Explicit multiplicative relations between Gauss sums

Brian J. Murray

Department of Mathematics, Louisiana State University, Baton Rouge, LA 70803-4918, USA

Received 6 August 2002; revised 19 June 2006
Available online 23 January 2007
Communicated by David Goss

Abstract

H. Hasse conjectured that all multiplicative relations between Gauss sums essentially follow from the Davenport–Hasse product formula and the norm relation for Gauss sums. While this is known to be false, very few counterexamples, now known as sign ambiguities, have been given. Here, we provide an explicit product formula giving an infinite class of new sign ambiguities and resolve the ambiguous sign in terms of the order of the ideal class of quadratic primes.

© 2007 Elsevier Inc. All rights reserved.

Keywords: Gauss sums; Sign ambiguities; Davenport–Hasse product formula; Multiplicative relations

1. Preliminaries

Let $e$ be an integer, $e > 2$, and let $p$ be a prime, $p \equiv 1 \pmod{e}$. Let $\mathbb{F}_p$ be the finite field of $p$ elements with multiplicative group $\mathbb{F}_p^\times$ generated by $\gamma$. For $k > 1$, let $\zeta_k$ denote a primitive $k$th root of unity. We then define a multiplicative character $\chi : \mathbb{F}_p^\times \to \mathbb{Q}(\zeta_e)$ by $\chi(\gamma) = \zeta_e$. We extend the character to all of $\mathbb{F}_p$ by setting $\chi(0) = 0$. For $a \in \mathbb{Z}$, define the Gauss sum $\tau(a)$ to be

$$\tau(a) = \sum_{\alpha \in \mathbb{F}_p} \chi^a(\alpha) \zeta_p^a \in \mathbb{Q}(\zeta_{ep}).$$

We note that as $\chi$ has order $e$, we need only consider $a \mod e$ and thus, have $e$ distinct Gauss sums.

E-mail address: murray@math.lsu.edu.
For \( j \in (\mathbb{Z}/e\mathbb{Z})^\times \), let \( \sigma_j \) be the automorphism of \( \mathbb{Q}(\zeta_{ep}) \) defined by \( \zeta_e \mapsto \zeta^j_e \) and \( \zeta_p \mapsto \zeta_p \). Then for any \( a \in \mathbb{Z}/e\mathbb{Z}, \ j \in (\mathbb{Z}/e\mathbb{Z})^\times, \sigma_j(\tau(a)) = \tau(ja) \).

Closely related to the Gauss sums are the Jacobi sums, which have the advantage of being integers of \( \mathbb{Q}(\zeta_e) \), rather than \( \mathbb{Q}(\zeta_{ep}) \). For \( e, p, \) and \( \chi \) as before and \( m, n \in \mathbb{Z} \), we define the Jacobi sum \( J(m, n) \) to be

\[
J(m, n) = \sum_{\alpha \in \mathbb{F}_p} \chi^m(\alpha)\chi^n(1 - \alpha) \in \mathbb{Q}(\zeta_e).
\]

Finally, for \( m + n \not\equiv 0 \pmod{e} \), Gauss and Jacobi sums are related by

\[
J(m, n) = \frac{\tau(m)\tau(n)}{\tau(m + n)}.
\] (2)

In addition to the notation introduced above, we will also use the following notation throughout. Let \( e \) be the product of two distinct primes and let \( G = (\mathbb{Z}/e\mathbb{Z})^\times \), the group of units modulo \( e \). \( G \) has subgroups \( H, H_2, \) and \( H_4 \) defined by

\[
H = \left\{ h \in G \mid \left( \frac{h}{e} \right) = 1 \right\},
\]

\[
H_2 = \{ h \in G \mid h \text{ is a quadratic residue modulo } e \},
\]

\[
H_4 = \{ h \in G \mid h \text{ is a biquadratic residue modulo } e \},
\]

and we note that \( H_4 < H_2 < H < G \). For a fixed primitive root \( \gamma \) modulo \( p \) and \( a \in \mathbb{F}_p^\times \), let \( \text{ind}_p(a) \) denote the unique \( i \in \mathbb{Z} \) such that \( a \equiv \gamma^i \pmod{p} \). Finally, for an ideal \( p \) of \( \mathcal{O}_K \), let \( o([p]) \) denote the order of the ideal class \([p]\) in the ideal class group \( C(K) \).

2. Introduction

Two main types of multiplicative relations exist between Gauss sums. The first is the norm relation. Connecting a Gauss sum and its complex conjugate, it states that for \( a \not\equiv 0 \pmod{e} \),

\[
\tau(a)\overline{\tau(a)} = \chi^a(-1)p,
\] or equivalently,

\[
\tau(a)\tau(-a) = \chi^a(-1)p.
\] (3)

The second type of relation is the Davenport–Hasse product formula for composite \( e \). It states that for \( e = mn \), with \( m, n > 1 \), and for \( 1 \leq t \leq m - 1 \),

\[
\chi^{tn}(n)\prod_{k=1}^{n-1} \frac{\tau(km+t)}{\tau(km)} = 1.
\] (4)

In [3, p. 465], H. Hasse conjectured that for fixed \( e \), all multiplicative relations connecting Gauss sums over \( \mathbb{F}_p \) could be derived from the norm relation and the Davenport–Hasse product formula. However, in 1966 K. Yamamoto, [9], provided a simple counterexample disproving the conjecture. This counterexample was a new type of multiplicative relation involving an ambiguous sign
not connected to elementary properties of Gauss sums. Shortly thereafter, working in the context of Jacobi sums, further sign ambiguities were discovered by Muskat, Muskat–Whiteman, and Muskat–Zee, [5–7]. While only nine sign ambiguities have been given explicitly, in [10], Yamamoto proved their existence for all composite $e$. Moreover, Yamamoto produced a formula giving the exact “number” of sign ambiguities to be expected in each case.

**Theorem 1.** (See Yamamoto [10].) For $e > 2$, there are exactly $2^{r-1} - 1$ multiplicatively independent Gauss sum relations that are not direct consequences of the norm relation and the Davenport–Hasse relations, where $r$ is the number of distinct prime divisors of $e$, or, if $e \equiv 2 \pmod{4}$, $r$ is the number of distinct prime divisors of $e/2$.

Thus, if $e$ is the product of two distinct odd primes, there is exactly one “missing” multiplicative relation. In this paper, we present a product formula which gives this “missing” sign ambiguity for an infinite class of such $e$’s. In particular, we prove the following:

**Main Theorem 1.** Let $q_1$, $q_2$ be primes with $q_1 \equiv 5 \pmod{8}$, $q_2 \equiv 3 \pmod{4}$, and $q_2$ a biquadratic residue modulo $q_1$. Let $e = q_1q_2$, $p$ be a prime, $p \equiv 1 \pmod{e}$, and $p$ be a prime ideal of $\mathcal{O}_{\mathbb{Q}(\sqrt{-e})}$ dividing $p$. Then, if $t_0$ is a quadratic nonresidue modulo $q_1$ and $q_2$, we have

$$\prod_{t \in H_4} \frac{\tau(t)}{\tau(t_0t)} = u\zeta^{-k_0},$$

(5)

where

$$k_0 \equiv \begin{cases} -q_1 \text{ind}_{\gamma}(q_1) \pmod{e}, & \text{if } e = q_1 \cdot 3, \\ 3(1 - t_0)q_2 \text{ind}_{\gamma}(q_2) \pmod{e}, & \text{if } e = 5 \cdot q_2, \\ 0 \pmod{e}, & \text{if } \gcd(e, 15) = 1, \end{cases}$$

and

$$u = \begin{cases} +1, & \text{if } o([p]) \equiv 1 \pmod{2}, \\ -1, & \text{if } o([p]) \equiv 0 \pmod{2}. \end{cases}$$

The proof of our main theorem is in three parts. We first show that the product formula holds when considered as an ideal relation. Splitting the quotient of Eq. (5) and factoring each ideal using the Stickelberger formula, the factorizations are shown to be identical by proving a result concerning biquadratic coset sums. This proves that the product formula is a multiplicative relation up to a unit of absolute value one. Secondly, we determine the unit up to sign, and finally we resolve the ambiguous sign via the order of the ideal class of $p$.

### 3. Biquadratic coset sums

For the remainder of the paper, we restrict our attention to values of $e$ as in Theorem 1, i.e. $e = q_1q_2$, with $q_1 \equiv 5 \pmod{8}$, $q_2 \equiv 3 \pmod{4}$, and $q_2$ a biquadratic residue modulo $q_1$. For any positive integer $n$ and for any $a \in \mathbb{Z}/n\mathbb{Z}$ or $a \in \mathbb{Z}$, let $L_n(a)$ denote the least positive integer congruent to $a$ modulo $n$. If $n = e$ we will suppress the subscript, i.e. $L = L_e$. 
Proof of our product formula as an ideal relation will depend on the evaluation of the eight biquadratic coset sums of $G/H_4$. For $i = 0, \ldots, 7$, let $c_i$ denote these cosets. Then the biquadratic coset sums are the integer sums

$$
\sum_{a \in c_i} L(a), \quad \text{for } i = 0, \ldots, 7.
$$

We now consider these sums.

**Proposition 2.** Let $e = q_1 q_2$ and $G$ be as stated. Then there is a $g \in G$ such that $G/H_4 = \{ \pm H_4, \pm g H_4, \pm g^2 H_4, \pm g^3 H_4 \}$.

**Proof.** Let $g_{q_1}$ and $g_{q_2}$ denote primitive roots modulo $q_1$ and $q_2$, respectively. Then

$$(\mathbb{Z}/e\mathbb{Z})^\times \cong (\mathbb{Z}/q_1\mathbb{Z})^\times \times (\mathbb{Z}/q_2\mathbb{Z})^\times \cong \langle g_{q_1} \rangle \times \langle g_{q_2} \rangle.$$

Let $\psi : \langle g_{q_1} \rangle \times \langle g_{q_2} \rangle \to (\mathbb{Z}/e\mathbb{Z})^\times$ be the isomorphism given by the Chinese Remainder Theorem. Now, $a \in H_4$ is a biquadratic residue, so $\psi^{-1}(a) = (g_{q_1}^\alpha, g_{q_2}^\beta)$ is a biquadratic residue. But $(g_{q_1}^\alpha, g_{q_2}^\beta)$ is a biquadratic residue if and only if each coordinate is. Since $q_1 \equiv 1 \pmod{4}$, $g_{q_1}^\alpha$ is a biquadratic residue if and only if $\alpha \equiv 0 \pmod{4}$, and as $q_2 \equiv 3 \pmod{4}$, the biquadratic residues modulo $q_2$ are exactly the quadratic residues, so $g_{q_2}^\beta$ is a biquadratic residue if and only if $\beta \equiv 0 \pmod{2}$. Hence, $H_4 \cong \langle g_{q_1}^4 \rangle \times \langle g_{q_2}^2 \rangle$, and

$$|H_4| = |\langle g_{q_1}^4 \rangle| \cdot |\langle g_{q_2}^2 \rangle| = \left( \frac{q_1 - 1}{4} \right) \left( \frac{q_2 - 1}{2} \right) = \frac{\phi(e)}{8}.$$

Let $g = \psi(g_{q_1}, g_{q_2})$ and consider $g H_4 \in G/H_4$. Computing powers of $g$, we see that $g^4 \in H_4$, but $g^i \notin H_4$ for $i = 1, 2, 3$. Thus $g H_4$ has order 4 in $G/H_4$. On the other hand, we see that $-g H_4$ also has order 4, but with powers distinct from those of $g H_4$. Therefore, since

$$|G/H_4| = \frac{\phi(e)}{\phi(e)/8} = 8,$$

we have that

$$G/H_4 = \{ \pm H_4, \pm g H_4, \pm g^2 H_4, \pm g^3 H_4 \}. \quad \Box$$

We will now prove three lemmas concerning the coset sums of $G/H_4$. We first prove that the coset sums $\sum_{a \in H_4} L(g^j a)$ are equal for $j = 0, \ldots, 3$. By symmetry, this will imply that the other four coset sums, $\sum_{a \in H_4} L(-g^j a)$, are equal to each other as well. We proceed in three lemmas.

**Lemma 3.** Let $e = q_1 q_2$, $G$, and $H_4$ be as above. Then

$$\sum_{a \in H_4} L(a) = \sum_{a \in H_4} L(g^2 a).$$
Proof. From Proposition 2, \(H_4 \cong \langle g_4^4 \rangle \times \langle g_4^2 \rangle\). Let \(T_4\) denote the biquadratic residues modulo \(q_1\) and \(N_2\) denote the quadratic residues modulo \(q_2\). Let \(a_1 \in \mathbb{Z}\) be such that \(a_1q_2 \equiv 1 \pmod{q_1}\) and \(a_2 \in \mathbb{Z}\) be such that \(a_2q_1 \equiv 1 \pmod{q_2}\). Then by the Chinese Remainder Theorem,

\[
L(H_4) = \left\{ L(ta_1q_2 + na_2q_1) \mid t \in L_{q_1}(T_4), \ n \in L_{q_2}(N_2) \right\}.
\]  

Setting \(\mathcal{H}_4 = L(H_4)\), \(T_4 = L_{q_1}(T_4)\), and \(N_2 = L_{q_2}(N_2)\), Eq. (6) becomes

\[
\mathcal{H}_4 = \left\{ L(ta_1q_2 + na_2q_1) \mid t \in T_4, \ n \in N_2 \right\}.
\]  

Combining and re-indexing, we have

\[
\mathcal{H}_4 = \left\{ L(tq_2 + nq_1) \mid t \in T_4, \ n \in N_2 \right\}
\]

and need only show that

\[
\sum_{t \in T_4} \sum_{n \in N_2} L(tq_2 + nq_1) = \sum_{t \in T_4} \sum_{n \in N_2} L(L(g^2)(tq_2 + nq_1)).
\]

Setting \(g_0 = L(g)\), for the second summand we then have

\[
L(g_0^2(tq_2 + nq_1)) = L((g_0^2t)q_2 + (g_0^2n)q_1) = \sum_{t' \in T_4} \sum_{n' \in N_2} L(-t'q_2 + n'q_1),
\]

for some \(t' \in T_4, n' \in N_2\), where the second equality follows since for any \(t \in T_4\), \(g_0^2t \equiv -t' \pmod{q_1}\), \(t' \in T_4\), so again re-indexing, we are reduced to showing that

\[
\sum_{t \in T_4} \sum_{n \in N_2} L(tq_2 + nq_1) = \sum_{t \in T_4} \sum_{n \in N_2} L(-tq_2 + nq_1). \tag{8}
\]

Since \(0 \leq t < q_1\) and \(0 \leq n < q_2\), we have that \(0 \leq tq_2 + nq_1 < 2e\), and thus

\[
L(tq_2 + nq_1) = \begin{cases} 
 tq_2 + nq_1, & \text{if } tq_2 + nq_1 < e, \\
 tq_2 + nq_1 - e, & \text{if } tq_2 + nq_1 > e.
\end{cases}
\]

For fixed \(t \in T_4\), \(tq_2 + nq_1 > e \iff n > \frac{q_1q_2 - tq_2}{q_1} \iff n > q_2 - \frac{tq_2}{q_1}\). Let \(k_t = \#\{n \in N_2 \mid n > q_2 - \frac{tq_2}{q_1}\}\).

Similarly, for the right summand of Eq. (8) we have that \(-e < -tq_2 + nq_1 < e\), and thus

\[
L(-tq_2 + nq_1) = \begin{cases} 
 -tq_2 + nq_1, & \text{if } -tq_2 + nq_1 > 0, \\
 -tq_2 + nq_1 + e, & \text{if } -tq_2 + nq_1 < 0.
\end{cases}
\]
Again fixing $t \in \mathcal{T}_4$, $-tq_2 + nq_1 < 0 \Leftrightarrow n < \frac{tq_2}{q_1}$. Let $l_t = \# \{ n \in \mathcal{N}_2 \mid n < \frac{tq_2}{q_1} \}$. Proof of the lemma is now reduced to proof of the equality of the integer sums

$$\sum_{t \in \mathcal{T}_4} \left( -ek_t + \sum_{n \in \mathcal{N}_2} tq_2 + nq_1 \right) = \sum_{t \in \mathcal{T}_4} \left( e(t + \sum_{n \in \mathcal{N}_2} -tq_2 + nq_1) \right).$$

Combining results,

$$\sum_{a \in \mathcal{H}_4} L(a) - \sum_{a \in \mathcal{H}_4} L(g^2a) = \sum_{t \in \mathcal{T}_4} \left( -ek_t + \sum_{n \in \mathcal{N}_2} tq_2 + nq_1 \right) - \sum_{t \in \mathcal{T}_4} \left( e(t + \sum_{n \in \mathcal{N}_2} -tq_2 + nq_1) \right)$$

$$= \sum_{t \in \mathcal{T}_4} \left( -e(k_t + l_t) + tq_2(2 - 1) \right).$$

and thus it is only necessary to determine $k_t + l_t$.

Now,

$$l_t = \# \{ n \in \mathcal{N}_2 \mid n < \frac{tq_2}{q_1} \} = \# \{ n \in \mathcal{N}_2 \mid q_2 - n > q_2 - \frac{tq_2}{q_1} \},$$

and since $n$ is a quadratic residue modulo $q_2$, $q_2 - n$ is also a nonresidue and $l_t$ is then equal to the number of quadratic nonresidues greater than $q_2 - \frac{tq_2}{q_1}$. But $k_t$ is the number of quadratic residues modulo $q_2$ greater than $q_2 - \frac{tq_2}{q_1}$, and since the sets of residues and nonresidues are disjoint, $k_t + l_t$ is the number of units modulo $q_2$ greater than $q_2 - \frac{tq_2}{q_1}$. Thus for each $t \in \mathcal{T}_4$, we have

$$k_t + l_t = q_2 - \left\lfloor q_2 - \frac{tq_2}{q_1} \right\rfloor = q_2 - q_2 + \left\lfloor \frac{tq_2}{q_1} \right\rfloor = \left\lfloor \frac{tq_2}{q_1} \right\rfloor.$$

But, since both $t$ and $q_2$ are biquadratic residues modulo $q_1$,

$$\left\lfloor \frac{tq_2}{q_1} \right\rfloor = \frac{tq_2}{q_1} - \frac{L_{q_1}(tq_2)}{q_1} = \frac{tq_2}{q_1} - \frac{t'}{q_1},$$

for some $t' \in \mathcal{T}_4$. Re-indexing and summing over $t$,

$$\sum_{t \in \mathcal{T}_4} \left\lfloor \frac{tq_2}{q_1} \right\rfloor = \sum_{t \in \mathcal{T}_4} \left( \frac{tq_2}{q_1} - \frac{t}{q_1} \right) = \sum_{t \in \mathcal{T}_4} \left( \frac{t(q_2 - 1)}{q_1} \right).$$

Therefore,
\[
\sum_{t \in T_4} (-e(k_t + l_t) + tq_2(q_2 - 1)) = \sum_{t \in T_4} \left( tq_2(q_2 - 1) - e \left\lfloor \frac{tq_2}{q_1} \right\rfloor \right)
\]

\[
=q_2(q_2 - 1) \sum_{t \in T_4} t - q_1q_2 \sum_{t \in T_4} \left( \frac{t(q_2 - 1)}{q_1} \right)
\]

\[
=q_2(q_2 - 1) \sum_{t \in T_4} t - q_2(q_2 - 1) \sum_{t \in T_4} t
\]

\[
= 0.
\]

Hence,

\[
\sum_{a \in H_4} L(a) = \sum_{a \in H_4} L(g^2 a),
\]

proving the lemma. □

**Lemma 4.** With notation as before,

\[
\sum_{a \in H_4} L(ga) = \sum_{a \in H_4} L(g^3 a).
\]

**Proof.** As in the previous lemma, for \(a \in H_4, a = L(tq_2 + nq_1)\) for some \(t \in T_4, n \in N_2\). Then,

\[
L(ga) = L(g_0(tq_2 + nq_1)) = L(g_0tq_2 - n'q_1) \quad \text{for some } n' \in N_2,
\]

since \(g_0\) is a nonsquare modulo \(q_2\) and \(q_2 \equiv 3 \pmod{4}\).

On the other hand,

\[
L(g^3 a) = L(g_0^3(tq_2 + nq_1))
\]

\[
= L(g_0(-t'q_2 + n'q_1))
\]

\[
= L((-g_0t')q_2 + (g_0n')q_1),
\]

where the second equality follows from the proof of the previous lemma. And again, since \(g_0\) is a quadratic nonresidue modulo \(q_2\), \(g_0n' = -n''\), for some \(n'' \in N_2\). Combining and re-indexing, we now need only show that

\[
\sum_{t \in T_4 \atop n \in N_2} L(g_0tq_2 - nq_1) = \sum_{t \in T_4 \atop n \in N_2} L(-g_0tq_2 - nq_1),
\]

or equivalently

\[
\sum_{t \in T_4 \atop n \in N_2} \left(\frac{(*)}{L(q_1(g_0t)q_2 - nq_1)}\right) = \sum_{t \in T_4 \atop n \in N_2} \left(\frac{(**)}{L(-q_1(g_0t)q_2 - nq_1)}\right).
\]
Now, \(-e < L_{q_1}(g_0 t)q_2 - nq_1 < e\), and thus

\[
(*) = \begin{cases} 
L_{q_1}(g_0 t)q_2 - nq_1, & \text{if } L_{q_1}(g_0 t)q_2 - nq_1 > 0, \\
L_{q_1}(g_0 t)q_2 - nq_1 + e, & \text{if } L_{q_1}(g_0 t)q_2 - nq_1 < 0.
\end{cases}
\]

For fixed \(t \in T_4\),

\[
L_{q_1}(g_0 t)q_2 - nq_1 < 0 \iff n > \frac{L_{q_1}(g_0 t)q_2}{q_1}.
\]

Let \(k_t = \#\{n \in \mathbb{N}_2 \mid n > \frac{L_{q_1}(g_0 t)q_2}{q_1}\}\).

For the right summand, \(-2e < -L_{q_1}(g_0 t)q_2 - nq_1 < 0\), and thus

\[
(**) = \begin{cases} 
-L_{q_1}(g_0 t)q_2 - nq_1 + e, & \text{if } -L_{q_1}(g_0 t)q_2 - nq_1 > -e, \\
-L_{q_1}(g_0 t)q_2 - nq_1 + 2e, & \text{if } -L_{q_1}(g_0 t)q_2 - nq_1 < -e.
\end{cases}
\]

For fixed \(t \in T_4\),

\[
-L_{q_1}(g_0 t)q_2 - nq_1 < -e \iff L_{q_1}(g_0 t)q_2 + nq_1 > e \\
\iff n > \frac{q_2(q_1 - L_{q_1}(g_0 t))}{q_1} \\
\iff q_2 - n < q_2 - \frac{q_2(q_1 - L_{q_1}(g_0 t))}{q_1} \\
\iff q_2 - n < \frac{L_{q_1}(g_0 t)q_2}{q_1}.
\]

Letting \(l_t = \#\{n \in \mathbb{N}_2 \mid q_2 - n < \frac{L_{q_1}(g_0 t)q_2}{q_1}\}\), we again need only show equality of the integer sums

\[
\sum_{t \in T_4} \left( e(k_t - l_t) + \sum_{n \in \mathbb{N}_2} L_{q_1}(g_0 t)q_2 - nq_1 \right) = \sum_{t \in T_4} \left( el_t + \sum_{n \in \mathbb{N}_2} -L_{q_1}(g_0 t)q_2 - nq_1 + e \right).
\]

Combining and simplifying, we have

\[
\sum_{a \in H_4} L(ga) - \sum_{a \in H_4} L(g^3a) \\
= \sum_{t \in T_4} \left( e(k_t - l_t) + \sum_{n \in \mathbb{N}_2} (2L_{q_1}(g_0 t)q_2 - e) \right) \\
= e \sum_{t \in T_4} (k_t - l_t) + \sum_{t \in T_4} 2L_{q_1}(g_0 t)q_2 - \sum_{t \in T_4} e \\
= e \sum_{t \in T_4} (k_t - l_t) + 2q_2 \left( \frac{q_2 - 1}{2} \right) \sum_{t \in T_4} L_{q_1}(g_0 t) - e \left( \frac{q_1 - 1}{4} \right) \left( \frac{q_2 - 1}{2} \right) \\
= e \sum_{t \in T_4} (k_t - l_t) + q_2(q_2 - 1) \sum_{t \in T_4} L_{q_1}(g_0 t) - e \frac{\phi(e)}{8}.
\]
But \( n \in \mathbb{N}_2 \Rightarrow q_2 - n \notin \mathbb{N}_2 \), so \( l_t \) is the number of nonsquares modulo \( q_2 \) less than \( \frac{L_{q_1}(g_0 t)q_2}{q_1} \). Thus, the number of squares less than \( \frac{L_{q_1}(g_0 t)q_2}{q_1} \) is given by \( \left\lfloor \frac{L_{q_1}(g_0 t)q_2}{q_1} \right\rfloor - l_t \). And since there are exactly \( \frac{q_2^2 - 1}{2} \) squares modulo \( q_2 \), the number of squares modulo \( q_2 \) greater than \( \frac{L_{q_1}(g_0 t)q_2}{q_1} \) is given by

\[
\frac{q_2^2 - 1}{2} - \left( \left\lfloor \frac{L_{q_1}(g_0 t)q_2}{q_1} \right\rfloor - l_t \right) = k_t.
\]

Hence, for each \( t \), \( k_t - l_t = \frac{q_2^2 - 1}{2} - \left\lfloor \frac{L_{q_1}(g_0 t)q_2}{q_1} \right\rfloor \), and as in Eq. (9),

\[
\sum_{t \in T_4} \left\lfloor \frac{L_{q_1}(g_0 t)q_2}{q_1} \right\rfloor = \sum_{t \in T_4} \left( \frac{L_{q_1}(g_0 t)(q_2 - 1)}{q_1} \right).
\]

Therefore,

\[
e \sum_{t \in T_4} (k_t - l_t) + q_2(q_2 - 1) \sum_{t \in T_4} L_{q_1}(g_0 t) - \frac{e \phi(e)}{8}
\]

\[
= e \sum_{t \in T_4} \left( \frac{q_2 - 1}{2} - \left\lfloor \frac{L_{q_1}(g_0 t)q_2}{q_1} \right\rfloor \right) + q_2(q_2 - 1) \sum_{t \in T_4} L_{q_1}(g_0 t) - \frac{e \phi(e)}{8}
\]

\[
= e \frac{\phi(e)}{8} - e \sum_{t \in T_4} \frac{L_{q_1}(g_0 t)(q_2 - 1)}{q_1} + q_2(q_2 - 1) \sum_{t \in T_4} L_{q_1}(g_0 t) - \frac{e \phi(e)}{8}
\]

\[
= e \frac{\phi(e)}{8} - q_2(q_2 - 1) \sum_{t \in T_4} L_{q_1}(g_0 t) + q_2(q_2 - 1) \sum_{t \in T_4} L_{q_1}(g_0 t) - \frac{e \phi(e)}{8}
\]

\[
= 0,
\]

and thus

\[
\sum_{a \in H_4} L(a) = \sum_{a \in H_4} L(g^3 a). \quad \square
\]

**Lemma 5.** With notation as before,

\[
\sum_{a \in H_4} L(a) + \sum_{a \in H_4} L(g^2 a) = \sum_{a \in H_4} L(ga) + \sum_{a \in H_4} L(g^3 a).
\]

**Proof.** Recall that \( H_2 \) denotes the quadratic residues modulo \( e \). Then, since the elements of the cosets \( H_4 \) and \( g^2 H_4 \) partition \( H_2 \), we have that

\[
\sum_{a \in H_4} L(a) + \sum_{a \in H_4} L(g^2 a) = \sum_{a \in H_2} L(a)
\]
and
\[ \sum_{a \in H_1} L(ga) + \sum_{a \in H_4} L(g^3a) = \sum_{a \in H_2} L(ga). \]

Hence, we need only show
\[ \sum_{a \in H_2} L(a) = \sum_{a \in H_2} L(ga). \]

From the proof of Proposition 2, we have that \( H_2 \cong (g_{q_1}^2) \times (g_{q_2}^2). \) Thus, if \( T_2 \) denotes the quadratic residues modulo \( q_1 \) and \( T_2 = L_{q_1}(T_2) \), then we must show that
\[ \sum_{t \in T_2, n \in \mathbb{N}_2} L(tq_2 + nq_1) = \sum_{t \in T_2, n \in \mathbb{N}_2} L(g_0(tq_2 + nq_1)). \]

Once more, since \( g_0 \notin \mathbb{N}_2 \),
\[ L(g_0(tq_2 + nq_1)) = L(g_0tq_2 + (g_0n)q_1) = L(g_0tq_2 - n'q_1), \]
and upon re-indexing we need only prove that
\[ \sum_{t \in T_2, n \in \mathbb{N}_2} L(tq_2 + nq_1) = \sum_{t \in T_2, n \in \mathbb{N}_2} L(g_0tq_2 - nq_1). \]

We proceed as in the previous two lemmas. For the left summand, we have \( 0 < L(tq_2 + nq_1) < 2e \), and thus
\[ L(tq_2 + nq_1) = \begin{cases} tq_2 + nq_1, & \text{if } tq_2 + nq_1 < e, \\ tq_2 + nq_1 - e, & \text{if } tq_2 + nq_1 > e. \end{cases} \]

Fixing \( n \in \mathbb{N}_2 \),
\[ tq_2 + nq_1 > e \iff t > q_1 - \frac{nq_1}{q_2} \iff q_1 - t < \frac{nq_1}{q_2}. \]

Let \( k_n = \# \{ t \in T_2 \mid q_1 - t < \frac{nq_1}{q_2} \}. \)

For the right summand, since \( L(g_0tq_2 - nq_1) = L(L_{q_1}(g_0t)q_2 - nq_1) \) and \( \mathbb{R} < L_{q_1}(g_0t)q_2 - nq_1 < e \),
\[ L(g_0tq_2 - nq_1) = \begin{cases} L_{q_1}(g_0t)q_2 - nq_1, & \text{if } L_{q_1}(g_0t)q_2 - nq_1 > 0, \\ L_{q_1}(g_0t)q_2 - nq_1 + e, & \text{if } L_{q_1}(g_0t)q_2 - nq_1 < 0. \end{cases} \]

Fixing \( n \in \mathbb{N}_2 \),
\[ L_{q_1}(g_0t)q_2 - nq_1 < 0 \iff L_{q_1}(g_0t) < \frac{nq_1}{q_2}. \]
Let \( l_n = \#\{t \in T_2 \mid L_{q_1}(g_0t) < \frac{nq_1}{q_2}\} \). Then we are again reduced to proving the equality of the integer sums

\[
\sum_{n \in \mathbb{N}_2} \left( -ek_n + \sum_{t \in T_2} tq_2 + nq_1 \right) = \sum_{n \in \mathbb{N}_2} \left( el_n + \sum_{t \in T_2} L_{q_1}(g_0t)q_2 - nq_1 \right).
\]

Now,

\[
\sum_{a \in H_2} L(a) - \sum_{a \in H_2} L(ga)
\]

\[
= \sum_{n \in \mathbb{N}_2} \left( -ek_n + \sum_{t \in T_2} tq_2 + nq_1 \right) - \sum_{n \in \mathbb{N}_2} \left( el_n + \sum_{t \in T_2} L_{q_1}(g_0t)q_2 - nq_1 \right)
\]

\[
= \sum_{n \in \mathbb{N}_2} \left( -e(k_n + l_n) + \sum_{t \in T_2} tq_2 + nq_1 - L_{q_1}(g_0t)q_2 + nq_1 \right)
\]

\[
= -e \sum_{t \in T_2} (k_n + l_n) + q_2 \left( \sum_{t \in T_2} \sum_{n \in \mathbb{N}_2} t - \sum_{n \in \mathbb{N}_2} \sum_{t \in T_2} L_{q_1}(g_0t) \right) + 2q_1 \sum_{n \in \mathbb{N}_2} n.
\]

It is well known that for primes congruent to 1 modulo 4, the sum of the squares is equal to the sum of the nonsquares, [4, Theorem 2.1]. Thus, since \( q_1 \equiv 1 \pmod{4} \), \( t \in T_2 \), and \( L_{q_1}(g_0t) \notin T_2 \), the middle two terms of the previous expression cancel, leaving only

\[
-e \sum_{t \in T_2} (k_n + l_n) + 2q_1 \sum_{n \in \mathbb{N}_2} n.
\]

Fixing \( n \in \mathbb{N}_2 \), \( k_n + l_n \) will be the number of units modulo \( q_1 \) less than \( \frac{nq_1}{q_2} \). So, for the first summation of (10), we have

\[
-e \sum_{n \in \mathbb{N}_2} (k_n + l_n) = -e \sum_{n \in \mathbb{N}_2} \left\lfloor \frac{nq_1}{q_2} \right\rfloor,
\]

leaving it necessary to prove only that

\[
-e \sum_{n \in \mathbb{N}_2} \left\lfloor \frac{nq_1}{q_2} \right\rfloor + 2q_1 \sum_{n \in \mathbb{N}_2} n = 0.
\]

Applying an argument similar to that leading up to Eq. (9),

\[
\sum_{n \in \mathbb{N}_2} \left\lfloor \frac{nq_1}{q_2} \right\rfloor = \sum_{n \in \mathbb{N}_2} \left( \frac{n(q_1 - 1)}{q_2} \right),
\]

and thus,
\[ -e \sum_{n \in \mathbb{N}_2} \left\lfloor \frac{nq_1}{q_2} \right\rfloor + 2q_1 \sum_{t \in \mathbb{Z}_2} n = 2q_1 \sum_{t \in \mathbb{Z}_2} n - e \sum_{n \in \mathbb{N}_2} \left\lfloor \frac{nq_1}{q_2} \right\rfloor + 2q_1 \sum_{t \in \mathbb{T}_2} n \]

\[ = q_1(q_1 - 1) \sum_{n \in \mathbb{N}_2} n - q_1q_2 \sum_{n \in \mathbb{N}_2} \left( \frac{n(q_1 - 1)}{q_2} \right) \]

\[ = q_1(q_1 - 1) \sum_{n \in \mathbb{N}_2} n - q_1(q_1 - 1) \sum_{n \in \mathbb{N}_2} n \]

\[ = 0. \]

Hence,

\[ \sum_{a \in H_4} L(a) + \sum_{a \in H_4} L(g^2a) = \sum_{a \in H_4} L(ga) + \sum_{a \in H_4} L(g^3a). \]

Combining the results from this section, we can now prove the following.

**Theorem 6.** For \( i = 0, 1, 2, 3 \), the coset sums \( \sum_{a \in H_4} L(g^i a) \) are equal, the coset sums \( \sum_{a \in H_4} L(-g^i a) \) are equal, and

\[ (1) \quad \sum_{a \in H_4} L(g^i a) < \sum_{a \in H_4} L(-g^i a), \quad \forall i. \]

Furthermore, for all \( i \),

\[ (2) \quad \sum_{a \in H_4} L(-g^i a) - \sum_{a \in H_4} L(g^i a) = \frac{h_K}{4} e, \]

where \( h_K \) denotes the class number of \( K = \mathbb{Q}(\sqrt{-e}) \).

**Proof.** By Lemmas 3–5, we have

\[ \sum_{a \in H_4} L(a) = \sum_{a \in H_4} L(g^1a) = \sum_{a \in H_4} L(g^2a) = \sum_{a \in H_4} L(g^3a). \]

But, for \( i = 0, \ldots, 3 \),

\[ \sum_{a \in H_4} L(g^i a) + L(-g^i a) = \sum_{a \in H_4} e = e \frac{\phi(e)}{8}, \]

and so

\[ \sum_{a \in H_4} L(-g^i a) = e \frac{\phi(e)}{8} - \sum_{a \in H_4} L(g^i a). \quad (11) \]

Therefore, since the \( \sum L(g^i a) \) are all equal, it must be that the \( \sum L(-g^i a) \) are equal as well.
By Dirichlet’s class number formula for imaginary quadratic fields, we have that

\[ eh_K = \sum_{a \in H} L(-a) - \sum_{a \in H} L(a). \]

But for \( i = 0, 1, 2, 3 \) the cosets \( g^i H_4 \) partition \( H \), so

\[ eh_K = \sum_{a \in H} L(-a) - \sum_{a \in H} L(a) = 4 \left( \sum_{a \in H_4} L(-g^i a) - \sum_{a \in H_4} L(g^i a) \right), \quad \forall i, \]

proving (2). And, since both \( e \) and \( h_K \) are positive, we have (1), completing the proof.

**Corollary 7.**

(1) *For* \( i = 0, 1, 2, 3 *,

\[ \sum_{a \in H_4} L(g^i a) \equiv \sum_{a \in H_4} L(-g^i a) \equiv 0 \pmod{e}. \]

(2) \( h_K \equiv 4 \pmod{8} \).

**Proof.** Combining Theorem 6(2) and Eq. (11), result (1) follows. Reducing Eq. (11) modulo 2 and reordering, we have \( \sum_{a \in H_4} L(-g^i a) - \sum_{a \in H_4} L(g^i a) \equiv 1 \pmod{2} \), for all \( i \). Thus, comparing with Theorem 6(2), we conclude that \( h_K \equiv 4 \pmod{8} \), completing the proof.

4. A product formula

Splitting the quotient in the product formula of our main theorem, we wish to prove

\[ \prod_{t \in H_4} \tau(t) = u \zeta_e^{-k_0} \prod_{t \in H_4} \tau(t_0 t); \quad (12) \]

or equivalently, letting \( \omega = \prod_{t \in H_4} \tau(t) \),

\[ \sigma_{t_0} (\omega) = \pm \zeta^2 \omega. \quad (13) \]
Let \( E = \mathbb{Q}(\zeta_{ep}) \), \( M = \mathbb{Q}(\zeta_e) \), and \( \hat{K} = (H_4)' \), the fixed field of \( H_4 \). Then \( G = (\mathbb{Z}/e\mathbb{Z})^\times \cong \text{Gal}(M/\mathbb{Q}) \) and we have the following field diagram with corresponding Galois groups over \( \mathbb{Q} \):

\[
\begin{array}{c}
\mathbb{Q}(\zeta_{ep}) = E & \xrightarrow{p-1} & G \times (\mathbb{Z}/p\mathbb{Z})^\times \\
\mathbb{Q}(\zeta_e) = M & \xrightarrow{\varphi(e)/8} & G \\
(H_4)' = \hat{K} & \xrightarrow{2} & G/H_4 \\
\mathbb{Q}(\sqrt{-e}, \sqrt{q_1}) = \hat{K} & \xrightarrow{2} & G/H_2 \\
\mathbb{Q}(\sqrt{-e}) = K & \xrightarrow{2} & G/H \\
\mathbb{Q} & \xrightarrow{r} & \{1\}.
\end{array}
\]

Using the results concerning the biquadratic coset sums from the previous section, we now show that \( \omega \in \hat{K} \) and that \( \omega \mathcal{O}_E \) and \( (\sigma_{0}(\omega))\mathcal{O}_E \) factor identically over \( \mathcal{O}_K \), proving Eq. (13) as an ideal relation. Then, using a result of Yamamoto from [10], we conclude that Eq. (13) is indeed a sign ambiguity.

**Lemma 8.** If \( X = \{a_i\}_{i=1}^r \) is a subset of the integers modulo \( e \) such that \( \sum_i a_i \equiv 0 \) (mod \( e \)), then

\[
\prod_{i=1}^r \tau(a_i) \in \mathbb{Q}(\zeta_e).
\]

**Proof.** Let \( c \in \mathbb{Z}/e\mathbb{Z} \) and consider the Jacobi sum product

\[
J(a_1, c)J(a_2, a_1 + c)J(a_3, a_1 + a_2 + c) \cdots J(a_r, a_1 + a_2 + \cdots + a_{r-1} + c).
\]

Using Eq. (2) to express each Jacobi sum as a quotient of Gauss sums, we then have

\[
(*) = \frac{\tau(a_1)\tau(c)}{\tau(a_1 + c)} \cdot \frac{\tau(a_2)\tau(a_1 + c)}{\tau(a_1 + a_2 + c)} \cdots \frac{\tau(a_r)\tau(a_1 + a_2 + \cdots + a_{r-1} + c)}{\tau(a_1 + a_2 + \cdots + a_r + c)}
\]

\[
= \frac{\tau(c)\tau(a_1)\tau(a_2) \cdots \tau(a_r)}{\tau(a_1 + a_2 + \cdots + a_r + c)} = \frac{\tau(a_1)\tau(a_2) \cdots \tau(a_r)}{\tau(a_1 + a_2 + \cdots + a_r + c)}, \text{ since } a_1 + a_2 + \cdots + a_r \equiv 0 \text{ (mod } e).)
\]

But for any \( \alpha, \beta \in \mathbb{Z} \), \( J(\alpha, \beta) \in \mathbb{Q}(\zeta_e) \Rightarrow (*) \in \mathbb{Q}(\zeta_e) \Rightarrow \prod_{i=1}^r \tau(a_i) \in \mathbb{Q}(\zeta_e). \square
Proposition 9. \( \omega \in \hat{K} \).

**Proof.** By Corollary 7, \( \sum_{a \in H_4} L(a) \equiv 0 \pmod{e} \), so \( \omega \in \mathbb{Q}(\zeta_e) \) by the lemma. Furthermore, \( \forall j \in H_4 \), \( \sigma_j \) will only permute the Gauss sums comprising \( \omega \). Thus, \( \omega \) is fixed by every automorphism from \( H_4 \), that is, \( \omega \in (H_4)' = \hat{K} \). \( \square \)

Theorem 10.

\[ \omega \mathcal{O}_M = \left( p^\alpha p^{\frac{h_K}{2}} \right) \mathcal{O}_M, \]

where \( \alpha = \sum_{t \in H_4} L(t) \) and \( p \) is a prime ideal of \( \mathcal{O}_K \) dividing \( p \).

**Proof.** Let \( p \) be a prime, \( p \equiv 1 \pmod{e} \), and let \( P \) be a prime ideal of \( \mathcal{O}_M \) dividing \( p \). Then by the Stickelberger relation, see [1], we have

\[ \omega \mathcal{O}_M = \left( \prod_{t \in H_4} \tau(t) \right) \mathcal{O}_M = \prod_{t \in H_4} p^{\sum_{a \in G} \left( \frac{L(ta^{-1})}{e} \right) \sigma_a} = p^{\sum_{t \in H_4} \left( \sum_{a \in G} \left( \frac{L(ta^{-1})}{e} \right) \sigma_a \right)} = p^{\sum_{a \in G} \left( \sum_{t \in H_4} \left( \frac{L(ta^{-1})}{e} \right) \sigma_a \right)}. \]

For \( a \in G/H_4 \),

\[ \sum_{t \in H_4} \left\{ \frac{ta^{-1}}{e} \right\} = \frac{1}{e} \sum_{t \in H_4} L(ta^{-1}). \]

But, by Theorem 6, there are only two possibilities for \( \sum_{t \in H_4} L(ta^{-1}) \). If \( ta^{-1} \in g^i H_4 \), for some \( i \), then \( \sum_{t \in H_4} L(ta^{-1}) = \sum_{t \in H_4} L(t) \). Let \( \alpha = \sum_{t \in H_4} L(t) \). If, on the other hand, \( ta^{-1} \in -g^i H_4 \), for some \( i \), then \( \sum_{t \in H_4} L(ta^{-1}) = \sum_{t \in H_4} L(-t) \). Let \( \beta = \sum_{t \in H_4} L(-t) \) and recall from Theorem 6 that \( \alpha < \beta \). But \( ta^{-1} \in g^i H_4 \iff a \in H \), so we have

\[ \omega \mathcal{O}_M = p^{\sum_{a \in G} \left( \sum_{t \in H_4} \left( \frac{L(ta^{-1})}{e} \right) \sigma_a \right)} = p^\alpha p^{\beta - \alpha} \sum_{a \notin H} \sigma_a = p^\alpha p^{\frac{h_K}{2}} \sum_{a \notin H} \sigma_a = p^\alpha \left( p^{\frac{h_K}{2}} \right) \sum_{a \notin H} \sigma_a = p^\alpha \left( p^{\frac{h_K}{2}} \right). \]
For \( a \in G \), consider \( (\sigma_a)|_K \). Since \( \text{Gal}(K/Q) \cong G/H \), \( (\sigma_a)|_K \) is nontrivial if and only if \( a \notin H \). Thus, if \( pO_K = p_1p_2 \), then
\[
p_1O_M = \prod_{a \in H} P^\sigma_a = P^{\sum_{a \in H} \sigma_a} \quad \text{and} \quad p_2O_M = \prod_{a \notin H} P^\sigma_a = P^{\sum_{a \notin H} \sigma_a}.
\]
Therefore, continuing (14),
\[
\omega O_M = p^a \left( P^{\sum_{a \in H} \sigma_a} \right)^{\frac{hK}{h}} = p^a (p_2O_M)^{\frac{hK}{h}} = p^a p_2^{\frac{hK}{h}} O_M. \quad \Box
\]

**Corollary 11.** \( \forall t \in H \), \( (\sigma_t(\omega))O_M = \omega O_M \).

**Proof.** Let \( t \in H \). Then,
\[
(\sigma_t(\omega))O_M = \sigma_t(\omega O_M) = p^a (\sigma_t(p))^\frac{hK}{h} O_M = (p^a p_2^{\frac{hK}{h}})O_M,
\]
since \( p \subseteq O_K \) and \( K \) is the fixed field of \( H \). \( \Box \)

**Remark 12.** Since \( \omega \) and \( \sigma_t(\omega) \) generate the same ideal in \( O_M \) and have the same absolute value, it follows that they can only differ by a unit of absolute value 1. But the only units of absolute value 1 in \( Q(\zeta_e) \) are \( \pm \zeta_e^k \), \( k = 1, \ldots, e \), [8], so we have that
\[
\sigma_t(\omega) = \pm \zeta_e^k \omega, \quad \text{for some} \ k \in \mathbb{Z}. \quad (15)
\]

Fix \( t_0 \in H \setminus H_2 \). Then \( \sigma_{t_0}(\omega) = \pm \zeta_e^{k_0} \omega \). We now determine \( k_0 \) explicitly.

**Theorem 13.**
\[
k_0 = \begin{cases} 
-q_1 \text{ ind}_{\mathbb{Z}}(q_1) \pmod{e}, & \text{if} \ e = q_1 \cdot 3, \\
3(1 - t_0)q_2 \text{ ind}_{\mathbb{Z}}(q_2) \pmod{e}, & \text{if} \ e = 5 \cdot q_2, \\
0 \pmod{e}, & \text{if} \ \gcd(e, 15) = 1.
\end{cases} \quad (16)
\]

**Proof.** As \( \omega, \sigma_{t_0}(\omega) \in \hat{K} \), we must have that \( \zeta_e^{k_0} \in \hat{K} \) as well. We first determine which roots of unity lie in \( \hat{K} \). Assume \( \zeta_n \in \hat{K} \) for some integer \( n > 2 \). Since \( \hat{K} \subseteq Q(\zeta_e) \), \( n \mid 2e \), and thus either \( n = q_1 \) or \( n = q_2 \) (note that \( Q(\zeta_{2q_1}) = Q(\zeta_{q_2}) \)). Furthermore, since \( [\hat{K} : Q] = 8, \phi(n) \mid 8 \). But the only odd primes \( n \) with \( \phi(n) \mid 8 \) are \( n = 3, 5 \). Hence, if \( \gcd(e, 15) = 1 \), then the only roots of unity in \( \hat{K} \) are \( \pm 1 \) and \( \sigma_{t_0}(\omega) = \pm \omega \), i.e., \( k_0 \equiv 0 \pmod{e} \). If \( e = q_1 \cdot 3 \), then powers of \( \pm \zeta_3 = \pm \zeta_e^{q_1} \) are the only possible roots of unity in \( \hat{K} \) and thus, \( k_0 \equiv 0 \pmod{q_1} \). Finally, if \( e = 5 \cdot q_2 \), then the only possible roots of unity in \( \hat{K} \) are powers of \( \pm \zeta_3 = \pm \zeta_e^{q_2} \) and \( k_0 \equiv 0 \pmod{q_2} \).

Assume \( e = q_1 \cdot 3 \). Using Eq. (4) with \( m = 3, n = q_1 \), and \( t = 2 \), we obtain the following Davenport–Hasse relation
\[
\chi_q^{q_1}(q_1) \prod_{k=0}^{q_1-1} \tau(3k + 2) = \tau(q_1) \prod_{k=1}^{q_1-1} \tau(3k). 
\]
Referring to Proposition 2, this relation can be rewritten as

$$\sigma_{t_0}(\omega) = \chi^{-2q_1(q_1)} \frac{\prod_{k=1}^{q_1-1} \tau(3k)}{\sigma_{l_0}^{2}(\omega)\sigma_{-l_0}^{2}(\omega)\sigma_{-1}(\omega)}.$$ 

Substituting this relation into $\sigma_{t_0}(\omega) = \pm \zeta e^{k_0}\omega$ and using the norm relation to reduce, we then have

$$\frac{p^{(q_1-1)/2}}{\sigma_{l_0}^{2}(\omega)\sigma_{-l_0}^{2}(\omega)} = \pm \zeta e^{k_0}\chi^{-2q_1(q_1)}.$$ 

Multiplying numerator and denominator by $\sigma_{-l_0}^{2}(\omega)$ and again using the norm relation, we obtain

$$\frac{\sigma_{-l_0}^{2}(\omega)}{\sigma_{-l_0}^{2}(\omega)} = \sigma_{-l_0}^{2} \left( \frac{\sigma_{t_0}(\omega)}{\omega} \right) = \pm \zeta e^{k_0}\chi^{-2q_1(q_1)}.$$ 

Substituting $\sigma_{t_0}(\omega)/\omega = \pm \zeta e^{k_0}$, the above reduces to $\zeta e^{-t_0^{2}k_0} = \zeta e^{k_0}\chi^{-2q_1(q_1)}$, and hence $\zeta e^{-k_0(t_0^2+1)} = \chi^{-2q_1(q_1)}$. Now, $\chi(q'') = \zeta$, so $\chi^{-2q_1(q_1)} = \chi^{2q_1(q_1)}(\gamma_{ind_{r}}(q_1)) = \zeta e^{2q_1(q_1)}$, and therefore $\zeta e^{-k_0(t_0^2+1)} = \zeta e^{2q_1(q_1)}$. But, as $k_0 \equiv 0 \pmod{q_1}$, we have

$$-k_0(t_0^2 + 1) \equiv 2q_1 ind_{r}(q_1) \pmod{q_1 \cdot 3}$$

$$\iff -k_0(t_0^2 + 1) \equiv 2q_1 ind_{r}(q_1) \pmod{3}$$

$$\iff k_0 \equiv -q_1 ind_{r}(q_1) \pmod{3}.$$ 

Hence, $k_0 \equiv -q_1 ind_{r}(q_1) \pmod{q_1 \cdot 3}$.

Now assume $e = 5 \cdot q_2$. We proceed as in the previous case. Applying Eq. (4) with $m = 5$, $n = q_2$, for $t = 1$ and $t \equiv t_0 \pmod{5}$, to $\sigma_{t_0}(\omega) = \pm \zeta e^{k_0}\omega$, we obtain

$$\sigma_{-l_0}^{2} \left( \frac{\sigma_{t_0}(\omega)}{\omega} \right) = \pm \zeta e^{-k_0}\chi^{q_2(1-t_0)}(q_2).$$ 

Substituting $\sigma_{t_0}(\omega)/\omega = \pm \zeta e^{k_0}$ and recalling that $k_0 \equiv 0 \pmod{q_2}$, we have

$$\zeta e^{-t_0^{2}k_0} = \zeta e^{-k_0+q_2(1-t_0) ind_{r}(q_2)} \iff \zeta e^{k_0(1-t_0^{2})} = \zeta e^{q_2(1-t_0) ind_{r}(q_2)}$$

$$\iff k_0(1 - t_0^{2}) \equiv q_2(1 - t_0) ind_{r}(q_2) \pmod{5q_2}$$

$$\iff k_0(1 - t_0^{2}) \equiv q_2(1 - t_0) ind_{r}(q_2) \pmod{5}$$

$$\iff k_0 \equiv 3(1 - t_0)q_2 ind_{r}(q_2) \pmod{5}.$$ 

Therefore, $k_0 \equiv 3(1 - t_0)q_2 ind_{r}(q_2) \pmod{5q_2}$, completing the proof. \qed
We claim that $\sigma t (\omega) = \pm \zeta k \omega$ is a sign ambiguity. We will need the following weakened version of a result in [10].

**Lemma 14.** Let $e = p_1 p_2$, for any primes $p_1, p_2$. Assume

$$\prod_i \tau(a_i) = \pm \zeta^k \prod_j \tau(b_j)$$

(17)

for some $a_i, b_j, k \in \mathbb{Z}$, and let $\Lambda = \{L(p_1 + p_2), L(p_1 - p_2), L(p_2 - p_1), L(-p_1 - p_2)\}$. If $\# \{i \mid a_i \in \Lambda\} - \# \{j \mid b_j \in \Lambda\} \equiv 1 \pmod{2}$, then Eq. (17) is not a direct consequence of the norm relation and the Davenport–Hasse product formula.

We are now able to prove a partial version of our main theorem. In the next section, we complete the proof with resolution of the sign ambiguity.

**Theorem 15.** Let $e = q_1 q_2$ with $q_1 \equiv 5 \pmod{8}$, $q_2 \equiv 3 \pmod{4}$, and $q_2$ a biquadratic residue modulo $q_1$. Let $p$ be prime, $p \equiv 1 \pmod{e}$. Let $H_4$ be the group of biquadratic residues modulo $e$ and let $t_0$ be a quadratic nonresidue modulo $q_1$ and $q_2$, i.e. $t_0 \in H \setminus H_2$. Then

$$\prod_{t \in H_4} \frac{\tau(t)}{\tau(t_0 t)} = \pm \zeta^{-k_0}$$

(18)

is a sign ambiguity, where $k_0$ is as in Theorem 13.

**Proof.** Rewriting (18), we want to show that

$$\omega \prod_{t \in H_4} \tau(t) = \pm \zeta^{-k_0} \prod_{t \in H_4} \sigma t (\omega)$$

(19)

is a sign ambiguity. By Remark 12, we have that $\sigma t (\omega) = \pm \zeta^k \omega$, so we need only verify that (19) does not follow from the norm relation or Davenport–Hasse.

As in Lemma 14, let $\Lambda = \{L(\pm q_1 \pm q_2)\}$. Let $a \in H_4$. Then $a = t q_2 + n q_1$, for some $t \in T_4$, $n \in N_2$ and we have

$$a \in \Lambda \iff t \equiv \pm 1 \pmod{q_1} \text{ and } n \equiv \pm 1 \pmod{q_2}.$$  

But $n$ is square modulo $q_2$ and since $q_2 \equiv 3 \pmod{4}$, $-1$ is a nonsquare. Therefore, $n \not\equiv -1 \pmod{q_2}$. Furthermore, $1 \in T_4 \Rightarrow -1 \not\in T_4$, and thus

$$a \in \Lambda \iff t \equiv 1 \pmod{q_1} \text{ and } n \equiv 1 \pmod{q_2}.$$  

For $a \in H_4$, consider $t_0 a = t_0 (t q_2 + n q_1) = (t_0 t) q_2 + (t_0 n) q_1$. We have

$$t_0 a \in \Lambda \iff t_0 t \equiv \pm 1 \pmod{q_1} \text{ and } t_0 n \equiv \pm 1 \pmod{q_2}.$$
But for \( t \in T_4 \), \( t_0t \) is a nonsquare and \( \pm 1 \) are both squares, so \( t_0a \not\equiv \pm 1 \) (mod \( q_1 \)). Therefore \( t_0a \not\in \Lambda \), \( \forall a \in H_4 \). Combining these results, we have that

\[
\#\{a \in H_4 \mid a \in \Lambda \} - \#\{a \in H_4 \mid t_0a \in \Lambda \} = 1 - 0 \equiv 1 \pmod{2},
\]

which, by the lemma, implies that (18) does not follow from Davenport–Hasse and the norm relation. Hence,

\[
\prod_{t \in H_4} \frac{\tau(t)}{\tau(t_0t)} = \pm \xi^{-k_0}
\]

is a sign ambiguity. \( \square \)

**Remark 16.** We remark that this product formula does, indeed, give an infinite set of new sign ambiguities. From the statement of the theorem, there are three restrictions on \( q_1 \) and \( q_2 \):

1. \( q_1 \equiv 5 \pmod{8} \),
2. \( q_2 \equiv 3 \pmod{4} \),
3. \( q_2 \) a biquadratic residue modulo \( q_1 \).

Replacing (3) with the stronger condition, \( q_2 \equiv 1 \pmod{q_1} \), and applying the Chinese Remainder Theorem the conditions can be reduced to \( q_1 \equiv 5 \pmod{8} \) and \( q_2 \equiv 3 \pmod{4q_1} \). But by Dirichlet’s theorem for primes in an arithmetic progression [2], there are infinitely many such primes \( q_1 \), and for fixed \( q_1 \), there are also infinitely many primes \( q_2 \). Thus, there are infinitely many values of \( e \) satisfying the theorem.

5. Resolution of ambiguity

We now turn to the resolution of the ambiguous sign in Theorem 15. In previous cases, Muskat, Muskat–Whiteman, and Muskat–Zee, [5–7], have obtained resolution via binary quadratic form decomposition of the prime \( p \). For example, we have the following from [5].

**Example 17.** (Muskat) Let \( e = 39 \) and let \( p \) be a prime such that \( p \equiv 1 \pmod{39} \). Then

\[
\tau(1)\tau(16)\tau(34) = u\xi^k\tau(2)\tau(17)\tau(32)
\]

is a sign ambiguity, where \( k = 13 \text{ind}_r 13 \) and

\[
u = \begin{cases} +1, & \text{if } p = x^2 + 39y^2, \\ -1, & \text{if } p = 3x^2 + 13y^2. \end{cases}
\]

Whereas resolution via binary quadratic forms depends on the representation of \( p \) in the form class group, \( \text{CF}(K) \), our method instead relies on an equivalent condition on the primes of \( \mathcal{O}_K \) above \( p \) in the ideal class group, \( C(K) \).

In Section 4, we exploited the fact that \( \omega \in \hat{K} \) to conclude that \( \sigma_i(\omega) = \pm \xi^{k_0} \omega \). We now determine the correct sign in each case by deciding whether the product of a certain root of unity and \( \omega \) is in \( \hat{K} \setminus K \) or in \( K \), and then connecting this to the order of the ideal classes above \( p \) in \( C(K) \).
Proposition 18. Let $k_0$ be as in Theorem 13. Then $\zeta_e^{\delta k_0} \omega \in \tilde{K}$, where $\delta = -1$ if gcd($e, 5$) = 1 and $\delta = 3(t_0 + 1)$ if $e = 5 \cdot q_2$.

Proof. As Proposition 2, either $[t_0] = [g]$ in $G/H_4$ or $[t_0] = [g^3]$ in $G/H_4$. Choose $t_1 \in H \setminus H_2$ such that $[t_1] \neq [t_0]$ in $G/H_4$. Then for all $t \in H \setminus H_2$, either $\sigma_t(\omega) = \sigma_{t_0}(\omega)$ or $\sigma_t(\omega) = \sigma_{t_1}(\omega)$.

Since $\tilde{K}$ is Galois over $Q$, $\omega \in \tilde{K} \Rightarrow \sigma_{t_1}(\omega) \in \tilde{K}$. Therefore, $\omega^{\tilde{K}} = (\sigma_{t_1}(\omega))^{\tilde{K}}$, and it follows that $\sigma_{t_1}(\omega) = (-1)^{\lambda_i} \zeta_e^{\delta k_1} \omega$, for some $\lambda_i, k_1 \in \mathbb{Z}$, and thus

$$\sigma_{t_1}(\omega) = \sigma_{t_1}((-1)^{\lambda_i} \zeta_e^{\delta k_1} \omega) = (-1)^{\lambda_i} \zeta_e^{\delta k_1} \sigma_{t_1}(\omega) = \zeta_e^{\delta k_1 + k_1} \omega. \quad (20)$$

Since $\tilde{K}$ is the fixed field of $H_2$, $\zeta_e^{\delta k_0} \omega \in \tilde{K}$ if and only if for all $t \in H \setminus H_2$, $\sigma_t(\zeta_e^{\delta k_0} \omega) = \zeta_e^{\delta k_0} \omega$. And, since $[t_i] = [t_1, \ldots, t_i]$, $\sigma_{t_i}(\omega) = \sigma_{t_1}^i(\omega) = \sigma_{t_1}^i(\sigma_{t_1}^i(\omega)) = \sigma_{t_1}^i(\omega)$, (21)

so without loss of generality, we may assume that $t = t_0$.

Let $e = q_1 \cdot 3$. Then by Eq. (20),

$$\sigma_{t_0}^2(\zeta_e^{-k_0} \omega) = \zeta_e^{-t_0^2 k_0} \sigma_{t_0}^2(\omega) = \zeta_e^{-t_0^2 k_0} (\zeta_e^{k_0} \omega) = \zeta_e^{-k_0 t_0^2 + k_0 t_0 + k_0} \omega.$$

Therefore, $\zeta_e^{-k_0} \omega$ is fixed by $\sigma_{t_0}^2$ if and only if $-k_0 t_0^2 + k_0 t_0 + k_0 \equiv -k_0 \pmod{q_1}$, that is,

$$\zeta_e^{-k_0} \omega \in \tilde{K} \iff -k_0 t_0^2 + k_0 t_0 + k_0 \equiv -k_0 \pmod{q_1} \text{ and } (mod q_3). \quad (22)$$

But for $e = q_1 \cdot 3, t_0 \in H \setminus H_2 \Rightarrow t_0 \equiv 2 \pmod{3}$, and thus $-k_0 t_0^2 + k_0 t_0 + k_0 \equiv -4k_0 + 2k_0 + k_0 \equiv -k_0 \pmod{3}$. And, by Theorem 13, $k_0$ is equivalent to 0 modulo $q_1$, so $0 \equiv -k_0 \equiv -k_0 t_0^2 + k_0 t_0 + k_0 \equiv (mod q_1)$. Hence, by (22), $\zeta_e^{-k_0} \omega \in \tilde{K}$.

If $e = 5 \cdot q_2$, then again by (21), we may assume $t = t_0$, and we have

$$\sigma_{t_0}^2(\zeta_e^{\delta k_0} \omega) = \zeta_e^{\delta k_0} \sigma_{t_0}^2(\omega) = \zeta_e^{\delta k_0} \sigma_{t_0}^2(\zeta_e^{k_0} \omega) = \zeta_e^{\delta k_0 t_0^2 + k_0 t_0 + k_0} \omega = \zeta_e^{k_0 (\delta t_0^2 + t_0 + 1)} \omega.$$

Hence, $\zeta_e^{\delta k_0} \omega$ is fixed by $\sigma_{t_0}^2$ if and only if $k_0 (\delta t_0^2 + t_0 + 1) \equiv \delta k_0 \pmod{q_2}$, (23)

Since $t_0$ is a nonsquare, $t_0 \equiv 2$ or 3 (mod 5) $\Rightarrow t_0^2 \equiv 4$ (mod 5), and

$$\delta t_0^2 + t_0 + 1 \equiv 3(t_0 + 1) \cdot 4 + t_0 + 1 \equiv 13(t_0 + 1) \equiv 3(t_0 + 1) \equiv \delta \pmod{5}.$$

Hence, $k_0 (\delta t_0^2 + t_0 + 1) \equiv \delta k_0 \pmod{5}$. And by Theorem 13, $k_0 \equiv 0 \pmod{q_2}$, so $k_0 (\delta t_0^2 + t_0 + 1) \equiv k_0 \delta \pmod{q_2}$ as well. Therefore, by (23), $\zeta_e^{\delta k_0} \omega \in \tilde{K}$.

Finally, let $e$ be such that gcd($e, 15$) = 1. Then, again by Theorem 13, $k_0 \equiv 0 \pmod{e}$, and $\sigma_{t_0}^2(\omega) = \zeta_e^{k_0 (t_0 + 1)} \omega = \zeta_e^{k_0 (t_0 + 1)} \omega = \omega$, implying that $\omega \in \tilde{K}$. \qed
Since \( \zeta_e^{\delta k_0} \omega \in \tilde{K} \), we must have that either \( \zeta_e^{\delta k_0} \omega \in K \subseteq \tilde{K} \) or \( \zeta_e^{\delta k_0} \omega \in \tilde{K} \setminus K \). First assume \( \zeta_e^{\delta k_0} \omega \in K \subseteq \tilde{K} \). Since \( t_0 \in H \) and \( K \) is the fixed field of \( H \), it follows that \( \sigma_{t_0}(\zeta_e^{\delta k_0} \omega) = \zeta_e^{\delta k_0} \omega \).

But

\[
\zeta_e^{\delta k_0} \omega = \sigma_{t_0}(\zeta_e^{\delta k_0} \omega) = \zeta_e^{t_0 \delta k_0} \sigma_{t_0} \omega \implies \sigma_{t_0} \omega = \zeta_e^{\delta k_0(1-t_0)} \omega,
\]

and for all \( e \), \( \delta k_0(1-t_0) \equiv k_0 \pmod{e} \). Therefore, \( \sigma_{t_0} \omega = \zeta_e^{k_0} \omega \).

On the other hand, if \( \zeta_e^{\delta k_0} \omega \in \tilde{K} \setminus K \), then it must be the case that \( \sigma_{t_0}(\zeta_e^{\delta k_0} \omega) = -\zeta_e^{\delta k_0} \omega \), which implies \( \sigma_{t_0} \omega = -\zeta_e^{k_0} \omega \). Therefore, to determine the correct sign in

\[
\prod_{t \in H_4} \frac{\tau(t)}{\tau(0_t)} = \pm \zeta_e^{-k_0},
\]

we need only determine whether or not \( \zeta_e^{\delta k_0} \omega \in K \).

**Lemma 19.** \( \zeta_e^{\delta k_0} \omega \in K \iff p^{h_K} \subseteq \mathcal{O}_K \) is principal.

**Proof.** If \( \zeta_e^{\delta k_0} \omega \in K \), then

\[
(\zeta_e^{\delta k_0} \omega)\mathcal{O}_K = \omega \mathcal{O}_E \cap \mathcal{O}_K = p_1^\alpha p_2^\beta = p_1^\alpha p_2^{\beta-\alpha} = p_1^\alpha p_2^{h_K/4},
\]

and \( p_1^\alpha p_2^{h_K/4} \) is principal. Therefore, \( p_2^{h_K/4} \) is principal as well.

If, on the other hand, \( p_1^{h_K/4} \) is principal, then there exists \( \omega' \in K \) such that \( \omega' \mathcal{O}_K = p_1^\alpha p_2^{h_K/4} \). Now,

\[
\omega' \mathcal{O}_K = p_1^\alpha p_2^{h_K} \implies \omega' \mathcal{O}_K = \omega \mathcal{O}_K \implies \omega' = \pm \zeta_e^{r} \omega, \quad \text{for some } r \in \mathbb{Z}.
\]

Since \( \omega' \in K \), it follows that \( \zeta_e^{r} \omega \in K \) and thus \( \sigma_{t_0}(\zeta_e^{r} \omega) = \zeta_e^{r} \omega \). But

\[
\zeta_e^{r} \omega = \sigma_{t_0}(\zeta_e^{r} \omega) = \zeta_e^{t_0 r} \sigma_{t_0} \omega \implies \sigma_{t_0} \omega = \zeta_e^{r(1-t_0)} \omega.
\]

Comparing Eqs. (24) and (25), we must have that \( \delta k_0(1-t_0) \equiv r(1-t_0) \pmod{e} \) and thus \( r \equiv \delta k_0 \pmod{e} \). Hence, \( \zeta_e^{\delta k_0} \omega \in K \). \( \square \)

We now complete the proof of our main theorem.

**Proof of Main Theorem 1.** By Theorem 15, we need only verify the value of \( u \). As in the preceding remarks, the value of \( u \) is dependent only on the ideal class of \( p^{h_K/4} \). We have

\[
u = \begin{cases} +1 & \iff \zeta_e^{\delta k_0} \omega \in K \iff [p^{h_K}] = 1, \\ -1 & \iff \zeta_e^{\delta k_0} \omega \in \tilde{K} \setminus K \iff [p^{h_K}] \neq 1. \end{cases}
\]

By Corollary 7, \( h_K \equiv 4 \pmod{8} \), and thus \( h_K/4 \equiv 1 \pmod{2} \). Therefore, \( [p^{h_K}] = 1 \iff [p^{h_K}] = 1 \iff o([p]) | h_K/4 \iff o([p]) \equiv 1 \pmod{2} \). \( \square \)
We conclude with an example of our main theorem as well as a demonstration of how resolution via binary quadratic forms is then quickly deduced.

**Example 20.** Let \( e = 155 = 5 \cdot 31 \), \( p \) be a prime \( p \equiv 1 \pmod{155} \), and \( \mathfrak{p} \subset \mathcal{O}_K \) be a prime ideal above \( p \). Then

\[
H_4 = \{1, 16, 36, 41, 51, 56, 66, 71, 76, 81, 101, 111, 121, 126, 131\}
\]

and we can take \( t_0 = 12 \). Thus, by Theorem 1,

\[
\prod_{t \in H_4} \frac{\tau(t)}{\tau(t_0 t)} = u_{155}^{\nu(2)(31) \text{ind}_{\mathfrak{p}}(31)},
\]

where

\[
u = \begin{cases} +1, & \text{if } o([\mathfrak{p}]) \equiv 1 \pmod{2}, \\ -1, & \text{if } o([\mathfrak{p}]) \equiv 0 \pmod{2}. \end{cases}\]

For instance, using PARI/GP we compute that for primes \( p < 20000 \),

\[
u = \begin{cases} +1 & \text{if } p = 311, 5581, 11471, 12401, 19531, 19841, \\ -1 & \text{if } p = 1861, 2791, 4651, 8681, 11161, 13331, 16741, 17981, 18911. \end{cases}\]

Now, \( o([\mathfrak{p}]) \equiv 1 \pmod{2} \Leftrightarrow [\mathfrak{p}] \in C(K)^4 \). Therefore, via the isomorphism between the ideal class group and the form class group, we have \( o([\mathfrak{p}]) \equiv 1 \pmod{2} \Leftrightarrow [\mathfrak{p}] \in C_F(K)^4 \). Again using PARI/GP, we compute the corresponding quadratic forms, giving

\[
u = \begin{cases} +1 & \text{if } p = x^2 + xy + 39y^2, \\ -1 & \text{if } p = 5x^2 + 5xy + 9y^2. \end{cases}\]

**Remark 21.** We remark that for values of \( e \) with larger class numbers, using the quadratic form resolution alone becomes increasingly difficult as the number of forms from which to choose will be \( h_K/4 \). For example, if \( e = 327 \), then \( h_K = 12 \), and there are three forms which give \( \nu = +1 \) and three which give \( \nu = -1 \). However, using information about the ideal class of a quadratic prime as above, a computational resolution is quickly achieved and, if necessary, resolution criteria using quadratic forms can be easily deduced.

**References**
