ON THE VALUE OF THE QUADRATIC GAUSS SUM

MATIAS RELYEA

Abstract. In this rather brief paper, we will define and prove several interesting properties of the Quadratic Gauss Sum, and eventually end with the main theorem of this paper: the sign of the Quadratic Gauss Sum. The proof that we will provide is one by Kronecker, although there are many more that can be interesting. This is not a generalization to Gauss Sums, but we will utilize the conventional notation with the Dirichlet Character χ for the sake of functionality.

Contents

1. Background

Definition 1.1 (Legendre Symbol)**.** For $\gcd(a,p) = 1$ where p is a prime, we define

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

There exist a substantial number of fundamental properties, but we will only utilize one such property in this paper: Euler's Criterion.

Theorem 1.2 (Euler's Criterion)**.** *Let* $\gcd(a,p) = 1$. *Then*

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

Proof. Assume $p \nmid a$. Recall Fermat's Little Theorem:

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

Date: Summer 2022.

We may factorize this as

$$\begin{aligned} a^{p-1} - 1 &\equiv 0 \pmod{p} \\ (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) &\equiv 0 \pmod{p} \\ a^{\frac{p-1}{2}} &\equiv \pm 1 \pmod{p}. \end{aligned}$$

Noticing that the Legendre Symbol maintains a value of ± 1, with exceptions for $p \mid a$, we can state that it is equivalent to our expression. Thus

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

■

We are now going to prove a seemingly trivial result. It is almost obvious through experimentation, but it is necessary to provide a rigorous proof. Although it is not crucial, it is important for the proof of a lemma that is used to prove Proposition **1.7**, and can be found in section 4 of [CR22].

Lemma 1.3. *There are an equal number of quadratic residues and quadratic non-residues, and*

$$\sum_{t=0}^{p-1} \left(\frac{t}{p}\right) = 0.$$

Proof. The second statement follows directly from the first, because the Legendre Symbol fluctuates between 1 and -1 for all residues modulo p. Thus, we must prove the first statement.

Notice that if we can prove that there are $\frac{p-1}{2}$ quadratic residues then we will have proven the statement. Recalling the definition of a quadratic residue, we have

$$x^2 \equiv a \pmod{p}.$$

All such solutions to this congruence are the squares of the residues modulo p, so we have $0^2, 1^2, 2^2, 3^2, \ldots, (p-1)^2$ (we can omit 0^2 as that is the trivial case). Let $b \in \{1, 2, 3, \ldots, p-1\}$. Then some $(p-b)^2$ belongs to the set of residues modulo p squared. Expanding this, we notice that $(p-b)^2 = p^2 - 2bp + b^2 \equiv b^2 \pmod{p}$. Thus we may write a congruence relating terms that are of the form $(p-b)^2$ and b^2. Then

$$1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2 \equiv (p-1)^2, (p-2)^2, (p-3)^2, \ldots, \left(\frac{p+1}{2}\right)^2 \pmod{p}.$$

In order to show that there are exactly $\frac{p-1}{2}$ quadratic residues, we must show that the above residues up to $\frac{p-1}{2}$ are distinct.

Assume that there exist some $a, b \in \{1, 2, 3, \ldots, \frac{p-1}{2}\}$, so that $a^2 \equiv b^2 \pmod{p}$. Then $p \mid a^2 - b^2$ and $p \mid (a-b)(a+b)$. Notice that $p \nmid (a+b)$ because even the maximum value of $a+b$ is indivisible by p. Thus $p \mid (a-b)$. However, if $p \mid (a-b)$,

then notice that $\mid a-b \mid < \frac{p-1}{2}$, which is clearly indivisible by p. Then $p \nmid (a-b)$. However, this contradicts our assumption, so $a = b$, and there are exactly $\frac{p-1}{2}$ quadratic residues, and naturally, $\frac{p-1}{2}$ quadratic nonresidues. ■

We will now prepare to prove a result that will be used later, namely Wilson's Theorem. We begin by proving the following proposition.

Proposition 1.4.

$$x^{p-1} - 1 \equiv (x-1)(x-2)(x-3)\cdots(x-p+1) \pmod{p}.$$

Proof. Let $a \in \mathbb{Z}/p\mathbb{Z}$, so its residue class is $[a]$. We may rewrite the expression above as

$$f(x) = (x^{p-1} - [1]) - (x-[1])(x-[2])(x-[3])\cdots(x-[p-1]).$$

It is clear that $f(x) \in \mathbb{Z}/p\mathbb{Z}[x]$. It is also clear that $\deg f(x) < p-1$ because the leading terms of the polynomial cancel, and that it has the $p-1$ roots given by $[1], [2], \ldots, [p-1]$. Thus $f(x)$ is identically zero, so that

$$x^{p-1} - [1] = (x-[1])(x-[2])(x-[3])\cdots(x-[p-1])$$
$$x^{p-1} - 1 \equiv (x-1)(x-2)(x-3)\cdots(x-p+1) \pmod{p}$$

hence proving the proposition. ■

Corollary 1.5 (Wilson's Theorem)**.**

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof. Let $x = 0$ in Proposition **1.4**. Then

$$0^{p-1} - 1 \equiv (0-1)(0-2)(0-3)\cdots(0-(p-1)) \pmod{p}$$
$$-1 \equiv (-1)(-2)(-3)\cdots(-(p-1)) \pmod{p}$$
$$(p-1)! \equiv -1 \pmod{p}.$$

■

We will now introduce the notion of a Gauss Sum. Note that throughout the remainder of this paper, ζ_p denotes a pth root of unity, or a root of the polynomial $x^p - 1$.

Definition 1.6 (Gauss Sum)**.** The Gauss Sum is defined as

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

However, in this paper, we will only consider the Gauss Sum when $a = 1$, and when $\chi(t)$ denotes the Legendre Symbol $(\frac{t}{p})$, hence a Quadratic Gauss Sum. We define the sum for $a = 1$ as

$$g(\chi) = \sum_{t=0}^{p-1} \chi(t)\zeta_p^{t}.$$

Notice that with this definition now equipped, we may rewrite Theorem **1.2** as

$$\chi(t) \equiv t^{\frac{t-1}{2}} \pmod{p}.$$

This notation will be used later.

We now introduce a key property of the Gauss Sum that begins our investigation of the sign of the Quadratic Gauss Sum.

Proposition 1.7.

$$g(\chi)^2 = (-1)^{\frac{p-1}{2}} p.$$

Proof. The proof can be found in section **4.3** of [CR22]. ■

Notice that if we take the square root of the left-hand-side and right-hand-side, we obtain the expression

$$g(\chi) = \pm\left(\sqrt{(-1)^{(p-1)/2}}\sqrt{p}\right).$$

The value of the Gauss Sum is determined by the nature of the prime p; with some experimentation, it is easy to see that when $p \equiv 1 \pmod 4$, $g(\chi) = \pm\sqrt{p}$, but when $p \equiv 3 \pmod 4$, $g(\chi) = \pm i\sqrt{p}$. We can summarize this as

$$g(\chi) = \begin{cases} \pm\sqrt{p} & \text{if } p \equiv 1 \pmod 4 \\ \pm i\sqrt{p} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Notice the $\pm$ sign. When Gauss was considering the value of the Quadratic Gauss Sum, it was imperative that he also consider the sign. Denoting the $\pm$ sign with an epsilon, and allowing it to take on $\epsilon = \pm 1$, we can begin to confront the problem. Whether ϵ is positive or negative is what we are attempting to determine.

We are now prepared to confront the final part of this paper.

2. The Final Result

2.1. **Several crucial properties.** We will not prove two of the following properties, as they lie beyond the purpose of this paper, but they are both incredibly important, and describe numerous characteristics of polynomials in different fields and rings.

Proposition 2.1. *The polynomial*

$$1 + x + x^2 + x^2 + \cdots + x^{p-1}$$

is irreducible, or non-factorizable, in $\mathbb{Q}[x]$, or the ring of polynomials with rational coefficients.

Proof. The proof may be found in chapter 6 section 4 of [IRR90]. ■

Proposition 2.2. *If we allow α to be some algebraic number, then α is the root of a unique monic irreducible polynomial $f(x) \in \mathbb{Q}[x]$. Furthermore, if there exists another polynomial $g(x) \in \mathbb{Q}[x]$, and it also has α as a root, i.e. $g(\alpha) = 0$, then it is true that $f(x) \mid g(x)$.*

Proof. The proof may be found in chapter 6 section 1 of [IRR90]. ■

Remark 2.3. It is important to notice that Proposition **2.2** implies that if some algebraic number ζ satisfies $g(\zeta) = 0$ for some polynomial $g(x) \in \mathbb{Q}[x]$, then we can see that it is true that

$$1 + x + x^2 + x^2 + \cdots + x^{p-1} \mid g(x).$$

This fact will be important later in our final proof.

The theory behind the final proof of the sign and hence value of the Quadratic Gauss Sum is the introduction of a polynomial with certain beneficial properties. We will now prove particular properties of components of this polynomial in order to further understand its components.

Proposition 2.4.

$$\prod_{k=1}^{(p-1)/2} (\zeta_p^{2k-1} - \zeta_p^{-(2k-1)})^2 = (-1)^{\frac{p-1}{2}} p.$$

Proof. The polynomial $x^p - 1$ has roots $1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$, so it may be written as the product

$$x^p - 1 = (x-1) \prod_{j=1}^{p-1} (x - \zeta_p^j).$$

If we divide the left-hand-side and right-hand-side by $(x-1)$ we obtain

$$\frac{x^p - 1}{x - 1} = \prod_{j=1}^{p-1} (x - \zeta_p^j)$$

$$1 + x + x^2 + x^3 + \cdots + x^{p-1} = \prod_{j=1}^{p-1} (x - \zeta_p^j).$$

Letting $x = 1$, we obtain

$$p = \prod_{r} (x - \zeta_p^r).$$

As indicated by the index r, this product runs over a complete set of representatives of the nonzero cosets modulo p. Since this set is abelian, or commutative, the left and right cosets modulo p are equivalent, so r ranges over elements $a \in G$ that satisfy $aH = Ha$ for some $H \subset G$, where $aH = Ha = \{ah = ha \mid h \in H\}$. It can be seen that the system of residues $\pm(4k-2)$ satisfies this property for $k = 1, 2, 3, \ldots, (p-1)/2$, $k \in \mathbb{Z}$. Thus we can substitute $r = \pm(4k-2)$ and change

the indices of the product to obtain

$$\begin{aligned}
p &= \prod_{k=1}^{(p-1)/2} (1-\zeta_p^{4k-2}) \prod_{k=1}^{(p-1)/2} (1-\zeta_p^{-(4k-2)}) \\
&= \prod_{k=1}^{(p-1)/2} (\zeta_p^{-(2k-1)} - \zeta_p^{2k-1}) \prod_{k=1}^{(p-1)/2} (\zeta_p^{2k-1} - \zeta_p^{-(2k-1)}) \\
&= \prod_{k=1}^{(p-1)/2} (\zeta_p^{-(2k-1)} - \zeta_p^{2k-1})(\zeta_p^{2k-1} - \zeta_p^{-(2k-1)}) \\
&= \prod_{k=1}^{(p-1)/2} (-1)(\zeta_p^{2k-1} - \zeta_p^{-(2k-1)})(\zeta_p^{2k-1} - \zeta_p^{-(2k-1)}) \\
&= (-1)^{\frac{p-1}{2}} \prod_{k=1}^{(p-1)/2} (\zeta_p^{2k-1} - \zeta_p^{-(2k-1)})^2,
\end{aligned}$$

so we are done. ■

We now prove another property, but this time denoting the value of a certain product given certain conditions on primes.

Proposition 2.5.

$$\prod_{k=1}^{(p-1)/2} (\zeta_p^{2k-1} - \zeta_p^{-(2k-1)}) = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod 4 \\ i\sqrt{p} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Proof. In order to prove this, we must first evaluate the product. Write

$$\prod_{k=1}^{(p-1)/2} (\zeta_p^{2k-1} - \zeta_p^{-(2k-1)}) = \prod_{k=1}^{(p-1)/2} \left(e^{\frac{2i\pi(2k-1)}{p}} - e^{\frac{2i\pi(-(2k-1))}{p}} \right).$$

Utilizing the polar form of a complex number $e^{i\theta} = \cos\theta + i\sin\theta$ and several negative angle identities, we have

$$\begin{aligned}
\prod_{k=1}^{(p-1)/2}\left(e^{\frac{2i\pi(2k-1)}{p}} - e^{\frac{2i\pi(-(2k-1))}{p}}\right) &= \prod_{k=1}^{(p-1)/2}\left[\left(\cos\frac{(4k-2)\pi}{p} + i\sin\frac{(4k-2)\pi}{p}\right)\right. \\
&\quad \left. - \left(\cos\frac{-(4k-2)\pi}{p} + i\sin\frac{-(4k-2)\pi}{p}\right)\right] \\
&= \prod_{k=1}^{(p-1)/2}\left(\cos\frac{(4k-2)\pi}{p} - \cos\frac{-(4k-2)\pi}{p}\right. \\
&\quad \left. + i\sin\frac{(4k-2)\pi}{p} - i\sin\frac{-(4k-2)\pi}{p}\right) \\
&= \prod_{k=1}^{(p-1)/2}\left(0 + 2i\sin\frac{(4k-2)\pi}{p}\right) \\
&= i^{\frac{p-1}{2}}\prod_{k=1}^{(p-1)/2} 2\sin\frac{(4k-2)\pi}{p}
\end{aligned}$$

Notice that

$$\sin\frac{4k-2}{p}\pi < 0$$

if

$$\frac{p+2}{4} < k \leq \frac{p-1}{2}.$$

By subtracting the bounds, we can determine exactly how many negative terms there are in this sin evaluation. Thus, there are

$$\frac{p-1}{2} - \frac{p+2}{4}$$

negative terms. This can be seen to be exactly $(p-1)/2$ or $(p-3)/2$ for $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$ respectively. Thus the result follows by completing the evaluation. ■

Notice that by Proposition **1.7** and Proposition **2.4**, we have that

$$g(\chi)^2 = \prod_{k=1}^{(p-1)/2}(\zeta_p^{2k-1} - \zeta_p^{-(2k-1)})^2$$

$$g(\chi) = \epsilon\prod_{k=1}^{(p-1)/2}(\zeta_p^{2k-1} - \zeta_p^{-(2k-1)}),$$

where $\epsilon = \pm 1$. If we are able to prove that $\epsilon = +1$, then we will have proven the sign and hence the value of the Quadratic Gauss Sum.

Now we prove a specific property of power series that will be used in the final proof.

Proposition 2.6. *Let there exist power series*

$$\sum_{n=0}^{\infty} \frac{a_n}{n!}x^n \text{ and } \sum_{n=0}^{\infty} \frac{b_n}{n!}x^n$$

such that $a_n, b_n \in \mathbb{Z}$. *If* p *is a prime such that* $p \mid a_i$ *for* $i \in \{0, 1, 2, \ldots, p-1\}$, *it is true that each coefficient* c_t *where* $t \in \{0, 1, 2, \ldots, p-1\}$ *of the product of the power series*

$$\sum_{n=0}^{\infty} c_n x^n$$

may be written in the form $p(A/B)$ *where* $p \nmid B$, *and* $A, B \in \mathbb{Z}$.

Proof. Let some $k \in \mathbb{N}$ and $0 \leq k \leq p-1$. We set some $i, j \in \mathbb{Z}$ to sum to k, and take the sum over all such i and j that sum to k of the coefficients of the power series to obtain

$$c_k = \sum_{i+j=k} \frac{a_i}{i!} \cdot \frac{b_j}{j!}.$$

Letting $j = k - i$, we have

$$\begin{aligned} \sum_{i=0}^{k} \frac{a_i}{i!} \cdot \frac{b_{k-i}}{(k-i)!} &= \sum_{i=0}^{k} \frac{1}{k!} \cdot \frac{k! a_i b_{k-i}}{i!(k-i)!} \\ &= \frac{1}{k!} \sum_{i=0}^{k} \binom{k}{i} a_i b_{k-i}. \end{aligned}$$

Since we assumed that $p \mid a_i$, we can say that $\binom{k}{i}$ for $0 \leq k \leq p-1$ is always an integer. Furthermore, $p \nmid t!$ because $t \leq p-1$. Thus c_k may be expressed in the form $p(A/B)$ for $p \nmid B$, and we are done.

■

2.2. **Proof that $\epsilon = +1$.** We are now going to prove the sign of the Quadratic Gauss Sum.

Theorem 2.7.

$$\epsilon = +1.$$

Proof. We begin the proof by considering some polynomial

$$f(x) = \sum_{j=1}^{p-1} \chi(j) x^j - \epsilon \prod_{k=1}^{(p-1)/2} (x^{2k-1} - x^{p-(2k-1)}).$$

Taking several values of $f(x)$, we can notice that

$$\begin{aligned} f(\zeta_p) &= \sum_{j=1}^{p-1} \chi(j)\zeta_p^j - \epsilon \prod_{k=1}^{(p-1)/2} (\zeta_p^{2k-1} - \zeta_p^{p-(2k-1)}) \\ &= g(\chi) - \epsilon \prod_{k=1}^{(p-1)/2} (\zeta_p^{2k-1} - (1)^p \zeta_p^{-(2k-1)}) \\ &= g(\chi) - g(\chi) = 0. \end{aligned}$$

Furthermore, $f(1) = 0$ by Lemma **1.3**.

By Remark **2.3** and the fact that $1 + x + x^2 + \cdots + x^{p-1}$ is irreducible in $\mathbb{Q}[x]$ in Proposition **2.1**, it must imply that the monic irreducible polynomial $x - 1$ is relatively prime to $1 + x + x^2 + \cdots + x^{p-1}$. Thus it is also true that $x^p - 1 \mid f(x)$, and for some other polynomial $h(x) \in \mathbb{Q}[x]$,

$$f(x) = (x^p - 1)h(x).$$

Substitute e^z for x to obtain

$$\sum_{j=1}^{p-1} \chi(j)e^{jz} - \epsilon \prod_{k=1}^{(p-1)/2} (e^{(2k-1)z} - e^{(p-(2k-1))z}) = (e^{pz} - 1)h(e^z). \tag{1}$$

Our objective is to determine the coefficient of some $z^{(p-1)/2}$ on the left-hand-side. In order to do this, we must find a way to simplify the product on the left-hand-side so that it contains some multiple of $z^{(p-1)/2}$. To do this, we utilize the power series expansion for e^x. Then

$$\begin{aligned} \epsilon \prod_{k=1}^{(p-1)/2} (e^{(2k-1)z} - e^{(p-(2k-1))z}) &= \epsilon \prod_{k=1}^{(p-1)/2} \left[\left(1 + (2k-1)z + \frac{((2k-1)z)^2}{2!} + \cdots \right) \right. \\ &\quad \left. - \left(1 + (p-(2k-1))z + \frac{((p-(2k-1))z)^2}{2!} + \cdots \right) \right] \\ &= \epsilon \prod_{k=1}^{(p-1)/2} \left(1 - 1 + (2k-1)z - (p-(2k-1))z \right. \\ &\quad \left. + \frac{((2k-1)z)^2}{2!} - \frac{((p-(2k-1))z)^2}{2!} + \cdots - \cdots \right) \\ &= \epsilon \prod_{k=1}^{(p-1)/2} \left(z((2k-1) - (p-(2k-1))) \right. \\ &\quad \left. + \frac{z^2((2k-1)^2 - (p-(2k-1))^2)}{2!} + \cdots \right). \end{aligned}$$

Ignoring the terms that are divisible by powers of z, we have the product

$$\epsilon \prod_{k=1}^{(p-1)/2} z(4k-p-2) = z^{\frac{p-1}{2}} \epsilon \prod_{k=1}^{(p-1)/2} (4k-p-2).$$

Returning to (1), we have

$$\sum_{j=1}^{p-1} \chi(j) e^{jz} - z^{\frac{p-1}{2}} \epsilon \prod_{k=1}^{(p-1)/2} (4k-p-2) = (e^{pz}-1)h(e^z).$$

We can find the coefficient of $z^{(p-1)/2}$ to be

$$\frac{\sum_{j=1}^{p-1} \chi(j) j^{\frac{p-1}{2}}}{(\frac{p-1}{2})!} - \epsilon \prod_{k=1}^{(p-1)/2} (4k-p-2).$$

Furthermore, by Proposition **2.6**, the coefficient of the right-hand-side of (1) may be written as $p(A/B)$ for $A, B \in \mathbb{Z}$ and $p \nmid B$. We equate the two coefficients and multiply the left-hand-side and right-hand-side by $B(\frac{p-1}{2})!$ to obtain

$$B\left(\frac{p-1}{2}\right)!\left(\frac{\sum_{j=1}^{p-1} \chi(j) j^{\frac{p-1}{2}}}{(\frac{p-1}{2})!} - \epsilon \prod_{k=1}^{(p-1)/2} (4k-p-2)\right) = B\left(\frac{p-1}{2}\right)!\frac{pA}{B}$$

$$B\sum_{j=1}^{p-1} \chi(j) j^{\frac{p-1}{2}} - B\left(\frac{p-1}{2}\right)!\epsilon \prod_{k=1}^{(p-1)/2} (4k-p-2) = pA\left(\frac{p-1}{2}\right)!.$$

Reducing modulo p, we have

$$B\sum_{j=1}^{p-1} \chi(j) j^{\frac{p-1}{2}} - B\left(\frac{p-1}{2}\right)!\epsilon \prod_{k=1}^{(p-1)/2} (4k-2) \equiv pA\left(\frac{p-1}{2}\right)! \pmod{p}$$

$$\equiv 0 \pmod{p}.$$

Thus

$$B\sum_{j=1}^{p-1} \chi(j) j^{\frac{p-1}{2}} \equiv B\left(\frac{p-1}{2}\right)!\epsilon \prod_{k=1}^{(p-1)/2} (4k-2) \pmod{p}$$

$$\sum_{j=1}^{p-1} \chi(j) j^{\frac{p-1}{2}} \equiv \left(\frac{p-1}{2}\right)!\epsilon \prod_{k=1}^{(p-1)/2} (4k-2) \pmod{p}.$$

However, by Theorem **1.2**, $\chi(j) \equiv j^{(p-1)/2} \pmod{p}$, so

$$\sum_{j=1}^{p-1} \chi(j) j^{\frac{p-1}{2}} \equiv \sum_{j=1}^{p-1} \chi(j)^2 \equiv \sum_{j=1}^{p-1} 1 \equiv p-1 \pmod{p}.$$

This means that

$$p-1 \equiv \left(\frac{p-1}{2}\right)!\epsilon \prod_{k=1}^{(p-1)/2} (4k-2) \pmod{p}$$
$$p-1 \equiv \epsilon(2\cdot 4\cdot 6\cdots(p-3)\cdot(p-1))\cdot(1\cdot 3\cdot 5\cdots(p-4)\cdot(p-2) \pmod{p}$$
$$-1 \equiv \epsilon(p-1)! \pmod{p}.$$

By Corollary **1.5**, $\epsilon(p-1)! \equiv \epsilon(-1) = -\epsilon \pmod{p}$, so

$$-\epsilon \equiv -1 \pmod{p}$$
$$\epsilon \equiv +1 \pmod{p}.$$

Since ϵ and $+1$ are either positive or negative, they are not only congruent modulo p, but equivalent, so

$$\epsilon = +1$$

and we are done. ■

This proves that the value of the Quadratic Gauss Sum is either $+\sqrt{p}$ or $+i\sqrt{p}$ for $p \equiv 1 \pmod{4}$ and $p \equiv 3 \pmod{4}$ respectively.

Acknowledgements

The author would like to thank Simon Rubinstein-Salzedo for clarification on a certain part of the proof of Theorem **2.7**.

References

[CR22] Matias Carl Relyea. *Proofs and Applications of Quadratic Reciprocity*. Academia.edu, 2022.

[IRR90] Kenneth Ireland, Michael Ira Rosen, and Michael Rosen. *A classical introduction to modern number theory*, volume 84. Springer Science & Business Media, 1990.