# ON GAUSS SUMS, CYCLOTOMIC NUMBER FIELDS AND STICKELBERGER'S THEOREM

KONSTANTIN DRAGOMIRETSKIY

01 June 2010

Undergraduate Honors Thesis
Advisor: Professor Harold Stark

University of California, San Diego
Department of Mathematics

Contents

## 1. Introduction

This undergraduate thesis will survey Gauss sums, starting from the classical Gauss sum analyzed by C. F. Gauss, and continuing to more general character sums. Along the way, the classical Gauss sum will be utilized to prove the famous law of quadratic reciprocity, which Gauss refered to as the "fundamental theorem" in the *Disquisitiones Arithmeticae*. Various decompositions and recursions of Gauss sums will be developed. Prime ideal factorizations will be developed through Stickelberg's theorem. Finally, a closing remarks on the Stickelberger element annihilating the cyclotomic class group and its generalization, the Brumer-Stark conjecture.

**Acknowledgement**
First and foremost, I would like to thank Dr. Harold Stark, the advisor for my undergraduate honors thesis and my concurrent algebraic number theory course professor. I would have prefered meeting Professor Stark as a graduate or postdoctoral student to be able to have much deeper dialogues in mathematics, nevertheless I feel very fortunate that our paths crossed and that I had the privilege of working with him. I thank him for his time invested into this thesis and wish him good luck with his book.

I thank Dr. Cristian Popescu for encouraging number theory to me during my undergraduate career and reaffiring my aspirations to become a mathematician.

I finally thank Dr. Lance Small, Dr. Audrey Terras, and Dr. Cristian Popescu for teaching me mathematics and for recommending me for the mathematics doctorate program at the University of California, Los Angeles.

*Konstantin Vitalyevich Dragomiretskiy*

## 2. Classical Gauss Sum

The Classical Gauss Sum was studied extensively by Carl Friedrich Gauss.

This section is series of exercises from *Abstract Algebra* by Dummit and Foote.

Put $K_p = \mathbb{Q}(\zeta_p)$, where $\zeta_p = exp(\frac{2\pi i}{p})$ and $p$ is an odd prime.
A finite dimensional $\mathbb{Q}$-vector space is called a number field.

$K_p$ is the $p$th cyclotomic number field. This is because the monic, irreducible polynomial over $\mathbb{Q}$ is the $p$th cyclotomic polynomial:
$\Phi_p(x) = \dfrac{x^p - 1}{x - 1} = 1 + x + \ldots + x^{p-1}$ and $\mathbb{Q}[x]/\langle \Phi_p(x) \rangle \cong K_p$

Put $G_p = \mathrm{Gal}(K_p/\mathbb{Q}) = \{\sigma \in \mathrm{Aut}(K_p/\mathbb{Q}) |\ \sigma(q) = q \ \ \forall q \in \mathbb{Q}\}$
$\forall a \in K_p, a = \sum_{i=1}^{\phi(p)} q_i \zeta_p^i = \sum_{i=1}^{p-1} q_i \zeta_p^i \quad for \quad q_i \in \mathbb{Q}$ where $\{\zeta_p^i\}_{i=1}^{p-1}$ is a power basis for $K_p$ over $\mathbb{Q}$. Hence $\tau \in G_p$ is completely determined by $\tau(\zeta_p) = \zeta_p^\alpha$ where $(\alpha, p) = 1$.

This observation elucidates the well-known isomorphism $G_p \cong \mathbb{Z}/p\mathbb{Z}^\times$.

**Definition 2.1.** $\eta_0 = \sum_{\tau \in H} \tau(\zeta_p)$ and $\eta_1 = \sum_{\tau \in \sigma H} \tau(\zeta_p)$
where $H$ is the unique normal subgroup of index 2 and the coset $\sigma H = G \setminus H$. $\eta_0$ and $\eta_1$ are called the two *periods* of $\zeta_p$ with respect to $H$.

By the aformentioned isomorphism, $G_p$ is cyclic, and hence the following one-to-one correspondence can be observed:

$\langle \tau_1 \rangle = \{\tau_i \in \mathrm{G} \ | \tau_i(\zeta_p) = \zeta_p^{g^i}\} \longleftrightarrow \{1, g, \ldots, g^{p-1}\} = \langle g \rangle = G_p.$

**Remark.** $\langle \tau_1 \rangle$ is cyclic by the action of composition.

**Lemma 2.1.** $\tau_1(\eta_0) = \eta_1$ *and* $\tau_1(\eta_1) = \eta_0$

*Proof.* $\tau_1(\eta_0) = \tau_1(\sum_{\tau \in H} \tau(\zeta_p)) = \sum_{\tau \in H} \tau_1(\tau(\zeta_p)) = \sum_{i=1}^{\frac{p-1}{2}} \tau_1(\tau_{2i}(\zeta_p)) = \sum_{i=1}^{\frac{p-1}{2}} \tau_{2i-1}(\zeta_p) =$
$\sum_{\tau \in \sigma H} \tau(\zeta_p) = \eta_1.$

$\tau_1(\eta_1) = \tau_1(\sum_{\tau\in\sigma H}\tau(\zeta_p)) = \sum_{\tau\in\sigma H}\tau_1(\tau(\zeta_p)) = \sum_{i=1}^{\frac{p-1}{2}}\tau_1(\tau_{2i-1}(\zeta_p)) = \sum_{i=1}^{\frac{p-1}{2}}\tau_{2i}(\zeta_p) = \sum_{\tau\in H}\tau(\zeta_p) = \eta_0.$ □

**Lemma 2.2.** *$\eta_0 = \sum_{a\equiv square}\zeta_p^a$ and $\eta_1 = \sum_{b\not\equiv square}\zeta_p^b$*

*Proof.* $a \in H \Leftrightarrow a = g^{2k}$ for some $k \in \mathbb{N} \Leftrightarrow a = (g^k)^2 = g_k^2 \Leftrightarrow$ a is a square, hence a is a square (modulo p) if and only if $a \in H$.

$\sum_{a\equiv square}\zeta_p^a = \sum_{i=1}^{\frac{p-1}{2}}\zeta_p^{g^{2i}} = \sum_{i=1}^{\frac{p-1}{2}}\tau_{2i}(\zeta_p) = \sum_{\tau\in H}\tau(\zeta_p) = \eta_0$

If b is not a square then b $\notin$ H and hence b $= g^{2i-1}$ for some i $\in \mathbb{N}$

$\sum_{b\not\equiv square}\zeta_p^b = \sum_{i=1}^{\frac{p-1}{2}}\zeta_p^{g^{2i-1}} = \sum_{i=1}^{\frac{p-1}{2}}\tau_{2i-1}(\zeta_p) = \sum_{i=1}^{\frac{p-1}{2}}\tau_1(\tau_{2i}(\zeta_p)) = \tau_1(\sum_{i=1}^{\frac{p-1}{2}}\tau_{2i}(\zeta_p)) = \tau_1(\eta_0) = \eta_1$ □

**Definition 2.2.** Let $k$ be a field and $K$ a cyclic extension with Galois group $G$ of order n, given $\alpha \in K$, the *Lagrange resolvent* is

$(\alpha, \zeta) = \alpha + \zeta\sigma(\alpha) + \ldots + \zeta^{n-1}\sigma^{n-1}(\alpha) = \sum_{i=0}^{n-1}\zeta^i\sigma^i(\alpha)$

where $\zeta$ is an *nth* root of unity and $\sigma$ is a generator of $G$.

**Lemma 2.3.** *$\eta_0 + \eta_1 = (\zeta_p, 1) = -1$ and $\eta_0 - \eta_1 = (\zeta_p, -1)$*

*Proof.* $\eta_0 + \eta_1 = \sum_{a\equiv square}\zeta_p^a + \sum_{b\not\equiv square}\zeta_p^b = \sum_{i=1}^{\frac{p-1}{2}}\tau_{2i}(\zeta_p) + \sum_{i=1}^{\frac{p-1}{2}}\tau_{2i-1}(\zeta_p) = \sum_{i=1}^{p-1}\tau_i(\zeta_p) = \tau_1(\zeta_p) + \tau_2(\zeta_p) + \ldots + \tau_{p-1}(\zeta_p) = \tau_1(\zeta_p) + \tau_1^2(\zeta_p) + \ldots + \tau_1^{p-2}(\zeta_p) + \zeta_p = \zeta_p + \tau_1(\zeta_p) + \ldots + \tau_1^{\phi(p)-1}(\zeta_p) = (\zeta_p, 1).$

$\eta_0 + \eta_1 = \sum_{i=1}^{p-1}\tau_i(\zeta_p) = \sum_{i=1}^{p-1}\zeta_p^i$ via rearrangement, and hence $\eta_0 + \eta_1 = \Phi_p(\zeta_p) - 1 = -1$, where $\Phi_p(x)$ is the $p$th cyclotomic polynomial.

$\eta_0 - \eta_1 = (\zeta_p^{g^2} + \zeta_p^{g^4} + \ldots + \zeta_p^{g^{p-1}}) - (\zeta_p^{g^1} + \zeta_p^{g^3} + \ldots + \zeta_p^{g^{p-2}}) =$
$\sum_{i=1}^{p-1} (-1)^i \tau_1^i(\zeta_p) = \sum_{i=0}^{p-2} (-1)^i \tau_1^i(\zeta_p) = (\zeta_p, -1).$ □

**Lemma 2.4.** $\sum_{i=1}^{p-1} \zeta_p^{i^2} = (\zeta_p, -1)$

*Proof.* Observe that $(p-k)^2 \equiv p^2 - 2pk + k^2 \equiv k^2 (mod\ p)$.
Put $\gamma = \sum_{i=0}^{p-1} \zeta_p^{i^2}$. $\gamma = \zeta_p^0 + \zeta_p^1 + \zeta_p^{2^2} + \ldots + \zeta_p^{(p-2)^2} + \zeta_p^{(p-1)^2} =$
$1 + 2(\zeta_p^1 + \zeta_p^{2^2} + \ldots + \zeta_p^{(\frac{p-1}{2})^2})$. Rewritting the residues 1, 2, ..., $\frac{p-1}{2}$ as powers of g, $\gamma = 1 + 2(\zeta_p^{(g^{a_1})^2} + \zeta_p^{(g^{a_2})^2} + \ldots + \zeta_p^{(g^{a_{\frac{p-1}{2}}})^2}) = 1 + 2(\zeta_p^{g^{2a_1}} + \zeta_p^{g^{2a_2}} + \ldots + \zeta_p^{g^{2a_{\frac{p-1}{2}}}}) = 1 + 2\eta_0$ since each exponent of g in the parenthesized sum is even and unique mod $\phi(p)$.
$\gamma = 1 + 2\eta_0 = 2\eta_0 - (-1) = 2\eta_0 - (\zeta_p, 1) = 2\eta_0 - (\eta_0 + \eta_1) = \eta_0 - \eta_1 = (\zeta_p, -1)$. □

**Lemma 2.5.** *$\tau(\gamma) = \gamma$ if $\tau \in H$ and $\tau(\gamma) = -\gamma$ if $\tau \notin H$*

*Proof.* $\tau \in H \Rightarrow \tau = \tau_{2i}$ for some i, $1 \leq i \leq \frac{p-1}{2} \Rightarrow \tau(\gamma) = \tau(\eta_0 - \eta_1) = \tau(\eta_0) - \tau(\eta_1) = \tau_{2i}(\eta_0) - \tau_{2i}(\eta_1) = \eta_0 - \eta_1 = \gamma$ since by Lemma 2.1, $\tau_2 = \tau_1 \circ \tau_1$ is the identity on both $\eta_0$ *and* $\eta_1$.
$\tau \notin H \Rightarrow \tau = \tau_{2i+1}$ for some i, $0 \leq i < \frac{p-1}{2} \Rightarrow \tau(\gamma) = \tau(\eta_0 - \eta_1) = \tau(\eta_0) - \tau(\eta_1) = \tau_{2i+1}(\eta_0) - \tau_{2i+1}(\eta_1) = \eta_1 - \eta_0 = -\gamma$ since $\tau_{2i+1} = \tau \circ \tau_{2i}$. □

**Lemma 2.6.** *$\bar{\gamma} = \gamma$ when $p \equiv 1 \pmod 4$ and $\bar{\gamma} = -\gamma$ when $p \equiv 3 \pmod 4$ where $\bar{\gamma}$ is the complex conjugate of $\gamma$.*

*Proof.* By Lemma 2.5, $\gamma$ is fixed by H, and thus $\mathbb{Q} \subseteq \mathbb{Q}(\gamma) \subseteq K^H$. It is easily verifiable that $\gamma \notin \mathbb{Q}$ and thus $\mathbb{Q}(\gamma) = K_p^H$, the subfield of $K_p$ fixed by $H$.
$Gal(\mathbb{Q}(\gamma)/\mathbb{Q}) \cong \frac{Gal(K_p/\mathbb{Q})}{Gal(K_p/\mathbb{Q}(\gamma))} = G/H = \langle \sigma_{-1} \rangle \cong \mathbb{Z}/2\mathbb{Z}$ where $\sigma_{-1}$ is complex conjugation.
A simple observation of orders gives us $\sigma_{-1} = \tau_1^{\frac{p-1}{2}} = \tau_{\frac{p-1}{2}}$.
$p \equiv 1 \pmod 4 \Rightarrow \frac{p-1}{2} \equiv 0 \pmod 2 \Rightarrow \tau_{\frac{p-1}{2}} \in H \Rightarrow \bar{\gamma} = \sigma_{-1}(\gamma) = \tau_{\frac{p-1}{2}}(\gamma) = \gamma$.

$p \equiv 3 \pmod 4 \Rightarrow \frac{p-1}{2} \equiv 1 \pmod 2 \Rightarrow \tau_{\frac{p-1}{2}} \notin H \Rightarrow \bar{\gamma} = \sigma_{-1}(\gamma) = \tau_{\frac{p-1}{2}}(\gamma) = -\gamma.$ $\square$

**Lemma 2.7.** $\gamma\bar{\gamma} = p$

*Proof.* $\bar{\gamma} = \sum_{i=0}^{p-2}(-1)^i\overline{\tau_1^i(\zeta_p)} = \sum_{i=0}^{p-2}(-1)^i\tau_1^{-i}(\zeta_p) \Rightarrow$

$\gamma\bar{\gamma} = (\sum_{i=0}^{p-2}(-1)^i\tau_1^i(\zeta_p))(\sum_{j=0}^{p-2}(-1)^j\tau_1^{-j}(\zeta_p)) = \sum_{i=0}^{p-2}\sum_{j-0}^{p-2}(-1)^{i-j}\tau_1^j(\frac{\tau_1^{i-j}(\zeta_p)}{\zeta_p})$

$= \sum_{k=0}^{p-2}(-1)^k\sum_{j=0}^{p-2}\tau_1^j(\frac{\tau_1^k(\zeta_p)}{\zeta_p})$ where $k = i - j$.

$k = 0 \Rightarrow \frac{\tau_1^k(\zeta_p)}{\zeta_p} = 1 \Rightarrow \tau_1^j(\frac{\tau_1^k(\zeta_p)}{\zeta_p}) = 1.$

$k \neq 0 \Rightarrow \frac{\tau_1^k(\zeta_p)}{\zeta_p} = \zeta_p^{g^k-1} = \zeta_p^{\alpha_k} = \tau_1^{\alpha_k}(\zeta_p)$ where $gcd(\alpha_k, p) = 1.$

$\gamma\bar{\gamma} = (-1)^0(p-1)+\sum_{k=1}^{p-2}(-1)^k\sum_{j=0}^{p-2}\tau_1^j(\frac{\tau_1^k(\zeta_p)}{\zeta_p}) = (p-1)+\sum_{k=1}^{p-2}(-1)^k\sum_{j=0}^{p-2}\tau_1^j(\zeta_p^{g^k-1}) =$

$(p-1))+\sum_{k=1}^{p-2}(-1)^k\sum_{j=0}^{p-2}\tau_1^j(\tau_1^{\alpha_k}(\zeta_p)) = (p-1)+\sum_{k=1}^{p-2}(-1)^k\tau_1^{\alpha_k}(\sum_{j=0}^{p-2}\tau_1^j(\zeta_p)) =$

$(p-1)+\sum_{k=1}^{p-2}(-1)^k\tau_1^{\alpha_k}[(\zeta_p, 1)] = (p-1)+\sum_{k=1}^{p-2}(-1)^k\tau_1^{\alpha_k}(-1) = (p-1)+$

$\sum_{k=1}^{p-2}(-1)^{k+1} = (p-1)+1-1+\ldots+1-1+1 = (p-1)+1 = p.$ $\square$

**Theorem 2.1.** $\gamma^2 = (-1)^{\frac{p-1}{2}}p$

*Proof.* This follows directly from Lemma 2.6 and Lemma 2.7. $\square$

We conclude that $\gamma = \pm\sqrt{(-1)^{\frac{p-1}{2}}p}$ with $[\mathbb{Q}(\gamma) : Q] = 2$.

**Remark.** By Galois correspondence, $\mathbb{Q}(\gamma)$ is the unique quadratic subfield of $K_p$.

## 3. Quadratic Reciprocity

We will use the results from the previous section to prove one of Gauss' favorite theorems, the law of quadratic reciprocity.

First we will define the Legendre symbol and develop lemmas and supplementary laws to assist the proof.

**Definition 3.1.** For odd prime p,

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ if } a \text{ is a quadratic residue } \pmod p \text{ and } a \not\equiv 0 \pmod p \\ -1 \text{ if } a \text{ is a quadratic non-residue } \pmod p \\ 0 \text{ if } a \equiv 0 \pmod p. \end{cases}$$

this is called the Legendre symbol.

**Lemma 3.1.** $\forall a, b \in \mathbb{Z}/p\mathbb{Z}^\times, (a+b)^p \equiv a^p + b^p \pmod p$

*Proof.* $(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}$ where $\binom{p}{i} = \frac{p!}{(p-i)!i!} \Rightarrow$
For $1 \leq i \leq p-1, i! \not\equiv 0 \pmod p$ and $(p-i)! \not\equiv 0 \pmod p$ since both $i$ and $p-i$ are both strictly less than $p$.
$\binom{p}{i}(p-i)!i! = p! \equiv 0 \pmod p \Rightarrow \binom{p}{i} \equiv 0 \pmod p$
$(a+b)^p = a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i} + b^p \equiv a^p + b^p \pmod p$. □

**Lemma 3.2.** *Let $p$ be an odd prime,* $\left(\frac{v}{p}\right) \equiv (v)^{\frac{p-1}{2}} \pmod p$

*Proof.* Let $p$ be an odd prime. $\mathbb{Z}/p\mathbb{Z}^\times$ is cyclic, with generator $g$.
If $v$ is a square modulo p, then $v = g^{2k}$ for some $k$, $0 \leq k \leq \frac{p-1}{2}$.
$v^{\frac{p-1}{2}} \equiv g^{(p-1)k} \equiv 1^k \equiv 1 \equiv \left(\frac{v}{p}\right)$.
Notice that this accounts for the case where $v \equiv 0 \pmod p$.
If $v$ is not a square modulo p, then $v = g^{2k+1}$ for some $k$, $0 \leq k < \frac{p-1}{2}$.
$v^{\frac{p-1}{2}} \equiv g^{(p-1)k+\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \equiv -1 \equiv \left(\frac{v}{p}\right)$. □

**Lemma 3.3.** *(Supplementary Law 1)* $\left(\frac{-1}{p}\right) = \begin{cases} 1 \text{ if } p \equiv 1 \pmod 4 \\ -1 \text{ if } p \equiv 3 \pmod 4 \end{cases}$

*Proof.* Put $v = -1$ in Lemma 3.2 $\square$

**Lemma 3.4.** *(Supplementary Law 2)* $\left(\frac{2}{p}\right) = \begin{cases} 1 \text{ if } p \equiv \pm 1 \pmod 8 \\ -1 \text{ if } p \equiv \pm 3 \pmod 8 \end{cases}$

*Proof.* Set $\zeta_8 = exp(\frac{2\pi i}{8})$ and $\beta = \zeta_8 + \zeta_8^{-1} = 2\cos\frac{2\pi}{8} = \sqrt{2}$.
$\beta^2 = (\zeta_8 + \zeta_8^{-1})^2 = \zeta_8^2 + 2 + \zeta_8^{-2} = 2$.
By Lemma 3.2: $\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \equiv (\beta^2)^{\frac{p-1}{2}} \equiv \beta^{p-1} \pmod p$.
Multiplying by $\beta$ on both sides yields: $\beta\left(\frac{2}{p}\right) \equiv \beta^p \pmod p$
By Lemma 3.1: $\beta^p = (\zeta_8+\zeta_8^{-1})^p \equiv \zeta_8^p+\zeta_8^{-p} \equiv (\zeta_8+\zeta_8^{-1})\left(\frac{2}{p}\right) \pmod p$.
$p \equiv \pm 1 \pmod 8 \Rightarrow \zeta_8^p + \zeta_8^{-p} = \zeta_8 + \zeta_8^{-1} = \beta \Rightarrow \left(\frac{2}{p}\right) \equiv 1 \pmod p$.
$p \equiv \pm 3 \pmod 8 \Rightarrow \zeta_8^p + \zeta_8^{-p} = \zeta_8^3 + \zeta_8^{-3} = (\zeta_8 + \zeta_8)(\zeta_8^2 - 1 + \zeta_8^{-1}) =$
$\beta(\zeta_8^2 + 2 + \zeta_8^{-1} - 3) = \beta(\beta^2 - 3) = -\beta \Rightarrow \left(\frac{2}{p}\right) \equiv -1 \pmod p$ $\square$

**Theorem 3.1.** *Let p, q be two distinct positive prime numbers, then*

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \text{ or } q \equiv 1 \pmod 4 \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

*Proof.* From the previous section, we analyzed $\gamma = \sum_{i=1}^{p-1} \zeta_p^{i^2} = \eta_0 - \eta_1$.
$\gamma$ is also expressible as $\gamma = \sum_{v=1}^{p-1} \left(\frac{v}{p}\right) \zeta_p^v$.
By Theorem 2.1, $\gamma^q = \gamma(\gamma^2)^{\frac{q-1}{2}} = \gamma((-1)^{\frac{p-1}{2}}p)^{\frac{q-1}{2}} = \gamma(-1)^{\frac{p-1}{2}\frac{q-1}{2}}p^{\frac{q-1}{2}}$
By Lemma 3.2, $\gamma^q \equiv \gamma(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) \pmod q$.
By Lemma 3.1, $\gamma^q = \left(\sum_{v=1}^{p-1}\left(\frac{v}{p}\right)\zeta_p^v\right)^q \equiv \sum_{v=1}^{p-1}\left(\frac{v}{p}\right)^q \zeta_p^{qv} \equiv \sum_{v=1}^{p-1}\left(\frac{v}{p}\right)\zeta_p^{qv} \equiv$
$\sum_{v=1}^{p-1}\left(\frac{q}{p}\right)\left(\frac{q}{p}\right)\left(\frac{v}{p}\right)\zeta_p^{qv} \equiv \left(\frac{q}{p}\right)\sum_{v=1}^{p-1}\left(\frac{qv}{p}\right)\zeta_p^{qv} \equiv \left(\frac{q}{p}\right)\gamma \pmod q$.
The last congruence is observable via variable change $v \to qv$

By equating both congruences of $\gamma^q \pmod q$,
$\gamma(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) \equiv \left(\frac{q}{p}\right)\gamma \Rightarrow \gamma^2(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) \equiv \left(\frac{q}{p}\right)\gamma^2 \Rightarrow$
$(\pm p)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) \equiv \left(\frac{q}{p}\right)(\pm p) \Rightarrow (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) \equiv \left(\frac{q}{p}\right) \pmod q$
$\pm p$ is coprime to $q$, and thus has an inverse modulo $q$.
Because $(-1)^n$, $\left(\frac{p}{q}\right)$, and $\left(\frac{q}{p}\right)$ take values in $\{\pm 1\}$, the congruence can be strengthened to an equality.
$p \text{ or } q \equiv 1 \pmod 4 \Rightarrow (p-1) \text{ or } (q-1) \equiv 0 \pmod 4 \Rightarrow \frac{p-1}{2}\frac{q-1}{2} \equiv 0 \pmod 2 \Rightarrow \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$
$p \equiv q \equiv 3 \pmod 4 \Rightarrow \frac{p-1}{2}\frac{q-1}{2} \equiv 1 \pmod 2 \Rightarrow \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ $\square$

Lemmas 3.3 and 3.4 and Theorem 3.1 give the full statement of quadratic reciprocity. The Legendre symbol being multiplicative (as we will see in the next section, the Legendre symbol is a quadratic multiplicative character), together with the lemmas and theorem, allow $\left(\frac{n}{p}\right)$ to be computed $\forall n \in \mathbb{Z}$.

**Example.** $\left(\frac{541}{7919}\right) = \left(\frac{7919}{541}\right) = \left(\frac{345}{541}\right) = \left(\frac{3}{541}\right)\left(\frac{5}{541}\right)\left(\frac{23}{541}\right) = \left(\frac{541}{3}\right)\left(\frac{541}{5}\right)\left(\frac{541}{23}\right) = \left(\frac{1}{3}\right)\left(\frac{1}{5}\right)\left(\frac{12}{23}\right) = \left(\frac{4}{23}\right)\left(\frac{3}{23}\right) = \left(\frac{3}{23}\right) = -\left(\frac{23}{3}\right) = -\left(\frac{2}{3}\right) = 1.$
The last equality agrees with both lemmas when 2 is viewed as -1 (mod 3) as well.

**Definition 3.2.** The generalization of the Legendre symbol is the Jacobi. Without restriction to composite $n > 0$, if $n = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$, then the Jacobi symbol $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1}\left(\frac{a}{p_2}\right)^{\alpha_2}\dots\left(\frac{a}{p_k}\right)^{\alpha_k}$. This is a product of Legendre symbols. It shares some properties common to the Legendre symbol, but loses a valuable property as well.

**Remark.** Both Supplementary Laws and Theorem 3.1 still hold when distinct primes $p$ and $q$ are replaced by composite $n$ and $m$ where both $n, m$ are positive and odd. Unfortunately, there is significant loss of information. Specifically, the Jacobi symbol does not share the

property: $\left(\frac{a}{n}\right) = 1 \Rightarrow$ *a is a square modulo n.* This is due to the indiscernability between an even parity of quadratic nonresidues in the product of the Jacobi symbol and the necessary condition of $a$ being a quadratic residue modulo all primes dividing $n$. Despite this, Jacobi symbols are still very useful in various algorithms such as in primality testing.

We will now state the law of cubic reciprocity, without proof, for the interest of the reader.

**Definition 3.3.** An *Eisenstein integer* is an element of $\mathbb{Z}[\zeta_3]$.

**Definition 3.4.** Let $\pi$ be and Eistenstein prime with $N(\pi) \neq 3$, and let $\alpha \in \mathbb{Z}[\zeta_3]$. If $\pi | \alpha$, set $\left(\frac{\alpha}{\pi}\right)_3 = 0$. If $\pi \not| \alpha$, let $\left(\frac{\alpha}{\pi}\right)_3$ be the unique power of $\zeta_3$ defined by

$$\alpha^{(N(\pi)-1)/3} \equiv \left(\frac{\alpha}{\pi}\right)_3 \pmod{\pi}$$

This symbol is multiplicative like the Legendre symbol. Lastly, if $\beta$ is a unit of $\mathbb{Z}[\zeta_3]$, define $\left(\frac{\alpha}{\pi}\right)_3 = 1$ for every $\alpha \in \mathbb{Z}[\zeta_3]$

**Definition 3.5.** Let $\alpha \in \mathbb{Z}[\zeta_3]$. $\alpha$ is called primary if $\alpha \equiv \pm 1 \pmod{3}$

**Theorem 3.2.** *(Cubic Reciprocity). Let $\alpha$ and $\beta$ be coprime primary Eisenstein integers. Then*

$$\left(\frac{\alpha}{\beta}\right)_3 = \left(\frac{\beta}{\alpha}\right)_3$$

For more information about cubic reciprocity see [3].

## 4. Gauss Sums

**Definition 4.1.** Given a finite abelian group $G$, the multiplicative homomorphism $\chi : G \hookrightarrow S^1 \subset \mathbb{C}^\times$ is called a character of $G$.
$g \in G, g = g_1^{a_1} \dots g_n^{a_n}$. $\chi_(g) = exp(2\pi i \sum_j \frac{a_j}{f_j})$ where $ord_G(g_j) = f_j$.
More generally, $\chi_{b_1,\dots,b_n}(g) = exp(2\pi i \sum_j \frac{b_j a_j}{f_j}) = \prod_j exp(2\pi i \frac{b_j a_j}{f_j}) = \prod_j \chi_{b_1,\dots,b_n}(g_j)^{a_j b_j}$ The group of characters is denoted by $\hat{G}$.

The definition of $\chi$ used in this paper will be $\chi(g) = \chi_{1,\dots,1}(g)$, omitting the trivial weights.

Let $\chi_0$ denote the trivial character, with $\chi_0(g) = 1\ \forall g \in G$.

The finite abelian group on which $\chi$ is defined will be a Galois group of a number field, typically $\mathbb{Z}/m\mathbb{Z}^\times$ corresponding to the $m$th cyclotomic number field.

**Definition 4.2.** G = $\mathbb{Z}/m\mathbb{Z}^\times$. $\chi$ can be extended by defining $\chi(n) = \chi(\bar{n})$ where $\bar{n}$ is the residue of n modulo m. Setting $\chi(n) = 0$ for n with gcd(n,m)>1, extends $\chi$ to the integers with periodicity, such that $\chi(n) = \chi(n+m)\ \forall n, \in \mathbb{Z}$. We say that $\chi$ is a character to the modulus m. This extended character $\chi$ is a Dirichlet character.

**Definition 4.3.** G = $\mathbb{Z}/m\mathbb{Z}^\times$. A character $\chi$ has a minimum modulus of definition, called the conductor, denoted $f(\chi)$. A character is called primitive if $f(\chi) = m$, and imprimitive otherwise, in which case $f(\chi) < m$.

**Example.** Let $m = 8$, then $\mathbb{Z}/m\mathbb{Z}^\times = \{1, 3, 5, 7\}$. Every non-trivial character is quadratic. By the multiplicative relationships, it is easily verifiable that {3,5} generate the group, and hence $\chi$ is defined by the values it takes on 3 and 5. This is the character table:

| $\chi$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| $\chi_1$ | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| $\chi_2$ | 0 | 1 | 0 | -1 | 0 | 1 | 0 | -1 |
| $\chi_3$ | 0 | 1 | 0 | 1 | 0 | -1 | 0 | -1 |
| $\chi_4$ | 0 | 1 | 0 | -1 | 0 | -1 | 0 | 1 |

$f(\chi_1) = 1 < 8$ and $f(\chi_2) = 4 < 8$, hence $\chi_1$ and $\chi_2$ are imprimitive ($\chi_1$ is obviously imprimitive because it is the trivial character!)

$\chi_3$ and $\chi_4$ are both primitive because they cannot be defined on a smaller modulus.

**Remark.** Unless stated otherwise, $\chi$ will be a primitive character.

**Definition 4.4.** The Gauss sum of Dirichlet character $\chi$ modulo N is $G_N(\chi, a) = \sum_{n=1}^{N} \chi(n)\zeta_N^{an}$ where $\zeta_N = exp(\frac{2\pi i}{N})$ and $\chi$ is a (primitive) character of (Galois) group $G$ $(= \mathbb{Z}/N\mathbb{Z}^\times)$. The notation $G_N(\chi) = G_N(\chi, 1)$ will be used if there is no ambiguity.

**Remark.** The Gauss sum generalizes the Langrange resolvent, defined in the previous section.

When $\chi$ is the trivial character, $G_p(\chi_0, 1) = \Phi_p(\zeta_p) - 1 = -1$.
When $\chi$ is the quadratic character, $G_p(\chi_2, 1) = \sum_{n=1}^{p} \chi_2(n)\zeta^n = \sum_{n=1}^{p} \left(\frac{n}{p}\right) \zeta^n$ where $\left(\frac{n}{p}\right)$ is the Legendre symbol.

The Classical Gauss sum from the Section 2 can now be viewed as the Gauss sum $G_p(\chi_2)$ where $\chi_2$ is the unique quadratic character of the Galois group.

**Lemma 4.1.** *Let $\chi$ and $\psi$ be characters modulo $m$. If $gcd(f(\chi), f(\psi)) = 1$, then $f(\chi\psi) = f(\chi)f(\psi)$*

*Proof.* Apply the Chinese Remainder Theorem. □

**Remark.** Lemma 4.1 allows us to factor characters modulo $m$. If $m = ab$, and $gcd(a, b) = 1$ then we can factor a character $\chi$ modulo $m$ into a product of characters $\chi_a$ and $\chi_b$ modulo $a$ and $b$, respectively.

**Lemma 4.2.** $gcd(a, m) = 1 \Rightarrow G_m(\chi, a) = \overline{\chi(a)}G_m(\chi, 1)$

*Proof.* $G_m(\chi, a) = \sum_{n=1}^{m} \chi(n)\zeta_m^{an} = \sum_{n=1}^{m} \overline{\chi(a)}\chi(a)\chi(n)\zeta_m^{an} = \sum_{n=1}^{m} \overline{\chi(a)}\chi(an)\zeta_m^{an} = \overline{\chi(a)} \sum_{n=1}^{m} \chi(an)\zeta_m^{an} = \overline{\chi(a)}G_m(\chi, 1)$. The last equality holds because $gcd(a, m) = 1 \Rightarrow n \to an$ is a bijection on $\mathbb{Z}/m\mathbb{Z}^\times$. □

**Lemma 4.3.** $gcd(a, m) > 1 \Rightarrow G_m(\chi, a) = 0$

*Proof.* $gcd(a,m) = d > 1 \Rightarrow m = rd$ and $a = bd$ and $gcd(r,b) = 1$
There exists a $c$, such that $\chi(c) \neq 1$ and $c \equiv 1 \pmod{r}$. The existence of such a $c$ arises from $\chi$ being non-trivial on the kernel of the mapping $h : \mathbb{Z}/m\mathbb{Z}^\times \longrightarrow \mathbb{Z}/r\mathbb{Z}^\times$. If it were trivial on the kernel, then $\chi$ would determine a character of $Im(h) \subseteq \mathbb{Z}/r\mathbb{Z}^\times$, extending to a character $\chi'$ of $\mathbb{Z}/m\mathbb{Z}^\times$, and $\chi'$ would induce $\chi$. This contradicts $\chi$ being primitive.
It is easy to show that $a \equiv ca \pmod{m}$, and thus $\zeta_m^a = \zeta_m^{ca}$
$\chi(c)G_m(\chi,a) = \sum_{n=1}^{m} \chi(cn)\zeta_m^{an} = \sum_{n=1}^{m} \chi(cn)\zeta_r^{can} = G_m(\chi,a)$ by the variable change $cn \longrightarrow n$, since $gcd(c,m) = 1$.
$(\chi(c) - 1)G_m(\chi,a) = 0 \Rightarrow G_m(\chi,a) = 0$, since $\chi(c) \neq 1$ □

We will now apply Lemmas 4.2 and 4.3 to generalize Theorem 2.1.

**Theorem 4.1.** *For primitive character $\chi$ with conductor $m$, if $gcd(a,m) = 1$ then $|G_m(\chi,a)| = \sqrt{m}$.*

*Proof.* $|G_m(\chi,a)|^2 = \overline{G_m(\chi,a)}G_m(\chi,a) = \sum_x \sum_y \chi(x)\overline{\chi(y)}\zeta_p^{(x-y)}$ where $x$ and $y$ run over the residues modulo $m$.
$x \equiv y \pmod{m} \Rightarrow \sum_{n \pmod{m}} \zeta_m^{n(x-y)} = \sum_{n \pmod{m}} 1 = m$
$x \not\equiv y \pmod{m} \Rightarrow \sum_{n \pmod{m}} \zeta_m^{n(x-y)} = \Phi_m(\zeta_m) = 0$
By Lemma 4.3, $gcd(x,m) > 1 \Rightarrow \chi(x) = 0$ $\sum_{n \pmod{m}} |G_m(\chi,n)|^2 =$
$\sum_{(n,m)=1} |G_m(\chi,n)|^2 = \sum_{(n,m)=1} \sum_x \sum_y \chi(x)\overline{\chi(y)}\zeta_m^{(x-y)} = \sum_{(n,m)=1} \sum_{x \pmod{m}} \chi(x)\overline{\chi(x)} =$
$\sum_{(n,m)=1} |\chi(x)|m = m \sum_{(n,m)=1} 1 = m\phi(m)$.
By Lemma 4.2, for $n$ coprime to $m$, $G_m(\chi,n) = \overline{\chi(n)}G_m(\chi,1) \Rightarrow$
$|G_m(\chi,n)|^2 = |\chi(n)|^2|G_m(\chi,1)|^2$.
Appealing to Lemmas 4.2 and 4.3, $|G_m(\chi,n)|^2 = \begin{cases} |G_m(\chi,1)|^2 & if\ gcd(n,m) = 1 \\ 0 & if\ gcd(n,m) > 1 \end{cases}$
$\sum_{n \pmod{m}} |G_m(\chi,n)|^2 = \sum_{(n.m)=1} |G_m(\chi,1)|^2 = \phi(m)|G_m(\chi,1)|^2$.
Equating the two yields $\phi(m)|G_m(\chi,1)|^2 = m\phi(m) \Rightarrow |G_m(\chi,1)|^2 = m$

$gcd(a,m) = 1 \Rightarrow |G_m(\chi,a)|^2 = |G_m(\chi,1)|^2 \Rightarrow |G_m(\chi,a)| = \sqrt{m}$ □

**Remark.** Clearly, by Lemma 4.3, $gcd(a,m) > 1 \Rightarrow |G_m(\chi, a)| = 0$

We will now develop a decomposition of a Gauss sum of composite modulus into simpler Gauss sums.

**Theorem 4.2.** *Let $m = ab$ with gcd(a,b)=1. Let $\chi = \chi_a\chi_b$ be a character modulo m. $G_m(\chi) = \overline{\chi_a(b_a^{-1})}G_a(\chi_a)\overline{\chi_b(a_b^{-1})}G_b(\chi_b)$ where $f(\chi_a) = a$ and $f(\chi_b) = b$.*

*Proof.* For any n, $1 \leq n \leq m$, we would like to write $n \equiv n_1 \pmod a$ and $n \equiv n_2 \pmod b$. By the Chinese Remainder Theorem,

$$n = \alpha n_1 + \beta n_2 \text{ where } \alpha \equiv \begin{cases} 1 \pmod a \\ 0 \pmod b \end{cases} \quad \text{and } \beta \equiv \begin{cases} 0 \pmod a \\ 1 \pmod b \end{cases}$$

Let $b_a$ denote the residue of $b \pmod a$ and $a_b$ the residue of $a \pmod b$. $\alpha = b_a b_a^{-1} = bb_a^{-1}$ and $\beta = a_b a_b^{-1} = aa_b^{-1}$ where $b_a^{-1}$ and $a_b^{-1}$ are integer representatives of the residues between 1 and their respecitve moduli.
$\chi(n) = \chi_m(n) = \chi_a(n)\chi_b(n) = \chi_a(\alpha n_1 + \beta n_2)\chi_b(\alpha n_1 + \beta n_2) = \chi_a(n_1)\chi_b(n_2)$

$$G_m(\chi) = \sum_{n=1}^{m} \chi_m(n)\zeta_m^n = \sum_{n_1,n_2} \chi_a(n_1)\chi_b(n_2)\zeta_m^{\alpha n_1 + \beta n_2} = \sum_{n_1,n_2} \chi_a(n_1)\chi_b(n_2)\zeta_m^{\alpha n_1}\zeta_m^{\beta n_2}$$

$$\zeta_m^{\alpha n_1} = exp(\frac{2\pi i \alpha n_1}{m}) = exp(\frac{2\pi i b b_a^{-1} n_1}{ab}) = exp(\frac{2\pi i b_a^{-1} n_1}{a}) = \zeta_a^{b_a^{-1}}$$

$$\zeta_m^{\beta n_2} = exp(\frac{2\pi i \beta n_2}{m}) = exp(\frac{2\pi i a a_b^{-1} n_2}{ab}) = exp(\frac{2\pi i a_b^{-1} n_2}{b}) = \zeta_b^{a_b^{-1}}$$

$$G_m(\chi) = \sum_{n_1,n_2} \chi_a(n_1)\chi_b(n_2)\zeta_a^{b_a^{-1}n_1}\zeta_b^{a_b^{-1}n_2} = \sum_{n_1} \chi_a(n_1)\zeta_a^{b_a^{-1}n_1} \sum_{n_2} \chi_b(n_2)\zeta_b^{a_b^{-1}n_2}.$$

Be Lemma 4.2, $\sum_{n_1} \chi_a(n_1)\zeta_a^{b_a^{-1}n_1} = \overline{\chi_a(b_a^{-1})} \sum_{n_1} \chi_a(n_1)\zeta_a^{n_1} = \overline{\chi_a(b_a^{-1})}G_a(\chi_a)$

and $\sum_{n_2} \chi_b(n_2)\zeta_b^{a_b^{-1}n_2} = \overline{\chi_b(a_b^{-1})} \sum_{n_2} \chi_b(n_2)\zeta_b^{n_2} = \overline{\chi_b(a_b^{-1})}G_b(\chi_b)$.

Substituting, we get $G_m(\chi) = \overline{\chi(b_a^{-1})}G_a(\chi_a)\overline{\chi(a_b^{-1})}G_b(\chi_b)$ □

**Remark.** The process in Theorem 4.2 can be repeated until $m$ is factored into prime powers. $m = \prod_{i=1}^{k} p_i^{\alpha_i} \Rightarrow G_m(\chi) = \mu \prod_i G_{p_i^{\alpha_i}}(\chi_{p_i^{\alpha_i}})$ where $\mu$ is the appropritate root of unity.

## 5. Quadratic Gauss Sums

We will now focus on quadratic Gauss sums and their decomposition.

**Definition 5.1.** The quadratic Gauss sum $g(a, N) = \sum_{n=1}^{N} \zeta_N^{an^2}$.

The quadratic Gauss sum can be decomposed into simpler quadratic Gauss sums, and ultimately factored analogously to the Gauss sum in Theorem 4.2.

**Lemma 5.1.** *For odd prime $p$, $g(a, p) = \left(\frac{a}{p}\right) g(1, p)$.*

*Proof.* Appealing to Lemma 2.4 and Lemma 4.2, we see that $gcd(a, p) = 1 \Rightarrow g(a, p) = \sum_{n=1}^{p} \zeta_p^{an^2} = \sum_{n=1}^{p} \chi_2(a)\zeta_p^{an} = G(\chi_2, a) = \overline{\chi_2(a)}G(\chi_2, 1) = \chi_2(a)G(\chi_2, 1) = \chi_2(a) \sum_{n=1}^{p} \chi(n)\zeta_p^n = \chi_2(a) \sum_{n=1}^{p} \zeta_p^{n^2} = \chi_2(a)g(1, p)$, where $\chi_2$ is the Legendre symbol. Likewise, if $gcd(a, p) = p \Rightarrow \chi_2(a) = 0$. □

**Remark.** By induction, Lemma 5.1 can be extended through the Jacobi symbol so that the restriction on $p$ is lifted from having to be prime to having to only be odd and positive. Even the restriction of being odd can be lifted, but the proof requires analytic computation.

We will now develop some recursion formulae, useful in the process of factorizing quadratic Gauss sums.

**Lemma 5.2.** *For odd prime $p$, and $j \geq 2$, $g(1, p^j) = pg(1, p^{j-2})$.*

*Proof.* Writing $n$ $p$-adically, $n = r + sp^{j-1}$ with $r$ a residue modulo $p^{j-1}$ and $s$ a residue modulo $p$. $n^2 = (r + sp^{j-1})^2 = r^2 + 2rsp^{j-1} + sp^{2j-2} \equiv r^2 + 2rsp^{j-1} \pmod{p^j}$.

$g(1, p^j) = \sum_{n=1}^{p^j} \zeta_{p^j}^{n^2} = \sum_r \sum_s \zeta_{p^j}^{r^2+2rsp^{j-1}} = \sum_r \sum_s \zeta_{p^j}^{r^2} \zeta_p^{2rs} = p \sum_{r, p|r} \zeta_{p^j}^{r^2}$.

$gcd(p, r) = p \Rightarrow \zeta_p^{2rs} = exp(2\pi is) = 1$, so the inner summation is $p$ as $s$ runs through the residues modulo $p$.

$gcd(p, r) = 1 \Rightarrow s \longrightarrow 2rs$ is a bijection on $\mathbb{Z}/p\mathbb{Z}$ and as $s$ runs through the residues modulo p, each $p$th root of unity appears once, so the inner summation is 0.

$g(1,p^j) = p\sum_{r,p|r} \zeta_{p^j}^{r^2} = p(\zeta_{p^j}^0 + \zeta_{p^j}^{p^2} + \zeta_{p^j}^{4p^2} + \ldots + \zeta_{p^j}^{p^2(j-1)^2}) = p(\zeta_{p^{j-2}}^0 + \zeta_{p^{j-2}}^1 +$

$\zeta_{p^{j-2}}^4 + \ldots + \zeta_{p^{j-2}}^{(j-2)^2-1}) = p\sum_{n=0}^{p^{j-2}-1} \zeta_{p^{j-2}}^{n^2} = p\sum_{n=1}^{p^{j-2}} \zeta_{p^{j-2}}^{n^2} = pg(1,p^{j-2})$ □

**Lemma 5.3.** *$g(1,2^j) = 2g(1,2^{j-2})$ for $j \geq 4$.*

*Proof.* Writing $n$ 2-adically, $n = r + s2^{j-2}$ with $r$ a residue modulo $2^{j-2}$ and $s$ a residue modulo 2. $n^2 = (r+s2^{j-2})^2 = r^2 + 2rs2^{j-2} + sp^{2j-4} \equiv r^2 + rs2^{j-1} \pmod{2^j}$.

$g(1,2^j) = \sum_{n=0}^{2^j-1} \zeta_{2^j}^{n^2} = \sum_r \sum_s \zeta_{2^j}^{r^2+rs2^{j-1}} = \sum_r \sum_s \zeta_{2^j}^{r^2}(-1)^{rs} = 2\sum_{2|r,r=0}^{2^{(j-1)}-1} \zeta_{2^j}^{r^2}$.

The last equality holds by the same arguement as in Lemma 5.2.

$g(1,2^j) = 2\sum_{2|r,r=0}^{2^{(j-1)}-1} \zeta_{2^j}^{r^2} = 4\sum_{2|r,r=0}^{2^{(j-2)}-1} \zeta_{2^j}^{r^2} = 4(\zeta_{2^j}^0 + \zeta_{2^j}^{2^2} + \zeta_{2^j}^{2^4} + \ldots + \zeta_{2^j}^{2^{(j-3)^2}}) =$

$4(\zeta_{2^{j-2}}^0 + \zeta_{2^{j-2}}^1 + \zeta_{2^{j-2}}^{2^2} + \ldots + \zeta_{2^{j-2}}^{2^{(j-4)^2}}) = 4\sum_{n=0}^{2^{(j-3)}-1} \zeta_{2^{j-2}}^{n^2} = 2\sum_{n=0}^{2^{(j-2)}-1} \zeta_{2^{j-2}}^{n^2} =$

$2g(1,2^{j-2})$. The second and sixth equalities are due to symmetry. □

**Lemma 5.4.** $g(1,p^j) = \begin{cases} p^{\frac{j}{2}} & p^j \equiv 1 \pmod 4 \\ ip^{\frac{j}{2}} & p^j \equiv 3 \pmod 4 \end{cases}$

*Proof.* $g(1,p^j) = pg(1,p^{j-2}) = \ldots = p^k g(1,p^{j-2k})$ after $k$ iterations.

$j \equiv 0 \pmod 2 \Rightarrow g(1,p^j) = \ldots = p^{\frac{j-2}{2}} g(1,p^2) = p^{\frac{j}{2}} g(1,1) = p^{\frac{j}{2}}$.

$j \equiv 1 \pmod 2 \Rightarrow g(1,p^j) = \ldots = p^{\frac{j-1}{2}} g(1,p) = p^{\frac{j-1}{2}} \sqrt{(-1)^{\frac{p-1}{2}} p} =$

$\sqrt{(-1)^{\frac{p-1}{2}}} p^{\frac{j}{2}} = \begin{cases} p^{\frac{j}{2}} \; if \; p \equiv 1 \pmod 4 \Leftrightarrow p^j \equiv 1 \pmod 4 \\ ip^{\frac{j}{2}} \; if \; p \equiv 3 \pmod 4 \Leftrightarrow p^j \equiv 3 \pmod 4 \end{cases}$ □

**Lemma 5.5.** $g(1,2^j) = \begin{cases} (1+i)2^{\frac{j}{2}} & 2^j \equiv 0 \pmod 4 \\ 0 & 2^j \equiv 2 \pmod 4 \end{cases}$

*Proof.* $g(1,2^j) = 2g(1,2^{j-2}) = \ldots = 2^k g(1,2^{j-2k})$ after $k$ iterations.

$2^j \equiv 0 \pmod 4 \Rightarrow g(1,2^j) = \ldots = 2^{\frac{j-2}{2}} g(1,4) = 2^{\frac{j-2}{2}}(i^1 + i^4 + i^9 + i^16) = 2(1+i)2^{\frac{j-2}{2}} = (1+i)2^{\frac{j}{2}}$.

$2^j \equiv 2 \pmod 4 \Rightarrow g(1,2^j) = \ldots = 2^{\frac{j-1}{2}} g(1,2) = 2^{\frac{j-1}{2}}(1-1) = 0$ □

**Lemma 5.6.** *Let $a$ be odd. Then $g(a,2^r) = \epsilon(a)\left(\frac{-2^r}{a}\right)g(1,2^r)$ where*

$$\epsilon(a) = \begin{cases} 1 \ if \ a \equiv 1 \pmod 4 \\ i \ if \ a \equiv 3 \pmod 4 \end{cases}$$

*Proof.* Let $\sigma_a : \zeta_{2^r} \longrightarrow \zeta_{2^r}^a$. Then $g(a,2^r) = \sigma_a(1,2^r) = \sigma_a(1+i)\sigma_a(2^{\frac{r}{2}})$.

$$\sigma_a(1+i) = 1 + i^a = \begin{cases} 1+i \ if \ a \equiv 1 \pmod 4 \\ 1-i \ if \ a \equiv 3 \pmod 4 \end{cases} = \left(\frac{-1}{a}\right)\epsilon(a)(1+i)$$

$$\sigma_a(2^{\frac{r}{2}}) = \left(\frac{2}{a}\right)^r 2^{\frac{r}{2}} = \left(\frac{2^r}{a}\right)2^{\frac{r}{2}} \Rightarrow g(a,2^r) = \epsilon(a)\left(\frac{-2^r}{a}\right)g(1,2^r) \qquad \square$$

Analogous to Theorem 4.2, there is a way to decompose a quadratic Gauss sum of composite modulus.

**Theorem 5.1.** *Let $m = ab$ with $gcd(a,b) = 1$. $g(1,m) = \mu g(1,a)g(1,b)$ where $\mu$ is an appropriate root of unity.*

*Proof.* For any n, $1 \leq n \leq m$, we would like to write $n \equiv n_1 \pmod a$ and $n \equiv n_2 \pmod b$. By the Chinese Remainder Theorem,

$$n = \alpha n_1 + \beta n_2 \text{ where } \alpha \equiv \begin{cases} 1 \pmod a \\ 0 \pmod b \end{cases} \quad \text{and } \beta \equiv \begin{cases} 0 \pmod a \\ 1 \pmod b \end{cases}$$

Let $b_a$ denote the residue of $b \pmod a$ and $a_b$ the residue of $a \pmod b$. $\alpha = b_a b_a^{-1} = b b_a^{-1}$ and $\beta = a_b a_b^{-1} = a a_b^{-1}$ where $b_a^{-1}$ and $a_b^{-1}$ are integer representatives of the residues between 1 and their respecitve moduli.

$n^2 = (\alpha n_1 + \beta n_2)^2 = \alpha^2 n_1^2 + 2\alpha\beta n_1 n_2 + \beta^2 n_2^2 = b_a^2 b_a^{-2} n_1^2 + a_b^2 a_b^{-2} + 2m b_a^{-1} a_b^{-1} \equiv b_a^2 b_a^{-2} n_1^2 + a_b^2 a_b^{-2} \pmod m \Rightarrow \zeta_m^{n^2} = \zeta_m^{(b_a^2 b_a^{-2})n_1^2 + (a_b^2 a_b^{-2})n_2^2} = \zeta_m^{(b_a^2 b_a^{-2})n_1^2}\zeta_m^{(a_b^2 a_b^{-2})n_2^2} = \zeta_a^{(b b_a^{-2})n_1^2}\zeta_b^{(a a_b^{-2})n_2^2} \Rightarrow g(1,m) = g(b b_a^{-2}, a)g(a a_b^{-2}, b)$.
$m = 2^j k$ where $k$ is odd and $j \geq 0 \Rightarrow g(1,m) = g(k k_{2^j}^{-2}, 2^j)g(2^j 2^{j}_{k}{}^{-2}, k)$.
Appealing to Lemma 5.1, the subsequent remark, and Lemma 5.6,
$g(1,m) = g(k k_{2^j}^{-2}, 2^j)g(2^j 2^{j}_{k}{}^{-2}, k) =$

$$\epsilon(k k_{2^j}^{-2})\left(\frac{-2^j}{k k_{2^j}^{-2}}\right)g(1,2^j)\left(\frac{2^j 2^{j}_{k}{}^{-2}}{k}\right)g(1,k) =$$

$$\left[\epsilon(k k_{2^j}^{-2})\left(\frac{-2^j}{k k_{2^j}^{-2}}\right)\left(\frac{2^j 2^{j}_{k}{}^{-2}}{k}\right)\right]g(1,2^j)g(1,k).$$

$k = \prod_{p_i odd} p_i^{a_i}$, so further decomposition of $g(1,k)$ is possible but the computation of the root of unity becomes rather cumbersome. $\square$

**Remark.** $m = \prod_{p_i prime} p_i^{a_i}$. Using Theorem 5.1 and great diligence, $g(1,m) = \mu \prod_{p_i prime} g(1, p_i^{a_i})$ where $\mu$, the appropriate root of unity, can be computed through methods in the proof of Theorem 5.1.

We conclude this section with an elegant equation for evaluating quadratic Gauss sums due to Dirichlet. The proof of the theorem uses analytic methods and is beyond the scope of this paper.

**Theorem 5.2.** *For any positive integer $b$, $g(1,b) = \dfrac{1+i^{-b}}{1+i^{-1}}\sqrt{b}$.*

*Proof.* See *Algebraic Number Theory* by S. Lang, pp. 88-90. [5] □

**Remark.** Theorems 5.1 and 5.2 allow $g(a,b)$ to be computed for any positive integers $a, b$.

## 6. Stickelberger's Theorem

To pursue the prime factorization of the Gauss sum, we will look at the Gauss sum as an ideal (or divisor) in the appropriate number field.

We must first introduce the Teichmüller character, which will be a canonical character dependent on a prime ideal that will be the basis for expressing all other characters. The existence of such a character will be justified by Hensel's lemma.

**Theorem 6.1.** *(Trivial case of Hensel's lemma). Let $K$ be a number field and let $\mathfrak{p}$ be a prime ideal in the ring of integers $\mathcal{O}_K$. Let $K_\mathfrak{p}$ be the completion of $K$ at the finite place $\mathfrak{p}$ and let $\mathcal{O}_\mathfrak{p}$ be the ring of integers in $K_\mathfrak{p}$. Let $f(x)$ be a polynomial with coefficients in $\mathcal{O}_\mathfrak{p}$ and suppose there exists $\alpha_0 \in \mathcal{O}_\mathfrak{p}$ such that*

$$f(\alpha_0) \equiv 0 \mod \mathfrak{p}, \quad f'(\alpha_0) \neq 0 \mod \mathfrak{p}$$

*Then there exist a root $\alpha \in K_\mathfrak{p}$ of $f(x)$, i.e. $f(\alpha) = 0$.*

*Proof.* See *http://planetmath.org/encyclopedia/HenselsLemma.html.* □

**Corollary.** *Let $p$ be a prime number. The ring of $p$-adic integers $\mathbb{Z}_p$ contains exactly $p-1$ distinct $(p-1)$th roots of unity. Furthermore, every $(p-1)$th root of unity is distinct modulo $p$.*

*Proof.* Notice that $\mathbb{Q}_p$, the $p$-adic rationals, is a field. Therefore $f(x) = x^{p-1} - 1$ has at most $p-1$ roots in $\mathbb{Q}_p$. Moreover, if we let $a \in \mathbb{Z}$ with $1 \leq a \leq p-1$ then $f(a) = a^{p-1} - 1 \equiv 0 \mod p$ by Fermat's little theorem. Since $f'(a) = (p-1)a^{p-2}$ is non-zero modulo $p$, the trivial case of Hensel's lemma implies that there exist a root of $x^{p-1} - 1$ in $\mathbb{Z}_p$ which is congruent to $a$ modulo $p$. Hence, there are at least $p-1$ roots in $\mathbb{Z}_p$, and we can conclude that there are exactly $p-1$ roots. □

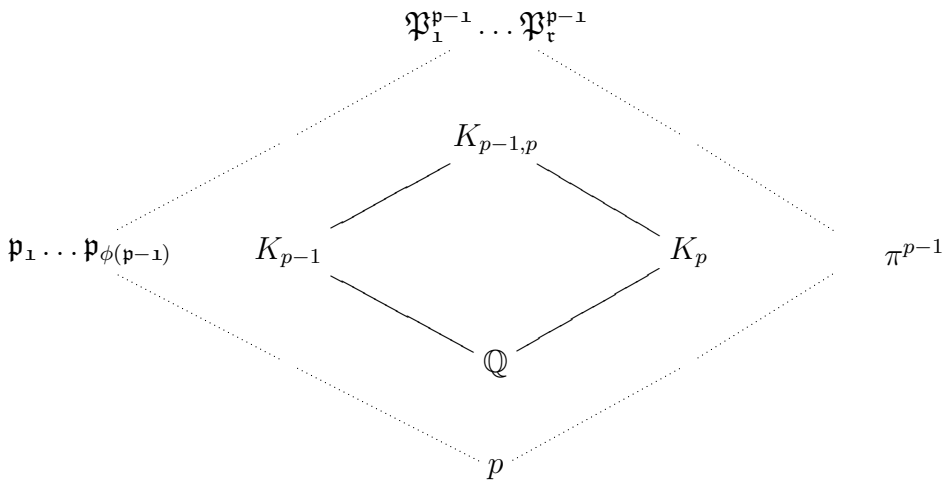
**Definition 6.1.** The Teichmüller character (or Teichmüller lift) is the unique character $\omega$ of $\mathbb{F}_p^\times$ satisfying $\omega(a) \equiv a \pmod{\mathfrak{p}}$.

**Lemma 6.1.** *The Teichmüller character generates the character group of $\mathbb{F}_p^\times$.*

*Proof.* $\mathbb{F}_p^\times$ is cyclic and $\omega(\zeta_{p-1} + \mathfrak{p}) = \zeta_{p-1}$, and so $\omega$ has order $p-1$. □

**Remark.** Every character of $\mathbb{F}_p^\times$ is expressable as $\omega^{-k}$. We will thus use $\overline{\omega(a)} \equiv a^{-1} \pmod{\mathfrak{p}}$ as our generator to avoid negative powers. From this point on, we will refer to $\omega$ as this generator.

The following lemmas will explain this diagram.




Put $K_n = \mathbb{Q}(\zeta_n)$ and let $K_{m,n}$ be the composite of $K_m$ and $K_n$.

It is well known in algebraic number theory that in a number field $K$, an ideal factors into a product of prime ideals, the algebraic integers of $K$. $\mathfrak{n} = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$

**Lemma 6.2.** *Let* $\mathfrak{n}$ *be an ideal of* $\mathcal{O}_K$. $\mathfrak{n} = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$.

$\sum_{i=1}^{r} e_i f_i = [K : \mathbb{Q}]$. *Where* $f_i = [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{Z}/n]$
$f_i$ *is called the inertial degree of* $\mathfrak{p}_i$.

*Proof.* $n^{[K:\mathbb{Q}]} = \mathbb{N}_{K/\mathbb{Q}}(n) = \prod_{i=1}^{r} \mathbb{N}_{K/\mathbb{Q}}(\mathfrak{p}_i)^{e_i} = \prod_{i=1}^{r} n^{e_i f_i} = n^{\sum_{i=1}^{r} e_i f_i}$ □

**Remark.** If K is a *Galois* extension, then $e_i = e$ and $f_i = f$ for $1 \leq i \leq r$ As a consequence, $efr = [K : \mathbb{Q}]$.

$K_p$ and $K_{p-1}$ are both Galois extensions because $\zeta_p$ and $\zeta_{p-1}$ generate the all of the $p$th and $(p-1)$st roots of unity in $K_p$ and $K_{p-1}$, respectively, thus the fields are normal, and because all number fields are separable.

**Theorem 6.2.** *Write* $m$ *in the form* $p^k n$, $p \nmid n$. *Then* $e = \phi(p^k)$ *and* $f$ *is the multiplicative order of* $p$ *modulo* $n$.

*Proof.* See *Number Fields* by D. Marcus pp. 76-78. [7] □

**Corollary.** *If $p \nmid n$, then $p$ splits in $\phi(m)/f$ distinct primes ideals in $\mathcal{O}_{K_{p-1}}$, where $f$ is the order of $p$ mod $m$.*

**Lemma 6.3.** *$p$ totally splits in $K_{p-1}$.*

*Proof.* Appealing to the corollary when $m = p-1$ gives us that $p$ splits into $\phi(p-1)$ distinct prime ideals because $f = 1$. □

**Lemma 6.4.** *$p$ totally ramifies in $K_p$.*

*Proof.* $\pi = (1-\zeta_p) | (1-\zeta_p^i)$ for $1 \leq i \leq p-1 \Rightarrow \pi^{p-1} | \prod_{i=1}^{p-1} (1-\zeta_p^i) = \Phi(1) = p$. For $\pi$, $(p-1)fr = efr = [K_p : \mathbb{Q}] = \phi(p) = p-1 \Rightarrow f = r = 1$. $\pi$ has full ramification index, and must be prime, otherwise it would factor causing $efr > [K_p : \mathbb{Q}]$. □

**Lemma 6.5.** $p = \prod \mathfrak{P}_{\mathfrak{1}}^{\mathfrak{p-1}} \dots \mathfrak{P}_{\phi(\mathfrak{p-1})}^{\mathfrak{p-1}}$ *in* $\mathcal{O}_{K_{p-1,p}}$.

*Proof.* Appealing to Lemmas 6.2, 6.3 and 6.4,
$p = \mathfrak{p}_{\mathfrak{1}} \dots \mathfrak{p}_{\phi(\mathfrak{p-1})}$ in $\mathcal{O}_{K_{p-1}} \Rightarrow r \geq \phi(p-1)$. $p = \pi^{p-1} \Rightarrow e \geq (p-1)$.
$ef \geq \phi(p-1)\phi(p) = [K_{p-1,p} : \mathbb{Q}] = efr \geq ef$. □

Now we know the structure of the factorization of $p$, and hence the Gauss sum with absolute value $p$. Stickelberger's theorem will explain the factorization of the Gauss sum in terms of prime ideals in $K_{p-1,p}$ . In full generality, $q = p^n \equiv 1 \pmod{m}$. The following theorems will state the general case, but the content of this paper will only analyze the case of $n = 1$ and $m = p-1$

**Definition 6.2.** For integer $k$, looking at $k \pmod{q-1}$, we write the $p$-adic expansion $k = k_0 + k_1 p + \ldots + k_{n-1} p^{n-1}$ with $0 \leq k_i \leq p-1$.

$$s(k) = \sum_{i=0}^{n-1} k_i \text{ and } \gamma(k) = \prod_{i=0}^{n-1} k_i!$$

Both $s(k)$ and $\gamma(k)$ are periodic $q-1$.

**Theorem 6.3.** *(Stickelberger's Theorem). For any integer $k$, we have the congruence*

$$\frac{G(\omega^k, \zeta_p^{Tr})}{(\zeta_p - 1)^{s(k)}} \equiv \frac{-1}{\gamma(k)} \pmod{\mathfrak{P}}$$

*In particular,*

$$ord_{\mathfrak{P}} G(\omega^k, \zeta_p^{Tr}) = s(k)$$

*Proof.* See *Cyclotomic Fields I,II* by S. Lang, pp. 7-9. [6] □

**Corollary.** *In the case of* $n = 1$, $q = p^n = p$ *and* $Tr(x) = x^{p^0} = x$.
$s(k) = k_0 \equiv k \pmod{q}$ *and* $\gamma(k) = k_0!$
*In this case, Stickelberger's Theorem states: for* $0 \leq k \leq p-1$

$$\frac{G(\omega^k, \zeta_p)}{(\zeta_p - 1)^k} \equiv \frac{-1}{k!} \pmod{\mathfrak{P}}$$

*in particular,*

$$ord_{\mathfrak{P}} G(\omega^k, \zeta_p) = k$$

*Proof.* Let $\mathfrak{p}$ be a prime ideal over $p$. $\omega(n) \equiv n^{-1} \pmod{\mathfrak{p}} = \pmod{\mathfrak{P}^{p-1}}$.

$$G_p(\omega) = \sum_{n=1}^{p-1} \omega(n)\zeta_p^n \equiv \sum_{n=1}^{p-1} n^{-1}(1-\pi)^n \pmod{\mathfrak{P}^{p-1}}$$

$$G_p(\omega) \equiv \sum_{n=1}^{p-1} n^{-1}(1 - n\pi) \pmod{\mathfrak{P}^2} \text{ since } \mathfrak{P}||\pi.$$

$$G_p(\omega) \equiv \sum_{n=1}^{p-1} n^{-1} + G_p(\omega) \equiv \sum_{n=1}^{p-1} \pi \equiv 0 - (p-1)\pi \equiv \pi \pmod{\mathfrak{P}^2}$$

Hence we have that, $\mathfrak{P}||G_p(\omega)$. Similarily, for $1 \leq k \leq p-2$,

$$G_p(\omega^k) = \sum_{n=1}^{p-1} \omega(n)^k \zeta_p^n \equiv \sum_{n=1}^{p-1} n^{-k}(1-\pi)^n \pmod{\mathfrak{P}^{p-1}}$$

$$G_p(\omega^k) \equiv \sum_{n=1}^{p-1} n^{-k} \sum_{j=0}^{n} (-1)^j \binom{n}{j} \pi^j \equiv$$

$$\sum_{j=0}^{k} \sum_{n=1}^{p-1} n^{-k}(1 + \alpha_1 n\pi + \alpha_2 n^2\pi^2 + \ldots + (-1)^k \frac{1}{k!} n^k \pi^k) \pmod{\mathfrak{P}^{k+1}}$$

For $1 \leq j \leq k-1$, $\sum_{n=1}^{p-1} n^{j-k}\alpha_j \pi^j \equiv \alpha_j \pi^j \sum_{n=1}^{p-1} n^{j-k} \equiv 0 \pmod{\mathfrak{P}^{k+1}}$

$$G_p(\omega^k) \equiv \sum_{n=1}^{p-1} (-1)\frac{1}{k!}\pi^k \equiv (-1)^{k+1}\frac{1}{k!}\pi^k \not\equiv 0 \pmod{\mathfrak{P}^{k+1}}.$$

Hence we have that, $\mathfrak{P}^k||G_p(\omega^k) \Rightarrow ord_{\mathfrak{P}} G(\omega^k) = k$. □

Stickelberger's Theorem gives us a correspondence between $k$th powers of a *particular* prime ideal $\mathfrak{P}$ exactly dividing the Gauss sums $G_p(\omega^k)$.

Using the result of the theorem, we can understand the full factorization of a *particular* Gauss sum $G_p(\omega^a)$

Take $\sigma_a = \sigma_{a,1} \in Gal(K_{p-1,p}/\mathbb{Q})$ such that $\sigma_a(\zeta_p) = \zeta_p$ and $\sigma_a(\omega) = \omega^a$.
$G_p(\omega)^{\sigma_a} = \sum_{n=1}^{p-1} \omega(n)^a \zeta_p^n = G_p(\omega^a)$.
$\mathfrak{P}^a || G_p(\omega^a) \Rightarrow (\mathfrak{P}^{\sigma_a^{-1}})^a || G_p(\omega^a)^{\sigma_a^{-1}} \Rightarrow (\mathfrak{P}^{\sigma_a^{-1}})^a || G_p(\omega)$

We now have the full factorization of $G_p(\omega) = \prod_{(a,p-1)=1} (\mathfrak{P}^{\sigma_a^{-1}})^a$.
Via conjugation, we know the full factorization of $G_p(\omega^k) = G_p(\omega)^{\sigma_k} = \prod_{(a,p-1)=1} (\mathfrak{P}^{\sigma_a^{-1}\sigma_k})^a$ for any $1 \leq k \leq p-2$ with $gcd(k, p-1) = 1$.

The following well known theorem in algebraic number theory provides a method for computing the primes $\mathfrak{p}$ and $\mathfrak{P}$ lying over $p$.

**Lemma 6.6.** *If $\chi$ has order $m$, then $G_p(\chi)^m \in K_m$.*

*Proof.* Let $\tau \in Gal(K_{m,p}/\mathbb{Q})$ such that $\tau(\zeta_p) = \zeta_p^v$ and $\tau(\zeta_m) = \zeta_m$. In fact, $\tau \in Gal(K_{m,p}/K_m)$.
$\tau(G_p(\chi)^m) = \tau(\sum_{n \pmod q} \chi(n)\zeta_p^n) = \sum_{n \pmod q} \chi(n)\zeta_p^{vn} = \overline{\chi(v)}^m G_p(\chi)^m$.
□

**Theorem 6.4.** *Let $\mathfrak{p}$ be a prime ideal (or divisor) in the number field $k$. If $\mathcal{O}_k[\theta] = \mathcal{O}_K$, then there is a prime ideal (or divisor) $\mathfrak{P}_i | \mathfrak{p}$ of $K/k$ of residue class degree (inertial degree) $f = deg(\overline{h_i(x)})$ given by $\mathfrak{P} = h_i(\theta) + \mathfrak{p}\mathcal{O}_K$ (or $\mathfrak{P} = (h_i(\theta), \mathfrak{p})$ as a divisor), where $h(x)$ is the (monic) irreducible polynomial of $\theta$ and $\overline{h(x)} = \prod \overline{h_i(x)}$ is the projection of $h(x)$ in $\mathbb{F}_q[x] \cong \mathcal{O}_k/\mathfrak{p}[x]$*

**Remark.** It is necessary that $\mathcal{O}_k[\theta] = \mathcal{O}_K$. For $\theta = \zeta_n$ this holds.

**Remark.** The proof is elementary but relatively long and can be found in many texts. The result of the theorem will be used for computational examples, hence the proof is excluded.

*Proof.* See *Number Fields* by D. Marcus pp.79-82. [7] or *Analytic Theory of Algebraic Numbers* by H. Stark Theorem, 8.1.3. [9] □

**Example.** Let $k = \mathbb{Q}$, $p = 7$ and $K = K_6$ where $\theta = \zeta_6$. $h(x) = \Phi_6(x) = x^2 - x + 1 \equiv (x-3)(x-5) \pmod 7$. There are exactly two primes $\mathfrak{p}_1, \mathfrak{p}_2$ dividing $p$, both of inertial degree 1. $\mathfrak{p}_1 = (\zeta_6 - 3, 7)$ and

$\mathfrak{p}_2 = (\zeta_6 - 5, 7)$. $K_6$ is a quadratic extension, hence $p = \mathfrak{p}_1\mathfrak{p}_2$.
To verify, $7 = (2+\sqrt{-3})(2-\sqrt{-3}) = (1+2\zeta_6)(3-2\zeta_6) =$
$[1 \cdot 7 + 2(\zeta_6 - 3)][(-1)\cdot 7 - 2(\zeta_6 - 5)]$.
Using our previous results, $p = \mathfrak{p}_1\mathfrak{p}_2 = \mathfrak{P}_1^6\mathfrak{P}_2^6$ in $K_{6,7}$.

**Definition 6.3.** The Stickelberger element is

$$\theta(k,\mathfrak{p}) = \sum_{c \in \mathbb{Z}/m\mathbb{Z}^\times} \langle \frac{kc}{q-1} \rangle \sigma_c^{-1} \in \mathbb{Q}[G]$$

where $\langle t \rangle \equiv t \pmod{Z}$ and $0 \leq \langle t \rangle \leq 1$ and $m$ is the order of the character $\omega^k \pmod{\mathfrak{p}}$. $\omega^k$ will be defined contextually.

**Lemma 6.7.** *For any integer $k$, we have $s(k) = (p-1)\sum_{i=0}^{n-1} \langle \frac{kp^i}{q-1} \rangle$.*

*Proof.* We may assume $1 \leq k \leq q-1$ since both sides of the equation are $(q-1)$-periodic in $k$. $k = k_0 + k_1 p + \ldots + k_{n-1}p^{n-1} \Rightarrow$
$kp^i = k_{n-i} + k_{n-(i-1)}p + \ldots + k_{n-1}p^{i-1} + k_0 p^i + k_1 p^{i+1} + \ldots + k_{n-(i+1)}p^{n-1} \Rightarrow$
$\langle \frac{kp^i}{q-1} \rangle = \frac{kp^i}{q-1} \Rightarrow \sum_{i=0}^{n-1} \langle \frac{kp^i}{q-1} \rangle = \sum_{i=0}^{n-1} \frac{kp^i}{q-1} = \frac{s(k)(1+p+\ldots+p^{n-1})}{q-1} =$
$\frac{s(k)\frac{q-1}{p-1}}{q-1} = \frac{s(k)}{p-1}$ □

**Theorem 6.5.** *$G_p(\omega^k, \zeta_p^{Tr}) = \mathfrak{P}^{(p-1)\theta(k,\mathfrak{p})} = \mathfrak{p}^{\theta(k,\mathfrak{p})}$ as ideals in $K_{p-1,p}$.*

*Proof.* $ord_{\sigma_c^{-1}\mathfrak{P}} G(\omega^k, \zeta_p^{Tr}) = ord_{\mathfrak{P}} \sigma_c G(\omega^k, \zeta_p^{Tr}) = ord_{\mathfrak{P}} G(\omega^{ck}, \zeta_p^{Tr}) =$
$s(kc)$ by Theorem 6.3. $\{\sigma_{p^i}\}$ fixes $G_p(\omega^k \zeta_p^T r)$ and hence fixes $\mathfrak{p}$ (this is the decomposition group of $\mathfrak{p}$) $\Rightarrow$ in the ideal $\mathfrak{p}^{\theta(k,\mathfrak{p})}$, $\sigma_c^{-1}\mathfrak{p}$ occurs with multiplicity $\sum_{i=0}^{n-1} \langle \frac{kcp^i}{q-1} \rangle = \frac{s(kc)}{p-1}$, by Lemma 6.6. Hence in the ideal $\mathfrak{P}^{(p-1)\theta(k,\mathfrak{p})}$, $\sigma_c^{-1}\mathfrak{P}$ occurs with multiplicity $(p-1)\frac{s(kc)}{p-1} = s(kc)$. □

**Example.** $n = 1$ and $q = p = 7$. The only primes above $p$ are $\mathfrak{P}_1\mathfrak{P}_2$ in $K_{6,7}$, and thus are the only primes dividing $G_p(\omega^k, \zeta_p)$

| $k$ | $G_p(\omega^k, \zeta_p)$ |
|---|---|
| 1 | $\mathfrak{P}^{(p-1)\theta(k,\mathfrak{p})} = \mathfrak{P}^{6(\langle\frac{1}{6}\rangle\sigma_1^{-1}+\langle\frac{5}{6}\rangle\sigma_5^{-1})} = \mathfrak{P}_1\mathfrak{P}_2^5$ |
| 2 | $\mathfrak{P}^{(p-1)\theta(k,\mathfrak{p})} = \mathfrak{P}^{6(\langle\frac{2}{6}\rangle\sigma_1^{-1}+\langle\frac{10}{6}\rangle\sigma_5^{-1})} = \mathfrak{P}_1^2\mathfrak{P}_2^4$ |
| 3 | $\mathfrak{P}^{(p-1)\theta(k,\mathfrak{p})} = \mathfrak{P}^{6(\langle\frac{3}{6}\rangle\sigma_1^{-1}+\langle\frac{15}{6}\rangle\sigma_5^{-1})} = \mathfrak{P}_1^3\mathfrak{P}_2^3$ |
| 4 | $\mathfrak{P}^{(p-1)\theta(k,\mathfrak{p})} = \mathfrak{P}^{6(\langle\frac{4}{6}\rangle\sigma_1^{-1}+\langle\frac{20}{6}\rangle\sigma_5^{-1})} = \mathfrak{P}_1^4\mathfrak{P}_2^2$ |
| 5 | $\mathfrak{P}^{(p-1)\theta(k,\mathfrak{p})} = \mathfrak{P}^{6(\langle\frac{5}{6}\rangle\sigma_1^{-1}+\langle\frac{25}{6}\rangle\sigma_5^{-1})} = \mathfrak{P}_1^5\mathfrak{P}_2^1$ |

**Theorem 6.6.** *Let $\mathcal{C}$ be the ideal class group of $\mathbb{Q}(\zeta_m)$. Then for all $b$ prime to $m$,*

$$(b - \sigma_b)\theta(m)$$

*annihilates $\mathcal{C}$*

*Proof.* (Sketch:) $\chi_{\mathfrak{p}} = \omega^{\mathbb{N}(\mathfrak{p}-1)/m}$ and put $\theta(m) = \sum_{c\in\mathbb{Z}(m)^\times} \langle\frac{c}{m}\rangle\sigma_c^{-1}$. As a special case of Theorem 6.5, we obtain the factorization

$$G_p(\chi_{\mathfrak{p}}, \zeta_p^{Tr}) = \mathfrak{p}^{\theta(m))}$$

Therefore, if $b$ is an integer prime to $m$, then

$$G_p(\chi_{\mathfrak{p}}, \zeta_p^{Tr})^{b-\sigma_b} = \mathfrak{p}^{\theta(m)(b-\sigma_b)}$$

$\theta(m)(b-\sigma_b)$ lies in $\mathbb{Z}[G]$. This gives us a factorization of the $\theta(m)(b-\sigma_b)$th power of the Gauss sum in terms of $\mathfrak{p}$ and its conjugates in $\mathbb{Q}(\zeta_m)$. In every ideal class there exists an ideal prime to $m$ (Hilbert). $\mathfrak{p}^{\theta(m)(b-\sigma_b)}$ is principal for every $\mathfrak{p} \nmid m$ □

## 7. Brumer-Stark Conjecture

The Brumer-Stark conjecture is the generalization of the Stickelberger ideal annihilating the ideal class group of $\mathbb{Q}(\mu_m)$.

**Conjecture.** *(Brumer-Stark). Every ideal $\mathfrak{a}$ of $K$ has the following property: There exists an element $\alpha \in K$ satisfying $|\alpha|_v = 1$ for every Archimedian place $v$ of $K$ such that $\mathfrak{a}^{\omega\theta_{S,K/k}} = (\alpha)$ and such that the extension $K(\sqrt[\omega]{\alpha})$ is Abelian.*

This conjecture has recently been proven by Dr. Cristian D. Popescu. In his seminar's closing remarks, he mentioned that he is working on a further generalization of the Brumer-Stark conjecture for non-Abelian extensions.

## References


[1] B. Berndt, R. Evans, and K. Williams *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts Vol. 21, Wiley-Interscience Publication, New York, 1998, pp. 1–57.

[2] H. Davenport *Multiplicative Number Theory*, 3rd ed., Springer-Verlag, New York, 2000, pp. 1–12.

[3] D. Dummit and R. Foote *Abstract Algebra*, 3rd ed., John Wiley and Sons Inc., New Jersey, 2004, pp. 637–638.

[4] E. Landau *Elementary Number Theory*, 2nd ed., Chelsea Publishing Company, New York, 1947, pp. 197–221.

[5] S. Lang *Algebraic Number Theory*, Addison-Wesley, Reading, 1970, pp. 71–98.

[6] S. Lang *Cyclotomic Fields, I,II*, Springer-Verlag, New York, 1978, 1980 pp. 71–98.

[7] D. Marcus *Number Fields*, Springer-Verlag, New York, 1977, pp. 55–98.

[8] T. Ono *An Introduction to Algebraic Number Theory*, Plenum Press, New York, 1990, pp. 44–57.

[9] H. Stark *Analytic Theory of Algebraic Numbers*, to be published.