Louisiana State University
LSU Scholarly Repository

LSU Doctoral Dissertations | Graduate School

2002

Explicit multiplicative relations between Gauss sums

Brian J. Murray
Louisiana State University and Agricultural and Mechanical College

Follow this and additional works at: https://repository.lsu.edu/gradschool_dissertations

 Part of the Applied Mathematics Commons

Recommended Citation

Murray, Brian J., "Explicit multiplicative relations between Gauss sums" (2002). *LSU Doctoral Dissertations*. 757.
https://repository.lsu.edu/gradschool_dissertations/757

This Dissertation is brought to you for free and open access by the Graduate School at LSU Scholarly Repository. It has been accepted for inclusion in LSU Doctoral Dissertations by an authorized graduate school editor of LSU Scholarly Repository. For more information, please contactgradetd@lsu.edu.

EXPLICIT MULTIPLICATIVE RELATIONS BETWEEN GAUSS SUMS

A Dissertation

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

in

The Department of Mathematics

by
Brian J. Murray
B.A., Mathematics, Washington University in St. Louis, 1997
M.S., Louisiana State University, 1999
August 2002

Acknowledgments

First and foremost, I would like to thank my advisor Dr. Paul van Wamelen for both his guidance and lack thereof. Throughout the development of this dissertation, I was involved in all decisions and was always offered support and advice. Rarely, however, was I given answers; for this, I am truly grateful. I would also like to thank Dr. van Wamelen for the informal nature of our relationship–although the last three years were challenging, they were certainly enjoyable.

This dissertation would not have been possible without the support of the Department of Mathematics at Louisiana State University. Specifically, I would like to thank my committee members, Professors George Cochran, Richard Litherland, Augusto Nobile, Louise Perkins, and Robert Perlis. I would like to thank Dan Cohen for helpful mathematical discussions as well as extremely helpful racquetball games. I am also grateful to Anthony Picado for keeping Lockett Hall running smoothly.

I would like to thank Robert Osburn for continued friendship, valued mathematical advice, and most importantly, indispensable commiseration.

Finally, I would like to thank my entire family for their continued support and encouragement of my education. This dissertation is dedicated to my wife, Ashley, whose love and support made this possible.

Table of Contents

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.

Introduction

C. F. Gauss first introduced the sums bearing his name in 1801 in his *Disquisitiones Arithmeticae*. This sum, $\sum_{n=0}^{k-1} \zeta_k^{mn^2}$, now known as a *quadratic* Gauss sum, was notoriously difficult to evaluate, even in the special case that $m = 1$ and k is an odd integer, [3]. Gauss was easily able to prove that this sum has the value $\pm\sqrt{k}$, or $\pm i\sqrt{k}$, depending on whether k was congruent to 1 or 3 modulo 4, but the resolution of the sign proved to be much more difficult. In May, 1801, Gauss conjectured that the plus sign held in each case and then, for the next four years, devoted time every week to proving the conjecture, [3, 10]. Finally, in August, 1805, Gauss proved his conjecture, recording in his diary "Wie der Blitz einschlägt, hat sich das Räthsel gelöst..." (as lightning strikes was the puzzle solved), [10]. Several years later, Gauss published a complete evaluation of the quadratic Gauss sum for all positive integers k. Using this evaluation, Gauss was able to give a fourth proof of his *Theorema Aureum*, or golden theorem, now known as the law of quadratic reciprocity. Since the initial work of Gauss, the determination of Gauss sums and the resolution of ambiguous signs has been fundamental in the study of reciprocity.

With the introduction of the multiplicative character χ modulo k in his treatise on primes in arithmetic progressions, G. L. Dirichlet was able to generalize the Gauss sum, [3]. This sum, $G(\chi) = \sum_{n=0}^{k-1} \chi(n)\zeta_k^{mn}$, is also called a Gauss sum as it coincides with the quadratic Gauss sum when χ has order 2 and k is taken to be a prime p not dividing m. In addition to providing the foundation for higher reciprocity laws, this generalization of the Gauss sum arises naturally in the study of cyclotomy and has many important applications throughout mathematics. Building on the initial work of Gauss, Dirichlet, and Jacobi, many well-known mathe-

maticians have made contributions to the theory of Gauss sums and the closely related Jacobi sums. These include L. Carlitz, A. Cauchy, S. Chowla, H. Davenport, G. Eisenstein, B. Gross, H. Hasse, N. M. Katz, N. Koblitz, L. Kronecker, E. E. Kummer, D. H. and E. Lehmer, L. J. Mordell, S. J. Patterson, C. L. Siegel, L. Stickelberger, and A. Weil, [3].

One powerful approach to simplifying the evaluation of Gauss sums is to study the multiplicative relations between them. The most basic of the multiplicative relations is the *norm relation* for Gauss sums, which states that the product of a Gauss sum and its complex conjugate is, up to a unit of absolute value one, equal to the prime p. From the norm relation, it is then clear that the Gauss sums divide p and thus generate ideals which factor only into prime ideals above p. Moreover, using Stickelberger's congruence for Gauss sums, the factorization of all Gauss sums can be given explicitly. Using these results of Stickelberger, H. Davenport and H. Hasse were able to formulate the second type of multiplicative relation between Gauss sums, the beautiful *Davenport-Hasse product formula*. Originally appearing in their 1934 paper *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, the Davenport-Hasse product formula provides an entire class of nontrivial multiplicative relations. In fact, in [8, pg.465], H. Hasse conjectured the norm relation and the Davenport-Hasse product formula were essentially the only multiplicative relations connecting Gauss sums over $\mathbf{F}_p$.

However, in K. Yamamoto's 1966 paper *On a conjecture of Hasse concerning multiplicative relations of Gaussian sums*, Yamamoto 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 and with the aid of a computer, further sign ambiguities were discovered by Muskat,

Muskat-Whiteman, and Muskat-Zee, [13, 15, 16]. Based on his difficulty in finding sign ambiguities, in [14] Muskat proposed that "... perhaps there are no more than the seven sign ambiguities noted above." To date only nine sign ambiguities have been given explicitly. While very few had been found, in [22], Yamamoto succeeded in not only proving that infinitely many exist, but also produced a formula giving the exact "number" of sign ambiguities to be expected in each case. Despite this guarantee of new sign ambiguities, very little has been done since 1975.

With the 1998 publication of *Gauss and Jacobi sums* by Berndt, Evans, and Williams, [3], there has been renewed interest in the study of Gauss sums. Additionally, the rapid evolution of computing power has made the computational techniques of Muskat, [14], much more effective. Building on these ideas, we provide an infinite class of new sign ambiguities.

In chapter 1, we quickly summarize some essentials of Algebraic Number Theory. Included are specifics about quadratic and cyclotomic number fields as well as a brief description of the ideal class group and Dirichlet's class number formula.

Chapter 2 continues with the necessary background for Gauss sums. After giving the basic definitions and properties of Gauss sums, we then cover multiplicative relations, Jacobi sums, the factorization of Gauss sums over cyclotomic fields, and sign ambiguities.

We present our main results in chapter 3. We first discuss the methodology behind the computer search for sign ambiguities. Then, after a digression into biquadratic coset sums, we present and prove our main theorem.

1. Background

1.1 Algebraic Number Theory

An *(algebraic) number field*, K, is a subfield of the complex numbers of finite degree over $\mathbf{Q}$. Let $[K : \mathbf{Q}]$ denote the degree of K over $\mathbf{Q}$. Within a number field K lies the *(algebraic) integers* $\mathcal{O}_K$, which consists of all elements of K that are roots of a monic polynomial with integral coefficients. Given a nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_K$, we can form the *residue field* $\mathcal{O}_K/\mathfrak{a}$. As the residue field is finite, we define the *norm* of $\mathfrak{a}$, to be $N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$, the number of elements in $\mathcal{O}_K/\mathfrak{a}$. While rings of integers are not necessarily unique factorization domains, they are Dedekind domains. That is, any nonzero ideal of $\mathcal{O}_K$ has a unique factorization into prime ideals of $\mathcal{O}_K$.

Let L be a finite extension of K. Then $\mathfrak{p}\mathcal{O}_L$ is an ideal of $\mathcal{O}_L$ *lying over* or *above* $\mathfrak{p}$, and has unique factorization $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$, where the $\mathfrak{P}_i$'s are the distinct prime ideals of L containing $\mathfrak{p}$. The exponents e_i are called the *ramification indices* of $\mathfrak{p}$ in $\mathfrak{P}_i$. In this situation we will also say that $\mathfrak{P}_i$ is an ideal of $\mathcal{O}_L$ *dividing* $\mathfrak{p}$, or equivalently, $\mathfrak{P}_i$ contains $\mathfrak{p}$.

Now, since for $i = 1, \ldots, g$, $\mathfrak{P}_i$ contains $\mathfrak{p}$, we have a residue field extension $\mathcal{O}_L/\mathfrak{P}_i$ over $\mathcal{O}_K/\mathfrak{p}$. The degree of this extension, denoted f_i, is called the *inertial degree* of $\mathfrak{p}$ in $\mathfrak{P}_i$. The number, g, of prime ideals lying over $\mathfrak{p}$, the ramification indices, e_i, and the inertial degrees, f_i, are related by the following, see [6], [10].

Theorem 1.1. *Let K be a number field with finite extension L and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. Then*

$$\sum_{i=1}^{g} e_i f_i = [L : K].$$

A prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ is said to be *inert* in L if $\mathfrak{p}\mathcal{O}_L$ is again a prime ideal in L. If the factorization of $\mathfrak{p}\mathcal{O}_L$ contains any ramification index $e_i > 1$, then we say

that $\mathfrak{p}$ is *ramified* in L. Finally, if $\mathfrak{p}$ is ramified in L, $g = 1$, and $e_1 = [L : K]$, then $\mathfrak{p}$ is said to be *totally ramified* in L.

If L is a Galois extension of K the situation is considerably nicer. In particular, Theorem 1.1 simplifies to the following.

Theorem 1.2. *Let K be a number field with Galois extension L and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. Then all of the prime ideals of $\mathcal{O}_L$ above $\mathfrak{p}$ have the same ramification index e, the same inertial degree f, and $efg = [L : K]$.*

Additionally, the action of the Galois group on the prime ideals is given in the following, [6].

Theorem 1.3. *Let L be a Galois extension of K and $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$. Then the Galois group $\mathrm{Gal}(L/K)$ acts transitively on the prime ideals of $\mathcal{O}_L$ containing $\mathfrak{p}$,* i.e. *if $\mathfrak{P}$ and $\mathfrak{P}'$ are primes ideals of $\mathcal{O}_L$ above $\mathfrak{p}$, then there is a $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\mathfrak{P}) = \mathfrak{P}'$.*

In the case of a Galois extension, $K \subseteq L$, an ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is ramified in L if $e > 1$ and *unramified* if $e = 1$. If $e = f = 1$, we say that the prime $\mathfrak{p}$ *splits completely* in L, and thus, by Theorem 1.1, $\mathfrak{p}\mathcal{O}_L$ splits into $[L : K]$ primes above $\mathfrak{p}$. Classifying which primes of a number field are ramified or which split completely is a fundamental problem in Algebraic Number Theory. We first consider this problem in *quadratic number fields*, or number fields of degree 2 over $\mathbf{Q}$.

If K is a quadratic number field, then $K = \mathbf{Q}(\sqrt{N})$, where $N \neq 0, 1$ is a squarefree integer. The *discriminant of K*,

$$d_K = \begin{cases} N, & \text{if } N \equiv 1 \pmod 4, \\ 4N, & \text{otherwise,} \end{cases}$$

completely determines the ring of integers of K. In particular,

$$\mathcal{O}_K = \begin{cases} \mathbf{Z}[\frac{1+\sqrt{N}}{2}] & \text{if } N \equiv 1 \pmod 4, \\ \mathbf{Z}[\sqrt{N}] & \text{otherwise.} \end{cases}$$

To determine how rational primes decompose in these number fields, we first need some definitions.

Definition 1.4. *Let m, n be positive integers and let a be an integer relatively prime to m. We say that a is an nth power residue modulo m if $x^n \equiv a \pmod m$ is solvable. In particular, if $n = 2$, we say a is a quadratic residue, and if $n = 4$, we say that a is a biquadratic residue.*

Definition 1.5. *If a is an integer and p an odd prime, then the Legendre symbol, $\left(\frac{a}{p}\right)$, is given by:*

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } a \equiv 0 \pmod p, \\ 1, & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1, & \text{if } a \text{ is a quadratic nonresidue modulo } p. \end{cases}$$

We remark that the Legendre symbol is multiplicative and depends only on the congruence class of a mod p.

We can now state a fundamental law of number theory formulated by Euler and Legendre, but first proven by Gauss.

Theorem 1.6 (Law of Quadratic Reciprocity). *Let p and q be odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

We can now give a complete classification of the decomposition of rational primes in quadratic number fields.

Proposition 1.7. *Let p be an odd prime and let K be a quadratic number field of discriminant d_K. Then*

(i) If $\left(\frac{d_K}{p}\right) = 0$, then $p\mathcal{O}_K = \mathfrak{p}^2$ for some prime $\mathfrak{p}$ of $\mathcal{O}_K$, (i.e. *p ramifies in K).*

(ii) If $\left(\frac{d_K}{p}\right) = 1$, then $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$ for some primes $\mathfrak{p} \neq \mathfrak{p}'$ of $\mathcal{O}_K$, (i.e. *p splits completely in K).*

(iii) If $\left(\frac{d_K}{p}\right) = -1$, then $p\mathcal{O}_K$ is again prime in $\mathcal{O}_K$, (i.e. *p is inert in K).*

1.2 Cyclotomic Number Fields

For a positive integer m, let $\zeta_m = e^{2\pi i/m}$. Then ζ_m is a root of $x^m - 1$, but not $x^n - 1$ for any $n < m$. Such a ζ_m is called a *primitive mth root of unity*. Since all powers of ζ_m are also roots of $x^m - 1$, we have that $x^m - 1 = (x-1)(x-\zeta_m)\cdots(x-\zeta_m^{m-1})$ and $M = \mathbf{Q}(\zeta_m)$ is the splitting field of the polynomial $x^m - 1$. Hence, M is Galois over $\mathbf{Q}$, [10, 20].

The field $M = \mathbf{Q}(\zeta_m)$ is called the *cyclotomic field of mth roots of unity*, or simply the *mth cyclotomic field*. The Galois group of cyclotomic number fields is particularly simple.

Theorem 1.8. $\mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q}) \cong (\mathbf{Z}/m\mathbf{Z})^\times$. *In particular, every $a \in (\mathbf{Z}/m\mathbf{Z})^\times$ corresponds to the automorphism $\sigma_a \in \mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q})$ sending $\zeta_m \mapsto \zeta_m^a$.*

Corollary 1.9. $[\mathbf{Q}(\zeta_m) : \mathbf{Q}] = \phi(m)$, *where $\phi(m)$ denotes the Euler phi function.*

Cyclotomic fields also have a beautiful algebraic structure.

Theorem 1.10. *The ring of algebraic integers in $\mathbf{Q}(\zeta_m)$ is $\mathbf{Z}[\zeta_m]$.*

Proposition 1.11. *If p is a prime and $p \nmid m$, then every prime ideal $P \subseteq \mathbf{Z}[\zeta_m]$ containing p is unramified.*

Combining these properties of cyclotomic number fields, we get a complete decomposition of rational primes in $\mathbf{Z}[\zeta_m]$.

Theorem 1.12 ([10],Th.2, pg.196). *Let p be a rational prime, $p \nmid m$, and let f be the least positive integer such that $p^f \equiv 1 \pmod{m}$. Then*

$$p\mathbf{Z}[\zeta_m] = P_1 P_2 \cdots P_g,$$

where each P_i has inertial degree f and $g = \phi(m)/f$.

Remark 1.13. *In particular, if p is a rational prime congruent to 1 modulo m, then $f = 1$ and p splits completely into $\phi(m)$ primes of $\mathbf{Z}[\zeta_m]$.*

For cyclotomic extensions of cyclotomic fields, the decomposition of rational primes is again surprisingly simple.

Theorem 1.14 ([10], Prop.13.2.9, pg.198). *Let p be a rational prime such that $p \nmid m$, $E = \mathbf{Q}(\zeta_m, \zeta_p)$, and let $P_1, \ldots, P_g$ be as in the previous theorem. Then for all i, $P_i\mathcal{O}_E = \wp_i^{p-1}$,* i.e. *$P_i$ ramifies in $\mathcal{O}_E$, and thus*

$$p\mathcal{O}_E = (\wp_1 \wp_2 \cdots \wp_g)^{p-1}.$$

Finally, we have the following two results concerning units of absolute value 1 in cyclotomic fields, [3, 10, 20].

Theorem 1.15. *If all the algebraic conjugates of an algebraic integer α over $\mathbf{Q}$ have absolute value 1, then α is a root of unity.*

Theorem 1.16. *Let $M = \mathbf{Q}(\zeta_m)$. The only elements of absolute value 1 in $\mathcal{O}_M$ are $\pm\zeta_m^i$, $i = 1, 2, \ldots, m$. In particular, the only roots of unity in $\mathcal{O}_M$ are $\pm\zeta_m^i$.*

1.3 Class Field Theory

Given an ideal $I \subseteq \mathcal{O}_K$ and an element $\alpha \in K$, we can form $\alpha I = \{\alpha x \mid x \in I\}$. This is an $\mathcal{O}_K$-submodule of K and is called a *fractional ideal* of K. The set of all fractional ideals of K, denoted I_K, is closed under multiplication. Moreover, each fractional ideal is invertible and thus, I_K is a group. The ideals of I_K of the form

$\alpha\mathcal{O}_K$, for some $\alpha \in K^\times$, form a subgroup of I_K and are called *principal fractional ideals*, denoted P_K.

Definition 1.17. *The ideal class group of K, $C(K)$, is defined to be the quotient*

$$C(K) = I_K/P_K.$$

The order of $C(K)$ is denoted h_K and is called the class number of K.

It is well-known that for number fields K, $C(K)$ is a finite abelian group, [12], and so h_K is finite. Given an ideal $I \subseteq \mathcal{O}_K$, we will denote by $[I]$ its class in $C(K)$ and denote its order in the class group by $o([I])$.

The ideal class group is a measure of how close $\mathcal{O}_K$ is to being a principal ideal domain, i.e. $\mathcal{O}_K$ is a principal ideal domain if and only if $h_K = 1$. It is a classical problem of Number Theory to investigate the structure and order of $C(K)$.

As $C(K)$ is a finite abelian group, it is a product of cyclic groups of prime-power order. To understand the structure of the ideal class group of a quadratic number field K, it is important to understand its 2-Sylow subgroup. Using quadratic forms, Gauss proved that the number of cyclic factors of $C(K)$ with even order is equal to $t-1$, where t is the number of distinct primes dividing d_K. For specific classes of discriminants, d_K, much more can be said, see, for example, [4].

Concerning h_K, let us restrict our attention to imaginary quadratic number fields as these fields are the main focus of Chapters 2 and 3. For these fields, the class number h_K is easily obtained using Dirichlet's class number formula, [6, 7].

Theorem 1.18. *Let K be a quadratic number field of discriminant $d_K < 0$. Then*

$$h_K = \sum_{n=1}^{|d_K|-1} \left(\frac{d_K}{n}\right) n,$$

where $\left(\frac{d_K}{n}\right)$ is defined for $n = p_1 p_2 \dots p_r$, p_i prime, by $\left(\frac{d_K}{n}\right) = \prod_{i=1}^{r} \left(\frac{d_K}{p_i}\right)$.

2. Gauss Sums

2.1 Preliminaries

Let e be an integer, $e > 2$, and let p be a prime, $p \equiv 1 \pmod{e}$. Let $\mathbf{F}_p$ be the finite field of p elements with (cyclic) multiplicative group $\mathbf{F}_p^\times$ generated by γ. We can then define a multiplicative character

$$\chi \colon \mathbf{F}_p^\times \longrightarrow \mathbf{Q}(\zeta_e) \quad \text{by} \quad \chi(\gamma) = \zeta_e,$$

where ζ_e is a primitive eth root of unity. We extend the character to all of $\mathbf{F}_p$ by setting $\chi(0) = 0$.

Definition 2.19. *For $a \in \mathbf{Z}$, define the Gauss sum $\tau(a)$ to be*

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

Remark 2.20. *Since χ is a character of order e, we need only consider $a \bmod e$, and thus have e distinct Gauss sums, $\tau(0), \tau(1), \ldots, \tau(e-1)$.*

Remark 2.21. *By definition as sums of roots of unity, Gauss sums are algebraic integers in $\mathbf{Q}(\zeta_{ep})$.*

We now provide some elementary properties of Gauss sums. Further properties and proofs may be found in [3, 10].

Proposition 2.22. *For $a \not\equiv 0 \pmod{e}$,*

1. $\tau(0) = 0$
2. $\overline{\tau(a)} = \chi^a(-1)\tau(-a)$
3. $|\tau(a)| = p^{1/2}$.

The action of Galois group elements on Gauss sums can also be given explicitly, [20]. Let $E = \mathbf{Q}(\zeta_{ep}) = \mathbf{Q}(\zeta_e, \zeta_p)$ and $M = \mathbf{Q}(\zeta_e)$. Then $\mathrm{Gal}(E/\mathbf{Q})$ is given by the automorphisms σ_c, where $\gcd(c, ep) = 1$. Now, σ_c is completely determined by $\sigma_c(\zeta_e)$ and $\sigma_c(\zeta_p)$ and we have

1. σ_c fixes $\mathbf{Q}(\zeta_e)$ element-wise if and only if $c \equiv 1 \pmod{e}$,

2. σ_c fixes $\mathbf{Q}(\zeta_p)$ element-wise if and only if $c \equiv 1 \pmod{p}$.

Therefore, for $c \equiv 1 \pmod{p}$ with $\gcd(c, ep) = 1$, $\sigma_c(\zeta_e) = \zeta_e^c$ and $\sigma_c(\zeta_p) = \zeta_p$ and we conclude that $\mathrm{Gal}(E/\mathbf{Q}(\zeta_p)) \cong \mathrm{Gal}(M/\mathbf{Q})$. Applying these automorphisms to Gauss sums, we obtain the following proposition.

Proposition 2.23. *For $j \in (\mathbf{Z}/e\mathbf{Z})^\times$, $\sigma_j(\tau(a)) = \tau(ja)$.*

Proof. For $j \in (\mathbf{Z}/e\mathbf{Z})^\times$, $\sigma_j \in \mathrm{Gal}(M/\mathbf{Q}) \cong \mathrm{Gal}(E/\mathbf{Q}(\zeta_p))$, and

$$\sigma_j(\tau(a)) = \sigma_j\left(\sum_{\alpha \in \mathbf{F}_p} \chi^a(\alpha)\zeta_p^\alpha\right) = \sum_{\alpha \in \mathbf{F}_p} \sigma_j(\chi^a(\alpha))\sigma_j(\zeta_p^\alpha) = \sum_{\alpha \in \mathbf{F}_p} \chi^{ja}(\alpha)\zeta_p^\alpha = \tau(ja).$$

□

Two main types of multiplicative relations exist between Gauss sums. The first such relation follows from properties two and three of Proposition 2.22 and is often referred to as 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,

$$\tau(a)\tau(-a) = \chi^a(-1)p. \tag{2.1}$$

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

$$\chi^{tn}(n)\frac{\tau(t)}{\tau(tn)}\prod_{k=1}^{n-1}\frac{\tau(km+t)}{\tau(km)} = 1. \tag{2.2}$$

Example 2.24. *Let $e = 15$, p be a prime with $p \equiv 1 \pmod{e}$, and let χ be a multiplicative character $\chi\colon \mathbf{F}_p^\times \to \mathbf{Q}(\zeta_{15})$. Then, upon splitting the quotients of (2.2), we have the following six Davenport-Hasse relations along with the corresponding values of m, n, and t.*

1. $m = 3, n = 5, t = 1;\ \chi^5(5)\tau(1)\tau(4)\tau(7)\tau(10)\tau(13) = \tau(3)\tau(5)\tau(6)\tau(9)\tau(12)$

2. $m = 3, n = 5, t = 2;\ \chi^{10}(5)\tau(2)\tau(5)\tau(8)\tau(11)\tau(14) = \tau(3)\tau(6)\tau(9)\tau(10)\tau(12)$

3. $m = 5, n = 3, t = 1;\ \chi^3(3)\tau(1)\tau(6)\tau(11) = \tau(3)\tau(5)\tau(10)$

4. $m = 5, n = 3, t = 2;\ \chi^6(3)\tau(2)\tau(7)\tau(12) = \tau(5)\tau(6)\tau(10)$

5. $m = 5, n = 3, t = 3;\ \chi^9(3)\tau(3)\tau(8)\tau(13) = \tau(5)\tau(9)\tau(10)$

6. $m = 5, n = 3, t = 4;\ \chi^{12}(3)\tau(4)\tau(9)\tau(14) = \tau(5)\tau(10)\tau(12)$.

Another type of character sum closely related to the Gauss sum is the *Jacobi sum*, which has the added advantage of being an integer of $\mathbf{Q}(\zeta_e)$, rather than $\mathbf{Q}(\zeta_{ep})$.

Definition 2.25. *Let e, p, and χ be as before, and let $m, n \in \mathbf{Z}$. We define the Jacobi sum $J(m, n)$ to be*

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

Remark 2.26. *We again remark that as χ has order e, we need only consider m and n modulo e.*

Theorem 2.27. *If $m + n \not\equiv 0 \pmod{e}$, then $J(m, n) = \dfrac{\tau(m)\tau(n)}{\tau(m+n)}$.*

Proof. By the definition of $\tau(m)$,

$$\begin{aligned}
\tau(m)\tau(n) &= \sum_{\alpha}\sum_{\beta}\chi^m(\alpha)\chi^n(\beta)\zeta_p^{\alpha+\beta} \\
&= \sum_{\delta}\zeta_p^{\delta}\sum_{\alpha+\beta=\delta}\chi^m(\alpha)\chi^n(\beta) \\
&= \sum_{\alpha+\beta=0}\chi^m(\alpha)\chi^n(\beta) + \sum_{\delta\neq 0}\zeta_p^{\delta}\sum_{\alpha}\chi^m(\alpha)\chi^n(\delta-\alpha) \\
&= \chi^n(-1)\sum_{\alpha}\chi^{m+n}(\alpha) + \sum_{\delta\neq 0}\zeta_p^{\delta}\sum_{\alpha}\chi^m(\delta\alpha)\chi^n(\delta-\delta\alpha) \\
&= 0 + J(m,n)\sum_{\delta\neq 0}\chi^{m+n}(\delta)\zeta_p^{\delta} \\
&= J(m,n)\tau(m+n).
\end{aligned}$$

□

When possible, it is often desirable to express products of Gauss sums in terms of products of Jacobi sums as it is then clear that the product is an element of the smaller cyclotomic field $\mathbf{Q}(\zeta_e)$. It is also of interest to note that by Theorem 2.27, both the norm relation, (2.1), and the Davenport-Hasse product formula, (2.2), can be reformulated in terms of Jacobi sums.

We now consider the prime ideal factorization of Gauss sums. Again, let $M = \mathbf{Q}(\zeta_e)$, $E = \mathbf{Q}(\zeta_{ep})$, and let $\mathcal{O}_M$ and $\mathcal{O}_E$ denote their respective rings of integers. From the norm relation, (2.1), the ideal generated by $\tau(a)$ divides p, and thus factors only into primes above p. Let $P \subseteq \mathcal{O}_M$ be a prime ideal above the rational prime p. By Remark 1.13, since $p \equiv 1 \pmod{e}$, $p\mathcal{O}_M$ will split completely into $\phi(e)$ primes. Then, since $\mathrm{Gal}(M/\mathbf{Q})$ acts transitively on the primes of $\mathcal{O}_M$ above p, we have

$$p\mathcal{O}_M = \prod_{j\in(\mathbf{Z}/e\mathbf{Z})^\times} P_j,$$

where $P_j = \sigma_j(P)$, $\sigma_j \in \mathrm{Gal}(M/\mathbf{Q})$. Furthermore, by Theorem 1.14, each P_j ramifies totally in $\mathcal{O}_E$ and thus, for some prime ideal $\wp \subseteq \mathcal{O}_E$, we have $P\mathcal{O}_M =$

$\wp^{p-1}$, $\wp \cap \mathcal{O}_M = P$. Recalling that $\mathrm{Gal}(E/\mathbf{Q}(\zeta_p)) \cong \mathrm{Gal}(M/\mathbf{Q})$ and letting $\wp_j = \sigma_j(\wp)$, we then have

$$p\mathcal{O}_E = \prod_{j \in (\mathbf{Z}/e\mathbf{Z})^\times} \wp_j^{p-1} = \left(\prod_{j \in (\mathbf{Z}/e\mathbf{Z})^\times} \wp_j \right)^{p-1}.$$

Therefore, the ideal generated by $\tau(a)$ factors only into powers of the $\wp_j$. Specifically, we have the following factorization formula due to Stickelberger.

Theorem 2.28 (Stickelberger).

$$\tau(a)\mathcal{O}_E = \left(\prod_{j \in (\mathbf{Z}/e\mathbf{Z})^\times} \wp_{-j^{-1}}^{\{\frac{aj}{e}\}} \right)^{p-1},$$

where $-j^{-1}$ is taken modulo e and $\{x\}$ represents the fractional part of x.

Example 2.29. *Let $e = 15$, p be a prime with $p \equiv 1 \pmod{15}$, and $\wp$ be a prime ideal of $\mathcal{O}_E$ dividing p. Then $\tau(1)$ factors into powers of the $\phi(15) = 8$ distinct primes of $\mathcal{O}_E$ above p*

$$\tau(1)\mathcal{O}_E = \left(\wp_1^{\frac{14}{15}} \wp_2^{\frac{7}{15}} \wp_4^{\frac{11}{15}} \wp_7^{\frac{2}{15}} \wp_8^{\frac{13}{15}} \wp_{11}^{\frac{4}{15}} \wp_{13}^{\frac{8}{15}} \wp_{14}^{\frac{1}{15}} \right)^{p-1}.$$

In particular, if $p = 31$, then

$$\begin{aligned} \tau(1)\mathcal{O}_E &= \left(\wp_1^{\frac{14}{15}} \wp_2^{\frac{7}{15}} \wp_4^{\frac{11}{15}} \wp_7^{\frac{2}{15}} \wp_8^{\frac{13}{15}} \wp_{11}^{\frac{4}{15}} \wp_{13}^{\frac{8}{15}} \wp_{14}^{\frac{1}{15}} \right)^{30} \\ &= \wp_1^{28} \wp_2^{14} \wp_4^{22} \wp_7^{4} \wp_8^{26} \wp_{11}^{8} \wp_{13}^{16} \wp_{14}^{2}. \end{aligned}$$

2.2 Sign Ambiguities

In section 1, we saw two distinct types of multiplicative relations connecting Gauss sums: the norm relation, (2.1), and the Davenport-Hasse product formula, (2.2). It is natural to ask if any other multiplicative relations exist. In [8, p. 465], H. Hasse conjectured that the norm relation and the Davenport-Hasse product formula were essentially the only multiplicative relations connecting Gauss sums over $\mathbf{F}_p$. In [21],

K. Yamamoto proved Hasse's conjecture if the Gauss sums are considered as *ideals*, but provided a simple counterexample for $e = 12$ if the sums are instead considered as *numbers*. Further counterexamples were given for $e = 15, 20, 21, 24, 28, 39, 55,$ and 56 by Muskat, Muskat-Whiteman, and Muskat-Zee in [13, 15, 16]. For each counterexample, an explicit multiplicative relation was found involving a sign that could not be determined using elementary properties of Gauss sums and relations (2.1) and (2.2). Such relations have become known as *sign ambiguities*.

Definition 2.30. *A multiplicative relation of the form*

$$\prod_{i,j} \frac{\tau(i)}{\tau(j)} = u\zeta_e^k,$$

where $u = 1$ for some primes p, $u = -1$ for others, such that the sign cannot be connected to elementary properties of Gauss sums, the norm relation, nor the Davenport-Hasse product formula, is known as a sign ambiguity.

Illustration 2.31 (Muskat, [13]). *Let $e = 39$ and p be a prime, $p \equiv 1 \pmod{39}$. Then*

$$\tau(1)\tau(16)\tau(34) = \pm\zeta_e^{13\,ind_\gamma 13}\tau(2)\tau(17)\tau(32)$$

is a sign ambiguity, where $ind_\gamma a$ is the unique integer i such that $a \equiv \gamma^i \pmod{p}$ for a fixed primitive root $\gamma \bmod p$.

In [22], Yamamoto further investigated Hasse's conjecture and determined that sign ambiguities existed for all composite values of e. Moreover, Yamamoto was able to determine exactly how many multiplicatively independent relationships were "missing" in each case.

Theorem 2.32 (Yamamoto, [22]). *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* $e/2$.

While this shows that new multiplicative relations exist for all composite values of e, very few have been explicitly given.

We restrict attention to odd values of e with two distinct prime divisors, as sign ambiguities for many other values of e can be reduced to these cases. Furthermore, by Theorem 2.32, such values of e will have exactly one new multiplicatively independent relation. In this dissertation, we present a product formula explicitly producing the missing sign ambiguities for infinitely many values of e.

3. Results

3.1 Methodology

Initially, we obtained computational evidence using PARI/GP to aid intuition. This was accomplished by reformulating the problem in terms of linear algebra. Consider the Davenport-Hasse product formula (2.2),

$$\chi^{tn}(n)\frac{\tau(t)}{\tau(tn)}\prod_{k=1}^{n-1}\frac{\tau(km+t)}{\tau(km)}=1,$$

which, upon splitting the quotient becomes

$$\chi^{tn}(n)\tau(t)\prod_{k=1}^{n-1}\tau(km+t)=\tau(tn)\prod_{k=1}^{n-1}\tau(km).$$

Since Gauss sums are integers of $E=\mathbf{Q}(\zeta_{ep})$, the products above are integers as well, and we can consider the ideals they generate, that is,

$$\underbrace{\chi^{tn}(n)}_{\text{unit}}\underbrace{\tau(t)\prod_{k=1}^{n-1}\tau(km+t)}_{\text{ideal generator}}=\underbrace{\tau(tn)\prod_{k=1}^{n-1}\tau(km)}_{\text{ideal generator}}.$$

Thus, each Davenport-Hasse relation corresponds to distinct algebraic integers generating the same ideal. From this point of view, it is clear that finding multiplicative relations is equivalent to finding distinct generators of the same ideal.

This reformulation laid the foundation for the computer search for new multiplicative relations between Gauss sums. Using Stickelberger's factorization formula (Theorem 2.28), we first factored each of the $e-1$ distinct, non-trivial, Gauss sums; for example, recall the example for $e=15$:

Example 3.33. *Let $e=15$, p be a prime with $p\equiv 1 \pmod{15}$, $E=\mathbf{Q}(\zeta_{ep})$, and $\wp$ be a prime ideal of $\mathcal{O}_E$ dividing p. Then $\tau(1)$ and $\tau(2)$ factor into powers of the $\phi(15)=8$ distinct primes of $\mathcal{O}_E$ above p. We have*

$$\tau(1)\mathcal{O}_E=\left(\wp_1^{\frac{14}{15}}\wp_2^{\frac{7}{15}}\wp_4^{\frac{11}{15}}\wp_7^{\frac{2}{15}}\wp_8^{\frac{13}{15}}\wp_{11}^{\frac{4}{15}}\wp_{13}^{\frac{8}{15}}\wp_{14}^{\frac{1}{15}}\right)^{p-1}$$

and

$$\tau(2)\mathcal{O}_E = \left(\wp_1^{\frac{13}{15}}\wp_2^{\frac{14}{15}}\wp_4^{\frac{7}{15}}\wp_7^{\frac{4}{15}}\wp_8^{\frac{11}{15}}\wp_{11}^{\frac{8}{15}}\wp_{13}^{\frac{1}{15}}\wp_{14}^{\frac{2}{15}}\right)^{p-1}.$$

Each factorization is independent of the choice of the rational prime p in the sense that different p's will not alter the ratios of the exponents. Thus, each Gauss sum factorization can be represented as a vector of the exponents. Using the factorizations from Example 2.29, we have the correspondences

$$\tau(1)\mathcal{O}_E \longleftrightarrow \left[\frac{14}{15}, \frac{7}{15}, \frac{11}{15}, \frac{2}{15}, \frac{13}{15}, \frac{4}{15}, \frac{8}{15}, \frac{1}{15}\right]$$

and

$$\tau(2)\mathcal{O}_E \longleftrightarrow \left[\frac{13}{15}, \frac{14}{15}, \frac{7}{15}, \frac{4}{15}, \frac{11}{15}, \frac{8}{15}, \frac{1}{15}, \frac{2}{15}\right].$$

Representing all $e-1$ non-trivial Gauss sums in this way, we then formed a $\phi(e) \times (e-1)$ matrix, M_e, with the "factorizations" as the columns. For $e = 15$,

$$M_{15} = \begin{bmatrix}
\frac{14}{15} & \frac{13}{15} & \frac{4}{5} & \frac{11}{15} & \frac{2}{3} & \frac{3}{5} & \frac{8}{15} & \frac{7}{15} & \frac{2}{5} & \frac{1}{3} & \frac{4}{15} & \frac{1}{5} & \frac{2}{15} & \frac{1}{15} \\
\frac{7}{15} & \frac{14}{15} & \frac{2}{5} & \frac{13}{15} & \frac{1}{3} & \frac{4}{5} & \frac{4}{15} & \frac{11}{15} & \frac{1}{5} & \frac{2}{3} & \frac{2}{15} & \frac{3}{5} & \frac{1}{15} & \frac{8}{15} \\
\frac{11}{15} & \frac{7}{15} & \frac{1}{5} & \frac{14}{15} & \frac{2}{3} & \frac{2}{5} & \frac{2}{15} & \frac{13}{15} & \frac{3}{5} & \frac{1}{3} & \frac{1}{15} & \frac{4}{5} & \frac{8}{15} & \frac{4}{15} \\
\frac{2}{15} & \frac{4}{15} & \frac{2}{5} & \frac{8}{15} & \frac{2}{3} & \frac{4}{5} & \frac{14}{15} & \frac{1}{15} & \frac{1}{5} & \frac{1}{3} & \frac{7}{15} & \frac{3}{5} & \frac{11}{15} & \frac{13}{15} \\
\frac{13}{15} & \frac{11}{15} & \frac{3}{5} & \frac{7}{15} & \frac{1}{3} & \frac{1}{5} & \frac{1}{15} & \frac{14}{15} & \frac{4}{5} & \frac{2}{3} & \frac{8}{15} & \frac{2}{5} & \frac{4}{15} & \frac{2}{15} \\
\frac{4}{15} & \frac{8}{15} & \frac{4}{5} & \frac{1}{15} & \frac{1}{3} & \frac{3}{5} & \frac{13}{15} & \frac{2}{15} & \frac{2}{5} & \frac{2}{3} & \frac{14}{15} & \frac{1}{5} & \frac{7}{15} & \frac{11}{15} \\
\frac{8}{15} & \frac{1}{15} & \frac{3}{5} & \frac{2}{15} & \frac{2}{3} & \frac{1}{5} & \frac{11}{15} & \frac{4}{15} & \frac{4}{5} & \frac{1}{3} & \frac{13}{15} & \frac{2}{5} & \frac{14}{15} & \frac{7}{15} \\
\frac{1}{15} & \frac{2}{15} & \frac{1}{5} & \frac{4}{15} & \frac{1}{3} & \frac{2}{5} & \frac{7}{15} & \frac{8}{15} & \frac{3}{5} & \frac{2}{3} & \frac{11}{15} & \frac{4}{5} & \frac{13}{15} & \frac{14}{15}
\end{bmatrix}.$$

To factor the ideal generated by a product of Gauss sums, we need only to add the appropriate columns of M_e and multiply by $p-1$. Moreover, to find two distinct products of Gauss sums that generate the same idea, we need only find distinct sets of columns that have identical sums. Thus, multiplicative relations correspond exactly with elements of the nullspace of M_e. Using PARI/GP to compute a basis

for the nullspace of M_{15}, we obtain

$$N_{15} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & -1 & -1 & -1 & -1 & -1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & -1 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Looking at the second column of N_{15}, for example, we see that $\tau(1)\tau(6)$ and $\tau(2)\tau(5)$ generate the same ideal of $\mathcal{O}_E$; therefore, $\tau(1)\tau(6) = \mu \cdot \tau(2)\tau(5)$, for some unit $\mu \in E$.

The nullspace, however, spans all multiplicative relations, not just sign ambiguities. To isolate the new relations, we then coded the norm and Davenport-Hasse relations into another matrix, $\mathcal{M}_e$, and searched for relations from N_e that were not in the image of $\mathcal{M}_e$. This method produced a large number of *equivalent* new relations for relatively small values of e, ($e < 200$). While Theorem (2.32) guaranteed only one new relation for our choices of e, that one relation has many different forms as it must be considered modulo all of the other relations. However, given

a multiplicative relation, this method provided a simple computational test to determine if it followed from the norm relation and Davenport-Hasse.

In an effort to obtain a relatively simple representative of the new multiplicative relation, we restricted our search to values of $e \equiv 3 \pmod 4$ and, following Muskat, [14], we further restricted to products of Gauss sums fixed by a large number of automorphisms. In particular, we looked for Gauss sums that generated ideals which factored over $\mathcal{O}_K$, where $K = \mathbf{Q}(\sqrt{-e})$. Given such a product, $\omega \in \mathbf{Q}(\zeta_e) \subseteq \mathbf{Q}(\zeta_{ep})$, and an automorphism $\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta_e)/K)$, we have that $\sigma(\omega)\mathcal{O}_M = \omega\mathcal{O}_M$, and thus $\sigma(\omega) = \mu\omega$, for some unit $\mu \in \mathbf{Q}(\zeta_e)$. Relations of this type that do not follow from the known relations are sign ambiguities. Also, since ω generates an ideal factoring over $\mathcal{O}_K$, it will factor only into powers of the quadratic primes above p, i.e. if $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, then $\omega\mathcal{O}_E = \mathfrak{p}_1^{\alpha}\mathfrak{p}_2^{\beta}\mathcal{O}_E$, for some α, $\beta \in \mathbf{Z}$.

After analyzing large amounts of data, an interesting observation was made: for many values of e, there was a product of Gauss sums as above with $\omega\mathcal{O}_E = \mathfrak{p}_1^{\alpha}\mathfrak{p}_2^{\beta}\mathcal{O}_E$, such that $\beta - \alpha = h_K/4$, where h_K is the class number of K. Moreover, in these cases the number of individual Gauss sums comprising ω was small among all of the equivalent forms of this new relation. Based on this computational evidence, we make the following conjecture.

Conjecture 3.34. *Let $e = q_1q_2 \equiv 3 \pmod 4$ with q_1 a quadratic residue modulo q_2 and let σ be an automorphism of $\mathbf{Q}(\zeta_e)$ sending both $\sqrt{q_1}$ and $\sqrt{-q_2}$ to conjugates. If ω is a product of Gauss sums such that $\omega\mathcal{O}_E = p^{\alpha}\mathfrak{p}_1^{h_K/4}$, then $\sigma(\omega) = \pm\zeta_e^k\omega$ is a sign ambiguity.*

The conjecture provided a more effective method of gathering data. Rather than computing nullspaces, we instead looked for products of Gauss sums with the factorization from the conjecture and then quickly checked if each was in the image

of the matrix of known relations. Using the conjecture in this way, we were able to generate many more new sign ambiguities, ($e < 1000$). To prove the conjecture, we then looked for similarities among products of the above form for various values of e, and attempted to find a formula producing them.

In the next sections, we present a product formula giving a partial proof of the conjecture. In particular, we prove the conjecture for all values of e such that $e = q_1 q_2$, with $q_1 \equiv 5 \pmod 8, q_2 \equiv 3 \pmod 4$, and q_2 a biquadratic residue modulo q_1.

3.2 Biquadratic Coset Sums

For any positive integer n and for any $a \in \mathbf{Z}/n\mathbf{Z}$, let $L_n(a)$ denote the least positive *integer* congruent to a modulo n. Furthermore, for $a \in \mathbf{Z}$, we will also let $L_n(a) = L_n(\pi_n(a))$, where $\pi_n \colon \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ is the quotient map. This should not cause confusion as L_n simply returns the least positive *integer* congruent to $a \bmod n$. Finally, if $n = e$ we will suppress the subscript, i.e. $L = L_e$.

For the remainder of the dissertation, 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. Recall from Definition 1.4 that a is a biquadratic residue modulo m if $x^4 \equiv a \pmod m$ is solvable. Let $G = (\mathbf{Z}/e\mathbf{Z})^\times$ and let H_4 denote the biquadratic residues modulo e. The proof of our main theorem 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 sums

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

We now consider these sums.

Proposition 3.35. *Let $e = q_1 q_2$ and G be as stated. Then there is a $g \in G$ such that*

$$G/H_4 = \{\pm H_4, \pm gH_4, \pm g^2 H_4, \pm g^3 H_4\}.$$

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

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

Let $\psi \colon \langle g_{q_1} \rangle \times \langle g_{q_2} \rangle \to (\mathbf{Z}/e\mathbf{Z})^\times$ 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 $gH_4 \in G/H_4$. Computing powers of g, we see that $g^4 \in H_4$, but $g^i \notin H_4$ for $i = 1, 2, 3$. Thus gH_4 has order 4 in G/H_4. In particular, we have the following cosets of H_4

$$\begin{aligned}
H_4 &\xrightarrow{\psi^{-1}} \langle g_{q_1}^4 \rangle \times \langle g_{q_2}^2 \rangle \\
gH_4 &\xrightarrow{\psi^{-1}} (g_{q_1}, g_{q_2}) \left(\langle g_{q_1}^4 \rangle \times \langle g_{q_2}^2 \rangle\right) \\
g^2 H_4 &\xrightarrow{\psi^{-1}} (g_{q_1}^2, g_{q_2}^2) \left(\langle g_{q_1}^4 \rangle \times \langle g_{q_2}^2 \rangle\right) \\
g^3 H_4 &\xrightarrow{\psi^{-1}} (g_{q_1}^3, g_{q_2}^3) \left(\langle g_{q_1}^4 \rangle \times \langle g_{q_2}^2 \rangle\right)
\end{aligned}$$

Now consider $-gH_4$.

$$\begin{aligned}
\psi^{-1}(-gH_4) &= (-g_{q_1}, -g_{q_2})(\langle g_{q_1}^4\rangle \times \langle)g_{q_2}^2\rangle \\
&= (-1,-1))(g_{q_1}, g_{q_2})(\langle g_{q_1}^4\rangle \times \langle g_{q_2}^2\rangle) \\
&= (g_{q_1}^{\frac{q_1-1}{2}}, g_{q_2}^{\frac{q_2-1}{2}})(g_{q_1}, g_{q_2})(\langle g_{q_1}^4\rangle \times \langle g_{q_2}^2\rangle) \\
&= (g_{q_1}^{\frac{q_1+1}{2}}, g_{q_2}^{\frac{q_2+1}{2}})(\langle g_{q_1}^4\rangle \times \langle g_{q_2}^2\rangle) \\
&= (g_{q_1}^{2\alpha+1}, g_{q_2}^{2\beta})(\langle g_{q_1}^4\rangle \times \langle g_{q_2}^2\rangle),
\end{aligned}$$

for some $\alpha, \beta \in \mathbf{Z}$, since $q_1 \equiv 1 \pmod 4$ and $q_2 \equiv 3 \pmod 4$. Since the components of the coset $\psi^{-1}(-gH_4)$ have exponents of different parity, it clearly cannot be a power of $\psi^{-1}(gH_4)$. Computing powers of $-gH_4$ we see that it also has order 4 in G/H_4, with powers distinct from those of gH_4. Therefore, since

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

we have that

$$G/H_4 = \{\pm H_4, \pm gH_4, \pm g^2H_4, \pm g^3H_4\}.$$

□

We will now prove three lemmas concerning coset sums. We will 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 parts. We first show that

$$\sum_{a\in H_4} L(a) = \sum_{a\in H_4} L(g^2 a).$$

We then show that

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

And finally, we show that all four are equal by showing that

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

Lemma 3.36. *Let $e = q_1q_2$, G, and H_4 be as above. Then*

$$\sum_{a\in H_4} L(a) = \sum_{a\in H_4} L(g^2a).$$

Proof. From Proposition 3.35, we have that $H_4 \cong \langle g_{q_1}^4 \rangle \times \langle g_{q_2}^2 \rangle$. Let T_4 denote the biquadratic residues modulo q_1 and N_2 denote the quadratic residues modulo q_2. Let $a_1 \in \mathbf{Z}$ be such that $a_1q_2 \equiv 1 \pmod{q_1}$ and $a_2 \in \mathbf{Z}$ be such that $a_2q_1 \equiv 1 \pmod{q_2}$. Then by the Chinese Remainder Theorem,

$$L(H_4) = \{L(ta_1q_2 + na_2q_1) \mid t \in L_{q_1}(T_4), n \in L_{q_2}(N_2)\}. \tag{3.3}$$

Setting $\mathcal{H}_4 = L(H_4)$, $\mathcal{T}_4 = L_{q_1}(T_4)$, and $\mathcal{N}_2 = L_{q_2}(N_2)$, Equation (3.3) becomes

$$\mathcal{H}_4 = \{L(ta_1q_2 + na_2q_1) \mid t \in \mathcal{T}_4, n \in \mathcal{N}_2\}. \tag{3.4}$$

But, since q_2 is a biquadratic residue modulo q_1, $a_1 \in \mathcal{T}_4$ and $ta_1 \equiv t' \pmod{q_1}$, for some $t' \in \mathcal{T}_4$. And since $q_1 \equiv 1 \pmod 4$, $\left(\frac{q_1}{q_2}\right) = \left(\frac{q_2}{q_1}\right) = 1$, which implies that $a_2 \in \mathcal{N}_2$ and $na_2 \equiv n'$, for some $n' \in \mathcal{N}_2$. Combining and reindexing, we have

$$\mathcal{H}_4 = \{L(tq_2 + nq_1) \mid t \in \mathcal{T}_4, n \in \mathcal{N}_2\}$$

and need only show that

$$\sum_{\substack{t\in\mathcal{T}_4\\ n\in\mathcal{N}_2}} L(tq_2 + nq_1) = \sum_{\substack{t\in\mathcal{T}_4\\ n\in\mathcal{N}_2}} L(L(g^2)(tq_2 + nq_1)).$$

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

$$L\left(g_0^2(tq_2 + nq_1)\right) = L\left((g_0^2t)q_2 + (g_0^2n)q_1\right).$$

But g_0^2 and n are both squares modulo q_2, so $g_0^2 n \equiv n' \pmod{q_2}$ for some $n' \in \mathcal{N}_2$. Furthermore, for any $t \in \mathcal{T}_4$, $g_0^2 t \equiv -t' \pmod{q_1}$, for some $t' \in \mathcal{T}_4$, so

$$L\left((g_0^2 t)q_2 + (g_0^2 n)q_1\right) = L(-t'q_2 + n'q_1) \quad \text{for some } t' \in \mathcal{T}_4 \text{ and } n' \in \mathcal{N}_2.$$

Upon reindexing, we are reduced to showing that

$$\sum_{\substack{t \in \mathcal{T}_4 \\ n \in \mathcal{N}_2}} L(tq_2 + nq_1) = \sum_{\substack{t \in \mathcal{T}_4 \\ n \in \mathcal{N}_2}} L(-tq_2 + nq_1). \tag{3.5}$$

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 $t \in \mathcal{T}_4$,

$$tq_2 + nq_1 > e \iff n > \frac{q_1 q_2 - tq_2}{q_1} \iff n > q_2 - \frac{tq_2}{q_1}.$$

Let $k_t = \#\{n \in \mathcal{N}_2 \mid n > q_2 - \frac{tq_2}{q_1}\}$.

Similarly, for the right summand of Equation (3.5) 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 $t \in \mathcal{T}_4$, $-tq_2 + nq_1 < 0 \iff n < \frac{tq_2}{q_1}$. 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

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

We have

$$\begin{aligned}
\sum_{a\in\mathcal{H}_4} L(a) - \sum_{a\in\mathcal{H}_4} L(g^2a) &= \\
&= \sum_{t\in\mathcal{T}_4}\left(-ek_t + \sum_{n\in\mathcal{N}_2} tq_2 + nq_1\right) - \sum_{t\in\mathcal{T}_4}\left(el_t + \sum_{n\in\mathcal{N}_2} -tq_2 + nq_1\right) \\
&= \sum_{t\in\mathcal{T}_4}\left(-e(k_t+l_t) + \sum_{n\in\mathcal{N}_2} 2tq_2\right) \\
&= \sum_{t\in\mathcal{T}_4}\left(-e(k_t+l_t) + 2tq_2\sum_{n\in\mathcal{N}_2} 1\right) \\
&= \sum_{t\in\mathcal{T}_4}\left(-e(k_t+l_t) + 2tq_2\left(\frac{q_2-1}{2}\right)\right) \\
&= \sum_{t\in\mathcal{T}_4}\left(-e(k_t+l_t) + tq_2(q_2-1)\right).
\end{aligned}$$

Now,

$$\begin{aligned}
l_t &= \#\left\{n\in\mathcal{N}_2 \mid n < \frac{tq_2}{q_1}\right\} \\
&= \#\left\{n\in\mathcal{N}_2 \mid -n > \frac{-tq_2}{q_1}\right\} \\
&= \#\left\{n\in\mathcal{N}_2 \mid q_2 - n > q_2 - \frac{tq_2}{q_1}\right\}.
\end{aligned}$$

Since n is a quadratic residue modulo q_2, $q_2 - n$ is 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,

$$\begin{aligned}
k_t + l_t &= q_2 - \left\lceil q_2 - \frac{tq_2}{q_1}\right\rceil \\
&= q_2 - q_2 + \left\lfloor \frac{tq_2}{q_1}\right\rfloor \\
&= \left\lfloor \frac{tq_2}{q_1}\right\rfloor.
\end{aligned}$$

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 $t' \in \mathcal{T}_4$. Reindexing and summing over t,

$$\sum_{t\in\mathcal{T}_4} \left\lfloor \frac{tq_2}{q_1} \right\rfloor = \sum_{t\in\mathcal{T}_4} \left(\frac{tq_2}{q_1} - \frac{t}{q_1} \right) = \sum_{t\in\mathcal{T}_4} \left(\frac{t(q_2-1)}{q_1} \right). \tag{3.6}$$

Therefore,

$$\begin{aligned}
\sum_{t\in\mathcal{T}_4} (-e(k_t+l_t) + tq_2(q_2-1)) &= \sum_{t\in\mathcal{T}_4} (tq_2(q_2-1) - e(k_t+l_t)) \\
&= \sum_{t\in\mathcal{T}_4} \left(tq_2(q_2-1) - q_1q_2 \left\lfloor \frac{tq_2}{q_1} \right\rfloor \right) \\
&= q_2(q_2-1) \sum_{t\in\mathcal{T}_4} t - q_1q_2 \sum_{t\in\mathcal{T}_4} \left\lfloor \frac{tq_2}{q_1} \right\rfloor \\
&= q_2(q_2-1) \sum_{t\in\mathcal{T}_4} t - q_1q_2 \sum_{t\in\mathcal{T}_4} \left(\frac{t(q_2-1)}{q_1} \right) \\
&= q_2(q_2-1) \sum_{t\in\mathcal{T}_4} t - q_2(q_2-1) \sum_{t\in\mathcal{T}_4} t \\
&= 0.
\end{aligned}$$

Hence,

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

proving the lemma. □

Lemma 3.37. *With notation as before,*

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

Proof. As in the previous lemma, for $a \in H_4,\ a = L(tq_2+nq_1)$ for some $t \in \mathcal{T}_4,\ n \in \mathcal{N}_2$. Then,

$$\begin{aligned} L(ga) &= L(g_0(tq_2 + nq_1)) \\ &= L\left(g_0tq_2 + (g_0n)q_1\right) \\ &= L\left(g_0tq_2 - n'q_1\right), \quad \text{for some } n' \in \mathcal{N}_2, \end{aligned}$$

since g_0 is a nonsquare modulo q_2 and $q_2 \equiv 3 \pmod 4$.

On the other hand,

$$\begin{aligned} L(g^3a) &= L(g_0^3(tq_2 + nq_1)) \\ &= L\left(g_0(g_0^2(tq_2 + nq_1))\right) \\ &= L\left((g_0(-t'q_2 + n'q_1)\right) \\ &= L\left(-(g_0t')q_2 + (g_0n')q_1\right), \end{aligned}$$

where the third 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 $n'' \in \mathcal{N}_2$. Combining and reindexing, we now need only show that

$$\sum_{\substack{t\in\mathcal{T}_4\\ n\in\mathcal{N}_2}} L\left(g_0tq_2 - nq_1\right) = \sum_{\substack{t\in\mathcal{T}_4\\ n\in\mathcal{N}_2}} L\left(-g_0tq_2 - nq_1\right),$$

or equivalently

$$\sum_{\substack{t\in\mathcal{T}_4\\ n\in\mathcal{N}_2}} \overbrace{L\left(L_{q_1}(g_0t)q_2 - nq_1\right)}^{(*)} = \sum_{\substack{t\in\mathcal{T}_4\\ n\in\mathcal{N}_2}} \overbrace{L\left(-L_{q_1}(g_0t)q_2 - nq_1\right)}^{(**)}.$$

Now, $-e < L_{q_1}(g_0t)q_2 - nq_1 < e$, and thus

$$(*) = \begin{cases} L_{q_1}(g_0t)q_2 - nq_1, & \text{if } L_{q_1}(g_0t)q_2 - nq_1 > 0 \\ L_{q_1}(g_0t)q_2 - nq_1 + e, & \text{if } L_{q_1}(g_0t)q_2 - nq_1 < 0. \end{cases}$$

For fixed $t \in \mathcal{T}_4$,

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

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

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 $t \in \mathcal{T}_4$,

$$\begin{aligned} -L_{q_1}(g_0 t)q_2 - nq_1 < -e &\iff L_{q_1}(g_0 t)q_2 + nq_1 > e \\ &\iff n > \frac{q_2(q_1 - L_{q_1}(g_0 t))}{q_1} \\ &\iff q_2 - n < q_2 - \frac{q_2(q_1 - L_{q_1}(g_0 t))}{q_1} \\ &\iff q_2 - n < \frac{L_{q_1}(g_0 t)q_2}{q_1}. \end{aligned}$$

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

$$\sum_{t \in \mathcal{T}_4} \left(ek_t + \sum_{n \in \mathcal{N}_2} L_{q_1}(g_0 t)q_2 - nq_1 \right) = \sum_{t \in \mathcal{T}_4} \left(el_t + \sum_{n \in \mathcal{N}_2} -L_{q_1}(g_0 t)q_2 - nq_1 + e \right).$$

Combining and simplifying, we have

$$\begin{aligned} \sum_{a \in H_4} L(ga) - \sum_{a \in H_4} L(g^3 a) = & \\ &= \sum_{t \in \mathcal{T}_4} \left(e(k_t - l_t) + \sum_{n \in \mathcal{N}_2} (2L_{q_1}(g_0 t)q_2 - e) \right) \\ &= e \sum_{t \in \mathcal{T}_4} (k_t - l_t) + \sum_{\substack{t \in \mathcal{T}_4 \\ n \in \mathcal{N}_2}} 2L_{q_1}(g_0 t)q_2 - \sum_{\substack{t \in \mathcal{T}_4 \\ n \in \mathcal{N}_2}} e \\ &= e \sum_{t \in \mathcal{T}_4} (k_t - l_t) + 2q_2 \left(\frac{q_2 - 1}{2} \right) \sum_{t \in \mathcal{T}_4} L_{q_1}(g_0 t) - e \left(\frac{q_1 - 1}{4} \right) \left(\frac{q_2 - 1}{2} \right) \\ &= e \sum_{t \in \mathcal{T}_4} (k_t - l_t) + q_2(q_2 - 1) \sum_{t \in \mathcal{T}_4} L_{q_1}(g_0 t) - e\frac{\phi(e)}{8}. \end{aligned}$$

But $n \in \mathcal{N}_2 \implies q_2 - n \notin \mathcal{N}_2$, 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 $\frac{q_2-1}{2}$ squares modulo q_2, the number of squares modulo q_2 greater than $\frac{L_{q_1}(g_0 t)q_2}{2}$ is given by

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

Hence, for each t,

$$k_t - l_t = \left(\frac{q_2 - 1}{2} - \left\lfloor \frac{L_{q_1}(g_0 t)q_2}{q_1} \right\rfloor + l_t \right) - l_t = \frac{q_2 - 1}{2} - \left\lfloor \frac{L_{q_1}(g_0 t)q_2}{q_1} \right\rfloor,$$

and as in Equation (3.6),

$$\sum_{t \in \mathcal{T}_4} \left\lfloor \frac{L_{q_1}(g_0 t)q_2}{q_1} \right\rfloor = \sum_{t \in \mathcal{T}_4} \left(\frac{L_{q_1}(g_0 t)(q_2 - 1)}{q_1} \right).$$

Therefore,

$$\begin{aligned}
e \sum_{t \in \mathcal{T}_4} (k_t - l_t) + q_2(q_2 - 1) \sum_{t \in \mathcal{T}_4} L_{q_1}(g_0 t) - \frac{e\phi(e)}{8} &= \\
&= e \sum_{t \in \mathcal{T}_4} \left(\frac{q_2 - 1}{2} - \left\lfloor \frac{L_{q_1}(g_0 t)q_2}{q_1} \right\rfloor \right) + q_2(q_2 - 1) \sum_{t \in \mathcal{T}_4} L_{q_1}(g_0 t) - \frac{e\phi(e)}{8} \\
&= e \sum_{t \in \mathcal{T}_4} \frac{q_2 - 1}{2} - e \sum_{t \in \mathcal{T}_4} \left\lfloor \frac{L_{q_1}(g_0 t)q_2}{q_1} \right\rfloor + q_2(q_2 - 1) \sum_{t \in \mathcal{T}_4} L_{q_1}(g_0 t) - \frac{e\phi(e)}{8} \\
&= \frac{e\phi(e)}{8} - e \sum_{t \in \mathcal{T}_4} \frac{L_{q_1}(g_0 t)(q_2 - 1)}{q_1} + q_2(q_2 - 1) \sum_{t \in \mathcal{T}_4} L_{q_1}(g_0 t) - \frac{e\phi(e)}{8} \\
&= e\frac{\phi(e)}{8} - q_2(q_2 - 1) \sum_{t \in \mathcal{T}_4} L_{q_1}(g_0 t) + q_2(q_2 - 1) \sum_{t \in \mathcal{T}_4} L_{q_1}(g_0 t) - \frac{e\phi(e)}{8} \\
&= 0,
\end{aligned}$$

and thus

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

□

Lemma 3.38. *With notation as above,*

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

Proof. Let H_2 denote the *quadratic* residues modulo e. Then, since the elements of the cosets H_4 and g^2H_4 partition H_2, we have that

$$\sum_{a\in H_4} L(a) + \sum_{a\in H_4} L(g^2a) = \sum_{a\in H_2} L(a)$$

and

$$\sum_{a\in H_4} L(ga) + \sum_{a\in H_4} L(g^3a) = \sum_{a\in H_2} L(ga).$$

Hence, we need only show

$$\sum_{a\in H_2} L(a) = \sum_{a\in H_2} L(ga).$$

From the proof of Proposition 3.35, we have that $H_2 \cong \langle g_{q_1}^2\rangle \times \langle g_{q_2}^2\rangle$. Thus, if T_2 denotes the quadratic residues modulo q_1 and $\mathcal{T}_2 = L_{q_1}(T_2)$, then we must show that

$$\sum_{\substack{t\in\mathcal{T}_2\\ n\in\mathcal{N}_2}} L(tq_2+nq_1) = \sum_{\substack{t\in\mathcal{T}_2\\ n\in\mathcal{N}_2}} L(g_0(tq_2+nq_1)),$$

Once more, since $g_0 \notin \mathcal{N}_2$,

$$L\left(g_0(tq_2+nq_1)\right) = L\left(g_0tq_2+(g_0n)q_1\right) = L\left(g_0tq_2-n'q_1\right),$$

and upon reindexing we need only prove that

$$\sum_{\substack{t\in\mathcal{T}_2\\ n\in\mathcal{N}_2}} L(tq_2+nq_1) = \sum_{\substack{t\in\mathcal{T}_2\\ n\in\mathcal{N}_2}} L(g_0tq_2-nq_1).$$

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 $n \in \mathcal{N}_2$,

$$tq_2 + nq_1 > e \iff t > q_1 - \frac{nq_1}{q_2} \iff q_1 - t < \frac{nq_1}{q_2}.$$

Let $k_n = \#\{t \in \mathcal{T}_2 \mid q_1 - t < \frac{nq_1}{q_2}\}$.

For the right summand, since $L(g_0 t q_2 - nq_1) = L(L_{q_1}(g_0 t)q_2 - nq_1)$ and $-e < L_{q_1}(g_0 t)q_2 - nq_1) < e$,

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

Fixing $n \in \mathcal{N}_2$,

$$L_{q_1}(g_0 t)q_2 - nq_1 < 0 \iff L_{q_1}(g_0 t) < \frac{nq_1}{q_2}.$$

Let $l_n = \#\{t \in \mathcal{T}_2 \mid L_{q_1}(g_0 t) < \frac{nq_1}{q_2}\}$. Then we are again reduced to proving the equality of the integer sums

$$\sum_{n \in \mathcal{N}_2} \left(-ek_n + \sum_{t \in \mathcal{T}_2} tq_2 + nq_1 \right) = \sum_{n \in \mathcal{N}_2} \left(el_n + \sum_{t \in \mathcal{T}_2} L_{q_1}(g_0 t)q_2 - nq_1 \right).$$

Now,

$$\begin{aligned} \sum_{a \in H_2} L(a) - \sum_{a \in H_2} L(ga) = & \\ &= \sum_{n \in \mathcal{N}_2} \left(-ek_n + \sum_{t \in \mathcal{T}_2} tq_2 + nq_1 \right) - \sum_{n \in \mathcal{N}_2} \left(el_n + \sum_{t \in \mathcal{T}_2} L_{q_1}(g_0 t)q_2 - nq_1 \right) \\ &= \sum_{n \in \mathcal{N}_2} \left(-e(k_n + l_n) + \sum_{t \in \mathcal{T}_2} tq_2 + nq_1 - L_{q_1}(g_0 t)q_2 + nq_1 \right) \\ &= -e \sum_{t \in \mathcal{T}_2} (k_n + l_n) + q_2 \left(\sum_{\substack{t \in \mathcal{T}_2 \\ n \in \mathcal{N}_2}} t - \sum_{\substack{t \in \mathcal{T}_2 \\ n \in \mathcal{N}_2}} L_{q_1}(g_0 t) \right) + 2q_1 \sum_{\substack{t \in \mathcal{T}_2 \\ n \in \mathcal{N}_2}} n. \end{aligned}$$

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, [9, Theorem 2.1]. Thus, since $q_1 \equiv 1 \pmod 4$,

$t \in \mathcal{T}_2$, and $L_{q_1}(g_0 t) \notin \mathcal{T}_2$, the middle two terms of the previous expression cancel, leaving only

$$-e \sum_{t \in \mathcal{T}_2} (k_n + l_n) + 2q_1 \sum_{\substack{t \in \mathcal{T}_2 \\ n \in \mathcal{N}_2}} n. \tag{3.7}$$

Fixing $n \in \mathcal{N}_2$, $k_n + l_n$ will be the number of units modulo q_1 less than $\frac{nq_1}{q_2}$. So, for the first summation of (3.7), we have

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

leaving it necessary to prove only that

$$-e \sum_{n \in \mathcal{N}_2} \left\lfloor \frac{nq_1}{q_2} \right\rfloor + 2q_1 \sum_{\substack{t \in \mathcal{T}_2 \\ n \in \mathcal{N}_2}} n = 0.$$

Applying an argument similar to that leading up to Equation (3.6),

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

and thus,

$$\begin{aligned}
-e \sum_{n \in \mathcal{N}_2} \left\lfloor \frac{nq_1}{q_2} \right\rfloor + 2q_1 \sum_{\substack{t \in \mathcal{T}_2 \\ n \in \mathcal{N}_2}} n &= 2q_1 \sum_{\substack{t \in \mathcal{T}_2 \\ n \in \mathcal{N}_2}} n - e \sum_{n \in \mathcal{N}_2} \left\lfloor \frac{nq_1}{q_2} \right\rfloor \\
&= 2q_1 \left(\frac{q_1 - 1}{2} \right) \sum_{n \in \mathcal{N}_2} n - e \sum_{n \in \mathcal{N}_2} \left(\frac{n(q_1 - 1)}{q_2} \right) \\
&= q_1(q_1 - 1) \sum_{n \in \mathcal{N}_2} n - e \sum_{n \in \mathcal{N}_2} \left(\frac{n(q_1 - 1)}{q_2} \right) \\
&= q_1(q_1 - 1) \sum_{n \in \mathcal{N}_2} n - q_1 q_2 \left(\frac{q_1 - 1}{q_2} \right) \sum_{n \in \mathcal{N}_2} n \\
&= q_1(q_1 - 1) \sum_{n \in \mathcal{N}_2} n - q_1(q_1 - 1) \sum_{n \in \mathcal{N}_2} n \\
&= 0.
\end{aligned}$$

Hence,

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

□

Combining the results from this section, we now have the following.

Theorem 3.39. *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*

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

Furthermore, for all i,

$$\sum_{a \in H_4} L(-g^i a) - \sum_{a \in H_4} L(g^i a) = \left(\frac{h_K}{4}\right) e, \tag{2}$$

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

Proof. By Lemmas (3.36), (3.37), and (3.38), we have

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

But, for $i = 0, \ldots, 3$,

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

and so

$$\sum_{a \in H_4} L(-g^i a) = e\left(\frac{\phi(e)}{8}\right) - \sum_{a \in H_4} L(g^i a). \tag{3.8}$$

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.

Let $H = \mathrm{Gal}(\mathbf{Q}(\zeta_e)/\mathbf{Q}(\sqrt{-e})) = \{h \in G \mid \left(\frac{h}{e}\right) = 1\}$. Then 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 H is the union of the elements in $g^i H_4$ for $i = 0, 1, 2, 3$, so we have

$$\begin{aligned} eh_K &= \sum_{a \in H} L(-a) - \sum_{a \in H} L(a) \\ &= 4 \sum_{a \in H_4} L(-g^i a) - 4 \sum_{a \in H_4} L(g^i a), \quad \forall i, \\ &= 4 \left(\sum_{a \in H_4} L(-g^i a) - \sum_{a \in H_4} L(g^i a) \right), \quad \forall i, \end{aligned}$$

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

Corollary 3.40.

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. By Theorem 3.39 (2), $\sum_{a \in H_4} L(-g^i a) - \sum_{a \in H_4} L(g^i a) \equiv 0 \pmod e$ and thus $\sum_{a \in H_4} L(-g^i a) \equiv \sum_{a \in H_4} L(g^i a) \pmod e$. But, by statement (1) of Theorem 3.39, $\sum_{a \in H_4} L(-g^i a) \neq \sum_{a \in H_4} L(g^i a)$, so we must have that $\sum_{a \in H_4} L(g^i a) \equiv \sum_{a \in H_4} L(-g^i a) \equiv 0 \pmod e$, proving the first statement.

Reducing Equation 3.8 modulo 2, we have $\sum_{a \in H_4} L(-g^i a) \equiv 1 - \sum_{a \in H_4} L(g^i a) \pmod 2 \implies \sum_{a \in H_4} L(-g^i a) - \sum_{a \in H_4} L(g^i a) \equiv 1 \pmod 2$, for all i. Thus, comparing with Theorem 3.39 (2), we conclude that $h_K \equiv 4 \pmod 8$, completing the proof. □

3.3 A Product Formula

For values of e as in the previous section, we claim that $\omega = \prod_{t \in H_4} \tau(t)$ has the desired properties from the conjecture. For these values of e, we have the following

field diagram with corresponding Galois groups over $\mathbf{Q}$.

Field	**Galois Group over Q**
$\mathbf{Q}(\zeta_{ep}) = E$	$\longleftrightarrow G \times (\mathbf{Z}/p\mathbf{Z})^\times$
$\Big\vert\, p-1$	
$\mathbf{Q}(\zeta_e) = M$	$\longleftrightarrow G$
$\Big\vert\, \frac{\phi(e)}{8}$	
$(H_4)' = \widehat{K}$	$\longleftrightarrow G/H_4$
$\Big\vert\, 2$	
$\mathbf{Q}(\sqrt{-e}, \sqrt{q_1}) = \widetilde{K}$	$\longleftrightarrow G/H_2$
$\Big\vert\, 2$	
$\mathbf{Q}(\sqrt{-e}) = K$	$\longleftrightarrow G/H$
$\Big\vert\, 2$	
$\mathbf{Q}$	$\longleftrightarrow \{1\}.$

Using the results concerning the biquadratic coset sums from the previous section, we first show that $\omega \in \widehat{K}$ and that $\omega\mathcal{O}_E$ factors over $\mathcal{O}_K$. Then, using a result of Yamamoto from [22], we conclude that $\sigma_t(\omega) = \pm\zeta_e^k\omega$ is indeed a sign ambiguity.

Lemma 3.41. *Let $X = \{a_i\}_{i=1}^r$ be a subset of the integers modulo e such that $\sum_i a_i \equiv 0 \pmod{e}$, then*

$$\prod_{i=1}^{r} \tau(a_i) \in \mathbf{Q}(\zeta_e).$$

Proof. Let $c \in \mathbf{Z}/e\mathbf{Z}$ and consider the Jacobi sum product

$$J(a_1, c)J(a_2, a_1 + c)J(a_3, a_1 + a_2 + c) \cdots J(a_r, a_1 + a_2 + \cdots + a_{r-1} + c). \qquad (*)$$

We have,

$$\begin{aligned}(*) &= \frac{\tau(a_1)\tau(c)}{\tau(a_1+c)} \cdot \frac{\tau(a_2)\tau(a_1+c)}{\tau(a_1+a_2+c)} \cdots \frac{\tau(a_r)\tau(a_1+a_2+\cdots a_{r-1}+c)}{\tau(a_1+a_2+\cdots a_r+c)} \\ &= \frac{\tau(c)\tau(a_1)\tau(a_2)\cdots\tau(a_r)}{\tau(a_1+a_2+\cdots a_r+c)} \\ &= \tau(a_1)\tau(a_2)\cdots\tau(a_r), \quad \text{since } a_1+a_2+\cdots+a_r \equiv 0 \pmod{e}.\end{aligned}$$

But for any $\alpha, \beta \in \mathbf{Z}$, $J(\alpha,\beta) \in \mathbf{Q}(\zeta_e) \implies (*) \in \mathbf{Q}(\zeta_e) \implies \prod_{i=1}^{r} \tau(a_i) \in \mathbf{Q}(\zeta_e)$. □

Proposition 3.42. $\omega \in \widehat{K}$.

Proof. By Corollary 3.40, $\sum_{a\in H_4} L(a) \equiv 0 \pmod{e}$, so $\omega \in \mathbf{Q}(\zeta_e)$ by the lemma. Furthermore, $\forall j \in H_4$, σ_j will only permute the Gauss sums comprising ω. Thus, ω is fixed by every automorphism from H_4, that is, $\omega \in (H_4)' = \widehat{K}$. □

Although $\omega \in \widehat{K}$, we will first consider the ideal generated by ω in $\mathcal{O}_M$, i.e. $\omega\mathcal{O}_M$, so we can use the Stickelberger factorization formula.

Theorem 3.43.

$$\omega\mathcal{O}_M = (p^{\alpha}\mathfrak{p}^{\frac{h_K}{4}})\mathcal{O}_M,$$

where $\alpha = \sum_{t\in H_4} L(t)$ *and* $\mathfrak{p}$ *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 (corollary to) Stickelberger factorization formula,

$$\begin{aligned}\omega\mathcal{O}_M &= \left(\prod_{t\in H_4} \tau(t)\right)\mathcal{O}_M \\ &= \prod_{t\in H_4} P^{\sum_{a\in G}\left\{\frac{ta^{-1}}{e}\right\}\sigma_a} \\ &= P^{\sum_{t\in H_4}\left(\sum_{a\in G}\left\{\frac{ta^{-1}}{e}\right\}\sigma_a\right)} \\ &= P^{\sum_{a\in G}\left(\sum_{t\in H_4}\left\{\frac{ta^{-1}}{e}\right\}\right)\sigma_a}.\end{aligned}$$

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 3.39, 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 3.39 that $\alpha < \beta$. But $ta^{-1} \in g^i H_4 \iff a \in H$, so we have

$$\begin{aligned} \omega \mathcal{O}_M &= P^{\sum_{a \in G} \left(\sum_{t \in H_4} \left\{ \frac{ta^{-1}}{e} \right\} \right) \sigma_a} \\ &= P^{\alpha \sum_{a \in H} \sigma_a + \beta \sum_{a \notin H} \sigma_a} \\ &= p^\alpha P^{(\beta - \alpha) \sum_{a \notin H} \sigma_a} \\ &= p^\alpha P^{\frac{h_K}{4} \sum_{a \notin H} \sigma_a} \\ &= p^\alpha \left(P^{\sum_{a \notin H} \sigma_a} \right)^{\frac{h_K}{4}}. \end{aligned} \tag{3.9}$$

For $a \in G$, consider $(\sigma_a)|_K$. Since $\mathrm{Gal}(K/\mathbf{Q}) \cong G/H$, $(\sigma_a)|_K$ is nontrivial if and only if $a \notin H$. Thus, if $p\mathcal{O}_K = \mathfrak{p}_1 \mathfrak{p}_2$, then

$$\mathfrak{p}_1 \mathcal{O}_M = \prod_{a \in H} P^{\sigma_a} = P^{\sum_{a \in H} \sigma_a} \quad \text{and} \quad \mathfrak{p}_2 \mathcal{O}_M = \prod_{a \notin H} P^{\sigma_a} = P^{\sum_{a \notin H} \sigma_a}.$$

Therefore, continuing (3.9),

$$\omega \mathcal{O}_M = p^\alpha \left(P^{\sum_{a \notin H} \sigma_a} \right)^{\frac{h_K}{4}} = p^\alpha \left(\mathfrak{p}_2 \mathcal{O}_M \right)^{\frac{h_K}{4}} = p^\alpha \mathfrak{p}_2^{\frac{h_K}{4}} \mathcal{O}_M.$$

□

Corollary 3.44. *$\forall t \in H$, $(\sigma_t(\omega))\mathcal{O}_M = \omega \mathcal{O}_M$.*

Proof. Let $t \in H$. Then,

$$\begin{aligned}(\sigma_t(\omega))\mathcal{O}_M = \sigma_t\left(\omega\mathcal{O}_M\right) &= \sigma_t\left(p^\alpha \mathfrak{p}^{\frac{h_K}{4}}\right)\mathcal{O}_M \\ &= p^\alpha \sigma_t\left(\mathfrak{p}^{\frac{h_K}{4}}\right)\mathcal{O}_M \\ &= p^\alpha \left(\sigma_t(\mathfrak{p})\right)^{\frac{h_K}{4}}\mathcal{O}_M \\ &= \left(p^\alpha \mathfrak{p}^{\frac{h_K}{4}}\right)\mathcal{O}_M,\end{aligned}$$

since $\mathfrak{p} \subseteq \mathcal{O}_K$ and K is the fixed field of H. □

Remark 3.45. *Since ω and $\sigma_t(\omega)$ generate the same ideal in $\mathcal{O}_M$ and have the same absolute value, it follows that they can only differ by a unit of absolute value 1. But, by Theorems 1.15 and 1.16, the only units of absolute value 1 in $\mathbf{Q}(\zeta_e)$ are $\pm\zeta_e^k$, $k = 1, \ldots, e$, so we have that*

$$\sigma_t(\omega) = \pm\zeta_e^{k_t}\omega, \quad \textit{for some } k_t \in \mathbf{Z}. \tag{3.10}$$

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 3.46.

$$k_0 \equiv \begin{cases} -q_1\, ind_\gamma(q_1) \pmod e, & \textit{if } e = q_1 \cdot 3 \\ 3(1-t_0)q_2\, ind_\gamma(q_2) \pmod e, & \textit{if } e = 5 \cdot q_2 \\ 0 \pmod e, & \textit{if } \gcd(e,15) = 1. \end{cases} \tag{3.11}$$

Proof. As ω, $\sigma_{t_0}(\omega) \in \widehat{K}$, we must have that $\zeta_e^{k_0} \in \widehat{K}$ as well. We first determine which roots of unity lie in $\widehat{K}$. Assume $\zeta_n \in \widehat{K}$ for some integer $n > 2$. Since $\widehat{K} \subseteq \mathbf{Q}(\zeta_e)$, $n \mid 2e$, and thus either $n = q_1$, or $n = q_2$, (note that $\mathbf{Q}(\zeta_{2q_i}) = \mathbf{Q}(\zeta_{q_i})$). Furthermore, since $[\widehat{K} : \mathbf{Q}] = 8$, $\phi(n) \mid 8$. 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 $\widehat{K}$ are ± 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 $\widehat{K}$ and thus, $k_0 \equiv 0 \pmod{q_1}$. Finally, if $e = 5 \cdot q_2$, then the only possible roots of unity in $\widehat{K}$ are powers of $\pm\zeta_5 = \pm\zeta_e^{q_2}$ and $k_0 \equiv 0 \pmod{q_2}$.

Assume $e = q_1 \cdot 3$. Using Equation 2.2 with $m = 3$, $n = q_1$, and $t = 2$, we obtain the following Davenport-Hasse relation

$$\chi^{2q_1}(q_1) \prod_{k=0}^{q_1-1} \tau(3k+2) = \tau(2q_1) \prod_{k=1}^{q_1-1} \tau(3k).$$

Comparing with the eight cosets of G/H_4, this relation can be rewritten as

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

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

$$\frac{p^{(q_1-1)/2}}{\sigma_{t_0^3}(\omega)\sigma_{-t_0^2}(\omega)} = \pm\zeta_e^{k_0}\chi^{2q_1}(q_1).$$

Multiplying numerator and denominator by $\sigma_{-t_0^3}(\omega)$ and again using the norm relation, we obtain

$$\frac{\sigma_{-t_0^3}(\omega)}{\sigma_{-t_0^2}(\omega)} = \sigma_{-t_0^2}\left(\frac{\sigma_{t_0}(\omega)}{\omega}\right) = \pm\zeta_e^{k_0}\chi^{2q_1}(q_1).$$

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, $\chi(\gamma) = \zeta_e$, so $\chi^{2q_1}(q_1) = \chi^{2q_1}(\gamma^{ind_\gamma(q_1)}) = \zeta_e^{2q_1\, ind_\gamma(q_1)}$, and therefore $\zeta_e^{-k_0(t_0^2+1)} = \zeta_e^{2q_1\, ind_\gamma(q_1)}$. But, as $k_0 \equiv 0 \pmod{q_1}$, we have

$$\begin{aligned}
\zeta_e^{-k_0(t_0^2+1)} = \zeta_e^{2q_1\, ind_\gamma(q_1)} &\iff -k_0(t_0^2+1) \equiv 2q_1\, ind_\gamma(q_1) \pmod{q_1 \cdot 3} \\
&\iff -k_0(t_0^2+1) \equiv 2q_1\, ind_\gamma(q_1) \pmod{3} \\
&\iff k_0 \equiv -q_1\, ind_\gamma(q_1) \pmod{3}.
\end{aligned}$$

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

Now assume $e = 5 \cdot q_2$. We proceed as in the previous case. Applying Equation 2.2 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

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

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

$$\begin{aligned}
\zeta_e^{-t_0^2 k_0} = \zeta_e^{-k_0 + q_2(1-t_0)\, ind_\gamma(q_2)} &\iff \zeta_e^{k_0(1-t_0^2)} = \zeta_e^{q_2(1-t_0)\, ind_\gamma(q_2)} \\
&\iff k_0(1-t_0^2) \equiv q_2(1-t_0)\, ind_\gamma(q_2) \pmod{5q_2} \\
&\iff k_0(1-t_0^2) \equiv q_2(1-t_0)\, ind_\gamma(q_2) \pmod 5 \\
&\iff k_0 \equiv 3(1-t_0) q_2\, ind_\gamma(q_2) \pmod 5.
\end{aligned}$$

Therefore, $k_0 \equiv 3(1-t_0)q_2\, ind_\gamma(q_2) \pmod{5q_2}$, completing the proof. □

Remark 3.47. *Note that the congruences for k_0 in the previous theorem can be rewritten as*

$$k_0 \equiv \begin{cases} L_3(-ind_\gamma(q_1))q_1 \pmod e, & \text{if } e = q_1 \cdot 3 \\ L_5(3(1-t_0)\, ind_\gamma(q_2))q_2 \pmod e, & \text{if } e = 5 \cdot q_2 \\ 0 \pmod e, & \text{if } \gcd(e, 15) = 1. \end{cases} \tag{3.12}$$

We claim that $\sigma_{t_0}(\omega) = \pm\zeta_e^{k_0}\omega$ is a sign ambiguity. We will need the following weakened version of a result implied in [22].

Lemma 3.48. *Let $e = p_1p_2$, for any primes p_1, p_2. Assume*

$$\prod_i \tau(a_i) = \pm\zeta_e^k \prod_j \tau(b_j) \tag{3.13}$$

for some a_i, b_j, $k \in \mathbf{Z}$, and let $\Lambda = \{L(p_1+p_2), L(p_1-p_2), L(p_2-p_1), L(-p_1-p_2)\}$. If $\#\{i|a_i \in \Lambda\} - \#\{j|b_j \in \Lambda\} \equiv 1 \pmod 2$, then equation 3.13 is a not direct consequence of the norm relation and the Davenport-Hasse product formula.

Proof. We prove the contrapositive. A multiplicative relation (3.13) follows from the norm relation and Davenport-Hasse if and only if it can written as a linear combination of these relations. For any norm relation, $\tau(a)\tau(-a) = \chi^a(-1)p$, we have that $a \in \Lambda \iff -a \in \Lambda$. Thus, each use of a norm relation contributes an even number of elements to the set $\{i|a_i \in \Lambda\}$. Now consider the Davenport-Hasse relations. Splitting the quotient of (2.2) and reindexing the left side, we have that for $e = mn$, with $m, n > 1$, and for $1 \leq t \leq m-1$,

$$\chi^{tn}(n) \prod_{k=0}^{n-1} \tau(km+t) = \tau(tn) \prod_{k=1}^{n-1} \tau(km).$$

On the right hand side, none of the Gauss sums will contribute to $\{i|a_i \in \Lambda\}$, since $\gcd(tn, e)$ and $\gcd(km, e) \neq 1$. For the left side, fix t and assume $km + t \in \Lambda$. Then $km + t \equiv \pm m \pm n \pmod{e} \implies$ either $t = mx + n$ or $t = mx - n$, for some (unique) x. Without loss of generality, assume $t = mx + n$. Then $km + t \in \Lambda \iff km + (mx+n) = m(k+x) + n \in \Lambda \iff m(k+x) \equiv \pm m \pmod{n} \iff k + x \equiv \pm 1 \pmod{n} \iff k \equiv \pm 1 - x \pmod{n}$. Thus, for fixed t, there are exactly two values of k, $1 \leq k \leq n-1$, such that $km + t \in \Lambda$. Therefore, each use of a Davenport-Hasse relation contributes an even number of elements to the set $\{i|a_i \in \Lambda\}$. Hence, if a multiplicative relation (3.13) is written as a linear combination of norm and Davenport-Hasse relations, then each use of a relation will contribute an even number or elements to $\{i|a_i \in \Lambda\}$ and thus

$$\#\{i|a_i \in \Lambda\} - \#\{j|b_j \in \Lambda\} \equiv 0 \pmod{2},$$

proving the lemma. □

We are now able to state and prove our main theorem which gives a partial answer to Conjecture 3.34. In the next section, we will resolve the sign ambiguity.

Theorem 3.49. *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*

$$\prod_{t \in H_4} \frac{\tau(t)}{\tau(t_0 t)} = \pm \zeta_e^{-k_0} \tag{3.14}$$

is a sign ambiguity, where k_0 is as in Theorem 3.46.

Proof. Rewriting (3.14), we want to show that

$$\overbrace{\prod_{t \in H_4} \tau(t)}^{\omega} = \pm \zeta_e^{-k_0} \overbrace{\prod_{t \in H_4} \tau(t_0 t)}^{\sigma_{t_0}(\omega)} \tag{3.15}$$

is a sign ambiguity. By Remark 3.45, we have that $\sigma_{t_0}(\omega) = \pm \zeta_e^{k_0} \omega$, so we only verify that (3.15) does not follow from the norm relation or Davenport-Hasse.

As in Lemma 3.48, let $\Lambda = \{L(\pm q_1 \pm q_2)\}$. Let $a \in H_4$. Then $a = tq_2 + nq_1$, for some $t \in \mathcal{T}_4,\ n \in N_2$ and we have

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

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, $1 \in \mathcal{T}_4 \implies -1 \notin \mathcal{T}_4$, and thus

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

For $a \in H_4$, consider $t_0 a = t_0(tq_2 + nq_1) = (t_0 t)q_2 + (t_0 n)q_1$. We have

$$t_0 a \in \Lambda \iff t_0 t \equiv \pm 1 \pmod{q_1} \quad \text{and} \quad t_0 n \equiv \pm 1 \pmod{q_2}.$$

But for $t \in T_4,\ t_0 t$ is a nonsquare and ± 1 are both squares, so $t_0 a \not\equiv \pm 1 \pmod{q_1}$. Therefore $t_0 a \notin \Lambda,\ \forall a \in H_4$. Combining these results, we have that

$$\#\{a \in H_4 \mid a \in \Lambda\} - \#\{a \in H_4 \mid t_0 a \in \Lambda\} = 1 - 0 \equiv 1 \pmod 2,$$

which, by the lemma, implies that (3.14) does not follow from Davenport-Hasse and the norm relation. Hence,

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

is a sign ambiguity. □

Remark 3.50. *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 the third condition with the stronger

3′. $q_2 \equiv 1 \pmod{q_1}$,

and applying the Chinese Remainder Theorem, we then need only that $q_1 \equiv 5 \pmod 8$ *and* $q_2 \equiv 3 \pmod{4q_1}$. *But by Dirichlet's theorem for primes in an arithmetic progression [7], 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.*

3.4 Resolution of Ambiguity

We now turn to the resolution of the ambiguous sign in Theorem 3.49. In previous cases, Muskat, Muskat-Whiteman, and Muskat-Zee, [13, 15, 16], have obtained resolution via binary quadratic form decomposition of the prime p. For example, we have the following from [13].

Example 3.51 (Muskat). *Let $e = 39$ and let p be a prime such that $p \equiv 1 \pmod{39}$. Then*

$$\tau(1)\tau(16)\tau(34) = u\zeta_e^k \tau(2)\tau(17)\tau(32)$$

is a sign ambiguity, where $k = 13\, ind_\gamma 13$ and

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

Here, we take a related, but different approach. Whereas resolution via binary quadratic forms depends on the representation of p in the form class group, $C_F(K)$, our method instead relies on an equivalent condition on the primes of $\mathcal{O}_K$ above p in the ideal class group, $C(K)$.

To resolve the ambiguity, we again return to our diagram:

$$\begin{array}{ccc} \mathbf{Q}(\zeta_e) & \longleftrightarrow & G \\ {\scriptstyle \frac{\varphi(e)}{8}}\big| & & \\ \omega \in (H_4)' = \widehat{K} & \longleftrightarrow & G/H_4 \\ {\scriptstyle 2}\big| & & \\ \mathbf{Q}(\sqrt{-e}, \sqrt{q_1}) = \widetilde{K} & \longleftrightarrow & G/H_2 \\ {\scriptstyle 2}\big| & & \\ \mathbf{Q}(\sqrt{-e}) = K & \longleftrightarrow & G/H \\ {\scriptstyle 2}\big| & & \\ \mathbf{Q} & \longleftrightarrow & \{1\}. \end{array}$$

In the previous section, we exploited the fact that $\omega \in \widehat{K}$ to conclude that $\sigma_t(\omega) = \pm\zeta_e^{k_0}\omega$. We now resolve the sign by determining whether the product of a certain root of unity and ω is in $\widetilde{K} \setminus K$ or K, and then connecting this to the order of the ideal classes above p in $C(K)$.

Proposition 3.52. *Let k_0 be as in Theorem 3.46. Then $\zeta_e^{\delta k_0}\omega \in \widetilde{K}$, where $\delta = -1$ if $\gcd(e, 5) = 1$ and $\delta = 3(t_0 + 1)$ if $e = 5 \cdot q_2$.*

Proof. As $t_0 \in H \setminus H_2$, by Proposition 3.35, 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 $\widehat{K}$ is Galois over $\mathbf{Q}$, $\omega \in \widehat{K} \implies \sigma_{t_i}(\omega) \in \widehat{K}$. Therefore, $\omega\mathcal{O}_{\widehat{K}} = (\sigma_{t_i}(\omega))\mathcal{O}_{\widehat{K}}$, and it follows that

$$\sigma_{t_i}(\omega) = (-1)^{\lambda_i}\zeta_e^{k_i}\omega, \quad \text{for some } \lambda_i, k_i \in \mathbf{Z},$$

and thus

$$\sigma_{t_i^2}(\omega) = \sigma_{t_i}((-1)^{\lambda_i}\zeta_e^{k_i}\omega) = (-1)^{\lambda_i}\zeta_e^{t_i k_i}\sigma_{t_i}(\omega) = \zeta_e^{t_i k_i + k_i}\omega. \tag{3.16}$$

Since $\widetilde{K}$ is the fixed field of H_2, $\zeta_e^{\delta k_0}\omega \in \widetilde{K}$ if and only if for all $t \in H \setminus H_2$, $\sigma_{t^2}(\zeta_e^{\delta k_0}\omega) = \zeta_e^{\delta k_0}\omega$. And, since $[t_i] = [t_{1-i}^3]$,

$$\sigma_{t_i^2}(\omega) = \sigma_{t_{1-i}^6}(\omega) = \sigma_{t_{1-i}^2}\left(\sigma_{t_{1-i}^4}(\omega)\right) = \sigma_{t_{1-i}^2}(\omega), \tag{3.17}$$

so without loss of generality, we may assume that $t = t_0$. Let $e = q_1 \cdot 3$. Then by Equation (3.16),

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

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

$$\zeta_e^{-k_0}\omega \in \widetilde{K} \iff -k_0 t_0^2 + k_0 t_0 + k_0 \equiv -k_0 \pmod{q_1 \text{ and } 3}. \tag{3.18}$$

But for $e = q_1 \cdot 3$, $t_0 \in H \setminus H_2 \implies t_0 \equiv 2 \pmod 3$, 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 3.46, k_0 is equivalent to 0 modulo q_1, so $0 \equiv -k_0 \equiv -k_0 t_0^2 + k_0 t_0 + k_0 \pmod{q_1}$. Hence, by (3.18), $\zeta_e^{-k_0}\omega \in \widetilde{K}$.

If $e = 5 \cdot q_2$, then again by (3.17), we may assume $t = t_0$, and we have

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

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

$$\zeta_e^{\delta k_0}\omega \in \widetilde{K} \iff k_0(\delta t_0^2 + t_0 + 1) \equiv \delta k_0 \pmod{5 \text{ and } q_2}. \tag{3.19}$$

Since t_0 is a nonsquare, $t_0 \equiv 2 \text{ or } 3 \pmod{5} \implies t_0^2 \equiv 4 \pmod{5}$, 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 3.46, $k_0 \equiv 0 \pmod{q_2}$, so $k_0(\delta t_0^2 + t_0 + 1) \equiv k_0\delta \pmod{q_2}$ as well. Therefore, by (3.19), $\zeta_e^{\delta k_0}\omega \in \widetilde{K}$.

Finally, let e be such that $\gcd(e, 15) = 1$. Then, again by Theorem 3.46, $k_0 \equiv 0 \pmod{e}$, and

$$\sigma_{t^2}(\omega) = \zeta_e^{k_0(t_0+1)}\omega = \zeta_e^{0(t_0+1)}\omega = \omega,$$

implying that $\omega \in \widetilde{K}$. □

Since $\zeta_e^{\delta k_0}\omega \in \widetilde{K}$, we must have that either $\zeta_e^{\delta k_0}\omega \in K \subseteq \widetilde{K}$ or $\zeta_e^{\delta k_0}\omega \in \widetilde{K} \setminus K$. First assume $\zeta_e^{\delta k_0}\omega \in K \subseteq \widetilde{K}$. 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

$$\zeta_e^{\delta k_0}\omega = \sigma_{t_0}(\zeta_e^{\delta k_0}\omega) = \zeta_e^{t_0\delta k_0}\sigma_{t_0}(\omega) \implies \sigma_{t_0}(\omega) = \zeta_e^{\delta k_0(1-t_0)}\omega, \tag{3.20}$$

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 $\zeta_e^{\delta k_0}\omega \in \widetilde{K} \setminus K$, 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

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

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

Lemma 3.53. $\zeta_e^{\delta k_0}\omega \in K \iff \mathfrak{p}^{\frac{h_K}{4}} \subseteq \mathcal{O}_K$ *is principal.*

Proof. If $\zeta_e^{\delta k_0}\omega \in K$, then

$$(\zeta_e^{\delta k_0}\omega)\mathcal{O}_K = \omega\mathcal{O}_E \cap \mathcal{O}_K = \mathfrak{p}_1^{\alpha}\mathfrak{p}_2^{\beta} = p^{\alpha}\mathfrak{p}_2^{\beta-\alpha} = p^{\alpha}\mathfrak{p}_2^{\frac{h_K}{4}},$$

and $p^{\alpha}\mathfrak{p}_2^{h_K/4}$ is principal. Therefore, $\mathfrak{p}_2^{h_K/4}$ is principal as well.

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

$$\omega'\mathcal{O}_K = p^{\alpha}\mathfrak{p}^{\frac{h_K}{4}} \implies \omega'\mathcal{O}_{\widehat{K}} = \omega\mathcal{O}_{\widehat{K}} \implies \omega' = \pm\zeta_e^r\omega, \quad \text{for some } r \in \mathbf{Z}.$$

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

$$\zeta_e^r\omega = \sigma_{t_0}(\zeta_e^r\omega) = \zeta_e^{t_0 r}\sigma_{t_0}(\omega) \implies \sigma_{t_0}(\omega) = \zeta_e^{r-t_0 r}\omega = \zeta_e^{r(1-t_0)}\omega. \tag{3.21}$$

Comparing Equations (3.20) and (3.21), it must be the case that $\delta k_0(1-t_0) \equiv r(1-t_0) \pmod{e}$ and thus $r \equiv \delta k_0 \pmod{e}$. Hence, $\zeta_e^{\delta k_0}\omega \in K$. □

We now state our complete main theorem.

Theorem 3.54. *Let $e = q_1q_2$ with $q_1 \equiv 5 \pmod 8, q_2 \equiv 3 \pmod 4$, and q_2 a biquadratic residue modulo q_1. 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. Then*

$$\prod_{t \in H_4} \frac{\tau(t)}{\tau(t_0 t)} = u\zeta_e^{-k_0},$$

where

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

and

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

Proof. By Theorem 3.49, 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 $\mathfrak{p}^{h_K/4}$. We have

$$u = \begin{cases} +1 \iff \zeta_e^{\delta k_0}\omega \in K \iff [\mathfrak{p}^{\frac{h_K}{4}}] = 1, \\ -1 \iff \zeta_e^{\delta k_0}\omega \in \widetilde{K} \setminus K \iff [\mathfrak{p}^{\frac{h_K}{4}}] \neq 1. \end{cases}$$

By Corollary 3.40, $h_K \equiv 4 \pmod 8$, and thus $h_K/4 \equiv 1 \pmod 2$. Therefore, $[\mathfrak{p}^{\frac{h_K}{4}}] = 1 \iff [\mathfrak{p}]^{\frac{h_K}{4}} = 1 \iff o([\mathfrak{p}]) \mid \frac{h_K}{4} \iff o([\mathfrak{p}]) \equiv 1 \pmod 2$. □

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 3.55. *Let $e = 155 = 5 \cdot 31$, p be a prime $p \equiv 1 \pmod e$, 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 3.54 and Remark 3.47,

$$\prod_{t \in H_4} \frac{\tau(t)}{\tau(t_0 t)} = u\zeta_{155}^{(2)(31)\, ind_\gamma(31)},$$

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, $o([\mathfrak{p}]) \equiv 1 \pmod 2 \iff [\mathfrak{p}] \in C(K)^4$. Therefore, via the isomorphism between the ideal class group and the form class group, we have $o([\mathfrak{p}]) \equiv 1 \pmod 2 \iff$

$[\mathfrak{p}] \in C_F(K)^4$. *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 3.56. *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 $u = +1$ and three which give $u = -1$. 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

[1] B. C. Berndt and R. J. Evans. Sums of Gauss, Eisenstein, Jacobi, Jacobsthal, and Brewer. *Illinois J. Math.*, 23(3):374–437, 1979.

[2] B. C. Berndt and R. J. Evans. The determination of Gauss sums. *Bull. Amer. Math. Soc. (N.S.)*, 5(2):107–129, 1981.

[3] B. C. Berndt, R. J. Evans, and K. S. Williams. *Gauss and Jacobi sums*. John Wiley & Sons Inc., New York, 1998. A Wiley-Interscience Publication.

[4] P. E. Conner and J. Hurrelbrink. *Class number parity*. World Scientific Publishing Co., Singapore, 1988.

[5] P. E. Conner and J. Hurrelbrink. On the 4-rank of the tame kernel $K_2(\mathcal{O})$ in positive definite terms. *J. Number Theory*, 88(2):263–282, 2001.

[6] D. A. Cox. *Primes of the form $x^2 + ny^2$*. John Wiley & Sons Inc., New York, 1989. Fermat, class field theory and complex multiplication.

[7] H. Davenport. *Multiplicative number theory*. Springer-Verlag, New York, third edition, 2000. Revised and with a preface by Hugh L. Montgomery.

[8] H. Hasse. *Vorlesungen über Zahlentheorie*. Springer-Verlag, Berlin, 1964.

[9] R. H. Hudson. Generalizations of a classical theorem in number theory. *Math. Comp.*, 30(135):649–656, 1976.

[10] K. Ireland and M. Rosen. *A classical introduction to modern number theory*. Springer-Verlag, New York, second edition, 1990.

[11] G. J. Janusz. *Algebraic number fields*. American Mathematical Society, Providence, RI, second edition, 1996.

[12] D. A. Marcus. *Number fields*. Springer-Verlag, New York, 1977. Universitext.

[13] J. B. Muskat. On Jacobi sums of certain composite orders. *Trans. Amer. Math. Soc.*, 134:483–502, 1969.

[14] J. B. Muskat. Computers in number theory. In *Proceedings of the Science Research Council Atlas Symposium No. 2 held at Oxford, from 18–23 August 1969*, pages xvii+433, London, 1971. Academic Press.

[15] J. B. Muskat and A. L. Whiteman. The cyclotomic numbers of order twenty. *Acta Arith.*, 17:185–216, 1970.

[16] J. B. Muskat and Y.-c. Zee. Sign ambiguities of Jacobi sums. *Duke Math. J.*, 40:313–334, 1973.

[17] R. Osburn. Densities of 4-ranks of $K_2(\mathcal{O})$. *Acta Arith.*, 102(1):45–54, 2002.

[18] The PARI-Group, Bordeaux. *PARI/GP, Version 2.1.3*, 2000. available from `http://www.parigp-home.de/`.

[19] P. van Wamelen. Jacobi sums over finite fields. *Acta Arith.*, 102(1):1–20, 2002.

[20] L. C. Washington. *Introduction to cyclotomic fields*. Springer-Verlag, New York, 1982.

[21] K. Yamamoto. On a conjecture of Hasse concerning multiplicative relations of Gaussian sums. *J. Combinatorial Theory*, 1:476–489, 1966.

[22] K. Yamamoto. The gap group of multiplicative relationships of Gaussian sums. In *Symposia Mathematica, Vol. XV (Convegno di Strutture in Corpi Algebrici, INDAM, Rome, 1973)*, pages 427–440. Academic Press, London, 1975.

Vita

Brian J. Murray was born on November 19, 1974, in St. Charles, Missouri. He finished his undergraduate studies at Washington University in St. Louis in May 1997. In August 1997 he came to Louisiana State University to pursue graduate studies in mathematics and earned a master of science degree in mathematics in May 1999. He is currently a candidate for the degree of Doctor of Philosophy in mathematics, which will be awarded in August 2002.