On Sign Ambiguities of Multiplicative Relations Between Gauss Sums

by

Noboru AOKI

(Received October 3, 2013)
(Revised November 5, 2013)

1. Introduction

Let $m > 1$ be an integer and put $\zeta_m = e^{2\pi i / m}$. We denote by $K_m = \mathbb{Q}(\zeta_m)$ the $m$-th cyclotomic field, whose integer ring will be denoted by $\mathcal{O}_{K_m}$. Let $p$ be a prime number such that $p \equiv 1 \pmod{m}$. Throughout the present paper we fix a prime ideal $P$ of $\mathcal{O}_{K_m}$ dividing $p$. Since $p$ splits completely in $K_m$, the residue field $\mathcal{O}_{K_m}/P$ can be identified with the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Thus, the $m$-th power residue symbol defines a homomorphism

$$
\chi : \mathbb{F}_p^\times \rightarrow \mu_m,
$$

where $\mu_m$ denotes the group of $m$-th roots of unity in the complex number field. In other words, $\chi$ is a group homomorphism such that

$$
\chi(x) \equiv x^{\frac{m-1}{P}} \pmod{P}
$$

for any $x \in \mathcal{O}_{K_m} - P$. For an integer $a$ we define the Gauss sum $\tau(a)$ by

$$
\tau(a) = \sum_{t \in \mathbb{F}_p^\times} \chi(t)^a \zeta_p^t,
$$

(1)

where $\zeta_p = e^{2\pi i / p}$. Let us recall two types of formulas concerning products of Gauss sums; one is the norm relation

$$
\tau(a)\tau(-a) = \chi(-1)^a p,
$$

(2)

which holds for any $a \not\equiv 0 \pmod{m}$, and the other is the Davenport-Hasse multiplicative relation

$$
\frac{\tau(a)}{\tau(ad)} \prod_{k=1}^{d-1} \frac{\tau \left( a + \frac{km}{d} \right)}{\tau \left( \frac{km}{d} \right)} = \chi(d)^{-ad},
$$

(3)

where $d$ is a positive divisor of $m$ and $a$ is an integer such that $ad \not\equiv 0 \pmod{m}$.

For a formal sum

$$
\alpha = \sum_{a=1}^{m-1} c_a[a],
$$

where $c_a$ are coefficients.
of the symbols \([a] \ (a \in \{1, 2, \ldots, m-1\})\) with integral coefficients \(c_a \in \mathbb{Z}\), we define a product of Gauss sums

\[
\tau(\alpha) = \prod_{a=1}^{m-1} \tau(a)^{c_a}.
\]

Under this notation, a multiplicative relation between Gauss sums is by definition a formula of the form

\[
\tau(\alpha) = \varepsilon p^{s/2},
\]

where \(s = \sum_{a=1}^{m-1} c_a \in \mathbb{Z}\) and \(\varepsilon\) is a root of unity. Then it can be shown that \(\varepsilon\) is a root of unity contained in \(K_m\) (see [19, §19]). In 1964, Hasse [9] conjectured that (2) and (3) are essentially the only multiplicative relations between Gauss sums. This conjecture was, however, disproved by Yamamoto [19] in 1966; he showed that a counterexample exists when \(m = 12\). Moreover, in a subsequent paper [20] he determined the structure of the ‘gap group’ which measures the number of independent multiplicative relations between Gauss sums essentially distinct from (2) and (3) (see Theorem 2.9). In particular, Yamamoto’s theorem says that the square of the root of unity \(\varepsilon\) in (5) can be computed using (2) and (3), hence \(\varepsilon\) itself can be determined up to sign. It is, however, not easy in general to determine the sign. This problem, which is called the sign ambiguity problem, has been studied by many authors (see for example [7], [8], [11], [14], [15], [16], [18]).

If \(m\) is either a power of a prime number or the twice of a power of an odd prime number, then the gap group vanishes by Yamamoto’s theorem, hence every multiplicative relation between Gauss sums can be reduced to a combination of (2) and (3). On the contrary, in the case where \(m\) is a product of two distinct odd prime numbers, Yamamoto’s theorem implies that there is essentially only one exceptional multiplicative relation. Muskat [15] and Muskat-Zee [16] studied some special cases of this type. For example, the following results are proved in [15] or [16]:

**Theorem 1.1.** Suppose \(m = 39 = 3 \cdot 13\) or \(m = 21 = 3 \cdot 7\), and \(p \equiv 1 \pmod{m}\). Then the following statements hold:

(i) (Muskat) If \(m = 39\), then

\[
\tau(1)\tau(16)\tau(-17)\tau(-2)\tau(-32)\tau(34) = \varepsilon \chi(13)^3 p^3,
\]

where the sign ambiguity \(\varepsilon = \pm 1\) is given by

\[
\varepsilon = \begin{cases} 
1 & \text{if } p = u^2 + 39v^2 \ (3u, v \in \mathbb{Z}), \\
-1 & \text{if } p = 3u^2 + 13v^2 \ (3u, v \in \mathbb{Z}).
\end{cases}
\]

(ii) (Muskat-Zee) In the case of \(m = 21\), let \(u, v\) be integers such that \(p = u^2 + 7v^2\). Then

\[
\tau(1)\tau(4)\tau(-5)\tau(-3)\tau(-12)\tau(15) = \varepsilon \chi(7)^3 p^3,
\]

where the sign ambiguity \(\varepsilon = \pm 1\) is given by

\[
\varepsilon = \begin{cases} 
1 & \text{if } 3 \mid v, \\
-1 & \text{if } 3 \mid u.
\end{cases}
\]
Murray [14] and van Wamelen [18] generalized Theorem 1.1 (i) to the case where \( m = l_1 l_2 \) is a product of two primes \( l_1 \) and \( l_2 \) with \( l_1 \equiv 1 \pmod{4} \), \( l_2 \equiv 3 \pmod{4} \) satisfying certain additional arithmetic conditions (see [14, Main Theorem 1] and [18, Theorem 8] for more precise statements).

The purpose of this paper is to generalize Theorem 1.1 (ii). The main theorem of the present paper can be stated as follows (see Theorem 5.3 and Theorem 5.5):

**Theorem 1.2.** Let \( m = l_1 l_2 \) be a product of two distinct primes \( l_1, l_2 \) such that \( l_1 \equiv l_2 \equiv 3 \pmod{4} \) and \( \left( \frac{m}{l_1} \right) = 1 \). Let

\[
\prod_{a=1}^{m-1} \tau(a)^{\varepsilon_a} = \varepsilon \xi \sqrt{p},
\]

be a multiplicative relation between Gauss sums which is not deducible from (2) and (3), where \( \varepsilon = \pm 1 \) and \( \xi \) is a root of \( m \)-th root of unity. Then,

\[
\xi = \begin{cases}
1 & \text{if } l_1 > 3 \text{ and } l_2 > 3, \\
\chi(l)^l & \text{if } m = 3l.
\end{cases}
\]

Moreover, \( \varepsilon \) is given as follows: Let \( u, v \) be integers such that

\[
4p^{\frac{1}{2}(l_2+1)h(-l_1)} = u^2 + l_1 v^2,
\]

where \( h(-l_1) \) denote the class number of the imaginary quadratic field \( \mathbb{Q}(\sqrt{-l_1}) \). Then exactly one of \( u, v \) is divisible by \( l_2 \), and

\[
\varepsilon = \begin{cases}
1 & \text{if } l_2 \mid u, \\
-1 & \text{if } l_2 \mid v.
\end{cases}
\]

In the case of Theorem 1.2, the sign ambiguity \( \varepsilon \) is related to a ring class field of the imaginary quadratic field \( F = \mathbb{Q}(\sqrt{-l_1}) \). To be more precise, let \( \mathcal{O} \) be the order in \( F \) of conductor \( l_2 \). Then the class number \( h(\mathcal{O}) \) of \( \mathcal{O} \) is known to be divisible by 4. Under this notation, we can prove the following theorem, which was conjectured by van Wamelen in [18, Conjecture 21].

**Theorem 1.3 (See Corollary 5.8).** Let \( p\mathcal{O} = P \cap \mathcal{O} \). Then \( p^{\frac{h(\mathcal{O})}{4}} \mathcal{O} \) is a principal ideal in \( \mathcal{O} \), and

\[
\varepsilon = \begin{cases}
1 & \text{if } p^{\frac{h(\mathcal{O})}{4}} \mathcal{O} \text{ is principal}, \\
-1 & \text{if } p^{\frac{h(\mathcal{O})}{4}} \mathcal{O} \text{ is not principal}.
\end{cases}
\]

Theorems above suggest that the sign ambiguity problem can be interpreted into a class field theoretic problem. This idea can be clarified by a theorem of Deligne on the special values of \( \Gamma \)-functions. Given a multiplicative relation (5), it is known that the product of some special values of the \( \Gamma \)-function

\[
\tilde{G}_m(\alpha) = (2\pi i)^{-s/2} \prod_{a=1}^{m-1} \Gamma \left( \frac{a}{m} \right)^{\varepsilon_a}
\]
generates a finite abelian extension of $K_m$ ([12], [6]), and Deligne [6] showed that
\[
\left( \frac{K_m^{ab}}{K_m} \right)^P \tilde{\Gamma}_m(\alpha) = \varepsilon_{\alpha} \tilde{\Gamma}_m(\alpha),
\]
where $K_m^{ab}$ denotes the maximal abelian extension of $K_m$, $\left( \frac{K_m^{ab}}{K_m} \right)^P$ denotes the Artin symbol and $\varepsilon_{\alpha} = \varepsilon_{\alpha}(P)$ is the root of unity $\varepsilon$ appeared in (5). Thus the map sending $P$ to $\varepsilon_{\alpha}(P)$ defines an algebraic Hecke character of $K_m$ corresponding to the abelian extension $K_m(\tilde{\Gamma}_m(\alpha))/K_m$. Note that we can compute $\tilde{\Gamma}_m(\alpha)$ explicitly using Euler’s reflection formula (22) and Gauss’ multiplication formula (23), and so we can determine the abelian extension explicitly. The result of the computation in the case of Theorem 1.2 will be given in the final section.

2. Multiplicative relations between Gauss sums

In order to study multiplicative relations between Gauss sums in a systematic way, we consider a free abelian group $R_m$ generated by the elements of $\mathbb{Z}/m\mathbb{Z} - \{0\}$. Thus an element of $R_m$ can be written as a formal sum
\[
\sum_{a \in \mathbb{Z}/m\mathbb{Z} - \{0\}} c_a [a],
\]
where $c_a \in \mathbb{Z}$. For any $a_1, \ldots, a_r \in \mathbb{Z}/m\mathbb{Z} - \{0\}$, we set
\[
[a_1, \ldots, a_r] = [a_1] + \cdots + [a_r].
\]
For example, $[1, 1, 2, 2, 2] = 2[1] + 3[2]$. Let $G_m = (\mathbb{Z}/m\mathbb{Z})^\times$. Then we can naturally regard $R_m$ as a $G_m$-module by setting
\[
t \cdot \sum_{a} c_a [a] = \sum_{a} c_a [ta]
\]
for any $t \in G_m$.

For any $\alpha = \sum_a c_a [a] \in R_m$, we define $\tau(\alpha)$ to be the product of Gauss sums
\[
\tau(\alpha) = \prod_{a \in \mathbb{Z}/m\mathbb{Z} - \{0\}} \tau(a)^{c_a}.
\]
Since $\tau(a) = -1$ if $a \equiv 0 \pmod{m}$ and $|\tau(a)| = \sqrt{p}$ otherwise, it follows that $|\tau(\alpha)| = \sqrt{p}^{s(\alpha)}$, where $s(\alpha)$ is an integer defined by
\[
s(\alpha) = \sum_{a \in \mathbb{Z}/m\mathbb{Z} - \{0\}} c_a.
\]
A multiplicative relation between Gauss sums is by definition a formula of the form
\[
\tau(\alpha) = \varepsilon p^{\frac{1}{2} s(\alpha)}
\]
where $\varepsilon$ is a root of unity.
Note that \( \tau(\alpha) \) a priori belongs to \( \mathbb{Q}(\zeta_{mp}) \) and need not belong to \( K_m \). In order to determine when \( \tau(\alpha) \) belongs to \( K_m \), we consider a submodule \( A_m \) of \( R_m \) defined by

\[
A_m = \left\{ \sum_{a \in \mathbb{Z}/m\mathbb{Z} - \{0\}} c_a[a] \in R_m \mid \sum_{a \in \mathbb{Z}/m\mathbb{Z} - \{0\}} c_a a = 0 \right\}.
\]

For example, \([a, -a] \in A_m\) for any \( a \in \mathbb{Z}/m\mathbb{Z} - \{0\} \), and \([1, 1, m - 2] \in A_m\) if \( m > 2 \). We set \( A_1 = \emptyset \) for convenience.

**Proposition 2.1.** We have \( \tau(\alpha) \in K_m \) for any \( \alpha \in A_m \).

To prove this, we recall some basic properties of Gauss sums. For any \( t \in (\mathbb{Z}/mp\mathbb{Z})^\times \), let \( \sigma_t \in \text{Gal}(\mathbb{Q}(\zeta_{mp})/\mathbb{Q}) \) denote the element defined by \( \sigma_t(\zeta_{mp}) = \zeta_{tmp} \).

**Lemma 2.2.** Suppose \( a \not\equiv 0 \) (mod \( m \)). Then

\[
\sigma_t(\tau(a)) = \chi(t)^{-at} \tau(ta)
\]

for any \( t \in (\mathbb{Z}/mp\mathbb{Z})^\times \). In particular \( \tau(a) = \chi(-1)^a \tau(-a) \).

**Proof.** Since \( \sigma_t(\chi(x)) = \chi(x)^t \) and \( \sigma_t(\zeta_p) = \zeta_p^t \), it follows that

\[
\sigma_t(\tau(a)) = \sum_{x \in \mathbb{F}_p^\times} \chi(x)^{at} \zeta_{tp}^x
\]

\[
= \sum_{x \in \mathbb{F}_p^\times} \chi(t^{-1}x)^{at} \zeta_{tp}^x
\]

\[
= \chi(t)^{-at} \sum_{x \in \mathbb{F}_p^\times} \chi(x)^{at} \zeta_{tp}^x
\]

\[
= \chi(t)^{-at} \tau(ta).
\]

The last statement immediately follows from this since \( \sigma_{-1} \) is the complex conjugate. This proves the lemma. \( \square \)

**Proof of Proposition 2.1.** Suppose \( t \equiv 1 \) (mod \( m \)). Then

\[
\sigma_t(\tau(\alpha)) = \chi(t)^{-at} \tau(ta)
\]

for any \( a \in \mathbb{Z}/m\mathbb{Z} \). Hence, if \( \alpha = \sum_a c_a[a] \in A_m \), then Lemma 2.2 shows that

\[
\sigma_t(\tau(\alpha)) = \chi(t)^{-a} \sum_a c_a \tau(\alpha) = \tau(\alpha)
\]

for any \( t \in (\mathbb{Z}/mp\mathbb{Z})^\times \) with \( t \equiv 1 \) (mod \( m \)). This proves that \( \tau(\alpha) \in \mathbb{Q}(\zeta_m) \). \( \square \)

Now, let \( \Gamma_m = \text{Gal}(K_m/\mathbb{Q}) \) and define the Stickelberger element \( \theta(\alpha) \) to be

\[
\theta(\alpha) = \sum_{t \in \Gamma_m} \left( \frac{at}{m} \right) \sigma_t^{-1} \in \mathbb{Q}[\Gamma_m],
\]

where \( \left( \frac{a}{m} \right) \) denotes the unique rational number such that \( 0 < \left( \frac{a}{m} \right) < 1 \), \( m \left( \frac{a}{m} \right) \in \mathbb{Z} \) and \( m \left( \frac{a}{m} \right) \equiv a \) (mod \( m \)).
For any $\alpha = \sum_a c_a[a] \in R_m$, let

$$\theta(\alpha) = \sum_{a \in \mathbb{Z}/m\mathbb{Z} - \{0\}} c_a \theta(a).$$

**Proposition 2.3.** Notation being as above, we have $\theta(\alpha) \in \mathbb{Z}[\Gamma_m]$ if and only if $\alpha \in A_m$.

**Proof.** If $\alpha = \sum_a c_a[a] \in R_m$, then

$$\theta(\alpha) = \sum_{a \in \mathbb{Z}/m\mathbb{Z} - \{0\}} c_a \theta(a) = \sum_{t \in G_m} \left( \sum_{a \in \mathbb{Z}/m\mathbb{Z} - \{0\}} c_a \left\lfloor \frac{ta}{m} \right\rfloor \right) \sigma_t^{-1}. \quad (10)$$

Since

$$\sum_{a \in \mathbb{Z}/m\mathbb{Z} - \{0\}} c_a \left\lfloor \frac{ta}{m} \right\rfloor \equiv \frac{1}{m} \sum_{a \in \mathbb{Z}/m\mathbb{Z} - \{0\}} c_a a \pmod{\mathbb{Z}},$$

it follows from (10) that $\theta(\alpha) \in \mathbb{Z}[\Gamma_m]$ if and only if $\alpha \in A_m$. This proves the proposition. \qed

Define a group homomorphism $\tilde{\theta} : R_m \rightarrow \mathbb{Q}[\Gamma_m]$ by

$$\tilde{\theta}(\alpha) = \theta(\alpha) - \frac{1}{2} s(\alpha) \nu$$

for any $\alpha \in R_m$, where

$$\nu = \sum_{\sigma \in \Gamma_m} \sigma \in \mathbb{Z}[\Gamma_m]$$

denotes the norm element. If $m > 1$, we define a subset $B_m$ of $A_m$ by

$$B_m = \{ \alpha \in A_m \mid \tilde{\theta}(\alpha) = 0 \}$$

$$= \left\{ \sum_{a \in \mathbb{Z}/m\mathbb{Z} - \{0\}} c_a[a] \in A_m \mid \sum_{a \in \mathbb{Z}/m\mathbb{Z} - \{0\}} c_a \left( \left\lfloor \frac{ta}{m} \right\rfloor - \frac{1}{2} \right) = 0 \ (\forall t \in G_m) \right\}.$$ 

We set $B_1 = \emptyset$ for convenience.

**Proposition 2.4.** Let $\alpha \in A_m$ and put $s = s(\alpha)$. Then $\tau(\alpha) = \varepsilon p^{s/2}$ for some root of unity $\varepsilon$ if and only if $\alpha \in B_m$.

Although this is a well-known fact (for example, see [19]), we give a proof for the sake of the reader. For this purpose, we recall Stickelberger’s theorem on the prime factorization of the ideal $\tau(a)^m \mathcal{O}_{K_m}$, where $\mathcal{O}_{K_m}$ denotes the integer ring of $K_m$.

**Theorem 2.5.** For any $a \in \mathbb{Z}/m\mathbb{Z} - \{0\}$, $\tau(a)^m$ belongs to $K_m$, and the prime ideal decomposition of the principal fractional ideal $\tau(a)^m \mathcal{O}_{K_m}$ is given by $\tau(a)^m \mathcal{O}_{K_m} = \mathcal{P}^{\theta(a)}$, where $\mathcal{P}$ denotes a prime ideal.

**Proof.** See [10] or [4]. \qed

**Corollary 2.6.** If $\alpha \in A_m$, then $\tau(\alpha) \in \mathcal{O}_{K_m}$ and $\tau(\alpha) \mathcal{O}_{K_m} = \mathcal{P}^{\theta(\alpha)}$. 

Proof. Since $\tau(\alpha)$ is always an algebraic integer, the first statement immediately follows from Proposition 2.1. The second statement then follows from Theorem 2.5. \qed

Proof of Proposition 2.4. Suppose $\tau(\alpha) = \varepsilon p^s$ for some root of unity $\varepsilon$. Then the ideal $\tau(\alpha)\mathcal{O}_{K_m}$ is invariant under the Galois action. On the other hand, we have

$$\sigma_\alpha(\mathcal{O}_{K_m}) = \mathcal{O}_{K_m}$$

for any $t \in G_m$. It follows that $\theta(t \cdot \alpha) = s\nu$ for any $t \in G_m$ by Corollary 2.6, hence $\alpha \in B_m$.

Conversely, suppose that $\alpha \in B_m$. Then $\tau(\alpha)\mathcal{O}_{K_m} = p^s\mathcal{O}_{K_m}$ by Corollary 2.6 again. It follows that $\sigma(\tau(\alpha)) = \varepsilon p^s$ for some unit $\varepsilon$ in $\mathcal{O}_{K_m}$. Moreover we have $|\sigma(\tau(\alpha))| = |\sigma(\varepsilon)|p^s$ for any $\sigma \in \Gamma_m$. Since $|\sigma(\tau(\alpha))| = p^s$ for any $\sigma \in \Gamma_m$, it follows that $|\sigma(\varepsilon)| = 1$ for any $\sigma \in \Gamma_m$. But, this holds only when $\varepsilon$ is a root of unity. This completes the proof. \qed

We define $D_m$ to be the subgroup of $R_m$ generated by the elements of the form $[a, -a]$ with $a \in \mathbb{Z}/m\mathbb{Z} - \{0\}$. Although it is clear from the formula (2) that $B_m$ contains $D_m$, the following proposition gives an explicit expression of $\tau(\alpha)$ for any $\alpha \in D_m$.

PROPOSITION 2.7. Let $a_1, \ldots, a_s \in \mathbb{Z}/m\mathbb{Z} - \{0\}$. Then

$$\tau([a_1, -a_1, \ldots, a_s, -a_s]) = \chi(-1)^{a_1+a_2+\cdots+a_s} p^s.$$

In particular, if either $m$ is odd or $[a_1, \ldots, a_s] \in A_m$, then $\tau([a_1, -a_1, \ldots, a_s, -a_s]) = p^s$.

Proof. This is an immediate consequence of (2). \qed

It is known that $B_m = D_m$ if and only if $m$ is either a prime or $m = 4$ (see [1]), and in the other cases there are another type of elements in $B_m$ corresponding to the Hasse-Davenport relation. To describe them, for any prime factor $l$ of $m$, we define

$$\gamma_l,a = \begin{cases} [a, a + d, a + 2d, \ldots, a + (l - 1)d, -la] & \text{(if $l$ is an odd prime)}, \\ [a, a + d, -2a, d] & \text{(if $l = 2$)} \end{cases}$$

where $d = m/l$ and $a$ is an element of $\mathbb{Z}/m\mathbb{Z}$ such that $la \neq 0$. Then it can be easily verified that $\gamma_l,a \in B_m$, hence $\gamma_l,a$ gives an multiplicative relation between Gauss sums. More precisely we have the following proposition.

PROPOSITION 2.8. If $l$ is a prime factor of $m$, then

$$\tau(\gamma_l,a) = \chi(l)^{-al} p^s$$

for any $a \in \mathbb{Z}/m\mathbb{Z}$ with $al \neq 0$, where

$$s = s(\gamma_l,a) = \begin{cases} l + 1 & \text{($l > 2$)}, \\ 4 & \text{($l = 2$)} \end{cases}.$$

Proof. Let $d = m/l$. First we consider the case where $l$ is an odd prime. From the Davenport-Hasse relation, we obtain

$$\prod_{k=0}^{l-1} \tau(a + kd) = \chi(l)^{-al} \tau(al) \prod_{k=1}^{l-1} \tau(ak).$$
It follows that

$$\tau(\gamma_l,a) = \tau(-al) \prod_{k=0}^{l-1} \tau(a + kd)$$

$$= \chi(l)^{-al} \tau(-al) \tau(al) \prod_{k=0}^{l-1} \tau(kd).$$

If \( m \) is odd, then \( \chi(-1) = 1 \). If \( m \) is even and \( l \neq 2 \), then \( \chi(-1)^l = 1 \). Therefore, \( \chi(-1)^l = 1 \) in both cases. Thus, by (2) we have

$$\tau(al)\tau(-al) = \chi(-1)^{al}p = p.$$ 

Similarly we have \( \chi(-1)^{al} = 1 \), so

$$\tau(kd)\tau(-kd) = \chi(-1)^{kd}p = p$$

for any \( k = 0, 1, \ldots, l - 1 \) by (2). Therefore

$$\prod_{k=1}^{l-1} \tau(kd) = \prod_{k=1}^{(l-1)/2} \tau(kd) \tau(-kd) = p^{(l-1)/2}.$$ 

Consequently we obtain

$$\tau(\gamma_l,a) = \chi(l)^{-al} \cdot p \cdot p^{(l-1)/2} = \chi(l)^{-al} p^{(l+1)/2}.$$ 

Next we consider the case \( l = 2 \). Applying the Davenport-Hasse relation again, we obtain

$$\tau(a)\tau(a + d) = \chi(2)^{-2a} \tau(2a)\tau(d).$$

Therefore

$$\tau(\gamma_2,a) = \tau(a)\tau(a + d) \tau(-2a)\tau(d)$$

$$= \chi(2)^{-2a} \tau(2a)\tau(-2a)\tau(d)^2$$

$$= \chi(2)^{-2a} \cdot \chi(-1)^{2a} p \cdot p$$

$$= \chi(2)^{-2a} p^2.$$ 

This proves the proposition. \( \square \)

Let \( S_m \) be the subgroup of \( R_m \) generated by \( D_m \) and the elements of the form (11). Then \( S_m \) is a subgroup of \( B_m \). Hasse’s conjecture mentioned in the introduction says that \( B_m = S_m \), which means that (2) and (3) are essentially the only multiplicative relations between Gauss sums. In [20] Yamamoto determined the structure of the quotient group \( B_m/S_m \), which is called the ‘gap group’.

**Theorem 2.9.** If \( m \geq 3 \), then

$$B_m/S_m \cong (\mathbb{Z}/2\mathbb{Z})^{2^{r-1}-1},$$

where \( r \) is the number of distinct prime factor of \( m \) (resp. \( m/2 \)) if \( m \not\equiv 2 \pmod{4} \) (resp. if \( m \equiv 2 \pmod{4} \)).

**Proof.** See [20, Theorem 17]. \( \square \)
Yamamoto’s theorem says that $2\alpha \in S_m$ for any $\alpha \in B_m$. Thus, using the multiplicative relations (2) and (3), we can determine $\tau(\alpha)^2$ explicitly for any $\alpha \in B_m$, and consequently we can determine $\tau(\alpha)$ up to sign.

**Remark 2.10.** Strictly speaking, Theorem 2.9 is not identical with what Yamamoto proved in [20]. To be more precise, define $B'_m$ by

$$B'_m = \begin{cases} B_m & \text{(if } m \text{ is odd)}, \\ B_m + \mathbb{Z}[m/2] & \text{(if } m \text{ is even)}. \end{cases}$$

It is then not hard to see that

$$B'_m = \{ \alpha \in R_m \mid \tilde{\theta}(\alpha) = 0 \}.$$ 

Moreover define $S'_m$ by

$$S'_m = \begin{cases} S_m & \text{(if } m \text{ is odd)}, \\ S_m + \mathbb{Z}[m/2] & \text{(if } m \text{ is even)}. \end{cases}$$

Yamamoto proved that $B'_m/S'_m \cong (\mathbb{Z}/2\mathbb{Z})^{2^r-1}$. However, since $S'_m \cap B_m = S_m$, the inclusion map $B_m \hookrightarrow B'_m$ induces an isomorphism $B_m/S_m \cong B'_m/S'_m$.

and so Theorem 2.9 holds.

**Corollary 2.11.**

(i) $B_m = S_m$ if and only if either $m = l^r$ with $l$ a prime or $m = 2l^r$ with $l$ an odd prime.

(ii) $B_m/S_m \cong \mathbb{Z}/2\mathbb{Z}$ if and only if either $m = l_1^r l_2^s$ with $l_1, l_2$ distinct primes or $m = 2l_1^r l_2^s$ with $l_1, l_2$ distinct odd primes.

**Example 2.12.** If $m = 12$, then $B_{12}/S_{12} \cong \mathbb{Z}/2\mathbb{Z}$ is generated by $\alpha = [1, 6, 8, 9]$, and

$$2\alpha = [1, 1, 6, 6, 8, 8, 9, 9]$$

$$= [1, 5, 9, 9] + [1, 7, 10, 6] + [2, 8, 8, 6] - [2, 10, 5, 7]$$

$$= \gamma_{3,1} + \gamma_{2,1} + \gamma_{2,2} - [2, -2] - [5, -5].$$

Yamamoto computed the product $\tau(\alpha)$ for $\alpha = [2, 5, 8, 9]$, which is connected with the element $[1, 6, 8, 9]$ by

$$[1, 6, 8, 9] + [2, -2] + [5, -5] = [2, 5, 8, 9] + \gamma_{2,1}.$$ 

Therefore

$$[2, 5, 8, 9] \equiv [1, 6, 8, 9] \pmod{S_{12}}.$$

**Example 2.13.** If $m = 15$, then $B_{15}/S_{15} \cong \mathbb{Z}/2\mathbb{Z}$ is generated by $\alpha = [1, 7, 10, 12]$, and

$$2\alpha = [1, 1, 7, 7, 10, 10, 12, 12]$$

$$= [1, 4, 7, 10, 13, 12] + [1, 6, 11, 12] + [2, 7, 12, 9] - [2, 13, 6, 9]$$

$$= \gamma_{5,1} + \gamma_{3,1} + \gamma_{3,2} - [2, -2] - [6, -6].$$
3. A characterization of $B_m$

Let $\psi$ be a Dirichlet character modulo $m$, namely $\psi$ is a multiplicative function on $(\mathbb{Z}/m\mathbb{Z})^\times$ with $\psi(1) = 1$. The conductor of $\psi$ is defined to be the minimal positive divisor $f$ of $m$ such that $\psi$ is a pull-back of a Dirichlet character modulo $f$ by the natural surjection $(\mathbb{Z}/m\mathbb{Z})^\times \rightarrow (\mathbb{Z}/f\mathbb{Z})^\times$. If the conductor of $\psi$ is $m$, $\psi$ is called a primitive character. As usual, we regard $\psi$ as a multiplicative function on $\mathbb{Z}$ by setting

$$\psi(a) = \begin{cases} \psi(a \mod f) & \text{(if } (a, f) = 1), \\ 0 & \text{(if } (a, f) > 1). \end{cases}$$

We say that $\psi$ is odd (resp. even) if $\psi(-1) = -1$ (resp. $\psi(-1) = 1$). Let $PC^-(m)$ be the set of primitive odd character of conductor $m$.

For a primitive character $\psi$ mod $d$ we define the 1-st generalized Bernoulli number by

$$B_{1,\psi} = \frac{1}{d\psi} \sum_{0 < u < d\psi} u\psi(u),$$

where $d\psi$ is the conductor of $\psi$. Then the following lemma is well known.

**Lemma 3.1.** Let $\psi_0$ be the trivial character of $G$.

(i) If $\psi = \psi_0$ then

$$\theta e_{\psi_0} = \frac{1}{2} \nu_G,$$

where $\nu_G = \sum_{t \in G} \sigma_t$ is the norm element.

(ii) If $\psi$ is even and $\psi \neq \psi_0$ then $\theta e_{\psi_0} = 0$.

(iii) If $\psi$ is odd then

$$\theta e_{\psi_0} = \left( B_{1,\psi} \prod_{l \mid m/d\psi} (1 - \overline{\psi(l)}) \right) e_{\psi},$$

where $d\psi$ is the conductor of $\psi$.

**Proposition 3.2.** For any divisor $d$ of $m$ and for any $\psi \in PC^-(m/d)$, we have

$$\psi(\tilde{\theta}(a)) = \frac{\varphi(m)}{\varphi(m/(a,d))} \psi \left( \frac{a}{(a,d)} \right) B_{1,\psi} \prod_{l \mid d/(a,d) \mid m/d} (1 - \overline{\psi(l)}).$$

**Proof.** For a proof see [13].

In order to obtain a simpler expression of the formula in Proposition 3.2, we introduce a ring structure into the module $R_m$ as follows: For any $a, b \in \mathbb{Z}/m\mathbb{Z}$, we define the product of two elements $[a], [b] \in R_m$ by

$$[a][b] = \begin{cases} [ab] & \text{(if } ab \neq 0), \\ 0 & \text{(if } ab = 0). \end{cases}$$

Moreover, extending this definition $\mathbb{Z}$-linearly, we define a product of two elements of $R_m$. For example, if $a_1, \ldots, a_s, b_1, \ldots, b_t \in \mathbb{Z}/m\mathbb{Z}$, then

$$[a_1, \ldots, a_s][b_1, \ldots, b_t] = [a_1b_1, \ldots, a_1b_t, \ldots, a_s b_1, \ldots, a_s b_t].$$
It is then easy to see that this defines a ring structure on $R_m$.

Now, for any divisor $d$ of $m$, we define an element $T_d(a) \in R_{m/d}$ by

$$T_d(a) = \begin{cases} \frac{\psi(m)}{\psi(m/d)} \left[ \frac{a}{(a, d)} \right] \prod_{l|d/(a, d)} \left[ 1, -l' \right] \left( \frac{m}{d} \left( \frac{a}{(a, d)} \right) \right), & \text{if } \frac{m}{d} \equiv \frac{a}{(a, d)} \mod 1, \\ 0, & \text{otherwise}. \end{cases}$$

where $l$ runs over the prime divisors of $d/(a, d)$ not dividing $m/d$ and $l'$ is an integer such that

$$l' \equiv 1 \mod m/d.$$ 

Extending this $\mathbb{Z}$-linearly to $R_m$, we obtain a group homomorphism $T_d : R_m \rightarrow R_{m/d}$; if $a = \sum c_{a} \alpha \in R_m$ then

$$T_d(a) = \sum_{\alpha} c_{\alpha} T_d(a).$$

PROPOSITION 3.3. For any $\psi \in PC^-(m/d)$, we have

$$\psi(\tilde{\theta}(a)) = \psi(T_d(a)) B_{1, \psi}.$$

Proof. This is a restatement of Proposition 3.2. □

COROLLARY 3.4. Notation being as above, we have

$$B_m = \{ \alpha \in A_m \mid \psi(T_d(\alpha)) = 0 (\forall d \mid m, \forall \psi \in PC^-(m/d)) \}.$$

Proof. This follows from Proposition 3.3 since $B_{1, \psi} \neq 0$ for any primitive odd character $\psi$. □

The following proposition shows that the map $T_d$ is a natural one.

PROPOSITION 3.5. If $d_1 d_2 \mid m$, then $T_{d_2} \circ T_{d_1} = T_{d_1 d_2}$.

Proof. This is essentially proved in [2], we give a proof for the sake of the reader. Let $a \in \mathbb{Z}/m \mathbb{Z} - \{0\}$. Then

$$T_{d_2}(T_{d_1}(a)) = T_{d_2} \left( \frac{\psi(m)}{\psi(m/d_1)} \left[ \frac{a}{(a, d_1)} \right] \prod_{l|d_1/(a, d_1)} \left[ 1, -l' \right] \left( \frac{m}{d_1} \left( \frac{a}{(a, d_1)} \right) \right) \right)$$

$$= \frac{\psi(m)}{\psi(m/(a, d_1))} \left( \prod_{l|d_1/(a, d_1)} \left[ 1, -l' \right] \right) T_{d_2} \left( \frac{a}{(a, d_1)} \right)$$

$$= \frac{\psi(m)}{\psi(m/(a, d_1))} \left( \prod_{l|d_1/(a, d_1)} \left[ 1, -l' \right] \right) T_{d_2} \left( \frac{m}{d_1} \left( \frac{a}{(a, d_1)}, d_2 \right) \right)$$

$$= \frac{\psi(m)}{\psi(m/(a, d_1))} \left( \prod_{l|d_2/(a, d_1), d_2} \left[ 1, -l' \right] \right) \frac{a}{(a, d_1 d_2)}.$$
\[
\frac{1}{\varphi(m)} \varphi\left(\frac{m}{(a, d_1, d_2)}\right) \prod_{\substack{(d_1, d_2) \mid (m, d_1, d_2) \setminus \{1, \ldots, \ell'\}}} [1, -l'] = T_{d_1, d_2}(a).
\]

This proves Proposition 3.5.

**PROPOSITION 3.6.** The submodule \(B_m\) of \(R_m\) is characterized as follows:

\[
B_m = \left\{ \alpha \in R_m \mid \begin{array}{l}
\psi(\alpha) = 0 \ (\forall \psi \in PC^{-}(m)), \\
T_d(\alpha) \in B_{m/d} \ (\forall d \mid m, \ d > 1)
\end{array} \right\}.
\]

*Proof.* Note that for any \(\alpha \in R_m\) the following equivalences hold by Corollary 3.4:

\[
\alpha \in B_m \iff \begin{array}{l}
\psi(\alpha) = 0 \ (\forall \psi \in PC^{-}(m)), \\
T_d(\alpha) \in B_{m/d} \ (\forall d \mid m, \ d > 1, \ \forall \psi \in PC^{-}(m/d)).
\end{array}
\]

The second condition of the right hand side holds if and only if the condition

\[
\psi(T_e(\alpha)) = 0 \ (\forall e \mid m \text{ and } \forall \psi \in PC^{-}(m/e)) \quad (12)
\]

holds for any \(d\) with \(1 < d \mid m\). If we put \(e = dd'\) and \(\beta_d = T_d(\alpha)\), then \(T_e(\alpha) = T_{d'}(\beta_d)\) by Proposition 3.5. Hence the condition (12) is equivalent to

\[
\psi(T_{d'}(\beta_d)) = 0 \ (\forall \psi \in PC^{-}(m/dd')).
\]

But this holds if and only if \(\beta_d \in B_{m/d}\) by Corollary 3.4 again. Therefore

\[
\alpha \in B_m \iff \begin{array}{l}
\psi(\alpha) = 0 \ (\forall \psi \in PC^{-}(m)), \\
T_d(\alpha) \in B_{m/d} \ (\forall d \mid m, \ d > 1)
\end{array}.
\]

This proves the proposition.

\[\square\]

4. **A generator of \(B_m/S_m\) when \(r = 2\)**

In what follows, we always assume that \(m = l_1l_2\) is a product of distinct odd prime numbers \(l_1, l_2\) satisfying

\[l_1 \equiv l_2 \equiv 3 \pmod{4}.
\]

By symmetry, we may assume that

\[
\begin{pmatrix}
l_1 \\
l_2
\end{pmatrix} = 1.
\]

Let \(G = (\mathbb{Z}/m\mathbb{Z})^\times\) and define subgroups \(G_1, G_2, H_1, H_2, H\) of \(G\) as follows:

\[
G_1 = \{ t \in G \mid t \equiv 1 \pmod{l_2} \},
\]

\[
G_2 = \{ t \in G \mid t \equiv 1 \pmod{l_1} \},
\]

\[
H_1 = \{ t^2 \mid t \in G_1 \},
\]

\[
H_2 = \{ t^2 \mid t \in G_2 \},
\]

\[
H = H_1H_2.
\]
Then $G_i \cong (\mathbb{Z}/l_i \mathbb{Z})^\times$ for $i = 1, 2$ and $G = G_1 G_2$. Moreover we have $G/H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We identify $G$ with the Galois group $\text{Gal}(K_m/\mathbb{Q})$ in the usual way. Let $K_i = \mathbb{Q}(\zeta_{l_i})$. Then $\text{Gal}(K_m/K_{l_2}) = H_1$ and $\text{Gal}(K_m/K_{l_2}) = H_2$.

Now, let

$$
\eta_i = \sum_{t \in H_i} [t] \in R_{l_i},
$$

$$
\eta = \eta_1 \eta_2 = \sum_{t \in H} [t] \in R_m.
$$

It is clear from the definition that

$$
[t] \eta_1 = \eta_1 (\forall t \in H_1),
$$

$$
[t] \eta = \eta (\forall t \in H).
$$

**PROPOSITION 4.1.** Let

$$
\alpha = \eta + [-l_2] \eta_1 \in R_m.
$$

Then $\alpha$ is a generator of the gap group $B_m/S_m$, and satisfies

$$
2\alpha = \gamma_2 \eta_1 + [l_1, -l_1] \eta_2 - \eta.
$$

Proof. Let $\psi \in PC^{-}(m)$. Then $\psi \neq \left( \frac{m}{l} \right)$ since $\left( \frac{m}{l} \right)$ is an even character. It follows that $\psi(\alpha) = 0$. Thus, in order to prove that $\alpha \in B_m$, it suffices to show that $T_{l_1}(\alpha) \in B_{l_2}$ and $T_{l_2}(\alpha) \in B_{l_1}$.

First, we have

$$
T_{l_1}(\alpha) = \frac{l_1 - 1}{2} [1, -l_1^\prime] \eta_2.
$$

Since $(-l_1/l_2) = 1$, we have $[-l_1] \eta_2 = [-1] \eta_2$, hence (15) can be rewritten as

$$
T_{l_1}(\alpha) = \frac{l_1 - 1}{2} [1, -1] \eta_2,
$$

which shows that $T_{l_1}(\alpha) \in D_{l_2}$. Next, we have

$$
T_{l_2}(\alpha) = \left( \frac{l_2 - 1}{2} [1, -l_2^\prime] + (l_2 - 1) [-1] \right) \eta_1
$$

$$
= (l_2 - 1) [1, -1] \eta_1,
$$

which shows that $T_{l_2}(\alpha) \in D_{l_1}$. Hence $\alpha \in B_m$.

In order to obtain the formula (14), we prove the following lemma.

**LEMMA 4.2.** Let $u$ be the element of $\mathbb{Z}/m\mathbb{Z}$ such that

$$
u \equiv \left\{ \begin{array}{ll} 1 & (\text{mod } l_1), \\
-1 & (\text{mod } l_2). \end{array} \right.$$

Then the following formulas hold.

(i) $[1, u] \alpha = \gamma_{l_2} \eta_1$.

(ii) $[1, -u] \alpha = \gamma_1 \eta_2 - [l_1, -l_1] \eta_2 + [l_2, -l_2] \eta_1$.

(iii) $[u, -u] \alpha = [u, -u] \eta + [l_2, -l_2] \eta_1$. 

Using the identity
\[ 2[1] = [1, u] + [1, -u] - [u, -u], \]
we have
\[ 2\alpha = 2[1]\alpha \]
\[ = [1, u]\alpha + [1, -u]\alpha - [u, -u]\alpha \]
\[ = [1, u]\eta_1\eta_2 + [1, u][-l_2]\eta_1 + [1, -u]\eta_1\eta_2 + [1, -u][-l_2]\eta_1 - [u, -u]\alpha. \]

Define \( \tilde{l}_2 \in \mathbb{Z}/m\mathbb{Z} \) by
\[ \tilde{l}_2 \equiv \begin{cases} 1 \pmod{l_1}, \\ 0 \pmod{l_2}. \end{cases} \]
Then, since \([1, u]\eta_2 = \gamma_2 - \tilde{l}_2, -l_2\), it follows that
\[ [1, u]\eta_1\eta_2 = ([\gamma_2 - \tilde{l}_2, -l_2])\eta_1 \]
\[ = \gamma_2\eta_1 - [l_2, -l_2]\eta_1 \]
\[ = \gamma_2\eta_1 - 2[-l_2]\eta_1. \]
Moreover, we have \([1, u][-l_2]\eta_1 = 2[-l_2]\eta_1\), and so
\[ [1, u]\alpha = \gamma_2\eta_1. \]

On the other hand, if we define \( \tilde{l}_1 \in \mathbb{Z}/m\mathbb{Z} \) by
\[ \tilde{l}_1 \equiv \begin{cases} 0 \pmod{l_1}, \\ 1 \pmod{l_2}, \end{cases} \]
then \([1, -u]\eta_1 = \gamma_1 - [\tilde{l}_1, -l_1]\), hence
\[ [1, -u]\eta_1\eta_2 = \gamma_1\eta_2 - [l_1, -l_1]\eta_2 \]
\[ = \gamma_1\eta_2 - [l_1, -l_1]\eta_2. \]
Here the last equality holds since \([l_1]\eta_2 = [l_1]\eta_2\). Moreover,
\[ [1, -u][-l_2]\eta_1 = [1, -1][-l_2]\eta_1 = [l_2, -l_2]\eta_1, \]
which belongs to \( D_m \). Therefore
\[ [1, -u]\alpha = \gamma_1\eta_2 - [l_1, -l_1]\eta_2 + [l_2, -l_2]\eta_1, \]
which proves the lemma. \( \square \)

Now, we return to the proof of Proposition 4.1. From Lemma 4.2 we obtain
\[ 2\alpha = \gamma_2\eta_1 + \gamma_1\eta_2 - [l_1, -l_1]\eta_2 - [u, -u]\eta, \]
which proves (14).

It remains to show that \( \alpha \) generates the quotient group \( B_m/S_m \), or equivalently \( \alpha \not\in S_m \).
To see this, define an integer valued function \( s_1 \) on \( R_m \) by
\[ s_1(\beta) = \sum_{b \in (\mathbb{Z}/m\mathbb{Z})^\times} cb \]
for any $\beta = \sum b \chi(b) \in \mathbb{R}_m$. Recall that $S_m$ is generated by the elements of the form $\gamma_{l_1,\alpha}$, $\gamma_{l_2,\beta}$ and $[c,-c]$, and all of them have even $s_1$, hence $s_1(S_m) = 2\mathbb{Z}$. But, since $l_1 \equiv l_2 \equiv 3 \pmod{4}$, it follows that $s_1(\alpha) = s_1(\eta) \equiv 1 \pmod{2}$. This proves that $\alpha \not\in S_m$ as desired. The proof of Proposition 4.1 is now complete.

**Example 4.3.** If $m = 21$, then $B_{21}/S_{21} \cong \mathbb{Z}/2\mathbb{Z}$ is generated by $\alpha = [1, 4, 9, 15, 16, 18]$, and

$$2\alpha = [1, 1, 4, 4, 9, 9, 15, 15, 16, 16, 18, 18] = \gamma_{3,1} + \gamma_{3,2} + \gamma_{3,4} + \gamma_{7,1} \equiv [7, -7] - [8, -8] - [5, -5] - [10, -10].$$

**Example 4.4.** If $m = 77 = 7 \cdot 11$ ($l_1 = 11, l_2 = 7$), then $B_{77}/S_{77}$ is generated by $\alpha = [1, 4, 16, 25, 23, 15, 60, 9, 36, 67, 37, 71, 53, 58] + [-7][1, 8, 2, 7, 6]$, and

$$2\alpha = \gamma_{11} \eta_1 + \gamma_{7} \eta_2 - [11, -11] \eta_2 - [34, -34] \eta.$$

**Proposition 4.5.** Let $\alpha$ be as in Proposition 4.1. Then

$$\tau(\alpha) = \begin{cases} \pm p^{\frac{l_1 - 1}{2}} \cdot \frac{l_2 + 1}{2} & \text{if } l_1 \not\equiv 3 \text{ and } l_2 \not\equiv 3, \\ \pm \chi(l_1)^{l_1} p^{\frac{l_1 - 1}{2}} & \text{if } l_2 = 3, \\ \pm \chi(l_2)^{l_2} p^{\frac{l_2 - 1}{2}} & \text{if } l_1 = 3. \end{cases}$$

**Proof.** It follows from Proposition 4.1 that

$$\tau(\alpha)^2 = \frac{\tau(\gamma_{l_1,\eta_1}) \tau(\gamma_{l_2,\eta_2})}{\tau([l_1, -l_1]\eta_2) \tau([u, -u] \eta)}.$$

As for the numerator of the right hand side, Proposition 2.8 shows that

$$\tau(\gamma_{l_1,\eta_2}) = \left( \prod_{t \in H_2} \chi(t)_{l_1}^{-l_1} \right) \cdot p^{\frac{l_1 - 1}{2}} \frac{l_2 + 1}{2} = \delta_1 p^{\frac{l_1 - 1}{2}} \frac{l_2 + 1}{2},$$

$$\tau(\gamma_{l_2,\eta_1}) = \left( \prod_{t \in H_1} \chi(t)_{l_2}^{-l_2} \right) \cdot p^{\frac{l_2 - 1}{2}} \frac{l_2 + 1}{2} = \delta_2 p^{\frac{l_1 - 1}{2}} \frac{l_2 + 1}{2},$$

where

$$\delta_1 = \begin{cases} 1 \\ \chi(l_1)^{-l_1} & \text{if } l_2 \not\equiv 3, \\ \chi(l_1)^{-l_1} & \text{if } l_2 = 3, \end{cases} \quad \delta_2 = \begin{cases} 1 \\ \chi(l_2)^{-l_2} & \text{if } l_1 \not\equiv 3, \\ \chi(l_2)^{-l_2} & \text{if } l_1 = 3. \end{cases}$$

On the other hand, as for the denominator, we have

$$\tau([l_1, -l_1] \eta_2) = p^{\frac{l_1 - 1}{2}}, \quad \tau([u, -u] \eta) = p^{\frac{l_1 - 1}{2}} \frac{l_2 + 1}{2}.$$

Hence

$$\tau(\alpha)^2 = \delta_1 \delta_2 p^{\frac{l_1 - 1}{2}} \frac{l_2 + 1}{2} = \delta_1 \delta_2 p^{\frac{l_1 - 1}{2}} \frac{l_2 + 1}{2}.$$

Therefore, if $l_1 \not\equiv 3$ and $l_2 \not\equiv 3$, then $\tau(\alpha)^2 = p^{\frac{l_1 - 1}{2}} \frac{l_2 + 1}{2}$, and so

$$\tau(\alpha) = \pm p^{\frac{l_1 - 1}{2}} \frac{l_2 + 1}{2}.$$
If $l_2 = 3$, then
\[ \tau(\alpha)^2 = \chi(l_1) 2^n \prod p^{n-1}. \]
Taking the square roots of the both sides yields the formula for $\tau(\alpha)$. The case where $l_2 = 3$ can be proved quite similarly. \qed

5. Ring class fields

In this section we state our main theorems. For this end, we collect some basic facts on ring class fields of imaginary quadratic fields. We refer the reader to [5] for more details on ring class fields.

We start with a general setting. Let $F$ be an imaginary quadratic field and $\mathcal{O}$ the order in $F$ of conductor $f$. Thus
\[ \mathcal{O} = \mathbb{Z} + f \mathcal{O}_F, \]
where $\mathcal{O}_F$ is the integer ring of $F$. Let $I(\mathcal{O})$ denote the group of fractional proper $\mathcal{O}$-ideals and $P(\mathcal{O})$ the group of principal $\mathcal{O}$-ideals. Then the quotient group
\[ C(\mathcal{O}) = I(\mathcal{O}) / P(\mathcal{O}) \]
is called the ideal class group of $\mathcal{O}$ and its order $h(\mathcal{O})$ is called the class number of $\mathcal{O}$.

**Proposition 5.1.** Let $h_F$ be the class number of $F$ and $d_F$ the discriminant of $F$. Then the class number $h(\mathcal{O})$ is given by the formula
\[
\log(h(\mathcal{O})) = \frac{h_F f}{[\mathcal{O}^\times : \mathcal{O}_F^\times]} \prod_{l \mid f} \left(1 - \left(\frac{d_F}{l}\right) \frac{1}{l}\right),
\]
where the product is over the prime numbers dividing $f$ and $(d_F/l)$ denotes the Kronecker symbol.

**Proof.** See [5, Theorem 7.24]. \qed

Let $I_F(f)$ be the subgroup of $I_F$ generated by the ideals of $F$ prime to $f$ and $P_F(f)$ the subgroup of $I_F(f)$ generated by principal ideals of $F$ prime to $f$. Following Cox [5], we denote by $P_{F,\mathbb{Z}}(f)$ the subgroup of $I_F(f)$ generated by principal ideals of the form $\alpha \mathcal{O}_F$, where $\alpha \in \mathcal{O}_F$ satisfies
\[ \alpha \equiv a \pmod{f \mathcal{O}_F} \]
for some integer $a$ prime to $f$. Then
\[ C(\mathcal{O}) \cong I_F(f) / P_{F,\mathbb{Z}}(f). \]
(See [5, Proposition 7.22].) Let $P_{F,1}(f)$ be the subgroup of $I_F(f)$ generated by the principal ideals of the form $\alpha \mathcal{O}_F$ with $\alpha \in \mathcal{O}_F$ such that $\alpha \equiv 1 \pmod{f}$. Since
\[ P_{F,1}(f) \subset P_{F,\mathbb{Z}}(f) \subset I_F(f), \]
by class field theory there exists an abelian extension $L(f)/F$ such that the Artin map induces an isomorphism
\[ I_F(f) / P_{F,\mathbb{Z}}(f) \cong \text{Gal}(L(f)/F). \]
The class field $L(f)$ is called the ring class field of $\mathcal{O}$.

Now, let us return to the special case $m = l_1l_2$, where $l_1, l_2$ are prime numbers satisfying the following conditions:

(i) $l_1 \equiv l_2 \equiv 3 \pmod{4}$,

(ii) $\left(\frac{2}{l}\right) = 1$.

Let $F = \mathbb{Q}(\sqrt{-l_1})$, and let $\mathcal{O}_F$ denote the maximal order of $F$. Then the condition (ii) implies that $l_2$ is a remain prime in $F$. Let

$$O = \mathbb{Z} + l_2\mathcal{O}_F$$

be the order of conductor $l_2$ in $F$ and $h(O)$ the class number of $O$. Then by Proposition 5.1 we have

$$h(O) = \begin{cases} (l_2 + 1)h_F & \text{if } l_1 > 3, \\ (l_2 + 1) & \text{if } l_1 = 3, \end{cases}$$

where $h_F$ is the class number of $F$. Here, note that if $l_1 = 3$, then $l_2 \equiv 2 \pmod{3}$ since $(-3/l_2) = -1$.

Let $L(l_2)$ be the ring class field of $O$. Then the following proposition holds.

**Proposition 5.2.** Define the quartic field $M_0$ by

$$M_0 = \mathbb{Q}(\sqrt{-l_1}, \sqrt{-l_2}) = F(\sqrt{-l_2}).$$

Then $L(l_2) \cap K_2 = M_0$.

**Proof.** Note that $M_0$ is a subfield of $K_2$. First, we prove that $M_0 \subset L(l_2)$. For this, recall that the abelian extension $\mathbb{Q}(\sqrt{-l_2})/\mathbb{Q}$ corresponds to the subgroup

$$\mathbb{Q}^\times \left( H_{l_2} \times \prod_{p \neq l_2} \mathbb{Z}_p^\times \right)$$

of the idèle group of $\mathbb{Q}$, where $H_{l_2} = \{t^2 \mid t \in \mathbb{Z}_{l_2}^\times\}$ and $\mathbb{Z}_p^\times$ denotes the group of positive real numbers. Hence the abelian extension $M_0/F$ corresponds to the subgroup

$$N_{F/\mathbb{Q}}^{-1}\left( \mathbb{Q}^\times \left( H_{l_2} \times \prod_{p \neq l_2} \mathbb{Z}_p^\times \right) \right) = F^\times \left( N_{F/\mathbb{Q}}^{-1}(H_{l_2}) \times \prod_{v \neq l_2} \mathcal{O}_F^\times \right)$$

of the idèle group of $F$, where $N_{F/\mathbb{Q}}$ is the norm map for the extension $F/\mathbb{Q}$ and $v$ runs over the set of places of $F$ distinct from $l_2$. (Recall that $l_2$ is a remain prime in $F$ since $(-1/l_2) = -1$.) Obviously, the subgroup $(\mathbb{Z} + l_2\mathcal{O}_F_{l_2})^\times$ of $\mathcal{O}_F_{l_2}^\times$ satisfies

$$N_{F/\mathbb{Q}}((\mathbb{Z} + l_2\mathcal{O}_F_{l_2})^\times) \subset H_{l_2},$$

and so

$$F^\times \left( (\mathbb{Z} + l_2\mathcal{O}_F_{l_2})^\times \times \prod_{v \neq l_2} \mathcal{O}_F^\times \right) \subset F^\times \left( N_{F/\mathbb{Q}}^{-1}(H_{l_2}) \times \prod_{v \neq l_2} \mathcal{O}_F^\times \right).$$

Since the group in the right hand side corresponds to the ring class field $L(l_2)$, this implies that $M_0 \subset L(l_2)$.

Next, let $L(1)$ be the Hilbert class field of $F$. Note that $[L(1) : F] = h_F$ is odd and $\text{Gal}(L(l_2)/L(1))$ is isomorphic to a quotient group of the cyclic group $(\mathcal{O}_F/l_2\mathcal{O}_F)^\times$.
(see [5, Exercises 9.21]). Hence \( M_0 \) is the unique intermediate field in \( L(l_2)/F \) with \( [M_0 : F] = 2 \). Let \( Q^{ab} \) denote the maximal abelian extension of \( Q \). Then

\[
L(l_2) \cap K_m = L(l_2) \cap Q^{ab}.
\]

To see this, let \( R_m \) be the ray class field of \( F \) of conductor \( m \). Then, since \( L(l_2) \) is contained in \( R_m \) and \( K_m = R_m \cap Q^{ab} \), it follows that

\[
L(l_2) \cap K_m = (L(l_2) \cap R_m) \cap Q^{ab} = L(l_2) \cap Q^{ab}.
\]

It follows from (17) that \( L(l_2) \cap K_m \) is the maximal subextension of \( L(l_2)/F \) on which \( Gal(F/Q) \) acts trivially. But, since \( L(l_2)/F \) is a generalized dihedral extension (see [5, Theorem 9.18]), we see that \( M_0 = L(l_2) \cap K_m \). This completes the proof. \( \square \)

Let \( L(1) \) be the Hilbert class field of \( F \). Then \([L(1) : F] = h_F \) and \([L(l_2) : F] = h(\mathcal{O}) \). Since \( h_F \) is odd and \( L(l_2)/L(1) \) is a cyclic extension of degree \( l_2 + 1 \) or \( (l_2 + 1)/3 \), which is divisible by 4, there exists a unique intermediate field \( M \) such that \([M : F] = 4 \).

Let \( p \equiv 1 \pmod{m} \), \( p \) splits completely in \( Q(\zeta_m) \). Moreover, since \( L(l_2) \cap Q(\zeta_m) = M_0 \), it follows that \( p \) splits in \( M_0 \). Thus, if we denote by \( \left( \frac{M/F}{p} \right) \in Gal(M/F) \) the Artin symbol, then \( \left( \frac{M/F}{p} \right) \in Gal(M/M_0) \). Identifying the Galois group \( Gal(M/M_0) \) with \( \mu_2 = \{ \pm 1 \} \), we obtain a homomorphism

\[
\varepsilon : I_F(l_2) \longrightarrow \mu_2.
\]

Thus \( \varepsilon(p) = 1 \) if and only if \( p \) splits completely in \( M/F \).

We can now state our main theorems. First, suppose \( l_1 > 3 \) and \( l_2 > 3 \).

**Theorem 5.3.** Suppose \( l_1, l_2 > 3 \). If we put \( \alpha = \eta + [-l_2] \eta_1 \), then

\[
\tau(\alpha) = \varepsilon(p)^{l_2 + 1} \cdot \frac{l_2 + 1}{l_2 - 1}.
\]

Moreover, we have \( 4p^{h(\mathcal{O})/4} = u^2 + 11v^2 \) for some integers \( u, v \), exactly one of which is divisible by \( l_2 \), and \( \varepsilon(p) = 1 \) if and only if \( l_2 \mid v \).

**Example 5.4.** Consider the case where \( m = 77 = 11 \cdot 7 \). Since \( \left( \frac{11}{7} \right) = 1 \), we set \( l_1 = 11 \) and \( l_2 = 7 \). Let \( F = \mathbb{Q}(\sqrt{-11}) \) and \( \mathcal{O} = \mathbb{Z} + 7\mathcal{O}_F \). Then \( h_F = 1 \) and \( h(\mathcal{O}) = 8 \).

Let \( \alpha \) be the generator defined in Example 4.4. Then

\[
\tau(\alpha) = \varepsilon(p)^{10}
\]

with \( \varepsilon = \pm 1 \). Since \( h_F = 1 \), we have

\[
4p^2 = u^2 + 11v^2,
\]

for some integer \( u, v \). Then Theorem 5.3 implies that

\[
\varepsilon = \begin{cases} 
1 & \text{if } 7 \mid v, \\
-1 & \text{if } 7 \mid u.
\end{cases}
\]
Next, we consider the case where \( m = 3l \). In this case, \( \chi(l)^{1/3} \) is a cubic root of unity.

**Theorem 5.5.** Suppose \( m = 3l \).

(i) If \( l \equiv 1 \pmod{3} \) (i.e., \( l_1 = l, l_2 = 3 \), then \( 4p^{(l+1)/4}hF = u^2 + lv^2 \) for some integers \( u, v \), and exactly one of \( u \) and \( v \) is divisible by 3. Moreover, if we put \( \alpha = \eta + [-3] \eta \), then

\[
\tau(\alpha) = \varepsilon(p) \chi(l)^{1/3} p^{l+1}
\]

and \( \varepsilon(p) = 1 \) if and only if \( 3 | v \).

(ii) If \( l \equiv 2 \pmod{3} \) (i.e., \( l_1 = 3, l_2 = l \)), then \( 4p^{(l+1)/12} = u^2 + 3v^2 \) for some integers \( u, v \), and exactly one of \( u \) and \( v \) is divisible by 1. Moreover, if we put \( \alpha = \eta + [-l] \), then

\[
\tau(\alpha) = \varepsilon(p) \chi(l)^{1/4} p^{l+1}
\]

and \( \varepsilon(p) = 1 \) if and only if \( 1 | v \).

**Example 5.6.** (Muskat-Zee [16]). If \( m = 21 = 3 \cdot 7 \), then \( l_1 = 7 \) and \( l_2 = 3 \). Let \( F = \mathbb{Q}(\sqrt{-7}) \) and \( \mathcal{O} = \mathbb{Z} + 3 \mathcal{O}_F \). Then \( h_F = 1 \) and \( h(\mathcal{O}) = 4 \). Let

\[
\alpha = [1, 4, 16, [-3][1, 4, 16] = [1, 4, 16, 9, 15, 18].
\]

Then

\[
\tau(\alpha) = \varepsilon \chi(7)^{1/7} p^3
\]

with \( \varepsilon = \pm 1 \). We have \( p = u^2 + 7v^2 \) for some integers \( u, v \), and

\[
\varepsilon = \begin{cases} 
1 & \text{if } 3 | v, \\
-1 & \text{if } 3 | u.
\end{cases}
\]

**Example 5.7.** If \( m = 33 = 3 \cdot 11 \), then \( l_1 = 3 \) and \( l_2 = 11 \). Let \( F = \mathbb{Q}(\sqrt{-3}) \) and \( \mathcal{O} = \mathbb{Z} + 11 \mathcal{O}_F \). Then \( h_F = 1 \) and \( h(\mathcal{O}) = 4 \). Let

\[
\alpha = [1, 4, 16, 31, 25] + [-11] = [1, 4, 16, 31, 25, 22].
\]

Then

\[
\tau(\alpha) = \varepsilon \chi(11)^{1/11} p^3
\]

with \( \varepsilon = \pm 1 \). We have \( 4p = u^2 + 3v^2 \) for some integers \( u, v \), and

\[
\varepsilon = \begin{cases} 
1 & \text{if } 11 | v, \\
-1 & \text{if } 11 | u.
\end{cases}
\]

Let \( \mathfrak{p}_\mathcal{O} = p \cap \mathcal{O} \) be the prime ideal in \( \mathcal{O} \). Since \( p \) splits completely in \( \mathcal{M}_0 \), we have \( \mathfrak{p}_\mathcal{O}^{(\mathcal{O})/2} \) is principal. The following corollary gives an affirmative answer to the conjecture of van Wamelen ([18, Conjecture 21]).

**Corollary 5.8.** Notation being as above, \( \mathfrak{p}_\mathcal{O}^{(\mathcal{O})/2} \) is principal if and only if \( \varepsilon(p) = 1 \).
6. Proof of the main theorems

The purpose of this section is to prove Theorem 5.3, Theorem 5.5 and Corollary 5.8. After proving them, we will prove Theorem 1.2. In this section we write \( \tau_m(a) \) for \( \tau(a) \) to specify the Gauss sum \( \tau(a) \) depends on \( \chi \) whose order is \( m \). We also write \( \tau_1(a) \) for \( \tau_m(l_2^a) \) since \( \chi^{l_2} \) is the \( l_1 \)-th power residue symbol.

Let us start with two lemmas.

**Lemma 6.1.** Let \( l_2' \) be an integer prime to \( l_1 \) such that \( l_2 l_2' \equiv 1 \pmod{l_1} \). Let \( \lambda_2 \) be a prime ideal of \( K_m \) which divides \( l_2' \). Then

\[
\tau_m(a) \equiv \tau_1(l_2'a) \pmod{\lambda_2}.
\]

**Proof.** Let \( A, B \) be integers such that \( Al_2 + Bl_1 = 1 \). Then

\[
\frac{p-1}{m} = \frac{(p-1)A}{l_1} + \frac{(p-1)B}{l_2}.
\]

This implies that

\[
\left( \frac{x}{P} \right)_m \equiv \left( \frac{x}{P_1} \right)_{l_1} A \cdot \left( \frac{x}{P_2} \right)_{l_2} B \pmod{P},
\]

where \( P_1 = P \cap \mathbb{Q}(\zeta_{l_1}) \) and \( \cdot / P_1 \) is the \( l_1 \)-th power residue symbol. Since \( \mu_m(\mathbb{C}) \) maps injectively to \( (\mathcal{O}_{K_m}/P)^\times \) by the reduction map \( \mathcal{O}_{K_m} \rightarrow \mathcal{O}_{K_m}/P \), this implies that

\[
\left( \frac{x}{P} \right)_m = \left( \frac{x}{P_1} \right)_{l_1} A \cdot \left( \frac{x}{P_2} \right)_{l_2} B.
\]  \hspace{1cm} (17)

Since \( \left( \frac{x}{P_2} \right)_{l_2} \equiv 1 \pmod{\lambda_2} \) and \( A \equiv l_2' \pmod{l_1} \), it follows from (17) that

\[
\left( \frac{x}{P} \right)_{l_2} \equiv \left( \frac{x}{P_1} \right)_{l_1} l_2' \pmod{\lambda_2}.
\]

Therefore

\[
\tau_m(a) = \sum_{x \in \mathbb{F}_p^\times} \left( \frac{x}{P} \right)_m^a \zeta_p^x = \sum_{x \in \mathbb{F}_p^\times} \left( \frac{x}{P_1} \right)_{l_1}^a \zeta_p^x \pmod{\lambda_2} = \tau_1(l_2'a).
\]

This completes the proof. \( \square \)
Let $F = \mathbb{Q}(\sqrt{-1})$. Then the class number $h_F$ of $F$ is odd. Since $t \cdot \eta_1 = \eta_1$ for any $t \in (\mathbb{Z}/l_1\mathbb{Z})^\times$, it follows that $\sigma(\tau_l(\eta_1)) = \eta_1$ for any $\sigma \in \text{Gal}(K_l/F)$, hence $\tau_l(\eta_1)$ belongs to $F$. Consequently $\tau_l(\eta_1)$ belongs to $\mathcal{O}_F$, and so we can consider the ideal $\tau_l(\eta_1)\mathcal{O}_F$. The following lemma gives the prime ideal decomposition of the ideal $\tau_l(\eta_1)\mathcal{O}_F$.

**Lemma 6.2.** Let $p = \mathcal{O}_F \cap P$ be the prime ideal of $F$ lying under $P$. Then the prime ideal decomposition of the principal ideal $\tau_l(\eta_1)\mathcal{O}_F$ is given by

$$
\tau_l(\eta_1)\mathcal{O}_F = (p)^{\frac{l(l-1)}{2}}\mathcal{O}_F.
$$

**Proof.** Let $K_{l_1} = \mathbb{Q}(\zeta_{l_1})$ be the $l_1$-th cyclotomic field and put $P_1 = \mathcal{O}_{K_{l_1}} \cap P$. Then Corollary 2.6 shows that

$$
\tau_l(\eta_1)\mathcal{O}_{K_{l_1}} = p^{\theta(\eta_1)},
$$

where $\theta(\eta_1)$ is the Stickelberger element. For any character $\psi$ of $G_1$, we denote by $e_\psi$ the idempotent element. Then

$$
\theta(\eta_1) = \sum_{\psi \in \hat{G}_1} \theta(\eta_1)e_\psi.
$$

If $\psi = \psi_0$, then

$$
\theta(\eta_1)e_{\psi_0} = \frac{1}{4}(l_1 - 1)v_{G_1},
$$

and if $\psi \neq \psi_0$, $\bigotimes_{\psi_0}$, then $\sum_{\psi \in \hat{H}_1} \psi(t) = 0$, so

$$
\theta(\eta_1)e_\psi = 0.
$$

Finally, if $\psi = \bigotimes_{\eta_1}$, then

$$
\theta(\eta_1)e_\psi = -\frac{l_1 - 1}{2}h_Fe_\psi = -h_F\frac{1}{2}\rho v_{H_1}.
$$

Therefore

$$
\theta(\eta_1)\mathcal{O}_{K_{l_1}} = (p)^{\frac{l(l-1)}{2}}\mathcal{O}_{\mathbb{Z}_{l_1}}\mathcal{O}_{\mathbb{Z}_{l_1}} = (p)^{\frac{l(l-1)}{2}}h_F\mathcal{O}_{\mathbb{Z}_{l_1}} = (p)^{\frac{l(l-1)}{2}}\mathcal{O}_F.
$$

which proves the lemma. \qed

**Proposition 6.3.** Notation being as above, we have $\tau_l(\eta_1)^{(l_2+1)/2} \in \mathcal{O}$ and

$$
\tau_l(\eta_1)^{(l_2+1)/2} \mathcal{O} = (p)^{\frac{l(l-1)}{2}}\mathcal{O} = (p)^{\frac{l(l-1)}{2}}\mathcal{O}/(\mathcal{O})_{/2}.
$$

In particular, $P^{h_F}/2$ is a principal ideal of $\mathcal{O}$.

**Proof.** By Lemma 6.1 we have

$$
\tau_m(a) \equiv \tau_{m_1}(l_2a) \pmod{\lambda_2}
$$

for any $a \in \mathbb{Z}/m\mathbb{Z} - \{0\}$. It follows that

$$
\tau_m(a) \equiv \prod_{a \in H_1} \tau_{m_1}(l_2a) \equiv \prod_{a \in H_1} \tau_{m_1}(l_2a)^{(l_2+1)/2} \equiv \tau_{l_1}(l_2a)^{(l_2+1)/2} \equiv \tau_{l_1}(l_2a)^{(l_2-1)/2} \pmod{\lambda_2}
$$

for any $a \in \mathbb{Z}/m\mathbb{Z} - \{0\}$.
Since \( \left( \frac{l_2}{l_1} \right) = \left( \frac{l_2}{p} \right) = -1 \), we have

\[
\tau_{l_1}(\eta_1) = \tau_{l_1}(-1|\eta_1).
\]

Therefore

\[
\tau(\eta) \equiv \tau_{l_1}(-1|\eta_1) \frac{l_2+1}{p} \quad (\text{mod } \lambda_2).
\]

Consequently

\[
\tau_m(\alpha) = \tau_m(\eta)\tau_m([-l_2]\eta_1)
\equiv \tau_{l_1}([-1]\eta_1) \frac{l_2+1}{p} \tau_{l_1}([-1]\eta_1) \quad (\text{mod } \lambda_2)
\equiv \tau_{l_1}([-1]\eta_1) \frac{l_2+1}{p} \quad (\text{mod } \lambda_2)
\equiv \tau_{l_1}(\eta_1) \frac{l_2+1}{p} \quad (\text{mod } \lambda_2).
\]

On the other hand,

\[
\tau_m(\alpha) = \epsilon \frac{l_2-1}{p} \equiv \epsilon \quad (\text{mod } l_2).
\]

Since \( \lambda_2 \mathcal{O}_{K_u} \cap F = l_2 \mathcal{O}_F \), this implies that

\[
\tau_{l_1}(\eta_1) \frac{l_2+1}{p} \equiv \epsilon \quad (\text{mod } l_2 \mathcal{O}_F).
\]

(18)

which shows that \( \tau_{l_1}(\eta_1)^{(l_2+1)/2} \in \mathcal{O} \).

Proof of Theorem 5.3. Since

\[
\frac{\lambda(\mathcal{O})}{p \mathcal{O}^2} = \tau_{l_1}(\eta_1) \frac{l_2+1}{p} \frac{\eta_1}{4} \left( \frac{u - v \sqrt{-l_1}}{2} \right) \mathcal{O}
\]

by Proposition 6.3, it follows that

\[
\tau_{l_1}(\eta_1)^{\frac{l_2+1}{p}} \frac{\eta_1}{4} \left( \frac{u - v \sqrt{-l_1}}{2} \right) \mathcal{O}
\]

Since \( \tau_{l_1}(\eta_1) \in \mathcal{O}_F \), we have

\[
\tau_{l_1}(\eta_1)^{\frac{l_2+1}{p}} \frac{\eta_1}{4} \left( \frac{u - v \sqrt{-l_1}}{2} \right) = \frac{u + v \sqrt{-l_1}}{2}
\]

(19)

for some integers \( u, v \) with \( u \equiv v \pmod{2} \). Combining this with (19), we obtain

\[
4p \frac{\lambda(\mathcal{O})}{p \mathcal{O}^2} = u^2 + l_1v^2.
\]

Since \( p \equiv 1 \pmod{2} \), it follows from (18) and (20) that

\[
\left( \frac{u + v \sqrt{-l_1}}{2} \right)^2 \equiv \tau_{l_1}(\eta_1)^{\frac{l_2+1}{2}} \equiv \epsilon \quad (\text{mod } l_2).
\]

This implies that

\[
u^2 - l_1v^2 + 2uv \sqrt{-l_1} \equiv 4\epsilon \quad (\text{mod } l_2),
\]

which means that \( l_2 \mid uv \). If \( l_2 \mid v \), then

\[
u^2 \equiv 4\epsilon \quad (\text{mod } l_2).
\]

(21)

Since \( l_2 \equiv 3 \pmod{4} \), we have \( \frac{4\epsilon}{l_2} = \epsilon \), hence (21) shows that \( \epsilon = 1 \).
On the other hand, if \( l_2 \mid u \), then
\[-l_1 v^2 \equiv 4\varepsilon \pmod{l_2}.\]
By a similar argument as above, we conclude that \( \varepsilon = -1 \).

Finally, we prove that \( \varepsilon = \varepsilon(p) \). To see this, note that \( v \equiv 0 \pmod{l_2} \) if and only if \( \tau_{l_1}(\eta_1)^{(l_2+1)/4} \in \mathcal{O} \). The latter condition holds if and only if \( p^{\frac{h(O)}{4}} \) is principal, or equivalently \( \varepsilon(p) = 1 \). Therefore \( \varepsilon = 1 \) if and only if \( \varepsilon(p) = 1 \). This completes the proof.

**Proof of Theorem 5.5.** We can prove Theorem 5.5 quite similarly as above if we replace (18) with the congruence
\[\tau_{l_1}(\eta_1) \overset{l_2+1}{\equiv} \varepsilon \chi(l)^l \pmod{l_2\mathcal{O}_F},\]
which derives from Proposition 4.5.

**Proof of Corollary 5.8.** If \( \varepsilon = 1 \), then \( l_2 \mid v \) and \( l_1 \nmid u \). Hence
\[2\tau_{l_1}(\eta_1) \overset{l_2+1}{\equiv} u \pmod{l_2},\]
which implies that \( \tau_{l_1}(\eta_1) \overset{l_2+1}{\in} P_{F,Z}(l_2) \). This shows that \( p^{\frac{h(O)}{4}} \) is principal.

On the other hand, if \( \varepsilon = -1 \), then \( l_2 \nmid u \) and \( l_1 \mid v \), hence
\[2\tau_{l_1}(\eta_1) \overset{l_2+1}{\equiv} v\sqrt{-l_1} \pmod{l_2},\]
which implies that \( \tau_{l_1}(\eta_1) \overset{l_2+1}{\notin} P_{F,Z}(l_2) \). This shows that \( p^{\frac{h(O)}{4}} \) is not principal.

**Proof of Theorem 1.2.** Proposition 2.7 and Proposition 2.8 show that \( \tau(\alpha)p^{-s(\alpha)/2} \) is an \( m \)-th root of unity for any \( \alpha \in S_m \). Therefore \( \varepsilon^m \) in Theorem 1.2 does not depend of the choice of a generator of \( B_m/S_m \). Hence Theorem 1.2 follows from Theorem 5.3 and Theorem 5.5.

### 7. Products of special values of \( \Gamma \)-functions

In this section we will give an explicit description of the field \( M \) defined in §5. For the time being, we assume that \( m \) is a general positive integer.

For \( \alpha = \sum a c_a[a] \in R_m \), define
\[
\Gamma_m(\alpha) = \prod_{a \in \mathbb{Z}/m\mathbb{Z} - \{0\}} \Gamma \left( \left( \frac{a}{m} \right) \right)^{c_a},
\]
\[
\tilde{\Gamma}_m(\alpha) = (2\pi i)^{-s(\alpha)/2} \Gamma_m(\alpha),
\]
\[
\tilde{\tau}_m(\alpha) = p^{-s(\alpha)/2} \tau_m(\alpha).
\]
If \( \alpha \in B_m \), then \( s(\alpha) \) is even and \( \tilde{\Gamma}_m(\alpha) \) is an algebraic number and generates an abelian extension of \( K_m \) (see [6]). More precisely the following theorem holds.
THEOREM 7.1. If \( \alpha \in B_m \), then \( \tilde{\Gamma}_m(\alpha) \) is an algebraic number and generates an abelian extension of \( K_m \). Moreover, for any prime ideal \( P \) of \( K_m \) not dividing \( m \), we have

\[
\left( \frac{K_m^b}{K_m} \right)_P \tilde{\Gamma}_m(\alpha) = \tilde{\tau}_m(\alpha)^{-1} \tilde{\Gamma}_m(\alpha),
\]

where \( \left( \frac{K_m^b}{K_m} \right)_P \) denotes the Artin symbol.

Proof. See [6, Theorem 7.18]. \( \square \)

LEMMA 7.2. For any \( a \in \mathbb{Z}/m\mathbb{Z} - \{0\} \),

\[
\Gamma_m([a, -a]) = \frac{2\pi}{2 \sin(\frac{2\pi}{m})}.
\]

Proof. By Euler’s reflection formula for the \( \Gamma \)-function, we have

\[
\Gamma(x) \Gamma(1-x) = \frac{\pi}{\sin \pi x}
\]

for any \( x \in \mathbb{R} - \mathbb{Z} \). Therefore,

\[
\Gamma_m([a, -a]) = \Gamma\left(\left(\frac{a}{m}\right)\right) \Gamma\left(1 - \left(\frac{a}{m}\right)\right) = \frac{\pi}{\sin\left(\frac{2\pi}{m}\right)}.
\]

The lemma immediately follows from this. \( \square \)

LEMMA 7.3. Let \( l \) be an odd prime number and put \( d = m/l \). Then

\[
\Gamma_m(\gamma_l, a) = \frac{(2\pi)^{\frac{l-1}{2}}}{\Gamma(\frac{m}{d})^{-1/2} \sin\left(\frac{\pi}{d}a\right)}.
\]

for any \( a \in \mathbb{Z} \) with \( la \not\equiv 0 \pmod{m} \).

Proof. By Gauss’ multiplicative formula, we have

\[
\prod_{k=0}^{l-1} \Gamma\left(\frac{x + \frac{k}{l}}{r}\right) = \Gamma(dx) \cdot \frac{(2\pi)^{\frac{l-1}{2}}}{\Gamma(\frac{m}{d})^{-1/2}}
\]

for any \( x \in \mathbb{R} - \mathbb{Z} \). It follows that

\[
\Gamma_m(\gamma_l, a) = \Gamma\left(\left(\frac{-al}{m}\right)\right) \prod_{k=0}^{l-1} \Gamma\left(\left(\frac{al + kd}{m}\right)\right)
\]

\[
= \Gamma\left(\left(\frac{-al}{m}\right)\right) \Gamma\left(\left(\frac{al}{m}\right)\right) \frac{(2\pi)^{\frac{l-1}{2}}}{\Gamma(\frac{m}{d})^{-1/2}}
\]

\[
= \frac{\pi}{\sin\left(\frac{\pi}{d}a\right)} \cdot \frac{(2\pi)^{\frac{l-1}{2}}}{\Gamma(\frac{m}{d})^{-1/2}}
\]

\[
= \frac{(2\pi)^{\frac{l-1}{2}}}{\Gamma(\frac{m}{d})^{-1/2} \cdot 2 \sin\left(\frac{\pi}{d}a\right)},
\]

from which the lemma easily follows. \( \square \)
Lemma 7.4. Let \( l \) be an odd prime number with \( l \equiv 3 \pmod{4} \) and \( h(-l) \) the class number of the imaginary quadratic field \( \mathbb{Q}(\sqrt{-l}) \). Let \( \delta(l) = 1/3 \) if \( l = 3 \) and \( \delta(l) = 0 \) otherwise. Then:

(i) \[ \sum_{(a/l)=1} \left( \frac{a}{l} \right) - \frac{1}{2} = -\frac{1}{2} h(-l). \]

(ii) \[ \prod_{(a/l)=1} 2 \sin \left( \frac{a}{l} \pi \right) = \sqrt{\gamma}. \]

Proof. The first formula (i) is well known. To prove (ii), let \( \zeta = e^{\pi i/l} \). Since \( \sin (\frac{\pi}{2l}) \pi = \sin (\frac{\pi}{6}) \pi \) and
\[
2 \sin \left( \frac{a}{l} \pi \right) = \frac{\zeta^a - \zeta^{-a}}{i},
\]

it follows that
\[
\left( \prod_{(a/l)=1} 2 \sin \left( \frac{a}{l} \pi \right) \right)^2 = \prod_{a=1}^{l-1} 2 \sin \left( \frac{a}{l} \pi \right) = \prod_{a=1}^{l-1} \frac{\zeta^a - \zeta^{-a}}{i} = i^{-(l-1)} \prod_{a=1}^{l-1} \zeta^a (1 - \zeta^{-2a}) = (-1)^{-\frac{l-1}{2}} \zeta^{\frac{l(l-1)}{2}} \prod_{a=1}^{l-1} (1 - \zeta^a) = (-1)^{-\frac{l-1}{2}} (-1)^{\frac{l-1}{2}} = l.
\]

Since \( \sin (\frac{\pi}{6}) \pi > 0 \) for any \( a \) with \( 0 < a < l \), the lemma follows. 

Now, we focus on the case where \( m = \ell_1 \ell_2 \). To state the next theorem, let
\[
\kappa = \begin{cases} 
1 & \text{if } \ell_1 > 3 \text{ and } \ell_2 > 3, \\
\frac{1}{\sqrt{\gamma}} & \text{if } m = 3l. 
\end{cases}
\]

Theorem 7.5. Let \( \alpha \) be as in Theorem 5.3. Then
\[
\Gamma_{\alpha}(\alpha) = \rho^{-1} \kappa \sqrt{-\ell_1}^{\frac{h(-\ell_1)-1}{2}} \sqrt{-\ell_2}^{\frac{h(-\ell_2)-1}{2}} \sqrt{\ell_2} \sqrt{\delta_0} \sqrt{h(\ell_2)},
\]
where \( \rho = \sqrt{\frac{1}{8}(l_1+1)(l_2+1) - \frac{1}{4}h(-l_1)+h(-l_2)+1} \) and \( \delta_0 \) is the fundamental unit of the real quadratic field \( \mathbb{Q}(\sqrt{\ell_1 \ell_2}) \).

Corollary 7.6. Let \( M \) be the subfield of \( L(\ell_2) \) defined in §5. Then
\[
M = M_0(\rho^{-1} \sqrt{\ell_2} \sqrt{\delta_0} \sqrt{h(\ell_2)}). 
\]

Proof. Since \( \varepsilon_\alpha(P) = \varepsilon(p) \), this follows from Theorem 7.1 and Theorem 7.5. 

**Lemma 7.7.** Notation being as above, we have

\[
\Gamma_m(\gamma_1, \eta_2) \Gamma_m(\gamma_2, \eta_1) = (2\pi)^{\frac{l_1 l_2 - 1}{2}} \kappa^2 \sqrt{l_1^{h(l_2)} - 1} \sqrt{l_2^{h(l_2)} - 1}.
\]

**Proof.** By Lemma 7.3 we have

\[
\Gamma_m(\gamma_1, \eta_2) = \prod_{a \in \mathcal{H}_2} \Gamma_m(\gamma_1, a)
\]

\[
= \prod_{a \in \mathcal{H}_2} \frac{(2\pi)^{\frac{l_1 + 1}{2} \frac{l_2 - 1}{2}}}{\mathcal{I}_1^{\frac{1}{2} h(-l_2) + \delta(l_2)} \sqrt{T_2}}.
\]

Quite similarly we have

\[
\Gamma_m(\gamma_2, \eta_1) = \frac{(2\pi)^{\frac{l_1 + 1}{2} \frac{l_2 - 1}{2}}}{\mathcal{I}_2^{\frac{1}{2} h(-l_1) + \delta(l_1)} \sqrt{T_1}}.
\]

Since \(I_1^\delta(l_2) I_2^\delta(l_1) = \kappa^{-2}\), we obtain

\[
\Gamma_m(\gamma_1, \eta_2) \Gamma_m(\gamma_2, \eta_1) = (2\pi)^{\frac{l_1 l_2 - 1}{2}} \kappa^2 \sqrt{l_1^{h(l_2)} - 1} \sqrt{l_2^{h(l_2)} - 1},
\]

which proves the lemma. \(\square\)

**Lemma 7.8.** We have

\[
\Gamma_m([l_1, -l_1] \eta_2) = \frac{(2\pi)^{\frac{l_1 - 1}{2}}}{\sqrt{T_2}}.
\]

**Proof.** By Lemma 7.2 we have

\[
\Gamma_m([l_1, -l_1] \eta_2) = \prod_{\langle \eta \rangle = 1} \frac{2\pi}{2 \sin((\frac{\eta}{l_2}) \pi)} = \frac{(2\pi)^{\frac{l_2 - 1}{2}}}{\sqrt{T_2}}.
\]

By Lemma 7.4 the denominator is equal to \((-1)^{(l_1 - 3)/4} \sqrt{T_1 T_2}\), and the lemma follows. \(\square\)

**Lemma 7.9.** Let \(\varepsilon_0\) be the fundamental unit of the real quadratic field \(\mathbb{Q}(\sqrt{t_1 t_2})\) and \(h(l_1 l_2)\) the class number of \(\mathbb{Q}(\sqrt{t_1 t_2})\). Then

\[
\Gamma_m([u, -u] \eta) = \frac{(2\pi)^{\frac{l_1 l_2 - 1}{2}}}{\sqrt{6}^0 h(l_1 l_2)}.
\]
Proof. Recall that \( G = (\mathbb{Z}/m\mathbb{Z})^\times \) and \( H = \{ t^2 \mid t \in G \} \). Then
\[
\Gamma_m([u, -u] \eta) = \prod_{a \in H} \frac{2\pi}{2 \sin \left( \frac{\langle u^a \rangle \pi}{m} \right)} .
\]
(24)

Since
\[
\{ a \in G \mid \left( \frac{a}{m} \right) = -1 \} = \{ \pm u^a \mid a \in H \} ,
\]
we have
\[
\prod_{a \in H} 2 \sin \left( \frac{\langle a \rangle \pi}{m} \right) = \left( \prod_{a \in H} 2 \sin \left( \frac{\langle u^a \rangle \pi}{m} \right) \right)^2 .
\]
Hence
\[
\left( \prod_{a \in H} 2 \sin \left( \frac{\langle u^a \rangle \pi}{m} \right) \right)^4 = \left( \prod_{a \in G} 2 \sin \left( \frac{\langle a \rangle \pi}{m} \right) \right)^2 .
\]
(25)

Here we note that
\[
\prod_{a \in G} 2 \sin \left( \frac{\langle a \rangle \pi}{m} \right) = 1 .
\]
(26)

To see this, let \( \Phi_m(x) \) be the \( m \)-th cyclotomic polynomial and put \( \zeta = e^{\pi i/m} \). Then, since \( |G| \equiv 0 \pmod{4} \), we have \( i^{|G|} = 1 \), hence
\[
\prod_{a \in G} 2 \sin \left( \frac{\langle a \rangle \pi}{m} \right) = \prod_{a \in G} (\zeta^a - \zeta^{-a}) = \prod_{a \in G} \zeta^a(1 - \zeta^{-2a}) = \prod_{a \in G} (1 - \zeta^{2a}) = \Phi_m(1) .
\]
But, since \( m \) is a product of two distinct odd primes, we have \( \Phi_m(1) = 1 \), and so (26) holds. Therefore
\[
\left( \prod_{a \in H} 2 \sin \left( \frac{\langle u^a \rangle \pi}{m} \right) \right)^4 = \frac{\left( \prod_{a \in G} 2 \sin \left( \frac{\langle a \rangle \pi}{m} \right) \right)^2}{\prod_{a \in G} 2 \sin \left( \frac{\langle a \rangle \pi}{m} \right)}
\]
\[
= \frac{\prod_{a \in G} 2 \sin \left( \frac{\langle a \rangle \pi}{m} \right)}{\prod_{a \in G} 2 \sin \left( \frac{\langle a \rangle \pi}{m} \right)} .
\]
We know that the last quantity equals \( \varepsilon_0^{2h(l_1l_2)} \) by Dirichlet’s class number formula. It follows from this and (25) that
\[
\left( \prod_{a \in H} 2 \sin \left( \frac{\langle u^a \rangle \pi}{m} \right) \right)^4 = \varepsilon_0^{2h(l_1l_2)} .
\]
Note that \( \sin \left( \frac{\langle u^a \rangle \pi}{m} \right) > 0 \) for any \( a \in G \) and \( \varepsilon_0 > 0 \). Therefore, taking the 4-th roots of the both sides yields
\[
\prod_{a \in H} 2 \sin \left( \frac{\langle u^a \rangle \pi}{m} \right) = \sqrt[4]{\varepsilon_0^{2h(l_1l_2)}} .
\]
Combining this with (24), we obtain the lemma. \( \square \)
Proof of Theorem 7.5. From Lemma 7.7, Lemma 7.8 and Lemma 7.9 we obtain
\[
\Gamma_m(\alpha)^2 = \frac{\Gamma_m(\gamma_2 \eta_2) \Gamma_m(\gamma_1 \eta_1)}{\Gamma_m([l_1, \eta_1 l_2])} = \frac{\Gamma_m([l_1, \eta_1 l_2])}{\Gamma_m(\gamma_2 \eta_2) \Gamma_m(\gamma_1 \eta_1)}
\]
\[
= \frac{\Gamma_m([l_1, \eta_1 l_2])}{\Gamma_m(\gamma_2 \eta_2) \Gamma_m(\gamma_1 \eta_1)} \cdot \frac{(2\pi)^{1/2} (l_1 l_2 - 1)}{\sqrt{l_1^2 (l_2 - 1)} \sqrt{l_2^2 (l_1 - 1)}}
\]
\[
= \frac{(2\pi)^{1/2} (l_1 l_2 - 1)}{\sqrt{l_1^2 (l_2 - 1)} \sqrt{l_2^2 (l_1 - 1)}} \cdot \frac{\sqrt{l_1^2 (l_2 - 1)} \sqrt{l_2^2 (l_1 - 1)}}{(2\pi)^{1/2} (l_1 l_2 - 1)}
\]
\[
= (2\pi)^{1/2} (l_1 l_2 - 1) \cdot \Gamma_m([l_1, \eta_1 l_2]) \cdot \Gamma_m(\gamma_2 \eta_2) \Gamma_m(\gamma_1 \eta_1)
\]
Therefore
\[
\Gamma_m(\alpha)^2 = (2\pi)^{1/2} (l_1 l_2 - 1) \cdot \frac{\sqrt{l_1^2 (l_2 - 1)} \sqrt{l_2^2 (l_1 - 1)}}{(2\pi)^{1/2} (l_1 l_2 - 1)} \cdot \frac{\sqrt{l_1^2 (l_2 - 1)} \sqrt{l_2^2 (l_1 - 1)}}{(2\pi)^{1/2} (l_1 l_2 - 1)}
\]
Dividing the both sides by \((2\pi)^{1/2}\alpha/2\), we obtain Theorem 7.5. 

References


Department of Mathematics
Rikkyo University
Nishi-Ikebukuro, Toshima-ku
Tokyo 171–8501, Japan
E-mail: aoki@rikkyo.ac.jp