \to \{0, 1\}\) we define

\[
Q_f(X) := \{Q \in Q(X) : \text{ord}_{q_i} Q = f(j)\}.
\]

Then \(Q(X)\) is the disjoint union of \(Q_f(X)\), for all \(f \in \{0, 1\}^J\). For a fixed \(f \in \{0, 1\}^J\), define \(L = f^{-1}(0)\) and \(T = f^{-1}(1)\). Then we can write \(d = \prod_{i \in I} \pi_i \cdot \prod_{j \in L} (-q_j)^{n_j} \cdot \prod_{t \in T} (-q_t)^{n_t}\). For \(Q \in Q_f(X)\), we write \(Q = \prod_{k \in K} (-q_k) \cdot \prod_{t \in T} (-q_t)\).

By Proposition 4.3 and Corollary 4.5, we have, for each \(i \in I\),

\[
w_{\pi_i}(\chi_{dQ}) = \eta \cdot \frac{\pi_i}{|\pi_i|} \cdot \frac{dQ}{\pi_i} \cdot \frac{\pi_i - 1}{\pi_i} \cdot G(\chi_{dQ}^{\pi_i}) = \eta \cdot \frac{\pi_i}{|\pi_i|} \cdot \frac{d}{\pi_i} \cdot \frac{\pi_i - 1}{\pi_i} \cdot G(\chi_{d}^{\pi_i}) \cdot \frac{Q}{\pi_i} \cdot \frac{1}{\prod_{k \in K} (-q_k)^{n_k}} \cdot \prod_{t \in T} (-q_t)^{n_t}.
\]

Also for each \(k \in K\),

\[
w_{q_k}(\chi_{dQ}) = w_{q_k}(\chi_{d1}(-q_k)) = \frac{d_1}{-q_k} = \prod_{i \in I} \frac{-q_k}{\pi_i}.
\]

and for \(l \in L\),

\[
w_{q_l}(\chi_d) = w_{q_l}(\chi_{Qd}).
\]

Therefore,

\[
\frac{w(\chi_{dQ})}{w(\chi_{dQ})} = -i \prod_{i \in I} w_{\pi_i}(\chi_{dQ}) \prod_{i \in L} w_{q_l}(\chi_{dQ}) \prod_{k \in K} w_{q_k}(\chi_{dQ}) \prod_{t \in T} w_{q_t}(\chi_{dQ})
\]

\[
= -i \prod_{i \in I} \left( w_{\pi_i}(\chi_d) \prod_{k \in K} \frac{-q_k}{\pi_i} \prod_{t \in T} \frac{-q_t}{\pi_i} \right) \left( \prod_{i \in L} w_{q_l}(\chi_d) \right) \left( \prod_{k \in K} w_{q_k}(\chi_d) \right) \left( \prod_{t \in T} w_{q_t}(\chi_d) \right)
\]

\[
= \frac{w(\chi_d)}{w(\chi_d)} \prod_{i \in I} \left( \prod_{k \in K} \frac{-q_k}{\pi_i} \prod_{t \in T} \frac{-q_t}{\pi_i} \right) \prod_{i \in L} \left( \prod_{i \in I} \frac{-q_i}{\pi_i} \frac{\chi_{dQ}}{\chi_d} \right) \prod_{k \in K} \left( \prod_{i \in I} \frac{-q_k}{\pi_i} \frac{\chi_{dQ}}{\chi_d} \right) \prod_{t \in T} \left( \prod_{i \in I} \frac{-q_t}{\pi_i} \frac{\chi_{dQ}}{\chi_d} \right)
\]

\[
= \frac{w(\chi_d)}{w(\chi_d)} \prod_{i \in I} \prod_{k \in K} \left( \frac{-q_k}{\pi_i} \right)^2 \prod_{i \in L} \prod_{t \in T} \left( \frac{-q_t}{\pi_i} \right)^2 \prod_{k \in K} \prod_{t \in T} \left( \frac{-q_k}{\pi_i} \frac{\chi_{dQ}}{\chi_d} \right) \prod_{k \in K} \prod_{t \in T} \left( \frac{-q_t}{\pi_i} \frac{\chi_{dQ}}{\chi_d} \right),
\]

where \(p_i = \pi_i \bar{\pi}_i\). Here we use \(\left( \frac{-q_k}{\pi_i} \right)^2 \left( \frac{-q_t}{p_i} \right)^2\). We note that for all \(Q \in Q_f(X)\), the terms

\[
\prod_{i \in I} \prod_{t \in T} \left( \frac{-q_t}{\pi_i} \frac{\chi_{dQ}}{\chi_d} \right)
\]

in (16) are equal.
As before, let $Q_{f,a,m}(X)$ be the set of elements in $Q_f(X)$ that is equivalent to $a$ modulo $m$, and $P := \prod_{i \in I} p_i$. Then,

$$\sum_{Q \in Q_f(X)} \frac{w(\chi_d Q)}{w_2(\chi_d Q)} = \sum_{Q \in Q_f(X)} \frac{w(\chi_d)}{w_2(\chi_d)} \prod_{i \in I} \prod_{k \in K} \left( \frac{-q_k}{p_i} \right)^{\frac{n}{\pi_i}} \prod_{t \in T} \left( \frac{-q_t}{\pi_i} \right)^4 \left( \prod_{i \in I} \frac{w_1(\chi_d Q)}{w_2(\chi_d)} \right) \left( \sum_{Q \in Q_f(X)} \prod_{i \in I} \prod_{k \in K} \left( \frac{-q_k}{p_i} \right)^2 \right)$$

$$= \frac{w(\chi_d)}{w_2(\chi_d)} \prod_{i \in I} \prod_{t \in T} \left( \frac{-q_t}{\pi_i} \right)^4 \left( \prod_{t \in T} \frac{w_1(\chi_d Q)}{w_2(\chi_d)} \right) \left( \sum_{a,+} \sum_{b=ma(P)}_{b \# 0(q_j)} \frac{|Q_{b,P\widehat{d}_2}(X)|}{\Omega_{a,P\widehat{d}_2}(X)} \right)$$

where $Q_{b,P\widehat{d}_2}(X)$ is the subset of $Q(X)$ consisting of integers $x$ satisfying $x \equiv b \pmod{P\widehat{d}_2}$. Similarly consider $\Omega_{b,P\widehat{d}_2}(X)$ is the set of positive integers $x$ such that $x \leq X$, that each prime divisor of $x$ is congruent to 3 modulo 4, and that $x \equiv b \pmod{P\widehat{d}_2}$. Then one can easily see that the map

$$x \mapsto |x|, \quad \Omega_{b,P\widehat{d}_2}(X) \cup Q_{-b,P\widehat{d}_2}(X) \to \Omega_{b,P\widehat{d}_2}(X) \cup \Omega_{-b,P\widehat{d}_2}(X)$$

is bijective. Since $P\widehat{d}_2 \equiv 1 \pmod{4}$, $b$ and $-b$ are both quadratic residues or both quadratic non-residues modulo $P\widehat{d}_2$. Therefore

$$\sum_{a,+} \sum_{b=ma(P)}_{b \# 0(q_j)} \frac{|Q_{b,P\widehat{d}_2}(X)|}{\Omega_{a,P\widehat{d}_2}(X)} = \sum_{a,+} \sum_{b=ma(P)}_{b \# 0(q_j)} \frac{|Q_{b,P\widehat{d}_2}(X)|}{\Omega_{a,P\widehat{d}_2}(X)}$$

and the same holds for $\sum_{a,-}$. By Proposition 4.9,

$$\sum_{Q \in Q_f(X)} \frac{w(\chi_d Q)}{w_2(\chi_d Q)} = \sum_{a,+} \sum_{b=ma(P)}_{b \# 0(q_j)} \frac{|Q_{b,P\widehat{d}_2}(X)|}{\Omega_{a,P\widehat{d}_2}(X)} - \sum_{a,-} \sum_{b=ma(P)}_{b \# 0(q_j)} \frac{|Q_{b,P\widehat{d}_2}(X)|}{\Omega_{a,P\widehat{d}_2}(X)} \ll o(1) \frac{X}{(\log X)^{\frac{3}{2}}}$$

Therefore,

$$\sum_{Q \in Q(X)} \frac{w(\chi_d Q)}{w_2(\chi_d Q)} = \sum_{f \in \{0,1\}} \sum_{Q \in Q_f(X)} \frac{w(\chi_d Q)}{w_2(\chi_d Q)} \ll o(1) \frac{X}{(\log X)^{\frac{3}{2}}}$$
so for any \( \epsilon > 0 \), there is a \( X_0 \) such that
\[
\sum_{Q \in \mathcal{Q}(X)} \frac{w(\chi_{dQ})}{w_2(\chi_{dQ})} \leq c \cdot \epsilon \cdot \frac{X}{(\log X)^{1/2}},
\]
for all \( X \geq X_0 \), where \( c \) is the constant in the statement of Lemma 4.9. Hence
\[
\lim_{X \to \infty} \frac{1}{|\mathcal{Q}(X)|} \sum_{Q \in \mathcal{Q}(X)} \frac{w(\chi_{dQ})}{w_2(\chi_{dQ})} \leq \lim_{X \to \infty} \frac{1}{|\mathcal{Q}(X)|} \cdot c \cdot \epsilon \cdot \frac{X}{(\log X)^{1/2}} \leq \epsilon,
\]
again by Lemma 4.9. \( \square \)

\section*{Acknowledgement}

The first author is supported by the National Research Foundation of Korea (NRF) funded by the Ministry of Education, under the Basic Science Research Program (2018R1C1C1004264). He would like to thank Professor Peter J. Cho and Professor Yoonbok Lee for useful discussion. He also thanks IBS-CGP for their hospitality and financial support. The second author is supported by Global Ph. D. Fellowship Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2015H1A2A1032119). The third author is supported by IBS-R003-D1. The second and the third authors also thank UNIST for their hospitality.

\section*{References}

[BFL08] W. D. Banks, J. B. Friedlander, and F. Luca. Integers without divisors from a fixed arithmetic progression. \textit{Forum Math.}, 20(6):1005 – 1037, 2008.

[IR90] Kenneth Ireland and Michael Rosen. \textit{A classical introduction to modern number theory}, volume 84 of \textit{Graduate Texts in Mathematics}. Springer-Verlag, New York, second edition, 1990.

[Mat79] C. R. Matthews. Gauss sums and elliptic functions. II. The quartic sum. \textit{Invent. Math.}, 54(1):23–52, 1979.

[Mbo98] Oumar D. Mbodj. Quadratic Gauss sums. \textit{Finite Fields Appl.}, 4(4):347–361, 1998.

[MvdV03] P. Meijer and M. van der Vlugt. The evaluation of Gauss sums for characters of 2-power order. \textit{J. Number Theory}, 100(2):381–395, 2003.

[Roh11] David E. Rohrlich. Root numbers. In \textit{Arithmetic of L-functions}, volume 18 of \textit{IAS/Park City Math. Ser.}, pages 353–448. Amer. Math. Soc., Providence, RI, 2011.

[RS09] K. Rubin and A. Silverberg. Point counting on reductions of CM elliptic curves. \textit{J. Number Theory}, 129(12):2903 – 2923, 2009.

[Sch88] Norbert Schappacher. \textit{Periods of Hecke characters}, volume 1301 of \textit{Lecture Notes in Mathematics}. Springer-Verlag, Berlin, 1988.

[Sil94] Joseph H. Silverman. \textit{Advanced topics in the arithmetic of elliptic curves}, volume 151 of \textit{Graduate Texts in Mathematics}. Springer-Verlag, New York, 1994.

[ST68] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. \textit{Ann. of Math. (2)}, 88:492–517, 1968.

[Wat11] Mark Watkins. Computing with Hecke Grössencharacters. In \textit{Actes de la Conférence “Théorie des Nombres et Applications”}, volume 2011 of \textit{Publ. Math. Besançon Algèbre Théorie Nr.}, pages 119–135. Presses Univ. Franche-Comté, Besançon, 2011.

[Wil74] Kenneth S. Williams. Mertens’ theorem for arithmetic progressions. \textit{J. Number Theory}, 6:353 – 359, 1974.

[Wir61] E. Wirsing. Das asymptotische verhalten von summen über multiplikative funktionen. \textit{Math. Ann.}, 143:75 – 102, 1961.

[Wir67] E. Wirsing. Das asymptotische verhalten von summen über multiplikative funktionen. ii. \textit{Acta Math. Acad. Sci. Hungar.}, 18:411 – 467, 1967.
3-3 Imjeongro 13-gil, Yongsan-gu, Seoul 04319, Republic of Korea

E-mail address: kyjeongg@gmail.com
E-mail address: jigu.kim.math@gmail.com
E-mail address: Taekyung.Kim.Maths@gmail.com