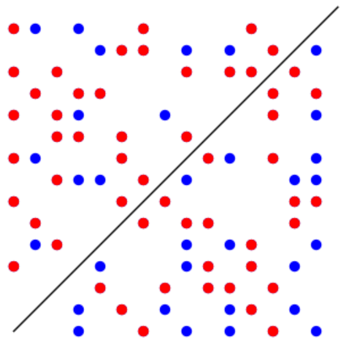
Pretty Patterns of Perfect Powers mod $\mathfrak{p}$

Emily A. Kirkman

Under the advisement of William A. Stein



A thesis submitted to the
University of Washington
Department of Mathematics
in partial fulfillment of the
requirements for the
Bachelor of Science Degree
with Distinction

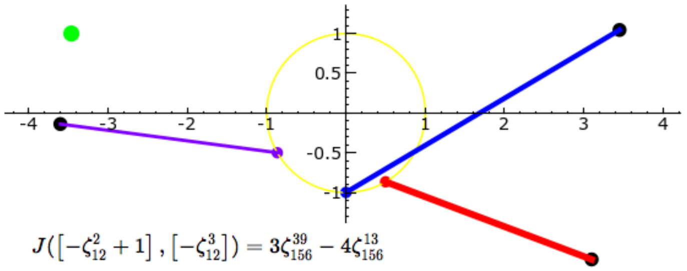
June 6, 2008

"In elementary number theory courses, quadratic
reciprocity often appears as a curiosity, no more profound
than many other curiosities. In fact, as the above discussion
illustrates, it should be considered the first result in
class field theory, which helps explain why
Euler, Lagrange, Legendre, and Gauss
devoted so much attention to it."

– J. S. Milne, while discussing quadratic extensions of $\mathbb{Q}$

Acknowledgements: Foremost I would like to thank my advisor, William Stein, for guiding me through the thesis process by both inspiring new directions and supplying endless enthusiasm. His confidence in his students has made an immense difference for me, and opened many opportunities during my undergraduate studies.

Contents



$$J([-\zeta_{12}^{2}+1]\,,[-\zeta_{12}^{3}])=3\zeta_{156}^{39}-4\zeta_{156}^{13}$$

1 Introduction

In an elementary number theory course, a student would begin to consider possible criteria for determining the solvability of a congruence involving a perfect square $x^2 \equiv a \pmod{p}$, for some prime p and $a \in \mathbb{Z}/p\mathbb{Z}$. This would typically culminate in a proof of the *Law of Quadratic Reciprocity*, an incredible result for determining the solvability of such perfect squares, which was first proven by Gauss in 1796. There are immediate applications that a student could grasp: determining the solvability of the quadratic equation $ax^2 + bx + c \equiv 0 \pmod{n}$, computing square roots, and proving the existence of infinitely many primes in some arithmetic progressions are among the easily accessible results.

Unfortunately, many undergraduate texts end the story there, often without even mentioning the existence of more general reciprocity laws. We wish instead to take this consideration a step further, and examine the solvability for higher perfect powers. In particular, we uncover analogous ideas for odd prime powers given by *Eisenstein's Reciprocity Law*, (which we prove in Section 5).

When attempting to prove the laws of cubic and biquadratic reciprocity, Gauss wrote that *"...the previously accepted principles of arithmetic are in no way sufficient for the foundations of a general theory, that such a theory necessarily demands that to a certain extent the domain of higher arithmetic needs to be endlessly enlarged..."[Ir, 108].* In order to prove the main theorem, we must develop some machinery based in algebraic number theory. Such a task results in a tour of m-th power residue symbols, Dirichlet characters, sums of Gauss and Jacobi, $\mathfrak{p}$-adic valuations and a general congruence relation due to Ludwig Stickelberger.

Throughout this paper, we assume general knowledge of undergraduate abstract algebra as well as elementary number theory. We now continue the introduction by presenting first the quadratic case, then follow with some immediate generalizations to congruences of higher powers, (i.e. we consider $x^m \equiv a \pmod{p}$, for p prime and $m \in \mathbb{N}$).

1.1 Perfect Squares mod p

We introduce this theory by considering the following example:

Example 1.1. *Suppose we wish to determine whether $x^2 \equiv 19$ (mod 31) has a solution. The naive way to decide this involves attempting the computation for different values of x, until we reach the desired result. For our particular example, we compute:*

$$\begin{gathered} 1^2 = 1 \equiv 1 \ (mod\, 31) \\ 2^2 = 4 \equiv 4 \ (mod\, 31) \\ \vdots \\ 9^2 = 81 \equiv 19 \ (mod\, 31). \end{gathered}$$

And thus, $x = 9$ is a solution to the congruence.

However, for large numbers this method could take a while; in fact the complexity of this algorithm is exponential in terms of the number of digits of p. But such a problem is not a lost cause. We will reveal a simpler method of determining whether or not a solution exists, without actually having to compute the solution itself. This allows us to develop a polynomial time algorithm that answers the question in the preceding example. There are two main elements of this improved algorithm to consider: Euler's Criterion (Proposition 1.4) and a binary arithmetic trick for computing large powers mod p. To convey Euler's Criterion in the usual language, we first introduce a few terms.

Definition 1.2. For a fixed prime p and nonzero $a \in \mathbb{Z}/p\mathbb{Z}$, a is a *quadratic residue* mod p if a is congruent to a perfect square mod p. Similarly, a is a *quadratic nonresidue* mod p if a is not congruent to a perfect square mod p.

Hence in the example above, we are simply asking if 19 is a *quadratic residue* mod 31. We make one more definition, designating a notation to represent the quadratic residues and nonresidues mod p.

Definition 1.3. For an odd prime p, the *Legendre Symbol* $\left(\frac{a}{p}\right)$ is defined by:

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

From the definition, we can immediately prove some basic properties of the Legendre symbol. For both of the following propositions, we assume that a and b are not divisible by p, since the results would then be trivial in both cases. We will see in the first proposition that there is an easy way to compute whether or not a is a quadratic residue mod p.

Proposition 1.4 (Euler's Criterion)**.** [Ir, Prop 5.1.2.a] Given an odd prime p and $a, b \in \mathbb{Z}$,

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

Proof. By Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$, and thus

$$a^{p-1} - 1 \equiv 0 \pmod{p}.$$

By factoring, we obtain

$$a^{p-1} - 1 = (a^{(p-1)/2} + 1)(a^{(p-1)/2} - 1) \equiv 0 \pmod{p},$$

which implies that $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$. For a proof that $a^{(p-1)/2} \equiv 1$ if and only if a is a quadratic residue mod p, we refer the reader to the more general Proposition 1.18, taking $m = 2$ and $q = p$. We then acknowledge as a corollary that

$$a^{(p-1)/2} \equiv -1 \pmod{p} \iff a \text{ is a quadratic nonresidue mod } p,$$

since there are only two possible outcomes for $a^{(p-1)/2} \pmod{p}$. Therefore, $a^{(p-1)/2} \pmod{p}$ defines the Legendre symbol exactly. □

Corollary. The number of quadratic residues mod p is equal to the number of quadratic nonresidues mod p.

Proof. By the factorization in the proof above, it is obvious that $a^{(p-1)/2} \equiv 1 \pmod{p}$ has exactly $(p-1)/2$ solutions. In other words, there are $(p-1)/2$ quadratic residues mod p. Similarly, there are also $(p-1)/2$ quadratic nonresidues mod p. □

Also fairly obvious from the definition, we can make sense of multiplication for Legendre symbols. The following proposition is necessary for both understanding and proving quadratic reciprocity.

Proposition 1.5. [Ir, Prop 5.1.2.b] Given an odd prime p and a, b in $\mathbb{Z}$,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Proof. By the rules of exponentiation, $(ab)^{(p-1)/2} = a^{(p-1)/2}\ b^{(p-1)/2}$. Applying the result from Proposition 1.4 to both sides of the equation, we get

$$\begin{aligned} (ab)^{(p-1)/2} &\equiv \left(\frac{ab}{p}\right) \pmod{p}, \\ a^{(p-1)/2}\ b^{(p-1)/2} &\equiv \left(\frac{a}{p}\right)\ \left(\frac{b}{p}\right) \pmod{p}. \end{aligned}$$

Hence by the above equality, we have

$$\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\ \left(\frac{b}{p}\right) \pmod{p}.$$

Since both sides above are equal to ± 1 and $p \geq 3$, we observe that the above equivalence is actually an equality. □

From a computation standpoint, Euler's Criterion gives us a much better idea of how to attack our original example. In fact, there is a simple polynomial time algorithm when applying a certain trick for computing large powers mod n. When computing $a^m \pmod{n}$, we represent m as a binary number and regard a^m as the product of a^{2^i}, for all i where the binary digit is one. Hence the number of required multiplications decreases (from $m-1$ to the number of digits in the binary representation).

Example 1.6. *Recall that we wish to determine whether or not $x^2 \equiv 19 \pmod{31}$ is solvable. We compute the Legendre symbol via Proposition 1.4:*

$$19^{(31-1)/2} = 19^{15} \equiv 1 \pmod{31}.$$

Therefore, 19 is a quadratic residue mod 31 and we conclude $x^2 \equiv 19 \pmod{31}$ is solvable. We remark for emphasis that we have determined a solution exists, however we have not directly computed a value of x that satisfies the congruence.

Furthermore, we show the computation using the binary representation algorithm. Now we have

$$19^{15} = 19^{2^3} \cdot 19^{2^2} \cdot 19^{2^1} \cdot 19 \equiv 9 \cdot 28 \cdot 20 \cdot 19 \equiv 1 \pmod{31}.$$

In fact, this optimized computation of the Legendre symbol is already implemented in Sage. We use this implementation in the following example.

Example 1.7. *For very large p, a direct computation of the solution to the congruence $x^2 \equiv a \pmod{p}$ would be quite difficult. We give an example where it is trivial (with Euler's Criterion) to determine whether a solution exists, but hard to find such a solution. We define a and p in Sage:*

```
p = next_prime(2^500)
a = 5*next_prime(p)+2^18
```

The optimized implementation in Sage allows us to quickly compute whether or not a is a quadratic residue mod p. *The command,*

```
legendre_symbol(a,p)
```

returns the value 1. *Hence, we have determined that a solution to the congruence $x^2 \equiv a \pmod{p}$ exists, without computing it directly.*

We now use this implementation of the Legendre symbol along with the code in the example below to consider the quadratic residues and nonresidues over many different primes. Using only what we have established so far, we would have to apply Euler's Criterion to all $\left(\frac{q}{p}\right)$ that we wish to compute. But there appears to be a pattern in the figure generated by the following example. In fact, it is *almost* symmetric along $p = q$.

Example 1.8. *We consider $\left(\frac{q}{p}\right)$, where q and p are both prime. The following Sage code computes the Legendre symbols for the first 20 primes and plots them in a matrix (Figure 1). We remark that some formatting details have been omitted, although the following code will produce a similar image. In particular, we've chosen to label each cell with an "R", "N", or "0" to represent whether it is a residue, nonresidue, or multiple of p respectively.*

```
r = 20
np = [nth_prime(i+2) for i in range(r)]
leg = [[legendre_symbol(np[i], np[j]) for i in range(r)] for j in range(r)]
matrix_plot(matrix(leg), cmap='Oranges')
```

By the looks of Figure 1, one would presume that there is a forthcoming theorem. In fact, Gauss's Law of Quadratic Reciprocity describes exactly the pattern we are seeing for quadratic residues.

Theorem 1.9 (The Law of Quadratic Reciprocity)**.** Let p and q be distinct odd primes. Then

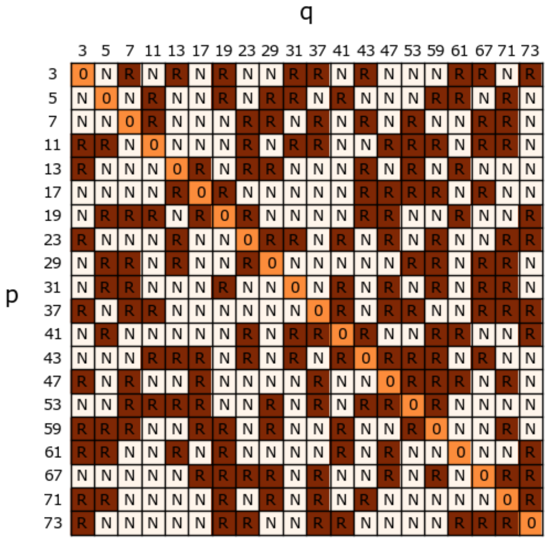
$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)\ (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Furthermore, we have

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

(ii) $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8}, \\ -1 & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases}$

Figure 1: Quadratic Residues



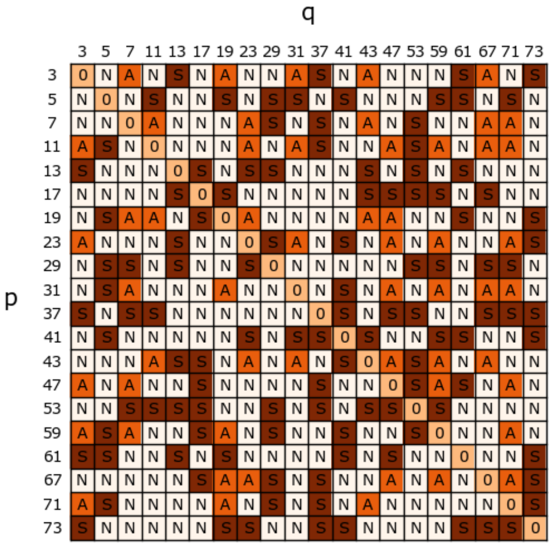
	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73
3	0	N	R	N	R	N	R	N	N	R	R	N	R	N	N	N	R	R	N	R
5	N	0	N	R	N	N	R	N	R	R	N	R	N	N	N	R	R	N	R	N
7	N	N	0	R	N	N	N	R	R	N	R	N	R	N	R	N	N	R	R	N
11	R	R	N	0	N	N	N	R	N	R	R	N	N	R	R	R	N	R	R	N
13	R	N	N	N	0	R	N	R	R	N	N	N	R	N	R	N	R	N	N	N
17	N	N	N	N	R	0	R	N	N	N	N	N	R	R	R	R	N	R	N	N
19	N	R	R	R	N	R	0	R	N	N	N	N	R	R	N	N	R	N	N	R
23	R	N	N	N	R	N	N	0	R	R	N	R	N	R	N	R	N	N	R	R
29	N	R	R	N	R	N	N	R	0	N	N	N	N	N	R	R	N	R	R	N
31	N	R	R	N	N	N	R	N	N	0	N	R	N	R	N	R	N	R	R	N
37	R	N	R	R	N	N	N	N	N	N	0	R	N	R	R	N	N	R	R	R
41	N	R	N	N	N	N	N	R	N	R	R	0	R	N	N	R	R	N	N	R
43	N	N	N	R	R	R	N	R	N	R	N	R	0	R	R	R	N	R	N	N
47	R	N	R	N	N	R	N	N	N	N	R	N	N	0	R	R	R	N	R	N
53	N	N	R	R	R	R	N	N	R	N	R	N	R	R	0	R	N	N	N	N
59	R	R	R	N	N	R	R	N	R	N	N	R	N	N	R	0	N	N	R	N
61	R	R	N	N	R	N	R	N	N	N	N	R	N	R	N	N	0	N	N	R
67	N	N	N	N	N	R	R	R	R	N	R	N	N	R	N	R	N	0	R	R
71	R	R	N	N	N	N	R	N	R	N	R	N	R	N	N	N	N	N	0	R
73	R	N	N	N	N	N	R	R	N	N	R	R	N	N	N	N	R	R	R	0

We will see that Theorem 1.9 is the result of a more general theorem proven in Section 5. We also offer an alternative proof in Section 3.3, after building a few preliminary details. But for now, we return to our matrix plot and decipher the pattern related to us by Gauss.

Example 1.10. *Using the law of Quadratic Reciprocity, we expect that for all p, q prime with q a quadratic residue mod p, we will have symmetry across $q = p$ if and only if $\frac{p-1}{2} \cdot \frac{q-1}{2}$ is even. We use a similar computation below, but this time we change the matrix entry to 2 for all residues where $\frac{p-1}{2} \cdot \frac{q-1}{2}$ is even. (This will result in the matrix plot displaying an additional shade of orange). We have also labeled the cells as before, except that the "R" for residue is replaced by either an "A" or an "S", respectively denoting anti-symmetric and symmetric. The following code will produce a similar image to Figure 2, although certain plotting details have been omitted in the main text to conserve space. The full plotting detail can be found in Appendix section 1.*

```
r = 20
np = [nth_prime(i+2) for i in range(r)]
leg = [[legendre_symbol(np[i], np[j]) for i in range(r)] for j in range(r)]
for i in range(r):
    for j in range(r):
        if leg[i][j] == 1 and Mod((np[i]-1)*(np[j]-1)//4,2) == 0:
            leg[i][j] = 2
matrix_plot(matrix(leg), cmap='Oranges')
```

Figure 2: Quadratic Residues (with symmetry)



p \ q	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73
3	0	N	A	N	S	N	A	N	N	A	S	N	A	N	N	N	S	A	N	S
5	N	0	N	S	N	N	S	N	S	S	N	S	N	N	N	S	S	N	S	N
7	N	N	0	A	N	N	N	A	S	N	S	N	A	N	S	N	N	A	A	N
11	A	S	N	0	N	N	N	A	N	A	S	N	N	A	S	A	N	A	A	N
13	S	N	N	N	0	S	N	S	S	N	N	N	S	N	S	N	S	N	N	N
17	N	N	N	N	S	0	S	N	N	N	N	N	S	S	S	S	N	S	N	N
19	N	S	A	A	N	S	0	A	N	N	N	N	A	A	N	N	S	N	N	S
23	A	N	N	N	S	N	N	0	S	A	N	S	N	A	N	A	N	N	A	S
29	N	S	S	N	S	N	N	S	0	N	N	N	N	N	S	S	N	S	S	N
31	N	S	A	N	N	N	A	N	N	0	N	S	N	A	N	A	N	A	A	N
37	S	N	S	S	N	N	N	N	N	N	0	S	N	S	S	N	N	S	S	S
41	N	S	N	N	N	N	N	S	N	S	S	0	S	N	N	S	S	N	N	S
43	N	N	N	A	S	S	N	A	N	A	N	S	0	A	S	A	N	A	N	N
47	A	N	A	N	N	S	N	N	N	N	S	N	N	0	S	A	S	N	A	N
53	N	N	S	S	S	S	N	N	S	N	S	N	S	S	0	S	N	N	N	N
59	A	S	A	N	N	S	A	N	S	N	N	S	N	N	S	0	N	N	A	N
61	S	S	N	N	S	N	S	N	N	N	N	S	N	S	N	N	0	N	N	S
67	N	N	N	N	N	S	A	A	S	N	S	N	N	A	N	A	N	0	A	S
71	A	S	N	N	N	N	A	N	S	N	S	N	A	N	N	N	N	N	0	S
73	S	N	N	N	N	N	S	S	N	N	S	S	N	N	N	N	S	S	S	0

The two supplementary laws attached to the theorem allow us to consider all squares mod p, instead of restricting a to be a prime number. We consider the following example, where we use the supplementary laws and the multiplicativity of the Legendre symbol to determine whether or not there exists a solution to the congruence $x^2 \equiv 30 \pmod{392,923,759}$.

Example 1.11. *We use prime factorization in conjunction with Quadratic Reciprocity to show that 30 is a square mod $p = 392,923,759$. First we note that,*

$$\left(\frac{30}{p}\right) = \left(\frac{2 \cdot 3 \cdot 5}{p}\right) = \left(\frac{2}{p}\right) \cdot \left(\frac{3}{p}\right) \cdot \left(\frac{5}{p}\right).$$

And now we compute each Legendre symbol on the right hand side. First we compute

$$p \equiv -1 \pmod{8},$$

and thus by (ii) we have

$$\left(\frac{2}{392,923,759}\right) = 1.$$

Further,

$$\left(\frac{3}{392,923,759}\right) = \left(\frac{392,923,759}{3}\right) = \left(\frac{1}{3}\right) = 1.$$
$$\left(\frac{5}{392,923,759}\right) = \left(\frac{392,923,759}{5}\right) = \left(\frac{4}{5}\right) = 1.$$

Therefore we conclude that $\left(\frac{30}{p}\right) = 1$, as desired.

This idea of factorization allows us to think outside the box of perfect powers as well. We present one more example before moving onto generalizations of quadratic reciprocity. Here, we use Theorem 1.9 to prove a seemingly unrelated result.

Example 1.12. [Ste, Exer 4.9] *Given $n \in \mathbb{Z}$, we consider the integer $n^2 + n + 1$. We will use quadratic reciprocity to show that such an integer has no divisors of the form $6k - 1$. First, we show that a restriction of n to primes $p = 6k - 1$ is sufficient. We take p, q to be prime such that neither is of the form $6k - 1$. We have,*

$$p \not\equiv 5 \pmod 6,$$
$$q \not\equiv 5 \pmod 6.$$

We note that by definition, both p and q are not congruent to $0 \pmod 6$*. We also know that neither p nor q can be congruent to* $4 \pmod 6$*, since then*

$$p = 4 + 6k \implies 2 \mid p \text{ and } p \neq 2 \implies p \text{ is not prime.}$$

Thus p and q are congruent to one of $\{1, 2, 3\} \pmod 6$*. By taking all possible combinations of values for p and q, we can show that the product pq will never be congruent to* $5 \pmod 6$*:*

$$pq \equiv 1 \cdot 1 \equiv 1 \pmod 6$$
$$pq \equiv 1 \cdot 2 \equiv 2 \pmod 6$$
$$pq \equiv 1 \cdot 3 \equiv 3 \pmod 6$$
$$pq \equiv 2 \cdot 2 \equiv 4 \pmod 6$$
$$pq \equiv 2 \cdot 3 \equiv 0 \pmod 6$$
$$pq \equiv 3 \cdot 3 \equiv 3 \pmod 6.$$

Hence, the restriction of the proof to only primes $p = 6k - 1$ is sufficient. So we take

$$p = 6k - 1 \mid n^2 + n + 1.$$

This implies that

$$p \mid 4n^2 + 4n + 4,$$

which can be factored to show that

$$p \mid (2n + 1)^2 + 3.$$

Therefore, -3 is a quadratic residue mod $6k - 1$*. We now apply Theorem 1.9 along with multiplication of the Legendre symbol to find $\left(\frac{-3}{6k-1}\right)$:*

$$\left(\frac{-3}{6k-1}\right) = \left(\frac{-1}{6k-1}\right)\left(\frac{3}{6k-1}\right)$$

Computing the symbols on the right, we get

$$\left(\frac{-1}{6k-1}\right) = (-1)^{\frac{6k-2}{2}} = (-1)^{3k-1},$$
$$\left(\frac{3}{6k-1}\right) = (-1)^{\frac{6k-2}{2}\cdot\frac{2}{2}}\left(\frac{6k-1}{3}\right) = (-1)^{3k-1}\left(\frac{-1}{3}\right) = (-1)^{3k-1}(-1) = (-1)^{3k}.$$

Therefore,

$$\left(\frac{-3}{6k-1}\right) = (-1)^{3k-1}(-1)^{3k} = (-1)^{6k-1}.$$

Since $6k-1$ *is odd for all* $k \in \mathbb{Z}$, *we have found that* -3 *is a quadratic nonresidue* mod $p = 6k-1$, *which is a contradiction. We conclude that for all* $n \in \mathbb{Z}$, *the integer* n^2+n+1 *is not divisible by any integer of the form* $6k-1$. □

The preceding example shows an application of quadratic reciprocity in determining the behavior of arithmetic progressions. Similarly, it can be shown that there are infinitely many primes in the form of many different arithmetic progressions. We refer the reader to [Es, Section 7.5] for numerous examples.

1.2 Generalizations to Perfect Powers mod $\mathfrak{p}$

We now consider the solvability of $x^m \equiv a \pmod{p}$, for $m \in \mathbb{N}$. As previously alluded to, we must expand our ideas of arithmetic. We begin by making some basic definitions of algebraic number theory.

Definition 1.13. A *number field* is a field $K \subset \mathbb{C}$ such that $[K : \mathbb{Q}] = n \in \mathbb{N}$, i.e. K is a finite extension of $\mathbb{Q}$.

Definition 1.14. The *ring of integers* $\mathcal{O}_K$ of a number field K is the set of all algebraic integers in K.

In general, we extend our previous interpretation of the integers to the ring of algebraic integers $\mathcal{O}_K$, for some number field K containing an m-th root of unity ζ_m. A prime ideal $\mathfrak{p} \in \mathcal{O}_K$ above p is considered prime to m if and only if $\gcd(N(\mathfrak{p}), m) = 1$, where $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$ is the norm of $\mathfrak{p}$. Alternatively, we could say that m is prime to $\mathfrak{p}$ if $(m) \not\subset \mathfrak{p}$.

Thus for $\zeta_m \in K$ and $\mathfrak{p}$ prime to m, the multiplicative group $(\mathcal{O}_K/\mathfrak{p})^*$ contains a subgroup generated by $\zeta_m \pmod{\mathfrak{p}}$ of order m. Hence $n \mid (N(\mathfrak{p})-1)$, and we make the following definition:

Definition 1.15. [Le, §4.1] Let K be a number field containing a primitive m-th root of unity ζ_m ($m \in \mathbb{N}$), and let $\mathfrak{p}$ be a prime ideal in the ring of integers $\mathcal{O}_K$. For $\alpha \in \mathcal{O}_K$, we define the *m-th power residue symbol* $\left(\frac{\alpha}{\mathfrak{p}}\right)_m$ to be

1. $\left(\frac{\alpha}{\mathfrak{p}}\right)_m = 0$ if $\alpha \in \mathfrak{p}$,
2. If $\alpha \notin \mathfrak{p}$, $\left(\frac{\alpha}{\mathfrak{p}}\right)_m$ is the unique m-th root of unity such that

$$\alpha^{\frac{N(\mathfrak{p})-1}{m}} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right)_m \pmod{\mathfrak{p}}.$$

Further, we extend this definition for any ideal $\mathfrak{a}$ that is prime to m, by taking the product of all $\left(\frac{\alpha}{\mathfrak{p}_i}\right)_m$, where $\mathfrak{p}_i$ is in the prime decomposition of $\mathfrak{a}$.

Example 1.16 (Power Residue Symbols)**.** *We provide a programming example in* [Sage] *of computing power residue symbols directly from the definition.*

```
def power_residue_symbol(alpha, p, m):
    if p.divides(alpha): return 0
    elif not p.is_prime():
        return prod(power_residue_symbol(alpha,ell,m)^e
                for ell, e in p.factor())
    F = p.residue_field()
    N = p.norm()
    r = F(alpha)^((N-1)/m)
    k = p.number_field()
    for kr in k.roots_of_unity():
        if r == F(kr):
            return kr
```

Although we will continue to use the above function definition throughout this thesis, we remark that it does not represent optimized code. It is presented merely as a straightforward example which is sufficient for the computation of the examples contained in this paper.

Using the above function definition, we can compute a table of values [Le, Exer. 4.2]. We take $K = \mathbb{Q}(i), \mathfrak{p} = (3)$ *and compute the quartic power residue symbol for each of the following* α*:*

```
m = 4
K.<a> = QQ[I]
p = K.ideal(3)
G.<w> = p.residue_field()
z = G.zeta()
alpha = [ G.lift(z^i) for i in range(G.zeta_order()) ]
chi_alpha = [ power_residue_symbol(a, p, m) for a in alpha ]
```

In particular, we've shown that we are able to compute the power residue symbol for complex-valued α*. The preceding code fills lists of corresponding values depicted in the table below:*

α	1	2	i	$1+i$	$2+i$	$2i$	$1+2i$	$2+2i$
$\left(\frac{\alpha}{\mathfrak{p}}\right)_4$	1	1	-1	$-i$	i	-1	i	$-i$

Before moving on, we quickly address the multiplicativity of power residue symbols:

Proposition 1.17. Let $\left(\frac{\cdot}{\mathfrak{p}}\right)_m$ denote the m-th power residue symbol mod $\mathfrak{p}$. Then for $\alpha, \beta \in \mathbb{Z}$,

$$\left(\frac{\alpha\beta}{\mathfrak{p}}\right)_m = \left(\frac{\alpha}{\mathfrak{p}}\right)_m \left(\frac{\beta}{\mathfrak{p}}\right)_m .$$

Proof. Analogous to our proof of Proposition 1.5 for Legendre symbols, we simply apply the rules of exponentiation to expand the expression:

$$\left(\frac{\alpha\beta}{\mathfrak{p}}\right)_m \equiv (\alpha\beta)^{(N(\mathfrak{p})-1)/m} \equiv \alpha^{(N(\mathfrak{p})-1)/m}\beta^{(N(\mathfrak{p})-1)/m} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right)_m \left(\frac{\beta}{\mathfrak{p}}\right)_m.$$

□

We can now present the relationship between the power residue symbol and the solvability of $x^m \equiv a \pmod{p}$ in the following proposition.

Proposition 1.18. [Ir, Prop 7.1.2] Let $\mathbb{F}_q$ denote a finite field of size q, and $\mathbb{F}_q^*$ the multiplicative group of $\mathbb{F}_q$. For $\alpha \in \mathbb{F}_q^*$, we have that $x^m \equiv \alpha \pmod{q}$ has solutions if and only if

$$\alpha^{(q-1)/(m,q-1)} = 1.$$

In particular, $x^m \equiv \alpha \pmod{\mathfrak{p}}$ is solvable if and only if $\left(\frac{\alpha}{\mathfrak{p}}\right)_m = 1$.

Proof. It is a well-known fact that $\mathbb{F}_q^*$ is cyclic for any prime q. Thus given a generator $\mathbb{F}^* = \langle g \rangle$, and two elements $x = g^a$ and $y = g^b$, we have that

$$x^m = (g^a)^m = g^b = \alpha$$

is equivalent to

$$am \equiv b \ (mod\ q-1).$$

Thus $x^m \equiv \alpha \pmod{q}$ has solutions if and only if $\alpha^{(q-1)/(m,q-1)} = 1$, as desired. Further, by choosing $q = N(\mathfrak{p}) \equiv 1 \pmod{m}$, we have

$$\alpha^{(q-1)/(m,q-1)} = \alpha^{(N(\mathfrak{p})-1)/m} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right)_m \pmod{\mathfrak{p}}.$$

□

Therefore, we can return our attention to the table computed in Example 1.2, and see that 1 and 2 are both quartic residues mod 3. We will further demonstrate this proposition while introducing some useful notation in the following example. Analogous to Example 1.1, we use the cubic residue character to show that $x^3 \equiv 19 \pmod{31}$ is solvable:

Example 1.19 (The Cubic Residue Character)**.** *We apply the above proposition taking $\mathbb{F} = \mathbb{Z}[\omega]/31\mathbb{Z}[\omega]$, where $\omega = (-1+\sqrt{-3})/2$, (and thus $D = \mathbb{Z}[\omega]$ is the ring of Eisenstein integers). The norm in D is given by complex conjugation, and thus $N(31) = 31^2$. Therefore,*

$$x^3 \equiv 19 \pmod{31} \textit{ is solvable } \iff \left(\frac{19}{31}\right)_3 = 1.$$

We apply Definition 1.15 directly:

$$19^{(N(31)-1)/3} \equiv 19^{(31^2-1)/3} \equiv 19^{320} \equiv 1 \pmod{31} \Rightarrow \left(\frac{19}{31}\right)_3 = 1.$$

Hence, this equation is solvable.

But as we found in the quadratic case, deciding for which primes p there exists a solution to the congruence $x^m \equiv a \pmod{p}$ can be a more difficult problem. A further complication to this quest is the notion of associate elements. Recall from algebra that two elements a and b in an integral domain R are considered *associates* if $a = bu$, for u a unit in R. We can make sense of this definition in terms of ideals in a unique factorization domain R, by defining a unit $u \in R$ such that $(u) = R$, and replacing the notion of "divides" with containment of ideals (i.e., $a \mid b$ is equivalent to $(b) \subseteq (a)$). Then $a, b \in R$ are associate if $(a) = (b)$. For example, in the ring D as defined in the previous example, each nonzero element will have 6 associates.

We need to find a way to discuss a representative of each prime in R, without considering its associates. We establish a definition to resolve this ambiguity.

Definition 1.20. We say that a nonzero element $\alpha \in \mathbb{Z}[\zeta_k]$ is *primary* if it is coprime to k and $\alpha \equiv n$ $(mod\ (1-\zeta_k)^2)$, for some $n \in \mathbb{Z}$.

In the ring D of Eisenstein integers given in the example above, we say that an element $\alpha \in D$ is primary if for $\alpha = a + b\omega$, we have $a \equiv \pm 1 \pmod{3}$ and $b \equiv 0 \pmod{3}$.

We may now state the main theorem.

2 The Eisenstein Reciprocity Law

Theorem 2.1 (The Eisenstein Reciprocity Law)**.** Let ℓ be an odd prime, where $a \in \mathbb{Z}$ is prime to ℓ, and $\beta \in \mathbb{Z}[\zeta_l]$ are primary elements. Suppose also that a and β are relatively prime. Then

$$\left(\frac{a}{\beta}\right)_\ell = \left(\frac{\beta}{a}\right)_\ell.$$

Further, we have the following supplementary laws:

(i) $\left(\frac{\zeta}{a}\right)_\ell = \zeta^{(a^{\ell-1}-1)/\ell}$,

(ii) $\left(\frac{1-\zeta}{a}\right)_\ell = \left(\frac{\zeta}{a}\right)_\ell^{(\ell-1)/2}$.

By temporarily granting this general reciprocity law, we see that Theorem 1.9 is an immediate corollary. Further, we can go on to define the Law of Cubic Reciprocity as well:

Corollary (The Law of Cubic Reciprocity)**.** *Let* π_1, π_2 *be primary such that* $N(\pi_1), N(\pi_2) \neq 3, N(\pi_1) \neq N(\pi_2)$*. Then*

$$\left(\frac{\pi_1}{\pi_2}\right)_3 = \left(\frac{\pi_2}{\pi_1}\right)_3.$$

We remark in the above corollary that the Law of Cubic Reciprocity has its own supplementary laws for handling primes and units, and thus by factorization this theorem can be applied to nd the cubic residue symbol of any number.

Proposition 2.2 (Supplementary Laws for Cubic Reciprocity)**.** [Le, Prop 7.7] For ρ a cube root of unity (such as $\rho = \frac{-1+\sqrt{-3}}{2}$ in the case above when discussing the ring of Eisenstein integers), and $a \in \mathbb{Z}$, we have the supplementary laws:

(i) $\left(\frac{\rho}{a}\right)_3 = \rho^{\frac{1-a}{3}}$.

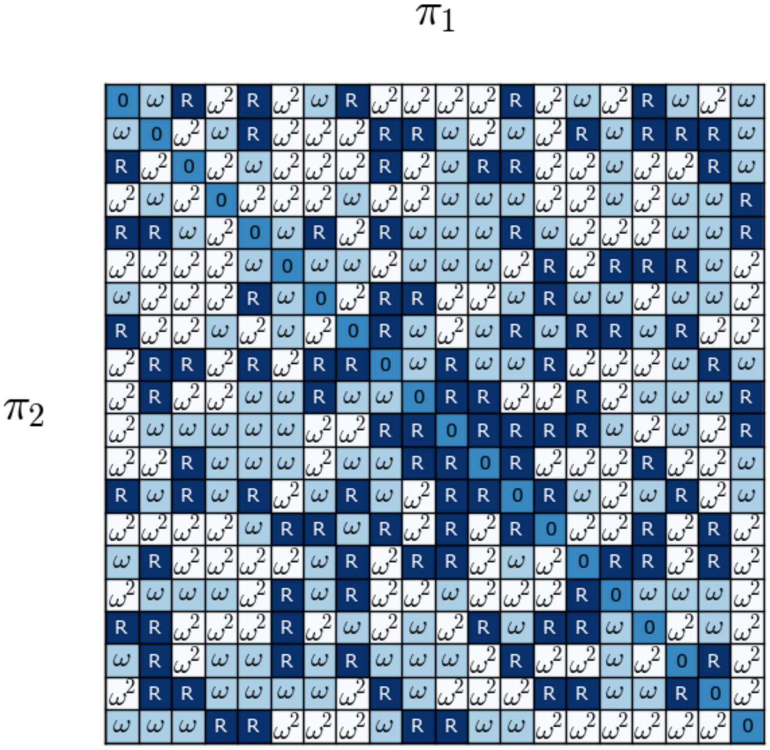
(ii) $\left(\frac{1-\rho}{a}\right)_3 = \rho^{\frac{a-1}{3}}$.

Example 2.3. *We can immediately apply this Corollary (Cubic Reciprocity) to a programming example as before. Here, we generate a table of cubic residues for primary primes* π_1 mod *primary primes* π_2*. Note that we make use of the code in Example 1.2 to define the cubic residue symbol. Also, we introduce below a simple function for determining whether a prime in* $\mathbb{Z}[\omega]$ *is primary.*

```
def cubic_is_primary(n):
    g = n.gens_reduced()[0]
    a,b = g.polynomial().coefficients()
    return Mod(a,3)!=0 and Mod(b,3)==0

r = 10
m=3
D.<w> = NumberField(x^2+x+1)
it = D.primes_of_degree_one_iter()
pp = []
while len(pp) < r:
    k = it.next()
    if cubic_is_primary(k):
        pp.append(k)

n = [ [ power_residue_symbol(pp[i].gens_reduced()[0], pp[j], m) \
                for i in range(r) ] for j in range(r) ]

# Convert to integer matrix for gradient colors
for i in range(r):
    for j in range(r):
        if n[i][j] == w:
            n[i][j] = int(-1)
        elif n[i][j] == w^2:
            n[i][j] = int(-2)
        elif n[i][j] == 1:
            n[i][j] = int(1)

matrix_plot(matrix(n),cmap="Blues")
```

The above code will produce an image similar to Figure 3, although some plotting details are omitted to conserve space. For the full plotting detail, we refer the reader to Appendix section 1-2.

Figure 3: Cubic Residues (with symmetry)



π_1

π_2

0	ω	R	ω^2	R	ω^2	ω	R	ω^2	ω^2	ω^2	ω^2	R	ω^2	ω	ω^2	R	ω	ω^2	ω
ω	0	ω^2	ω	R	ω^2	ω^2	ω^2	R	R	ω	ω^2	ω	ω^2	R	ω	R	R	R	ω
R	ω^2	0	ω^2	ω	ω^2	ω^2	ω^2	R	ω^2	ω	R	R	ω^2	ω^2	ω	ω^2	ω^2	R	ω
ω^2	ω	ω^2	0	ω^2	ω^2	ω^2	ω	ω^2	ω^2	ω	ω	ω	ω^2	ω^2	ω	ω^2	ω	ω	R
R	R	ω	ω^2	0	ω	R	ω^2	R	ω	ω	ω	R	ω	ω^2	ω^2	ω^2	ω	ω	R
ω^2	ω^2	ω^2	ω^2	ω	0	ω	ω	ω^2	ω	ω	ω	ω^2	R	ω^2	R	R	R	ω	ω^2
ω	ω^2	ω^2	ω^2	R	ω	0	ω^2	R	R	ω^2	ω^2	ω	R	ω	ω	ω^2	ω	ω	ω^2
R	ω^2	ω^2	ω	ω^2	ω	ω^2	0	R	ω	ω^2	ω	R	ω	R	R	ω	R	ω^2	ω^2
ω^2	R	R	ω^2	R	ω^2	R	R	0	ω	R	ω	ω	R	ω^2	ω^2	ω^2	ω	R	ω
ω^2	R	ω^2	ω^2	ω	ω	R	ω	ω	0	R	R	ω^2	ω^2	R	ω^2	ω	ω	ω	R
ω^2	ω	ω	ω	ω	ω	ω^2	ω^2	R	R	0	R	R	R	R	ω	ω^2	ω	ω^2	R
ω^2	ω^2	R	ω	ω	ω	ω^2	ω	ω	R	R	0	R	ω^2	ω^2	ω^2	R	ω^2	ω^2	ω
R	ω	R	ω	R	ω^2	ω	R	ω	ω^2	R	R	0	R	ω	ω^2	ω	R	ω^2	ω
ω^2	ω^2	ω^2	ω^2	ω	R	R	ω	R	ω^2	R	ω^2	R	0	ω^2	ω^2	R	ω^2	R	ω^2
ω	R	ω^2	ω^2	ω^2	ω^2	ω	R	ω^2	R	R	ω^2	ω	ω^2	0	R	R	ω^2	R	ω^2
ω^2	ω	ω	ω	ω^2	R	ω	R	ω^2	ω^2	ω	ω^2	ω^2	ω^2	R	0	ω	ω	ω	ω^2
R	R	ω^2	ω^2	ω^2	R	ω^2	ω	ω^2	ω	ω^2	R	ω	R	R	ω	0	ω^2	ω	ω^2
ω	R	ω^2	ω	ω	R	ω	R	ω	ω	ω	ω^2	R	ω^2	ω^2	ω	ω^2	0	R	ω^2
ω^2	R	R	ω	ω	ω	ω	ω^2	R	ω	ω^2	ω^2	ω^2	R	R	ω	ω	R	0	ω^2
ω	ω	ω	R	R	ω^2	ω^2	ω^2	ω	R	R	ω	ω	ω^2	ω^2	ω^2	ω^2	ω^2	ω^2	0

We now take a moment to present an example that uses the Law of Cubic Reciprocity to determine whether or not there exists a solution to a complex-valued cubic congruence. In the following example, we correct an error found in a given exercise [Ir, 9.16], by replacing $2 - 3\omega$ with $2 + 3\omega$. We make this substitution so that the computation of the function λ (defined below) agrees with [Ir].

Example 2.4. *We will show that $x^3 \equiv 2 + 3\omega (mod\ 11)$ is not solvable for x in $\mathbb{Z}[\omega]$, where $\mathbb{Z}[\omega]$ denotes the ring of Eisenstein integers: We use the cubic reciprocity law. Note that $11 \equiv 2(mod\ 3), 2 \equiv 2(mod\ 3)$, and $3 \equiv 0(mod\ 3) \Rightarrow 11$ and $2 + 3\omega$ are primary. Also note that $N(11) \neq N(2 + 3\omega)$, so we have*

$$\left(\frac{2+3\omega}{11}\right)_3 = \left(\frac{11}{2+3\omega}\right)_3.$$

Thus $x^3 \equiv 2 + 3\omega(mod\ 11)$ solvable $\Leftrightarrow x^3 \equiv 11(mod\ 2 + 3\omega)$. Consider the map $\lambda : \mathbb{Z}[\omega] \to \mathbb{Z}$ defined by $\lambda(a + b\omega) = (a^2 - ab + b^2)$. $\lambda(2 + 3\omega) = 7$ thus we can consider:

$$x^3 \equiv 11(mod\ 2 + 3\omega) \Leftrightarrow x^3 \equiv 11(mod\ 7) \text{ is solvable in } \mathbb{Z}$$

Since $x^3 \equiv a(mod\ 7)$ is solvable in $\mathbb{Z} \Leftrightarrow a \equiv 1$ or $6(mod\ 7)$. $11 \equiv 4(mod\ 7)$ implies that $x^3 \equiv 2 + 3\omega(mod\ 11)$ is not solvable for x in $\mathbb{Z}[\omega]$, as desired.

We now shift our focus to developing a proof of Theorem 2.1. We will begin in the next section by defining and exploring some useful preliminary material.

3 Preliminaries

3.1 Dirichlet Characters

Throughout the remainder of this paper, we will frequently refer to *Dirichlet characters*, which are the building blocks of Gauss and Jacobi sums. We present a formal definition, as well as some elementary properties of these characters. Although the following definition is nonstandard, it is equivalent to the standard definition and will be sufficient for our purposes.

Definition 3.1. [Be, §1.6] A *Dirichlet character* on $\mathbb{F}_p$ is a nonzero map $\chi : \mathbb{F}_p^* \to \mathbb{C}^*$ that satisfies the following two properties:

1. $\chi(ab) = \chi(a)\chi(b),\ \forall a, b \in \mathbb{F}_p^*$,
2. $\chi(a) = 0 \iff (a, p) > 1$.

Example 3.2. *A simple example is the trivial Dirichlet character defined by,*

$$\epsilon(a) = 1,\ \forall a \in \mathbb{F}_p^*.$$

Given ϵ as in the previous example, we extend the definition of Dirichlet characters to include 0 in the domain of χ. For all $\chi \neq \epsilon$, we let $\chi(0) = 0$, and $\epsilon(0) = 1$. Henceforth we may consider Dirichlet characters $\chi : \mathbb{F}_p \to \mathbb{C}$.

Example 3.3. *Another example of a Dirichlet character is the m-th power residue symbol (Def 1.15). In fact, Proposition 1.17 satisfies the first property, and the second is satisfied directly by the definition. (Recall also that we have shown this for the Legendre symbol, and thus the Legendre symbol is also a Dirichlet character).*

The following proposition defines some of the basic properties of Dirichlet characters.

Proposition 3.4. [Ir, §8.1.1] *Let χ be a Dirichlet character and $a \in \mathbb{F}_p^*$. Then*

1. $\chi(1) = 1$
2. *$\chi(a)$ is a $(p-1)$th root of unity*
3. $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$

Proof.

1. $\chi(1) = \chi(1 \cdot 1) = \chi(1) \cdot \chi(1)$. $\chi(1) \neq 0 \Rightarrow \chi(1) = 1$.
2. $a^{p-1} = 1 \Rightarrow 1 = \chi(1) = \chi(a^{p-1}) = \chi(a)^{p-1}$.
3. $1 = \chi(1) = \chi(a^{-1}a) = \chi(a^{-1})\chi(a) \Rightarrow \chi(a^{-1}) = \chi(a)^{-1}$.
   By (2), $\chi(a) \in \mathbb{C}$ and $|\chi(a)| = 1 \Rightarrow \chi(a)^{-1} = \overline{\chi(a)}$. □

As we move on to Gauss sums, we will want to consider the summation of Dirichlet characters. Thus we present the following proposition as a segue to the next section, where it will prove useful in Proposition 3.7.

Proposition 3.5. [Ir, §8.1.2] Let χ be a Dirichlet character and define ϵ as in Example 3.2. If $\chi \neq \epsilon$, then $\sum_{t\in\mathbb{F}_p} \chi(t) = 0$. If $\chi = \epsilon$, the value of the sum is p.

Proof. The second assertion is clearly true, since $1 + 1 + ... + 1(p\ times) = p$. Now consider when $\chi \neq \epsilon$. Hence, there must exist an $a \in \mathbb{F}_p$ such that $\chi(a) \neq 1$. Then

$$\chi(a)\sum_{t\in\mathbb{F}_p}\chi(t) = \sum_{t\in\mathbb{F}_p}\chi(a)\chi(t) = \sum_{t\in\mathbb{F}_p}\chi(at)$$

If t runs over all elements of $\mathbb{F}_p$, then so does at. Thus,

$$\sum_{t\in\mathbb{F}_p}\chi(at) = \sum_{t\in\mathbb{F}_p}\chi(t)$$

Since $\chi(a)\sum_{t\in\mathbb{F}_p}\chi(t) = \sum_{t\in\mathbb{F}_p}\chi(t)$ and $\chi(a) \neq 1$, $\sum_{t\in\mathbb{F}_p}\chi(t)$ must equal 0. □

3.2 Gauss Sums

We can now define Gauss sums, which we will use a great deal in our later proofs. In this section we present a general definition and prove some fundamental properties, although we will later wish to develop a more specific definition. (Namely, we will want to use the inverse of the power residue symbol we'll raise ζ to a function Tr, which we will define in Section 4.2). To avoid confusion, we will introduce new notation for such a specification. A simple example of this specification is the quadratic Gauss sum, defined in Section 3.3.

Definition 3.6. *Let χ be a Dirichlet character on $\mathbb{F}_p$, and let $a \in \mathbb{F}_p$. The Gauss sum on $\mathbb{F}_p$ belonging to the character χ* is defined by

$$g_a(\chi) = \sum_{n=0}^{p-1}\chi(n)\,\zeta^{an}.$$

Since ζ denotes a primitive root of unity, we know from the definition that we can visualize these sums in the complex plane. In fact, we will prove a striking property about their location in respect to the origin (Lemma 3.8).

Proposition 3.7. [Ir, §8.2.1] *Define ϵ as in Example 3.2.*

1. $a \neq 0$ *and* $\chi \neq \epsilon \Rightarrow g_a(\chi) = \chi(a^{-1})g_1(\chi)$.
2. $a \neq 0$ *and* $\chi = \epsilon \Rightarrow g_a(\epsilon) = 0$.
3. $\chi \neq \epsilon \Rightarrow g_0(\chi) = 0$.
4. $\chi = \epsilon \Rightarrow g_0(\epsilon) = p$.

Proof.

1. $a \neq 0$ and $\chi \neq \epsilon \Rightarrow \chi(a)g_a(\chi) = \chi(a)\sum_t \chi(t)\zeta^{at} = g_1(\chi)$.
2. $a \neq 0$ and $\chi = \epsilon \Rightarrow g_a(\epsilon) = \sum_t \epsilon(t)\zeta^{at} = \sum_t \zeta^{at} = 0$, (by Lemma 4.4.7 in [Ste]).

For the remaining cases, note that $g_0(\chi) = \sum_t \chi(t)\zeta^{0t} = \sum_t \chi(t)$. Hence (3) and (4) are satisfied by Proposition 3.5. □

These basic properties pave the way to some more insightful propositions. For an illustration of the following proposition, we refer the reader to Figure 4 and point out that the Gauss sum (black dot) of all nontrivial characters has distance $\sqrt{5}$ from the origin in the complex plane.

Lemma 3.8. [Ir, Prop 8.2.2] If $\chi \neq \epsilon$, then $|g_1(\chi)| = \sqrt{p}$.

Proof. Proposition 3.7 gives us a way to implicitly compute $|g_a(\chi)|^2$. Going in through the back door, we consider the sum $\sum_a g_a(\chi)\overline{g_a(\chi)}$. We use case (1) of the preceding proposition:

$$\begin{aligned}\overline{g_a(\chi)} &= \overline{\chi(a^{-1})g_1(\chi)} = \chi(a)\overline{g_1(\chi)}.\\ g_a(\chi) &= \chi(a^{-1})g(\chi).\end{aligned}$$

And thus for any $a \in \mathbb{F}_p$, we have

$$g_a(\chi)\overline{g_a(\chi)} = \chi(a^{-1})\chi(a)g_1(\chi)\overline{g_1(\chi)} = |g_1(\chi)|^2.$$

Hence the sum over all $a \in \mathbb{F}_p$ is equal to $(p-1)|g_1(\chi)|^2$.

Alternatively, we could compute the sum directly from the definition. First, we define

$$\delta(x,y) := p^{-1}\sum_t \zeta_p^{t(x-y)}.$$

It is obvious from Proposition 3.5 that

$$\delta(x,y) = \begin{cases} 1 & \text{if } x \equiv y \pmod{p}, \\ 0 & \text{if } x \not\equiv y \pmod{p}. \end{cases}$$

Then we can write

$$\sum_a g_a(\chi)\overline{g_a(\chi)} = \sum_a\sum_x\sum_y \chi(x)\overline{\chi(y)}\zeta^{a(x-y)} = \delta(x,y)p\sum_x\sum_y \chi(x)\overline{\chi(y)} = (p-1)p.$$

Therefore, $p(p-1) = (p-1)|g_1(\chi)|^2 \implies |g_1(\chi)|^2 = p$. □

By itself, the preceding lemma is quite interesting. An analogue for quadratic Gauss sums is needed in the following section, as a step in the proof of Quadratic Reciprocity. But it is useful also for characterizing $g_1(\bar{\chi})$ and $\overline{g_1(\chi)}$ in relation to $g_1(\chi)$. We will see that in conjunction with the following proposition, it enables us to develop a precise expression for $g_1(\chi)g_1(\bar{\chi})$.

Proposition 3.9. [Be, Thm 1.1.4.b.] If $\chi \neq \epsilon$, then $\overline{g_a(\chi)} = \chi(-1)g_a(\bar{\chi})$.

Proof. We show this directly from the definition,

$$\overline{g_a(\chi)} = \overline{\sum_{t=0}^{p-1} \chi(t)\zeta^{at}} = \sum_{t=0}^{p-1} \overline{\chi(t)}\zeta^{-at} = \sum_{t=0}^{p-1} \bar{\chi}(-t)\zeta^{at} = \bar{\chi}(-1)g_a(\bar{\chi}) = \chi(-1)g_a(\bar{\chi}).$$

□

Combining the previous lemma and proposition, we remark that we can equivalently write

$$g_1(\chi)g_1(\bar{\chi}) = \chi(-1)p,$$

which we will reference later on in our proof of the Stickelberger congruence (page 32).

The purpose of the following section is to provide a powerful example using Gauss sums. Although the Law of Quadratic Reciprocity is implied by Eisenstein Reciprocity, we construct an independent proof using only the tools we have formulated so far. In fact there are over 200 proofs of Quadratic Reciprocity in existence (see [Lem] for a reference list), many of which rely on Gauss sums.

3.3 A Proof of Quadratic Reciprocity

In order to prove quadratic reciprocity, it would make sense to consider the Gauss sums composed of Legendre symbols, which we've already shown to be Dirichlet characters. We can go ahead and make this into a formal definition.

Definition 3.10. A *quadratic Gauss sum* is the sum given by

$$g_a = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta^{an}.$$

The following proof follows [Es, Thm 7.3.1], by filling in the details left to the reader. To complete the proof, we must first introduce two lemmas.

Lemma 3.11. [Es, Thm 7.2.1] For the quadratic Gauss sum, g_1, we have

$$g_1^2 = \left(\frac{-1}{p}\right) p.$$

Proof. This is simply a special case of the conclusion drawn from Lemma 3.8 and Proposition 3.9. We take χ to be the Legendre symbol, and note that the quadratic Gauss sum

$$(g_1(\chi))^2 = g_1(\chi)g_1(\bar{\chi}) = \chi(-1)p = \left(\frac{-1}{p}\right) p.$$

□

Lemma 3.12. [Es, Exer 7.2.2] Let p and q be odd primes. Then for the quadratic Gauss sum, g_1, we have

$$g_1^q = \left(\frac{q}{p}\right) g \ (\mathrm{mod}\ q).$$

Proof. First we show that $g_1^q \equiv g_q \pmod q$. From the definition,

$$g_1^q = \left(\sum_{a \bmod p} \left(\frac{a}{p}\right) \zeta^a \right)^q .$$

When expanding the right hand side by the exponent q, the multinomial theorem gives the coefficients for each term in the sum. However, since q is prime it is clear that $q \mid \binom{q}{k_1,k_2,\ldots,k_{p-1}}$ unless some $k_i = q$ and the rest are 0. Hence, we can simplify,

$$\begin{aligned}
g_1^q &\equiv \sum_{a \bmod p} \left[\left(\frac{a}{p}\right)^q \zeta^a q \right] \pmod q \\
&\equiv \sum_{a \bmod p} \left[\left(\frac{a}{p}\right) \left(\frac{a}{p}\right)^{q-1} \zeta^a q \right] \pmod q \\
&\equiv \sum_{a \bmod p} \left[\left(\frac{a}{p}\right) \zeta^a q \right] \pmod q \\
&\equiv g_q \pmod q.
\end{aligned}$$

Now we use Lemma 3.11 to compute g_1^q in a different manner. Recall that $g_1^2 = \left(\frac{-1}{p}\right) p$. We denote this value with a P below.

$$g_1^{q-1} = (g_1^2)^{(q-1)/2} = P^{(q-1)/2} \equiv \left(\frac{P}{q}\right) \pmod q.$$

Multiplying both sides of the congruence by g_1,

$$g_1^q \equiv g_1 \left(\frac{P}{q}\right) \pmod q. \tag{1}$$

Now adjoining our initial claim and applying Proposition 3.7.1, we have

$$g^q = g_q = \left(\frac{q}{p}\right) g_1 \equiv \left(\frac{P}{q}\right) g_1 \ (\mathrm{mod}\ q).$$

Multiplying through the congruence by g_1, and again replacing $g_1^2 = P$, we get

$$\left(\frac{q}{p}\right) P \equiv \left(\frac{P}{q}\right) P \ (\mathrm{mod}\ q).$$

And therefore,

$$\left(\frac{q}{p}\right) \equiv \left(\frac{P}{q}\right) \pmod q.$$

Plugging back into Equation 1, we conclude

$$g_1^q \equiv g_1 \left(\frac{q}{p}\right) \pmod{q}.$$

□

We now proceed with the proof of quadratic reciprocity. Given the result of Lemma 3.12, with q, p and g_1 defined as above, we have

$$g_1^q = \left(\frac{q}{p}\right) g_1 \pmod{q},$$
$$g_1^{q-1} = \left(\frac{q}{p}\right) \pmod{q}.$$

The fact that q is an odd prime implies that $2|(q-1)$. Hence,

$$g_1^{q-1} = (g_1^2)^{(q-1)/2}.$$

By Lemma 3.11,

$$g_1^{q-1} = (g_1^2)^{(q-1)/2} = \left[p\left(\frac{-1}{p}\right)\right]^{(q-1)/2}.$$

Therefore,

$$\left(\frac{q}{p}\right) \equiv \left[p\left(\frac{-1}{p}\right)\right]^{(q-1)/2} \pmod{q}.$$

By putting $a = -1$ into Proposition 1.4, we get $(-1)^{(p-1)/2} = \left(\frac{-1}{p}\right)$. (The equivalence is actually an equality because the Legendre symbol must be ±1). Thus substituting into the above equivalence, we have

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

Also by Proposition 1.4 (now taking $a = p$), we have

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

Once again, the equivalence holds as an equality since the Legendre symbol will be ±1. By symmetry of q and p, we have

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

as desired. □

We leave the proofs of the supplementary laws as an exercise to the reader.

3.4 Jacobi Sums

Jacobi sums naturally arise when we attempt to multiply Gauss sums. Since Gauss sums are not multiplicative, we must find a relation to keep track of the deviation. To do so, we introduce *Jacobi sums.* In particular, Theorem 3.14.4 will reveal a stunning relationship between Jacobi sums and the multiplication of Gauss sums.

For the duration, let $g(\chi)$ denote $g_1(\chi)$.

Definition 3.13. [Ir, §8.3] Let χ and λ be characters of $\mathbb{F}_p$. The *Jacobi sum of* χ *and* λ is defined by

$$J(\chi, \lambda) = \sum_{a+b=1} \chi(a)\lambda(b)$$

The following theorem is useful for determining the values of Jacobi sums.

Theorem 3.14. [Ir, Thm 8.3.1] For χ and λ nontrivial characters and ϵ as before, we have the following relations:

1. $J(\epsilon, \epsilon) = p$.
2. $J(\epsilon, \chi) = 0$.
3. $J(\chi, \chi^{-1}) = -\chi(-1)$.
4. $\lambda\chi \neq \epsilon \implies J(\chi, \lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}$.

Proof.

1. $J(\epsilon, \epsilon) = \sum_{a+b=1} 1 = p$.
2. Is given by the definition in conjunction with Proposition 3.5.
3. Since the function $\varphi : \mathbb{F} - \{1\} \to \mathbb{F} - \{-1\}$ given by $\varphi(a) = \frac{a}{1-a}$ is a bijection, we have

$$\sum_{a} \chi(a)\chi(1-a)^{-1} = \sum_{a\neq 1} \chi(a/(1-a)) = \sum_{b\neq -1} \chi(b) = -\chi(-1).$$

4. We compute the product of the Gauss sums in the same manner as [Le]:

$$g(\chi)g(\lambda) = \sum_{a,b\in\mathbb{F}_p} \chi(a)\lambda(b)\zeta^{a+b} = \sum_{a,c\in\mathbb{F}_p} \chi(a)\lambda(c-a)\zeta^{c},$$

by substituting $b = c - a$. Now we set $a = ct$. Hence, we may split the sum in two:

$$g(\chi)g(\lambda) = \sum_{a,c\neq 0} \chi(a)\lambda(c-a)\zeta^{c} + \sum_{a} \chi(a)\lambda(-a).$$

By part (2), the second sum is 0. We now evaluate the first sum substituting $a = ct$:

$$\begin{aligned}\sum_{a,c\neq 0} \chi(a)\lambda(c-a)\zeta^c &= \sum_{t,c\neq 0} \chi(c)\lambda(c)\zeta^c\chi(t)\lambda(1-t) \\ &= \sum_{c\neq 0} \chi\lambda(c) \cdot \sum_t \chi(t)\lambda(1-t) \\ &= g(\chi\lambda)J(\chi,\lambda),\end{aligned}$$

Hence, for all characters such that $\chi \neq \epsilon, \lambda \neq \epsilon$, and $\chi\lambda \neq \epsilon$, we get the relation:

$$g(\chi)g(\lambda) = g(\chi\lambda)J(\chi,\lambda).$$

□

Corollary. [Wa, Cor 6.3] If χ, λ are characters with orders that divide $m \in \mathbb{N}$, then

$$\frac{g(\chi)g(\lambda)}{g(\chi\lambda)}$$

is an algebraic integer in $\mathbb{Q}(\zeta_m)$.

Proof. Note that by definition, if χ_1, χ_2 have orders dividing m then $J(\chi_1, \chi_2)$ is an algebraic integer in $\mathbb{Q}(\zeta_m)$. So in the case where $\chi_1, \chi_2, \chi_1\chi_2 \neq \epsilon$, this follows as a direct result of the preceding Theorem. If χ_1 or χ_2 is trivial but not $\chi_1\chi_2$, then (letting χ denote the nontrivial character)

$$\frac{g(\chi)g(\epsilon)}{g(\chi\epsilon)} = \frac{g(\chi)}{g(\chi)} = 1.$$

Finally, if $\chi_1\chi_2 = \epsilon$, then

$$\frac{g(\chi_1)g(\chi_2)}{g(\epsilon)} = g(\chi_1)g(\chi_2).$$

□

One thing that is particularly striking about the relationship exposed in Theorem 3.14.4 is that it is recognizable from group cohomology theory, [Mi, eg 1.18.b]. Recall that an extension M of G for an abelian group M is given by the exact sequence

$$1 \to M \to E \xrightarrow{\pi} G \to 1.$$

For $\sigma \in G$ and a section $s : G \to E$ such that the composition $\pi \circ s = \text{id}$. Then we have the relation:

$$s(\sigma)s(\sigma') = \varphi(\sigma,\sigma')s(\sigma\sigma'),$$

where $\varphi(\sigma,\sigma') \in M$ is the difference of $s(\sigma)s(\sigma')$ and $s(\sigma\sigma')$, which both map to $\sigma\sigma' \in G$.

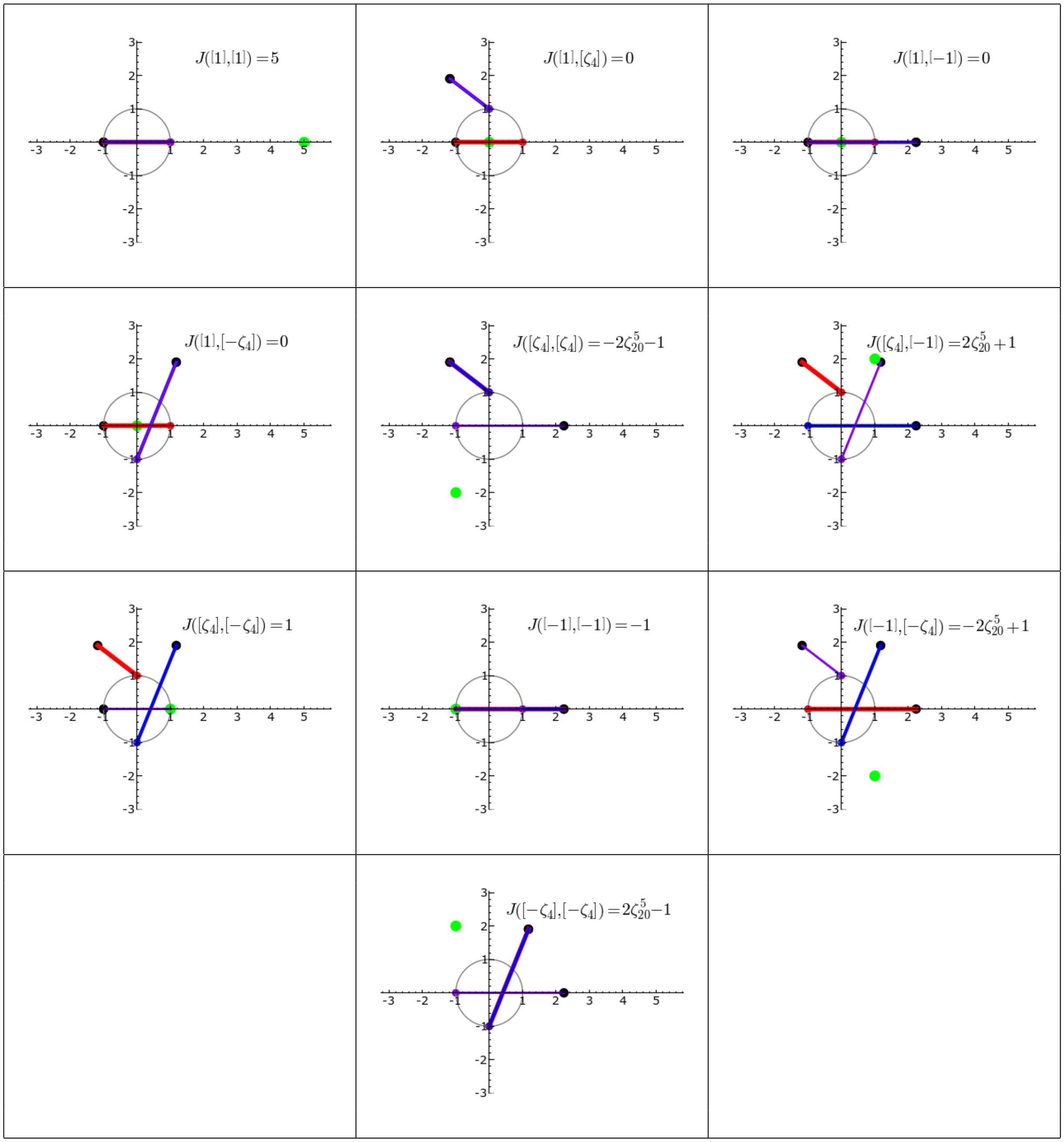
Example 3.15 (Jacobi Sums Implementation)**.** *Theorem 3.14 also lends itself to an easy implementation of Jacobi sums via case analysis. We present a programming example in [Sage]:*

```
def Jacobi_sum(e,f):
    # If they are both trivial, return p
    if e.is_trivial() and f.is_trivial():
        return (e.parent()).order() + 1
    # If they are inverses of each other, return -e(-1)
    g = e*f
    if g.is_trivial():
        return -e(-1)
    # If both are nontrivial, apply mult. formula:
    elif not e.is_trivial() and not f.is_trivial():
        return e.Gauss_sum()*f.Gauss_sum()/g.Gauss_sum()
    # If exactly one is trivial, return 0
    else:
        return 0
```

The implementation given in the previous example allows us to quickly compute the Jacobi sum for many combinations of Dirichlet characters. We can take advantage of this ability to better visualize the relationship between Gauss and Jacobi sums, by plotting several points in the complex plane. Figure 4 is a table of such plots for all pairs of Dirichlet characters in $\mathbb{F}_5$. The Dirichlet characters are drawn in red and blue points on the complex unit circle, connected respectively by red and blue lines to their individual Gauss sums. The product of the characters is drawn in purple, with a line connecting it to the product Gauss sum. The Jacobi sum is drawn as a green point. We remark that there were extensive plotting details in the Sage code used to generate these plots, so it has been omitted from the main text. However, the complete source code is available in Appendix section A-2.

We also remark that these sums of Dirichlet characters are particularly useful for computing the number of solutions to a polynomial with coefficients in a finite field. For a brief exposition, we refer the reader to [Ir, Section 8.4].

Figure 4: Exhaustive Plotting of Jacobi Sums for characters in $\mathbb{F}_5$



$J([1],[1]) = 5$

$J([1],[\zeta_4]) = 0$

$J([1],[-1]) = 0$

$J([1],[-\zeta_4]) = 0$

$J([\zeta_4],[\zeta_4]) = -2\zeta_{20}^5 - 1$

$J([\zeta_4],[-1]) = 2\zeta_{20}^5 + 1$

$J([\zeta_4],[-\zeta_4]) = 1$

$J([-1],[-1]) = -1$

$J([-1],[-\zeta_4]) = -2\zeta_{20}^5 + 1$

$J([-\zeta_4],[-\zeta_4]) = 2\zeta_{20}^5 - 1$

4 The Stickelberger Relation

Similar to our development of Jacobi sums when considering the multiplication of Gauss sums, we will need to develop an understanding of the prime ideal factorization of Gauss sums. To do so, we introduce a relation which is a direct consequence of the *Stickelberger Congruence*. This section is dedicated to proving these major theorems.

4.1 N-adic and $\mathfrak{p}$-adic Valuations

Definition 4.1. A *valuation* $|\cdot|$ on a field K is a function from K to $\mathbb{R}_{\geq 0}$ such that the following three properties hold:

1. $|a| = 0 \iff a = 0$.
2. $|ab| = |a||b|$.
3. $|1 + a| \leq c \iff |a| \leq 1$, for a constant $c \geq 1$.

Furthermore, two valuations $|\cdot|_1$ and $|\cdot|_2$ on a field K are considered *equivalent* if there exists a positive c such that for every $a \in K$, we have $|a|_1 = |a|_2^c$.

It is useful to define the order of a valuation as well. For $|a| = c^m$, we define $\text{ord}(a) = m$ to be the *order* of a. Hence, a translation of the second property in terms of order is given by $\text{ord}(ab) = \text{ord}(a) + \text{ord}(b)$. We will see in Proposition 4.5 that this relation holds in our motivated construction.

For our purposes in particular, we would like to define the N-adic valuation. In order to show the forthcoming definition is well-defined, we first present an existence and uniqueness lemma:

Lemma 4.2. [St, Lemma 16.2.5] Let $N \in \mathbb{N}$. Then for any nonzero $\alpha \in \mathbb{Q}$, there exists a unique $e \in \mathbb{Z}$, and $a, b \in \mathbb{Z}$ with $b > 0$ such that

1. $\alpha = N^e \frac{a}{b}$.
2. $N \nmid a$.
3. $\gcd(a, b) = 1$.
4. $\gcd(N, b) = 1$.

Proof. Let $\alpha = \frac{c}{d}$, where c, d are coprime integers with $d > 0$. Since $\mathbb{Z}$ is a unique factorization domain, there exists a smallest positive integer f such that $N \mid fd$. (Note that $f = 1$ if $N \mid d$). Equivalently, we write $\alpha = \frac{fc}{fd}$.

Then for some $r \in \mathbb{N}$, we have $N^r \mid fd$, but $\gcd(N, \frac{fd}{N^r}) = 1$. We let $s \geq 0$ be the largest power of N that divides fc, i.e., $N^s || fc$. Then clearly, $N \nmid \frac{fc}{N^s}$ and $\gcd(\frac{fc}{N^s}, \frac{fd}{N^r}) = 1$.

Then for $e = s - r,\ a = \frac{fc}{N^s},\ b = \frac{fd}{N^r}$, we have only left to show (1):

$$\alpha = \frac{fc}{fd} = N^{s-r}\frac{fc}{N^s}\frac{N^r}{fd} = N^e\frac{a}{b}.$$

□

Definition 4.3. For $N \in \mathbb{N}$ and any $\alpha \in \mathbb{Q}$, we define the *N-adic valuation* to be

$$\mathrm{ord}_N(\alpha) = \begin{cases} e & \textit{if } \alpha \neq 0 \\ \infty & \textit{if } \alpha = 0, \end{cases}$$

where e is defined as in Lemma 4.2.

It is also of note that in general, a useful classification for valuations is the notion of non-archimedian valuations. A valuation is *non-archimedian* if taking $c = 1$ satisfies (3) in Definition 4.1. If a valuation is not non-archimedian, then it is *Archimedian.* We remark that in general, archimedian valuations can be viewed as an absolute value. (In fact, there is a result proven by Gelfand-Tornheim that any field K with an archimedian valuation $|\cdot|_v$ is isomorphic to a subfield of $\mathbb{C}$, with $|\cdot|_v$ equivalent to the usual absolute value on $\mathbb{C}$). However, the N-adic valuation is non-archimedian, and it is actually defined instead as the logarithm of an absolute value.

As we saw with our generalization from $\mathbb{Z}$ to $\mathcal{O}_K$ for m-th power residues, we wish to expand this idea of order. We can continue to make sense of $\mathrm{ord}_\mathfrak{p}\mathfrak{a}$ as the greatest power of $\mathfrak{p}$ that divides $\mathfrak{a}$, by replacing *divides* with *contains* as we did before. We are using the fact, which is easy to check, that we have a proper containment in the ideal chain

$$\mathfrak{p} \supset \mathfrak{p}^2 \supset \mathfrak{p}^3 \supset \cdots$$

Further, we see that the intersection of all $\mathfrak{p}^n$ is $\{0\}$. Thus for any ideal $\mathfrak{a}$ there exists an $i \in \mathbb{N}$ such that $\mathfrak{a} \subseteq \mathfrak{p}^i$, but $\mathfrak{a} \not\subseteq \mathfrak{p}^{i+1}$. Using this fact, we make a formal definition.

Definition 4.4 (The $\mathfrak{p}$-adic Valuation)**.** [Ir, Def 12.2.8] Let $\mathfrak{p}$ be a prime ideal and $\mathfrak{a}$ an ideal of $\mathcal{O}_K$, for some algebraic number field K. We define $\mathrm{ord}_\mathfrak{p}\mathfrak{a}$ to be the unique nonnegative integer t such that $\mathfrak{a} \subset \mathfrak{p}^t$, but $\mathfrak{a} \not\subset \mathfrak{p}^{t+1}$.

Furthermore, we prove an immediate proposition that relates the ideal case back to the second axiom of valuations.

Proposition 4.5. [Ir, Prop 12.2.9.3] For $\mathfrak{p}, \mathfrak{a}, \mathfrak{b}$ defined as above, $\mathrm{ord}_\mathfrak{p}\mathfrak{a}\mathfrak{b} = \mathrm{ord}_\mathfrak{p}\mathfrak{a} + \mathrm{ord}_\mathfrak{p}\mathfrak{b}$.

Proof. We will use the following two facts [Ir, Prop 12.2.6-7]:

1. If $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ are ideals and $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c}$, then $\mathfrak{b} = \mathfrak{c}$.
2. If $\mathfrak{a}, \mathfrak{b}$ are ideals with $\mathfrak{a} \subset \mathfrak{b}$, then there exists an ideal $\mathfrak{c}$ such that $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$.

We let $t = \mathrm{ord}_\mathfrak{p}\mathfrak{a}$ and $s = \mathrm{ord}_\mathfrak{p}\mathfrak{b}$. Then by (2), we can write

$$\mathfrak{a} = \mathfrak{p}^t\mathfrak{a}_1 \qquad \mathfrak{b} = \mathfrak{p}^s\mathfrak{b}_1.$$

Then by definition, $\mathfrak{a}_1 \not\subset \mathfrak{p}$ and $\mathfrak{b}_1 \not\subset \mathfrak{p}$. Given our notation, we have

$$\mathfrak{a}\mathfrak{b} = \mathfrak{p}^{t+s}\mathfrak{a}_1\mathfrak{b}_1.$$

Now if $\mathfrak{a}\mathfrak{b} \subset \mathfrak{p}^{s+t+1}$, then again by (2), for some ideal $\mathfrak{c}$, we have

$$\mathfrak{a}\mathfrak{b} = \mathfrak{p}^{t+s+1}\mathfrak{c}.$$

Then by (1),

$$\begin{aligned} \mathfrak{a}\mathfrak{b} &= \mathfrak{p}^{s+t}\mathfrak{a}_1\mathfrak{b}_1 = \mathfrak{p}^{s+t}\mathfrak{p}\mathfrak{c} = \mathfrak{p}^{s+t+1}\mathfrak{c} \\ \implies &\qquad \mathfrak{a}_1\mathfrak{b}_1 = \mathfrak{p}\mathfrak{c} \\ \implies &\qquad \mathfrak{a}_1\mathfrak{b}_1 \subset \mathfrak{p}. \end{aligned}$$

Whence $\mathfrak{p}$ prime implies that either $\mathfrak{a}_1 \subset \mathfrak{p}$ or $\mathfrak{b}_1 \subset \mathfrak{p}$, which is a contradiction. Therefore,

$$\operatorname{ord}_{\mathfrak{p}}\mathfrak{a}\mathfrak{b} = t + s = \operatorname{ord}_{\mathfrak{p}}\mathfrak{a} + \operatorname{ord}_{\mathfrak{p}}\mathfrak{b}.$$

□

It will be useful in our proof of the Stickelberger Congruence to know that the $\mathfrak{p}$-adic valuation has the triangle inequality. Since the formulation of this proof is similar to the previous proposition, we will proceed to prove this property immediately.

Proposition 4.6 (The Triangle Inequality)**.** For $\mathfrak{a}, \mathfrak{b}, \mathfrak{p}$ as before, we have

$$\operatorname{ord}_{\mathfrak{p}}(\mathfrak{a} + \mathfrak{b}) \leq \operatorname{ord}_{\mathfrak{p}}\mathfrak{a} + \operatorname{ord}_{\mathfrak{p}}\mathfrak{b}.$$

Proof. Once again, let $t = \operatorname{ord}_{\mathfrak{p}}\mathfrak{a}$ and $s = \operatorname{ord}_{\mathfrak{p}}\mathfrak{b}$. Without loss of generality, we assume that $t \leq s$. As before, we have

$$\mathfrak{a} = \mathfrak{p}^t\mathfrak{a}_1 \qquad \mathfrak{b} = \mathfrak{p}^s\mathfrak{b}_1.$$

And thus,

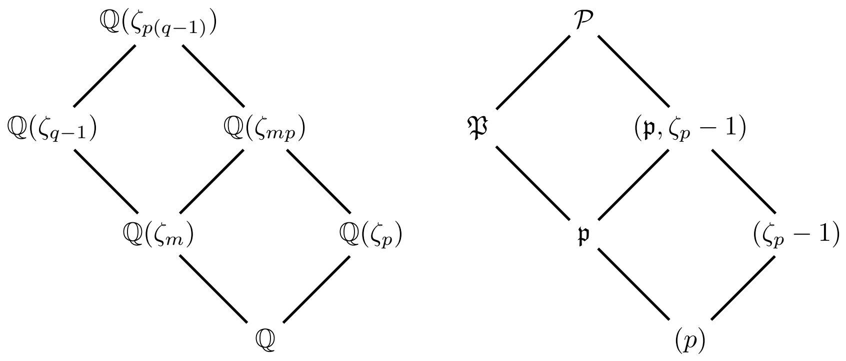
$$\mathfrak{a} + \mathfrak{b} = \mathfrak{p}^t\mathfrak{a}_1 + \mathfrak{p}^s\mathfrak{b}_1 = \mathfrak{p}^t(\mathfrak{a}_1 + \mathfrak{p}^{s-t}\mathfrak{b}_1).$$

Since $\mathfrak{a}_1 \not\subset \mathfrak{p}$, we conclude that $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{a} + \mathfrak{b}) = t < t + s = \operatorname{ord}_{\mathfrak{p}}\mathfrak{a} + \operatorname{ord}_{\mathfrak{p}}\mathfrak{b}$. □

As an example of the $\mathfrak{p}$-adic valuation, we will now introduce the fields and ideals to be used in our forthcoming proofs. After some brief notation introduction, we provide the $\mathfrak{p}$-adic valuation of some of these ideals.

From this point forth, let the following notation hold. Let p be a rational prime and define $\mathfrak{p} = (p)$ the prime ideal above p in $\mathbb{Q}(\zeta_m)$. (In particular, m corresponds to the m-th power residues as before.) So this definition makes sense, we restrict $p \equiv 1 \pmod{m}$. Let $q = p^f = N\mathfrak{p}$. Furthermore, we define $\mathfrak{P}$ a prime ideal above p in $\mathbb{Q}(\zeta_{q-1})$, and $\mathcal{P} = (\mathfrak{P}, \zeta_p - 1)$. These field containments and their corresponding ideals are shown in the Hasse diagram below (Figure 5).

Figure 5: [Le, Fig 11.1] Containment Diagram of Fields



Example 4.7. *[Ir, Lemma 14.4] We leave the following as an exercise to the reader, but remark that the computation is fairly straightforward with some background knowledge of the ramification index in cyclotomic fields. (See [Ir, §13.2]).*

1. $\text{ord}_{\mathcal{P}}(p\mathcal{O}_K) = p - 1$, where $K = Q(\zeta_{p(q-1)})$.
2. $\text{ord}_{\mathcal{P}}(1 - \zeta_p) = 1$.
3. $\text{ord}_{\mathcal{P}}\mathfrak{p} = p - 1$.

4.2 The Stickelberger Congruence

We start by setting up some common notation and definitions. Let p be a prime number and set $q = p^f$, for some fixed $f \in \mathbb{N}$. Given $a \in \mathbb{Z}$, define r by

$$a \equiv r \pmod{q-1},$$

for $0 \leq r \leq q - 1$. We write

$$r = a_0 + a_1 p + \cdots + a_{f-1} p^{f-1},$$

remarking that the existence and uniqueness of $\{a_0, ..., a_{f-1}\}$ is an elementary result derived from repeated application of the division algorithm. We may now define the following two functions, which will be used in the formulation of the Stickelberger Congruence:

$$s(a) := a_0 + a_1 + \cdots + a_{f-1}$$
$$\gamma(a) := a_0! a_1! \cdots a_{f-1}!$$

The next lemma will come in handy when we prove the Stickelberger Congruence. It gives a precise formula for the sum of $s(a)$ over all $a \pmod{q-1}$.

Lemma 4.8. [Ir, Lemma 14.3] Maintaining the above notation,

$$\sum_{a=1}^{q-2} s(a) = \frac{f(p-1)(q-2)}{2}.$$

Proof. We consider the sum $s(a) + s(q-1-a)$ by expanding each of the domain elements. By repeated application of the division algorithm, we find that $q-1 = (p-1)+(p-1)p+\cdots+(p-1)p^{f-1}$. Thus,

$$\begin{aligned} a &= a_0 + a_1 p + \cdots a_{f-1}p^{f-1} \\ \Longrightarrow \qquad q-1-a &= (p-1-a_0) + (p-1-a_1)p + \cdots + (p-1-a_{f-1})p^{f-1}. \end{aligned}$$

Hence, by the definition of $s(a)$,

$$\begin{aligned} s(a) + s(q-1-a) &= a_0 + a_1 + \cdots + a_{f-1} + (p-1-a_0) + (p-1-a_1) + \cdots + (p-1-a_{f-1}) \\ &= \underbrace{(p-1) + (p-1) + \cdots + (p-1)}_{f \text{ times}} \\ &= f(p-1). \end{aligned}$$

Summing both sides of the expression yields

$$2\sum_{a=1}^{q-2} s(a) = \sum_{a=1}^{q-2} s(a) + s(q-1-a) = \sum_{a=1}^{q-2} f(p-1) = f(p-1)(q-2).$$

We conclude that

$$\sum_{a=1}^{q-2} s(a) = \frac{f(p-1)(q-2)}{2}.$$

□

Definition 4.9. For a finite field $\mathbb{F}$ of size p^f, let $\mathrm{Tr} : \mathbb{F} \to \mathbb{Z}/p\mathbb{Z}$ denote the trace of $\alpha \in \mathbb{F}$, given by $\mathrm{Tr}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{f-1}}$.

Notation. As we have seen before, m-th power residues are Dirichlet characters. In order to use the developed machinery of Gauss sums toward the remaining proofs, we make a specific definition. For $\chi = \left(\frac{\cdot}{\mathfrak{p}}\right)_m$, we define *the corresponding Gauss sum of* χ to be

$$G_a(\chi) = \sum_{t\in\mathbb{F}} \chi(t)^{-a}\zeta^{\mathrm{Tr}(at)},$$

The reason for using the inverse will become obvious in the following proof. We also remark that similar to our previous shorthand, $G(\omega) = G_1(\omega)$.

We may now state the following theorem:

Theorem 4.10 (The Stickelberger Congruence)**.** [Le, Thm 11.10] Let $\mathfrak{P}$ be a prime ideal above p in $\mathbb{Q}(\zeta_{q-1})$, and let $\omega = \left(\frac{\cdot}{\mathfrak{P}}\right)^{-1}$. Then

$$\frac{G_a(\omega)}{\pi^{s(a)}} \equiv \frac{1}{\gamma(a)} \ (mod\ \mathcal{P}),$$

for all $a \in \mathbb{N}$, where $\pi = \zeta_p - 1$ and $\mathcal{P} = (\mathfrak{P}, \pi)$.

Lemmermeyer extends this theorem by stating, *"Since $\mathcal{P}||\pi$ and $\gamma(a)$ is a $\mathcal{P}$-adic unit, this implies in particular that $\mathcal{P}^{s(a)}||G_a(\omega^a)$."* This notation means that $s(a)$ is the largest power of $\mathcal{P}$ that divides $G_a(\omega)$. In other words, the Stickelberger Congruence implies that $s(a) = \text{ord}_{\mathcal{P}}(G_a(\omega))$.

We remark that we will continue to use the above notation of ω for the remainder of this paper. Specifically, we define

$$\omega(t) = \left(\frac{\rho}{\mathfrak{P}}\right),$$

for $\rho \in \mathbb{Q}(\zeta_{q-1})$, where $\bar{\rho} = t$.

We now proceed to prove Theorem 4.10. There are several proofs available of the Stickelberger Congruence; for a reference list see [Le, pg 391]. The following proof is originally due to Davenport-Hasse and published in 1934. It is used in the main text of [Ir] to prove the relation given in Theorem 4.13, and [Le, Exer 11.7] provides an outline with the details left as an exercise.

Proof of Theorem 4.10. We define a function $S(a)$ by

$$S(a) = \text{ord}_{\mathcal{P}}(G_a(\omega)),\ 1 \leq a < q.$$

It is then sufficient to show that $S(a) = s(a)$. We begin by proving several claims on $S(a)$:

(i) $S(a) \geq 0$.

Proof. This is obvious, since the $\mathcal{P}$-adic valuation is defined to be a logarithm of an absolute value. □

(ii) $S(a+b) \leq S(a) + S(b)$.

Proof. See Proposition 4.6. □

(iii) $S(a+b) \equiv S(a) + S(b) \pmod{p-1}$. *Proof.* From Corollary 3.14, we have the relation:

$$\beta\ G(\omega^{-(a+b)}) = G(\omega^{-a})G(\omega^{-b}),$$

where β is an algebraic integer in $\mathbb{Q}(\zeta_{q-1})$. Since $\mathcal{P}^{p-1} = \mathfrak{P}\mathbb{Q}(\zeta_{(q-1)p})$, we know that $p-1$ divides $\text{ord}_{\mathcal{P}}(\beta)$. Thus taking the $\mathcal{P}$-adic valuation of both sides yields:

$$S(a+b) \equiv S(a) + S(b) \pmod{p-1}.$$

□

(iv) $S(1) = 1$.

Proof. [Ir, Thm 14.3] We recall the definition of $G_1(\omega)$:

$$G_1(\omega) = \sum_{t \in \mathbb{F}} \omega(t)^{-1} \zeta_p^{\mathrm{Tr}(t)}.$$

We let $\lambda_p = 1 - \zeta_p$ and set $m_i \equiv \mathrm{Tr}(\bar{\zeta}_{q-1}^{i}) \pmod{p}$. We may rewrite our sum,

$$G_1(\omega) = \sum_{i=0}^{q-2} \zeta_{q-1}^{-i} (1 - \lambda_p)^{m_i}.$$

Similar to our multinomial theorem expansion in Lemma 3.12, the coefficients given by the binomial theorem for $(1 - \lambda_p)^{m_i}$ will vanish mod $\mathcal{P}^2$ except for

$$(1 - \lambda_p)^{m_i} \equiv 1 - m_i \lambda_p \pmod{\mathcal{P}^2}.$$

Hence, we can write

$$G_1(\omega) \equiv -\left(\sum_{i=0}^{q-2} m_i \zeta_{q-1}^{-i} \right) \lambda_p \pmod{\mathcal{P}^2}.$$

Since $m_i \equiv \zeta_{q-1}^{i} + \zeta_{q-1}^{pi} + \cdots + \zeta_{q-1}^{ip^{f-1}} \pmod{\mathcal{P}^2}$, we get

$$G_1(\omega) \equiv -\sum_{i=0}^{q-2} \zeta_{q-1}^{-i} \left(\zeta_{q-1}^{i} + \zeta_{q-1}^{pi} + \cdots + \zeta_{q-1}^{ip^{f-1}} \right) \lambda_p \pmod{\mathcal{P}^2}.$$

We notice immediately above that the sums $\sum_{i=0}^{q-2} \sum_{j=1}^{f-1} \zeta_{q-1}^{ip^j - i}$ cancel, while for $j = 0$, we have

$$\sum_{i=0}^{q-2} \zeta_{q-1}^{i-i} = \sum_{i=0}^{q-2} = q - 1.$$

Hence,

$$G_1(\omega) \equiv -(q-1)\lambda_p \pmod{\mathcal{P}^2}.$$

Since $q \equiv 0 \pmod{\mathcal{P}^2}$, we have

$$G_1(\omega) \equiv \lambda_p \pmod{\mathcal{P}^2}.$$

By Example 4.7.2, we know $\lambda_p \in \mathcal{P}$ but $\lambda_p \notin \mathcal{P}^2$. And thus we can conclude that

$$S(1) = \mathrm{ord}(G_1(\omega)) = 1.$$

□

(v) $S(ap) = S(a)$.

Proof. We show that $G(\omega^{ap}) = G(\omega^a)$, in which case the result holds by taking the valuation of both sides. Since $(t^p)^{p^{f-1}} = t^{p^f} = t \in \mathbb{Z}/p\mathbb{Z}$ and all the other terms cancel, we conclude that $\mathrm{Tr}(t) = \mathrm{Tr}(t^p)$. Hence,

$$G(\omega^{ap}) = \sum_t \omega(t)^{-ap}\zeta_p^{\mathrm{Tr}(t)} = \sum_t \omega(t^p)^{-a}\zeta_p^{\mathrm{Tr}(t^p)} = G(\omega^a).$$

□

(vi) $\sum_{a \bmod q-1} S(a) = \frac{f(p-1)(q-1)}{2}$.

Proof. Recall the conclusion drawn from Lemma 3.8 and Proposition 3.9,

$$g(\chi)g(\bar{\chi}) = \chi(-1)q,$$

for χ a character in $\mathbb{F}_q$. Applied to our situation, this relation is given by

$$G_a(\omega)G_{q-1-a}(\omega) = \omega(-1)^a q = \omega(-1)^a p^f.$$

Since $\mathrm{ord}_{\mathcal{P}}(p) = p-1$, we conclude

$$S(a) + S(q-1-a) = f(p-1),$$

by taking the valuation of both sides. Furthermore, the above equation should seem familiar. To complete the proof, we sum over both sides as in Lemma 4.8. □

Now, from (iii) and (iv) we get

$$\begin{aligned} S(a) &= S((a-1)+1) \\ &\equiv S(a-1) + S(1) \pmod{p-1} \\ &\equiv S(a-1) + 1 \pmod{p-1} \\ &\equiv S(a-1) + 2 \pmod{p-1} \\ &\vdots \\ &\equiv S(0) + a \pmod{p-1}. \end{aligned}$$

Hence by (i), $S(0) \geq 0 \implies S(a) \geq a$, for $0 \leq a < p-1$.

To show that $S(a) \leq a$, we apply (ii) and then (iv):

$$\begin{aligned} S(a) &= S(\underbrace{1+1+\cdots+1}_{a \text{ times}}) \\ &\leq \underbrace{S(1)+S(1)+\cdots+S(1)}_{a \text{ times}} \\ &\leq \underbrace{1+1+\cdots+1}_{a \text{ times}} \\ &\leq a. \end{aligned}$$

Thus we conclude that $S(a) = a$, for $0 \leq a < p-1$.

Now we take $a = a_0 + a_1 p + \cdots + a_{f-1}p^{f-1}$. Hence (ii) gives the inequality:

$$\begin{aligned} S(a) &= S(a_0 + a_1 p + \cdots + a_{f-1}p^{f-1}) \\ &\leq S(a_0) + S(a_1 p) + \cdots + S(a_{f-1}p^{f-1}). \end{aligned}$$

Hence (v) implies that

$$S(a) \leq S(a_0) + S(a_1) + \cdots + S(a_{f-1}).$$

Since we have shown that $S(a) = a$, we conclude that

$$S(a) \leq a_0 + a_1 + \cdots + a_{f-1} = s(a).$$

Finally, (vi) implies

$$\sum_{a \pmod{q-1}} S(a) = \frac{f(p-1)(q-1)}{2} = \sum_{a \pmod{q-1}} s(a),$$

by Lemma 4.8. Therefore, $S(a) = s(a)$. $\square$

Corollary. [Ir, Cor 14.3] $\operatorname{ord}_{\mathfrak{p}}(G(\omega)^m) = \frac{m}{p-1} s(\frac{q-1}{m})$.

Proof. By Example 4.7.3,

$$(p-1) \operatorname{ord}_{\mathfrak{p}}(G(\omega)^m) = \operatorname{ord}_{\mathcal{P}}(G(\omega)^m) = m \operatorname{ord}_{\mathcal{P}}(G(\omega)).$$

Now since $G(\omega) = G_a(\omega)$ with $a = (q-1)/m$, we have

$$(p-1) \operatorname{ord}_{\mathfrak{p}}(G(\omega)^m) = m \; s\left(\frac{q-1}{m}\right).$$

$\square$

The following lemma will give the full prime ideal decomposition of $G(\omega)^m$. Continuing from the corollary above, we consider all prime ideals in $\mathbb{Q}(\zeta_m)$ that contain $G(\omega)^m$. Since we have shown $|G(\omega)|^2 = q$, we can conclude

$$|G(\omega)^m|^2 = q^m = p^{fm}.$$

Therefore, the prime ideals in $\mathbb{Q}(\zeta_m)$ that contain $G(\omega)^m$ are those that contain p. Further, if $\mathfrak{q}$ is another prime ideal in $\mathbb{Q}(\zeta_m)$ that contains p, then there exists an automorphism $\sigma \in \operatorname{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ that maps $\mathfrak{p}$ to $\mathfrak{q}$. For t mod m, we denote $\mathfrak{p}^{\sigma_t^{-1}}$ by $\mathfrak{p}_t$.

Lemma 4.11. [Ir, Lemma 14.8] $\mathrm{ord}_{\mathfrak{p}_t}(G(\omega)^m) = \frac{m}{p-1}\ s\left(\frac{t(q-1)}{m}\right)$.

Proof. We let $r \in \mathbb{Z}$ such that $r \equiv t \pmod m$ and $r \equiv 1 \pmod p$. Then from direct computation,

$$G(\omega)^{\sigma_r} = \left(\sum_{i=0}^{q-1} \left(\frac{i}{\mathfrak{p}}\right)_m \zeta_m^{\mathrm{Tr}(i)}\right)^{\sigma_r} = \sum_{i=0}^{q-1} \left(\frac{i}{\mathfrak{p}}\right)_m \zeta_m^{\mathrm{Tr}(i)} = G_a(\omega),$$

where $a = \frac{t(q-1)}{m}$. Then it follows that

$$(G(\omega)^m)^{\sigma_t} = G_a(\omega)^m.$$

Now, observing that $\mathrm{ord}_{\mathfrak{p}_t}(G(\omega)^m) = \mathrm{ord}_{\mathfrak{p}}((G(\omega)^m)^{\sigma_t})$, we can make the remaining conclusions as in Corollary 4.2. □

4.3 The Stickelberger Relation

We can now state and prove the Stickelberger Relation, which will in turn take on a pivotal step in our proof of Eisenstein Reciprocity. In fact, most of the work has already been done by proving the Stickelberger Congruence in the preceding section. In this section we will merely give an expression for the prime decomposition of $\mathfrak{p}$, in terms of the Stickelberger element θ, which we define immediately.

Definition 4.12. For the remainder of this section, let $\theta := \sum \left\langle \frac{t}{m} \right\rangle \sigma_t^{-1}$, where $\langle x \rangle$ denotes the fractional part of x, and the sum is taken over all t such that $(t, m) = 1$ and $0 < t < m$.

Notation. For the remainder of this section, we let $\Gamma = \mathrm{Gal}(\mathbb{Q}(\zeta_{p(q-1)})/\mathbb{Q})$. Further, we let $Z = \{1, \sigma_p, ..., \sigma_p^{p^{f-1}}\}$ denote the decomposition group of $\mathfrak{p}$. Observe that we are implicitly recalling the elementary fact from Galois theory that Z is a cyclic group with generator σ_p. We remark that the Stickelberger element θ is in $\mathbb{Q}[Z]$.

Theorem 4.13 (The Stickelberger Relation)**.** [Le, Thm 11.12] For $m \in \mathbb{N}$, let $p \nmid m$ be prime, $\mathfrak{p}$ a prime ideal above p in $\mathbb{Q}(\zeta_m)$, and let $q = p^f = N\mathfrak{p}$ be the absolute norm of $\mathfrak{p}$. Then $\chi = \left(\frac{\cdot}{\mathfrak{p}}\right)_m^{-1}$ is a Dirichlet character of order m on $\mathbb{F}_q$, such that the corresponding Gauss sum $G(\chi)$ has the factorization

$$G(\chi)^m = \mathfrak{p}^{m\theta}.$$

Before presenting a proof, we consider the following example. Lemmermeyer provides a table of factorizations for Gauss sums $G(\chi)^m$ as we've defined over $\mathbb{F}_p$, with $p \equiv 1 \pmod m$. We've included this table as the following example, since it assists in the comprehension of Theorem 4.13. By our notation, $\mathfrak{p}_i$ denotes $\mathfrak{p}^{\sigma_i}$, with $\mathfrak{p}_1 = \mathfrak{p}$.

Example 4.14. [Le, §11.1]

m	$G(\chi^{-1})^m$	$G(\chi)^m$	$J(\chi,\chi)$
2	$\mathfrak{p}$	$\mathfrak{p}$	
3	$\mathfrak{p}_1\mathfrak{p}_2^2$	$\mathfrak{p}_1^2\mathfrak{p}_2$	$\mathfrak{p}_1$
4	$\mathfrak{p}_1\mathfrak{p}_3^3$	$\mathfrak{p}_1^3\mathfrak{p}_3$	$\mathfrak{p}_1$
5	$\mathfrak{p}_1\mathfrak{p}_2^3\mathfrak{p}_3^2\mathfrak{p}_4^4$	$\mathfrak{p}_1^4\mathfrak{p}_2^2\mathfrak{p}_3^3\mathfrak{p}_4$	$\mathfrak{p}_1\mathfrak{p}_3$
7	$\mathfrak{p}_1\mathfrak{p}_2^4\mathfrak{p}_3^5\mathfrak{p}_4^2\mathfrak{p}_5^3\mathfrak{p}_6^6$	$\mathfrak{p}_1^6\mathfrak{p}_2^3\mathfrak{p}_3^2\mathfrak{p}_4^5\mathfrak{p}_5^4\mathfrak{p}_6$	$\mathfrak{p}_1\mathfrak{p}_4\mathfrak{p}_5$
8	$\mathfrak{p}_1\mathfrak{p}_3^3\mathfrak{p}_5^5\mathfrak{p}_7^7$	$\mathfrak{p}_1^7\mathfrak{p}_3^5\mathfrak{p}_5^3\mathfrak{p}_7$	$\mathfrak{p}_1\mathfrak{p}_5$

Proof of Theorem 4.13. [Ir, §14.4] Lemma 4.11 gives the prime decomposition of $G(\omega)^m$,

$$\mathfrak{p}^{\pi'}, \text{ where } \rho = \frac{m}{p-1} \sum_{\sigma_{t_i} \in \Gamma/Z} s\left(\frac{t_i(q-1)}{m}\right) \sigma_{t_i}^{-1}.$$

To complete the proof, we will have to find another interpretation of $s(a)$. We follow [Le, Thm 11.12], and compute $s(a)$ by first characterizing the set of congruences:

$$\begin{aligned} a &= a_0 + a_1 p + \cdots + a_{f-1}p^{f-1} \\ ap &\equiv a_{f-1} + a_0 p + \cdots + a_{f-2}p^{f-1} \pmod{q-1} \\ &\vdots \\ ap^{f-1} &\equiv a_1 + a_2 p + \cdots + a_0 p^{f-1} \pmod{q-1}. \end{aligned}$$

And hence we have an expression for the i-th congruence,

$$ap^i = (q-1)\left\langle \frac{ap^{i-1}}{q-1} \right\rangle.$$

Taking the sum, we can include $s(a)$ implicitly

$$\sum_{i=0}^{f-1} \left\langle \frac{ap^i}{q-1} \right\rangle = s(a)\frac{1+p+\cdots+p^{f-1}}{q-1} = \frac{s(a)}{p-1}.$$

Solving for $s(a)$, we have found our desired interpretation:

$$s(a) = (p-1)\sum_{i=0}^{f-1} \left\langle \frac{ap^i}{q-1} \right\rangle.$$

We write

$$\pi' = \frac{m}{p-1} \sum_{\sigma_{t_i} \in \Gamma/Z} (p-1) \sum_{j=0}^{f-1} \left\langle \frac{t_i(q-1)}{m} \cdot \frac{p^j}{q-1} \right\rangle \sigma_{t_i}^{-1} = m \sum_{\sigma_{t_i} \in \Gamma/Z} \sum_{j=0}^{f-1} \left\langle \frac{t_i p^j}{m} \right\rangle \sigma_{t_i}^{-1}.$$

However, we can instead consider

$$\pi = m \sum_{\sigma_{t_i} \in \Gamma/Z} \sum_{j=0}^{f-1} \left\langle \frac{t_i p^j}{m} \right\rangle \sigma_{t_i}^{-1} \sigma_{p^j}^{-1},$$

since π and π' are equivalent on $\mathfrak{p}$, because σ_p fixes $\mathfrak{p}$. Reducing π, we find

$$\begin{aligned}\pi &= m \sum_{t \bmod m} \left\langle \frac{t}{m} \right\rangle \sigma_t^{-1} \\ &= m\theta.\end{aligned}$$

□

5 A Classic Proof of Eisenstein Reciprocity

We now have the background material necessary to prove the Eisenstein Reciprocity Law. We point out that [Ir], [Le], [Be], and [Es] have all used similar techniques to prove the preliminary results. However, they diverge here. [Es] omits the proof and [Be] gives it as a corollary of a more general result (which they also call Eisenstein Reciprocity, although it is initially due to Kummer). However, [Ir] and [Le] use nearly identical proofs, although [Le] initially restricts p to be congruent to 1 (mod m), and must make up for that later. Despite the differences in the texts, the presentation by [Ir] and [Le] seem the most natural as a generalization of cubic and quadratic reciprocity laws, (see [Le, Second Proof of Cubic Reciprocity] for a proof due to Eisenstein).

Essentially, we will chip away at an initial reciprocity relation stated below. The pivotal point of the proof comes when we apply Stickelberger's relation in 2, and we can express this result in terms of the generator of a principal ideal.

We will use notation consistent with the previous sections. In particular, recall that for the character $\chi = \left(\frac{\cdot}{\mathfrak{p}}\right)_m$, we have the corresponding Gauss sum

$$G_a(\chi) = \sum_{t \in \mathbb{F}} \chi(t)^{-a} \zeta^{\mathrm{Tr}(at)},$$

and set $G(\chi) = G_1(\chi)$.

Lemma 5.1. [Ir, Prop 14.5.3] Let $\mathfrak{p}$,$\mathfrak{q} \subset \mathbb{Q}(\zeta_m)$ be prime ideals prime to m, such that $N\mathfrak{p}$ and $N\mathfrak{q}$ are coprime. Let $\chi = \left(\frac{\cdot}{\mathfrak{p}}\right)^{-1}$. Then

$$\left(\frac{G(\chi)^m}{\mathfrak{q}}\right)_m = \left(\frac{N\mathfrak{q}}{\mathfrak{p}}\right)_m.$$

Proof. We consider the prime ideals $\mathfrak{p}$ and $\mathfrak{q}$. Let $N\mathfrak{q} = q^f$ be the absolute norm of $\mathfrak{q}$. We recall that by decomposition in cyclotomic fields, $q^f \equiv 1 \pmod{m}$. Hence, we have the following congruences:

$$\begin{aligned} G(\chi)^{q^f} &\equiv \sum_t \left(\frac{t}{\mathfrak{p}}\right)^{q^f} \zeta_m^{tq^f} \pmod{q} \\ &\equiv \sum_t \left(\frac{t}{\mathfrak{p}}\right) \zeta_m^{tq^f} \pmod{q} \\ &\equiv \left(\frac{q^f}{\mathfrak{p}}\right)_m G(\chi) \pmod{q} \\ &\equiv \left(\frac{N\mathfrak{q}}{\mathfrak{p}}\right)_m G(\chi) \pmod{q} \\ \implies \qquad G(\chi)^{q^f-1} &\equiv \left(\frac{N\mathfrak{q}}{\mathfrak{p}}\right)_m \pmod{q}. \end{aligned}$$

Alternatively,

$$G(\chi)^{q^f-1} = (G(\chi)^m)^{(q^f-1)/m} \equiv \left(\frac{G(\chi)^m}{\mathfrak{q}}\right)_m \pmod{\mathfrak{q}}.$$

Therefore, by combining these expressions we get

$$\left(\frac{G(\chi)^m}{\mathfrak{q}}\right)_m \equiv \left(\frac{N\mathfrak{q}}{\mathfrak{p}}\right)_m \pmod{\mathfrak{q}}.$$

Since $m \notin \mathfrak{q}$, we see that this congruence is actually an equality. □

We extend this proof to all ideals $\mathfrak{a}, \mathfrak{b}$ prime to m, by prime ideal decomposition and the usual multiplication of power residue symbols. Introducing some notation, we let $\Phi(\mathfrak{p}) = G(\chi_{\mathfrak{p}})^m$, where $\chi_{\mathfrak{p}} = \left(\frac{\cdot}{\mathfrak{p}}\right)_m^{-1}$. Then

$$\Phi(\mathfrak{a}) = \Phi(\mathfrak{p}_1)\Phi(\mathfrak{p}_2)\cdots\Phi(\mathfrak{p}_n),$$

for $\mathfrak{p}_1\mathfrak{p}_2...\mathfrak{p}_n$ the prime ideal factorization of $\mathfrak{a}$. We then have automatically,

Corollary (1)**.** [Ir, Cor 14.5.3.1] Let $\mathfrak{a}$,$\mathfrak{b} \subset \mathbb{Q}(\zeta_m)$ be ideals prime to m, such that $N\mathfrak{a}$ and $N\mathfrak{b}$ are coprime. Then

$$\left(\frac{N\mathfrak{b}}{\mathfrak{a}}\right)_m = \left(\frac{\Phi(\mathfrak{a})}{\mathfrak{b}}\right)_m.$$

We continue to develop this proposition with another corollary, this time considering the principal ideal $\mathfrak{a} = (\alpha)$. Before stating the corollary, we claim that for a principal ideal $\mathfrak{a} = (\alpha)$, there exists a unit element $\epsilon(\alpha) \in \mathbb{Q}(\zeta_m)$ such that

$$\Phi(\mathfrak{a}) = \epsilon(\alpha)\alpha^{m\theta}, \tag{2}$$

where θ is the Stickelberger element (Def 4.12). As evidence of this claim, we consider $(\Phi(\alpha)) = (\alpha)^{m\theta} = (\alpha^{m\theta})$, where $(\Phi(\mathfrak{a})) = \mathfrak{a}^{m\theta}$ is given by Theorem 4.13. We can now prove,

Corollary (2)**.** [Ir, Cor 14.5.3.2] Let $\mathfrak{a}, \mathfrak{b}$ be defined as above with $\mathfrak{a}$ a principal ideal generated by α. Then

$$\left(\frac{\epsilon(\alpha)}{\mathfrak{b}}\right)_m \left(\frac{\alpha}{N\mathfrak{b}}\right)_m = \left(\frac{N\mathfrak{b}}{\alpha}\right)_m,$$

where $\epsilon(\alpha)$ is a unit in $\mathbb{Q}(\zeta_m)$.

Proof. By our claim and the multiplicativity the power residue symbol, we have

$$\left(\frac{\Phi(\alpha)}{\mathfrak{b}}\right)_m = \left(\frac{\epsilon(\alpha)}{\mathfrak{b}}\right)_m \left(\frac{\alpha^{m\theta}}{\mathfrak{b}}\right)_m.$$

Then we have

$$\left(\frac{\alpha^{t\sigma_t^{-1}}}{\mathfrak{b}}\right)_m = \left(\frac{\alpha^{\sigma_t^{-1}}}{\mathfrak{b}}\right)_m^t = \left(\frac{\alpha^{\sigma_t^{-1}}}{\mathfrak{b}}\right)_m^{\sigma_t} = \left(\frac{\alpha}{\mathfrak{b}^{\sigma_t}}\right)_m,$$

since $(\alpha/\mathfrak{b})_m^\sigma = (\alpha^\sigma/\mathfrak{b}^\sigma)_m$. It then follows that

$$\left(\frac{\alpha^{m\theta}}{\mathfrak{b}}\right)_m = \prod_t \left(\frac{\alpha^{t\sigma_t^{-1}}}{\mathfrak{b}}\right)_m = \prod_t \left(\frac{\alpha}{\mathfrak{b}^{\sigma_t}}\right)_m = \left(\frac{\alpha}{N\mathfrak{b}}\right)_m.$$

Plugging this value back into our initial equation and using the result of Corollary (1), we have

$$\left(\frac{N\mathfrak{b}}{\alpha}\right)_m = \left(\frac{\Phi(\alpha)}{\mathfrak{b}}\right)_m = \left(\frac{\epsilon(\alpha)}{\mathfrak{b}}\right)_m \left(\frac{\alpha}{N\mathfrak{b}}\right)_m.$$

□

Henceforth, we let $m = \ell$ be an odd prime. By the above corollary, we deduce that the formula

$$\left(\frac{\alpha}{N\mathfrak{b}}\right)_\ell = \left(\frac{N\mathfrak{b}}{\alpha}\right)_\ell$$

is true if $\left(\frac{\epsilon(\alpha)}{\mathfrak{b}}\right)_\ell = 1$. With this notion in mind, we present the following lemma.

Lemma 5.2. [Le, Lemma 11.8] Let $\epsilon(\alpha)$ be defined as above. Then $\epsilon(\alpha)$ is a root of unity. Further, if α is primary and $m = l$ is an odd prime, then $\epsilon(\alpha) = \pm 1$.

Proof. Lemmermeyer cites a result due to Kronecker that the algebraic integers $\beta \in \mathbb{Q}(\zeta_m)$ with the property that $|\beta^\sigma| = 1$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ are roots of unity. Because $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is abelian, $|\epsilon(\alpha)| = 1$ implies $|\epsilon(\alpha)^\sigma| = 1$, for all σ. Hence we only need to show that $|\epsilon(\alpha)| = 1$.

We let σ_{-1} denote complex conjugation, (i.e., $\sigma_{-1} : \zeta_\ell \mapsto \zeta_\ell^{-1} = \overline{\zeta_\ell}$). Then we derive,

$$\begin{aligned} m\theta(1+\sigma_{-1}) &= \sum_t (t\sigma_t^{-1} + \sum_t t\sigma_t^{-1}\sigma_{-1} \\ &= \sum_t (t\sigma_t^{-1} + \sum_t t\sigma_{-t}^{-1} \\ &= \sum_t (t\sigma_t^{-1} + \sum_t (m-t)\sigma_{m-t}^{-1} \\ &= m\sum_t \sigma_t^{-1}. \end{aligned}$$

We have,

$$|N(\alpha)|^m = |\alpha^{m\theta}|^2 = \alpha^{m\theta(1+\sigma_{-1})} = \alpha^{m\sum \sigma_t^{-1}}.$$

Therefore,

$$N(\alpha) = \alpha^{\sum \sigma_t^{-1}} \implies |\epsilon(\alpha)| = 1.$$

We conclude that $\epsilon(\alpha)$ is a root of unity in $\mathbb{Q}(\zeta_\ell)$. We will use this fact in the second part of our proof, by letting $\epsilon(\alpha) = \zeta_\ell^i$, for some $i \in \mathbb{Z}$.

We now show that $\epsilon(\alpha) = \pm 1$, [Ir, Lemma 14.6]. We will need the assumption that α is primary, (i.e., $\alpha \equiv z \pmod{L^2}$, for $L = (1 - \zeta_\ell$ and $z \in \mathbb{Z}$). Since $L^\sigma = L$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ where $\mathbb{Q}(\zeta_\ell) \subset K$, we have

$$\alpha^\sigma \equiv z^{m\theta} \equiv z^{1+2+\cdots+(\ell-1)} \pmod{L^2}.$$

Then $z^{(\ell-1)/2} \equiv \pm 1 \pmod{\ell}$ implies that

$$\alpha^{m\theta} \equiv (\pm 1)^\ell \equiv \pm 1 \pmod{L^2}.$$

Hence we conclude that

$$\epsilon(\alpha) = \pm\zeta_\ell^i \equiv \pm 1 \pmod{L^2}.$$

We write $\zeta_\ell = 1 - L$ and the above congruence implies that

$$\begin{aligned} 1 - Li &\equiv \pm 1 \pmod{L^2} \\ 1 - Li &\equiv 1 \pmod{L^2} \qquad\qquad (*) \\ -Li &\equiv 0 \pmod{L^2} \\ \implies \quad L &\mid i \\ \implies \quad \ell &\mid i. \end{aligned}$$

We note that $(*)$ above holds because if $1 - Li \equiv -1 \pmod{L^2}$, then $L \mid 2$. Now, since $\ell \mid i$ and $\epsilon(\alpha) = \pm\zeta_\ell^i$, we conclude that $\epsilon(\alpha) = \pm 1$. □

Lemma 5.3. [Ir, Prop 14.5.4] Let $\alpha \in \mathbb{Q}(\zeta_\ell)$ be a primary element, and $\mathfrak{b} \subset \mathbb{Q}(\zeta_\ell)$ an ideal with $\ell \notin \mathfrak{b}$, with $N\mathfrak{b}$ prime to α. Then

$$\left(\frac{\alpha}{N\mathfrak{b}}\right)_\ell = \left(\frac{N\mathfrak{b}}{\alpha}\right)_\ell.$$

Proof. As we mentioned above, all that is left to show is that $\left(\frac{\epsilon(\alpha)}{\mathfrak{b}}\right)_\ell = 1$. By the previous lemma, we have that $\epsilon(\alpha) = \pm 1$. Since ℓ is odd, we know that a solution $x = \pm 1$ exists such that $x^\ell \equiv 1 \pmod{\mathfrak{b}}$. Hence by definition, $\left(\frac{\epsilon(\alpha)}{\mathfrak{b}}\right)_\ell = 1$. □

We can now conclude the Law of Eisenstein Reciprocity, by making a substitution into the previous lemma. We take $p \in Z$ prime such that $(p, \alpha) = 1$ and $p \neq \ell$. We let $\mathfrak{p}$ be a prime ideal above p in $\mathcal{O}_K$, for K some algebraic number field containing $\mathbb{Q}(\zeta_\ell)$. We denote the absolute norm of $\mathfrak{p}$ by $N\mathfrak{p} = p^f$. Substituting $\mathfrak{b} = \mathfrak{p}$ in the preceding lemma, we have

$$\left(\frac{\alpha}{p}\right)_\ell^f = \left(\frac{p}{\alpha}\right)_\ell^f.$$

Then since $f \mid [\mathbb{Q}(\zeta_\ell) : \mathbb{Q}] = (\ell - 1)$, we know that f and ℓ are coprime. Hence

$$\left(\frac{\alpha}{p}\right)_\ell = \left(\frac{p}{\alpha}\right)_\ell.$$

Finally, we have shown that for all $\beta \in \mathbb{Z}$ prime to ℓ and α and α primary,

$$\left(\frac{\alpha}{\beta}\right)_\ell = \left(\frac{\beta}{\alpha}\right)_\ell.$$

□

Proof of Supplementary Laws. [Le, Thm 11.9]

(i) $\left(\frac{\zeta}{a}\right)_\ell = \zeta^{(a^{\ell-1}-1)/\ell}$.

First, we show this equality for $a = p$ an odd prime. We let $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_g$. Then

$$\left(\frac{\zeta}{p}\right)_\ell = \prod_{j=1}^{g} \left(\frac{\zeta}{\mathfrak{p}_j}\right)_\ell = \prod_{j=1}^{g} \zeta^{(p^f-1)/\ell} = \zeta^{g\frac{p^f-1}{\ell}}.$$

The claim clearly holds for $a = p$, since

$$\frac{p^{fg}-1}{\ell} = \frac{p^f-1}{\ell} \cdot (p^{f(g-1)} + \cdots + p^f + 1) \equiv g \cdot \frac{p^f-1}{\ell} \pmod{\ell}.$$

To generalize to all a, we use induction on m, n dividing a (and subsequently the factors of m, n until full prime decomposition is achieved). The induction step is as follows:

$$\frac{(mn)^{\ell-1}-1}{\ell} = \frac{m^{\ell-1}-1}{\ell} \cdot n^{\ell-1} + \frac{n^{\ell-1}-1}{\ell} \equiv \frac{m^{\ell-1}-1}{\ell} + \frac{n^{\ell-1}-1}{\ell} \pmod{\ell}.$$

(ii) $\left(\frac{1-\zeta}{a}\right)_\ell = \left(\frac{\zeta}{a}\right)_\ell^{(\ell-1)/2}$.

We apply (i) to get

$$\left(\frac{1-\zeta}{a}\right)_\ell = (1-\zeta)^{(a^{\ell-1}-1)/2}.$$

We claim that $\left(\frac{\beta}{b}\right)_\ell = 1$ if (β, b) =1 and $\beta \in \mathbb{Z}[\zeta_\ell + \zeta_\ell^{-1}]$ is real-valued. Whence we can factor $\zeta^{-1}(1-\zeta)^2 \in \mathbb{R}$ from the right hand side in the above equation to get

$$\left(\frac{1-\zeta}{a}\right)_\ell = \zeta^{(\ell-1)(a^{\ell-1}-1)/2\ell} = \left(\zeta^{(a^{\ell-1}-1)/\ell}\right)^{(\ell-1)/2}.$$

Again applying (i), we have

$$\left(\frac{1-\zeta}{a}\right)_\ell = \left(\frac{\zeta}{a}\right)_\ell^{(\ell-1)/2}.$$

To prove our claim, we let $G = \mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q})$, and we let $H = \langle \tau \rangle$ be the subgroup generated by complex conjugation. Then since H is of order 2, we have

$$\left(\frac{\beta}{\mathfrak{p}^\tau}\right)_\ell = \left(\frac{\beta^\tau}{\mathfrak{p}^\tau}\right)_\ell = \left(\frac{\beta}{\mathfrak{p}}\right)_\ell^\tau = \left(\frac{\beta}{\mathfrak{p}}\right)_\ell^{-1}.$$

And hence,

$$\left(\frac{\beta}{p}\right)_\ell = \prod_{\sigma \in G/H} \left(\frac{\beta}{\mathfrak{p}^\sigma \mathfrak{p}^{\sigma\tau}}\right)_\ell = 1.$$

□

6 Further Readings

We conclude this thesis by discussing the connections of Eisenstein Reciprocity to some more advanced topics in number theory. Rather than focusing on proofs, we will put an emphasis on historical context and the ideas involved in each of these theories. We start by placing the main theorem into context by discussing the formation of other reciprocity laws, and then go on to explore a few topics in class field theory.

As Eisenstein Reciprocity is a generalization of the initial cases explored by Legendre, Gauss and Eisenstein, it would be natural to ask if any further generalizations exist. There are in fact more general reciprocity theorems, some of which we will state explicitly below. We lay out a general chronology of discoveries to put our main theorem into historical context.

6.1 History

Many of the current texts offer tidbits of history to frame their proofs. The facts in this section are mainly drawn from a very thorough preface in [Le], however some details from others (such as [Es], [Ir], and [Ste]) are potentially included without further reference since they may be considered common knowledge.

After proving Legendre's conjecture of quadratic reciprocity at the age of 19, Gauss went to work on cubic and biquadratic reciprocity laws. It was then that he realized the necessity of an expansion of arithmetic, and the ring of Gaussian integers ($\mathbb{Z}[i]$) was born. He went on to conjecture the law of Biquadratic Reciprocity, which was later proven (simultaneously with Cubic Reciprocity) by a 21 year old Eisenstein in 1844. By then, Jacobi and Kummer were both working toward a generalization of these laws. Kummer introduced the notion of ideal numbers, which resolved the obstacle of the failure of unique factorization in cyclotomic fields. Using these methods, Eisenstein went on to discover and prove Theorem 2.1.

Kummer first generalized our main theorem by proving a reciprocity law that worked in all *regular* cyclotomic fields, (i.e. for $K = \mathbb{Q}(\zeta_\ell)$, the class number of K is not divisible by ℓ). In particular, his methods revealed that for class number h coprime to ℓ, we can express the ℓ-th power residue symbol:

$$\left(\frac{\alpha}{\mathfrak{b}}\right)_\ell = \left(\frac{\mathfrak{a}}{\mathfrak{b}}\right)_\ell^h,$$

where $\mathfrak{a}^h = (\alpha)\mathcal{O}_K$.

At the turn of the century, Hilbert discovered a quadratic reciprocity law for all number fields with odd class number, and challenged others (in a problem he presented at the Congress of Mathematicians in Paris) to generalize Kummer's reciprocity law. In response, Furtwängler extends Kummer's law to include fields $\mathbb{Q}(\zeta_\ell)$ for irregular primes ℓ. But this result was later consumed as a special case of Takagi's proof that Kummer's law held for ℓ-th powers, which he developed with results from class field theory after realizing that Furtwängler's proof was an application of a special case. (Furtwängler's methods included use of the Hilbert class field). We state this general reciprocity law below, and remark that [Be] contains a proof that is quite accessible from the theory we've developed in this thesis.

Theorem 6.1 (Reciprocity for Prime Powers [Be, Thm. 14.3.1])**.** Let $k = \ell^n \neq 2, 4$ be a prime power for some prime ℓ and some $n \in \mathbb{N}$. Let u be a rational prime that is coprime to k, and let v be a primary integer of $K = \mathbb{Q}(e^{2\pi i/k})$. Then

1. $\left(\frac{v}{u}\right)_k = \left(\frac{u}{v}\right)_k$, *if* $\ell > 2$,
2. $\left(\frac{v}{u}\right)_k = \left(\frac{(-1)^{(u-1)/2}u}{v}\right)_k$, *if* $\ell = 2$.

The next mathematicians to seek a more general reciprocity law were Artin and Hasse, which led to the development of the *Weak Reciprocity Law of Hasse*, which in particular required that $\alpha \in \mathcal{O}_K$ be congruent to 1 (mod ℓ). (And hence did not imply Kummer's law). But it was Artin who developed the general reciprocity law that contained all the previously known reciprocity laws. To state Artin's law, we need to introduce the notation of the *global norm residue symbol* (also called the *Artin symbol*).

Definition 6.2 (The Artin Symbol)**.** [Le, §3.2] For a number field K and a Galois extension L, let $\mathfrak{p}$ be a prime ideal of K and $\mathfrak{P}$ be an unramified prime ideal of $\mathcal{O}_L$. We define the Frobenius automorphism $\phi \in G = \mathrm{Gal}(L/K)$ to be the automorphism that for all $\alpha \in \mathcal{O}_L \backslash \mathfrak{P}$, satisfies

$$\phi(\alpha) = \alpha^{N\mathfrak{p}} \pmod{\mathfrak{P}}.$$

In canonical notation (the Frobenius symbol), we have

$$\phi = \phi\mathfrak{p} = \left[\frac{L/K}{\mathfrak{P}}\right].$$

But further, for a given $\mathfrak{p}$, if L/K is an abelian extension, any choice of $\mathfrak{P} \mid \mathfrak{p}$ will give the same result. Thus we can write the Artin symbol,

$$\left(\frac{L/K}{\mathfrak{p}}\right) = \left[\frac{L/K}{\mathfrak{P}}\right].$$

Finally, since G is abelian, it makes sense to extend the definition multiplicatively. For an ideal $\mathfrak{a} \in K$ an ideal with the prime factorization $\mathfrak{a} = \prod \mathfrak{p}_i$, we define the Artin symbol

$$\left(\frac{L/K}{\mathfrak{a}}\right) = \prod_i \left(\frac{L/K}{\mathfrak{p}_i}\right).$$

Furthermore, we let C_K denote the idèle class group of a number field K. For a discussion of idèles in terms of ideals, we refer the reader to [St, Chapter 21]. We now state Artin's Reciprocity Law.

Theorem 6.3 (Artin's Reciprocity Law)**.** For an algebraic number field K and a finite extension L/K, the global norm symbol $\left(\frac{L/K}{\cdot}\right)$ induces an isomorphism

$$C_K/N_{L/K}C_L \simeq \mathrm{Gal}(L/K)^{ab},$$

where $G^{ab} = G/G'$ is G made abelian.

Hasse went on to derive all known reciprocity laws from Artin's and reformations of Artin's law in terms of local fields and cohomology were proven by Hasse and Tate, respectively. We will elaborate more on Artin's Reciprocity law in the following section, as well as discussing Chebotarëv's Density Theorem, the initial proof of which set up the techniques Artin used to satisfy his reciprocity proof.

6.2 Abelian Class Field Theory

Class field theory is the study and classification of all the Galois extensions of global and local fields, in terms of the field's own arithmetic. In this section, we aim to introduce some notions regarding abelian extensions, as it is the most basic area of the theory. We remark for the enthusiastic reader that there are quite a few resources freely available online, in particular [Len] gives an elementary introduction to Chebotarëv's theorem and [Mi] gives a thorough account of abelian class field theory.

6.2.1 The Artin Map

Given the goal of class field theory, it is no surprise that the isomorphism given in Artin's Reciprocity Law (known as the *Artin map* or the *reciprocity map*) is considered the main theorem. We remark that G^{ab} in the above theorem is the largest abelian group that G maps to, and hence this isomorphism is a necessary key to classifying all abelian extensions of $\mathrm{Gal}(L/K)$.

We also mentioned in the previous section that Hasse proved the existence of the local reciprocity map. However, we remark that he handled it in quite a round-about way, by deducing it from the global case. Since local fields are simpler, the easier proof should have been the restriction to local fields. However, this simply was not the chronological order of discovery. In fact, abelian extensions of local fields had been entirely classified by Hasse's method before Chevally finally produced a purely local proof of the local Artin map, using idèles. Furthermore, Chevally went on to prove that the global Artin map can be found from the local.

6.2.2 Chebotarëv's Density Theorem

In his proof of the reciprocity map, Artin credited Chebotarëv's proof of his density theorem. [Len] points out that Chebotarëv's method is applied in all known proofs of the reciprocity law, but it is typically no longer used in current proofs of the density theorem. Essentially, the reciprocity map gives direct access to abelian extensions, removing the need for Chebotarëv's trick. So what exactly is this result that Chebotarëv proved, and how did he accomplish it? First, we introduce the concept of density.

Definition 6.4. A set S of primes has density δ if as $x \to \infty$,

$$\frac{\#\{p \le x : p \in S\}}{\#\{p \le x : p \text{ prime}\}} \to \delta.$$

We can now state Chebotarëv's theorem.

Theorem 6.5. [Len, pg 15] Let f be a polynomial in $\mathbb{Z}[x]$ with leading coefficient 1, such that the discriminant $\triangle(f)$ does not vanish. Let G be the Galois group of f, and let C be its conjugacy class. Then the set of primes

$$S = \{p : p \nmid \triangle(f) \text{ and } \sigma_p \in C\}$$

has density $\delta = |C|/|G|$, where σ_p denotes the Frobenius substitution.

The heart of Cheboratëv's idea was to associate abelian extensions with cyclotomic extensions. In his appendix, [Len] provides a full proof using Cheboratëv's initial techniques. We sketch the main idea here. Essentially, for an abelian extension K over a field F, we let $G = \mathrm{Gal}(K/F)$. Adjoining ζ_m to F and K, we find that $\mathrm{Gal}(F(\zeta_m)/F) \simeq (\mathbb{Z}/m\mathbb{Z})^*$ and $\mathrm{Gal}(K(\zeta_m)/F) \simeq G \times H$. He then defines a lower and upper density by summing the Frobenius substitution over all τ, for $(\sigma, \tau) \in G \times H$, first holding σ fixed (for lower), and then over all σ (upper).

As a conclusion, we take a moment to review some other implications of this theorem. [Len] provides three elementary applications:

1. The prime ideals of $\mathcal{O}_K$ are equidistributed, for any number field $\mathcal{O}_K$.
2. Proving the density of quadratic forms. For example, he claims that all primes p such that $p = 3x^2 + xy + 4y^2,\ x, y \in \mathbb{Z}$ have density $1/5$.
3. The set of primes p with the property that $\frac{1}{p}$ has odd period length in base 10 decimal expansion has density $\frac{1}{3}$.

We remark that in (2) and (3) above, we are implicitly stating that these densities exist.

Appendix: Interact Demos in Sage

This appendix includes the full source code for the illustrative interact demos in Sage, which were created in conjunction with authoring this thesis. An example of these demonstrations can be found at:

`http://wiki.sagemath.org/interact/number_theory`

A-1: Symmetric Residue Tables

A-1-1. Quadratic Residues

```
{{{
@interact
def quad_res_plot(first_n_odd_primes = (20,200),display_size=[7..15]):

    # Compute list of lists of legendre symbols
    r = int(first_n_odd_primes)
    np = [nth_prime(i+2) for i in range(r)]
    leg = [[legendre_symbol(np[i], np[j]) for i in range(r)] for j in range(r)]
    for i in range(r):
        for j in range(r):
            if leg[i][j] == 1 and Mod((np[i]-1)*(np[j]-1)//4,2) == 0:
                leg[i][j] = 2
    m = matrix(leg)

    # Define plot structure
    MP = matrix_plot(m, cmap='Oranges')
    for i in range(r):
        if np[-1] < 100:
            MP += text('%d'%nth_prime(i+2),(-.75,r-i-.5), rgbcolor='black')
            MP += text('%d'%nth_prime(i+2), (i+.5,r+.5), rgbcolor='black')
        if len(np) < 75:
            MP += line([(0,i),(r,i)], rgbcolor='black')
            MP += line([(i,0),(i,r)], rgbcolor='black')
    if np[-1] < 100:
        for i in range(r): # rows
            for j in range(r): # cols
                if m[j][i] == 0:
                    MP += text('0',(i+.5,r-j-.5),rgbcolor='black')
                elif m[j][i] == -1:
                    MP += text('N',(i+.5,r-j-.5),rgbcolor='black')
                elif m[j][i] == 1:
                    MP += text('A',(i+.5,r-j-.5),rgbcolor='black')
                elif m[j][i] == 2:
                    MP += text('S',(i+.5,r-j-.5),rgbcolor='black')
    MP += line([(0,r),(r,r)], rgbcolor='black')
    MP += line([(r,0),(r,r)], rgbcolor='black')
    MP += line([(0,0),(r,0)], rgbcolor='black')
    MP += line([(0,0),(0,r)], rgbcolor='black')
    if len(np) < 75:
        MP += text('q',(r/2,r+2), rgbcolor='black', fontsize=15)
        MP += text('p',(-2.5,r/2), rgbcolor='black', fontsize=15)
    MP.show(axes=False, ymax=r, figsize=[display_size,display_size])
    html('Symmetry of Prime Quadratic Residues mod the first %d odd primes.'%r)
}}}
```

A-1-2. Cubic Residues

```
{{{
def power_residue_symbol(alpha, p, m):
    if p.divides(alpha): return 0
    if not p.is_prime():
        return prod(power_residue_symbol(alpha,ell,m)^e
                for ell, e in p.factor())
    F = p.residue_field()
    N = p.norm()
    r = F(alpha)^((N-1)/m)
    k = p.number_field()
    for kr in k.roots_of_unity():
        if r == F(kr):
            return kr

def cubic_is_primary(n):
    g = n.gens_reduced()[0]
    a,b = g.polynomial().coefficients()
    if Mod(a,3)!=0 and Mod(b,3)==0:
        return True
    else:
        return False

@interact
def cubic_sym(n=(10..35),display_size=[7..15]):

    # Compute list of lists of primary cubic residue symbols
    r = n
    m=3
    D.<w> = NumberField(x^2+x+1)
    it = D.primes_of_degree_one_iter()
    pp = []
    while len(pp) < r:
        k = it.next()
        if cubic_is_primary(k):
            pp.append(k)
    n = [ [ power_residue_symbol(pp[i].gens_reduced()[0], pp[j], m) \
                        for i in range(r) ] for j in range(r) ]

    # Convert to integer matrix for gradient colors
    for i in range(r):
        for j in range(r):
            if n[i][j] == w:
                n[i][j] = int(-1)
            elif n[i][j] == w^2:
                n[i][j] = int(-2)
            elif n[i][j] == 1:
                n[i][j] = int(1)
    m = matrix(n)

    # Define plot structure
    MP = matrix_plot(m,cmap="Blues")
    for i in range(r):
        MP += line([(0,i),(r,i)], rgbcolor=’black’)
        MP += line([(i,0),(i,r)], rgbcolor=’black’)
        for j in range(r):
            if m[i][j] == -2:
                MP += text(’$\omega^2$’,(i+.5,r-j-.5),rgbcolor=’black’)
            if m[i][j] == -1:
                MP += text(’$\omega $’,(i+.5,r-j-.5),rgbcolor=’black’)
            if m[i][j] == 0:
                MP += text(’0’,(i+.5,r-j-.5),rgbcolor=’black’)
            if m[i][j] == 1:
                MP += text(’R’,(i+.5,r-j-.5),rgbcolor=’white’)
    MP += line([(0,r),(r,r)], rgbcolor=’black’)
    MP += line([(r,0),(r,r)], rgbcolor=’black’)
    MP += line([(0,0),(r,0)], rgbcolor=’black’)
    MP += line([(0,0),(0,r)], rgbcolor=’black’)
    MP += text(’$ \pi_1$’,(r/2,r+2), rgbcolor=’black’, fontsize=25)
    MP += text(’$ \pi_2$’,(-2.5,r/2), rgbcolor=’black’, fontsize=25)

    html(’Symmetry of Primary Cubic Residues mod ’ \
          + ’%d primary primes in $ \mathbf Z[\omega]$.’%r)
    MP.show(axes=False, figsize=[display_size,display_size])
}}}
```

A-2: Plotting Jacobi Sums

```
{{{
def Jacobi_sum(e,f):
    # If they are both trivial, return p
    if e.is_trivial() and f.is_trivial():
        return (e.parent()).order() + 1

    # If they are inverses of each other, return -e(-1)
    g = e*f
    if g.is_trivial():
        return -e(-1)

    # If both are nontrivial, apply mult. formula:
    elif not e.is_trivial() and not f.is_trivial():
        return e.Gauss_sum()*f.Gauss_sum()/g.Gauss_sum()

    # If exactly one is trivial, return 0
    else:
        return 0

def latex2(e):
    return latex(list(e.values_on_gens()))

def Jacobi_plot(p, e_index, f_index, with_text=True):
    # Set values
    G = DirichletGroup(p)
    e = G[e_index]
    f = G[f_index]
    ef = e*f
    js = Jacobi_sum(e,f)
    e_gs = e.Gauss_sum()
    f_gs = f.Gauss_sum()
    ef_gs = (e*f).Gauss_sum()

    # Compute complex coordinates
    f_pt = list(f.values_on_gens()[0].complex_embedding())
    e_pt = list(e.values_on_gens()[0].complex_embedding())
    ef_pt = list(ef.values_on_gens()[0].complex_embedding())
    f_gs_pt = list(f_gs.complex_embedding())
    e_gs_pt = list(e_gs.complex_embedding())
    ef_gs_pt = list(ef_gs.complex_embedding())
    try:
        js = int(js)
        js_pt = [CC(js)]
    except:
        js_pt = list(js.complex_embedding())

    # Define plot structure
    S = circle((0,0),1,rgbcolor=’yellow’)  \
    + line([e_pt,e_gs_pt], rgbcolor=’red’, thickness=4) \
    + line([f_pt,f_gs_pt], rgbcolor=’blue’, thickness=3) \
    + line([ef_pt,ef_gs_pt], rgbcolor=’purple’,thickness=2) \
    + point(e_pt,pointsize=50, rgbcolor=’red’)  \
    + point(f_pt,pointsize=50, rgbcolor=’blue’) \
    + point(ef_pt,pointsize=50,rgbcolor=’purple’) \
    + point(f_gs_pt,pointsize=75, rgbcolor=’black’) \
    + point(e_gs_pt,pointsize=75, rgbcolor=’black’) \
    + point(ef_gs_pt,pointsize=75, rgbcolor=’black’) \
    + point(js_pt,pointsize=100,rgbcolor=’green’)
    if with_text:
        S += text(’$J(%s,%s) = %s$’%(latex2(e),latex2(f),latex(js)), \
            (3,2.5),fontsize=15, rgbcolor=’black’)
    else:
        html(’$$J(%s,%s) = %s$$’%(latex2(e),latex2(f),latex(js)))

    return S
}}}
```

A-2-1. Single Jacobi Sum Plots

```
{{{
@interact
def single_Jacobi_plot(p=prime_range(3,100), e_range=(0..100), f_range=(0..100)):
    e_index = floor((p-2)*e_range/100)
    f_index = floor((p-2)*f_range/100)
    S = Jacobi_plot(p,e_index,f_index,with_text=False)
    S.show(aspect_ratio=1)
}}}
```

A-2-2. Exhaustive Plotting of Jacobi Sums

```
{{{
@interact
def exhaustive_Jacobi_plot(p=prime_range(3,8)):
    ga = [Jacobi_plot(p,i,j) for i in range(p-1) for j in range(p-1)[i:]]

    for i in range(len(ga)):
        ga[i].save(’j%d.PNG’%i,figsize=4,aspect_ratio=1, \
                    xmin=-2.5,xmax=5, ymin=-2.5, ymax=2.5)
    # Since p is odd, will have n = p-1 even.  So 1+2+...+n = (n/2)*(n+1).
    # We divide this by rows of 2.
    rows = ceil(p*(p-1)/4)
    html('<table bgcolor=lightgrey cellpadding=2>')
    for i in range(rows):
        html('<tr><td align="center"><img src="cell://j%d.PNG"></td>'%(2*i))
        html('<td align="center"><img src="cell://j%d.PNG"></td></tr>'%(2*i+1))
    html('</table>')
}}}
```

References

[Be] Bruce Berndt, Ronald Evans and Kenneth S. Williams, *Gauss and Jacobi Sums*. Canadian Mathematical Society Series of Monographs and Advanced Texts, Volume 21. Wiley-Interscience (1998).

[Du] David Dummit and Richard M. Foote, *Abstract Algebra*. Third edition. Graduate Texts in Mathematics, 84. Wiley (2004).

[Es] Jody Esmonde and M. Ram Murty, *Problems in Algebraic Number Theory*. Second Edition. Springer-Verlag (2005).

[Ir] Kenneth Ireland and Michael Rosen, *A Classical Introduction to Modern Number Theory*. Second edition. Springer-Verlag (1990).

[Le] Franz Lemmermeyer, *Reciprocity Laws: From Euler to Eisenstein*. Springer-Verlag (2000).

[Lem] Franz Lemmermeyer, *Proofs of the Quadratic Reciprocity Law*. Retrieved June 19, 2008:

`http://www.rzuser.uni-heidelberg.de/~hb3/rchrono.html`

[Len] H. W. Lenstra, Jr. and P. Stevenhagen, *Chebotarëv and his density theorem*. Version 19950323:

`http://www.math.leidenuniv.nl/~hwl/papers/cheb.pdf (1995).`

[Mi] J. S. Milne, *Class Field Theory*. Version 4.00:

`http://www.jmilne.org/math/CourseNotes/math776.html (2008).`

[Sage] William Stein, *Sage Mathematics Software (Version 3.0.2)*, The Sage Group:

`http://www.sagemath.org/ (2007).`

[St] William Stein, *A Brief Introduction to Classical and Adelic Algebraic Number Theory*:

`http://wstein.org/papers/ant (2004).`

[Ste] William Stein, *Elementary Number Theory*. Springer-Verlag (2007).

[Wa] Lawrence C. Washington, *Introduction to Cyclotomic Fields*. Second Edition. Springer-Verlag (1997).