#A48 INTEGERS 11 (2011)

ENUMERATION OF TRIANGLES IN QUARTIC RESIDUE GRAPHS

Mark Budden
Department of Mathematics and Computer Science, Western Carolina University, Cullowhee, NC
mrbudden@email.wcu.edu

Nicole Calkins
Department of Mathematics, Armstrong Atlantic State University, Savannah, GA
ncalkins28@gmail.com

William Nathan Hack
Department of Mathematics, Armstrong Atlantic State University, Savannah, GA
nathan.hack@gmail.com

Joshua Lambert
Department of Mathematics, Armstrong Atlantic State University, Savannah, GA
Joshua.Lambert@armstrong.edu

Kimberly Thompson
Department of Mathematics, Armstrong Atlantic State University, Savannah, GA
sue144@hotmail.com

Received: 10/10/10, Accepted: 7/19/11, Published: 9/13/11

Abstract

For a fixed prime $p \equiv 1 \pmod 4$, we define the corresponding quartic residue graph and determine the number of triangles contained in such a graph. Our computation requires us to compute the number of pairs of consecutive quartic residues modulo p via the evaluation of certain quartic Jacobi sums.

1. Introduction

Although Raymond Paley's life passed by quickly, his impact resonated across multiple mathematical disciplines such as complex analysis, combinatorics, number theory, and harmonic analysis [2, 8, 9, 10]. Perhaps one of Paley's most notable contributions occurred when he brought the fields of combinatorics and number theory even closer together. One such mathematical achievement came about in

1933, when Paley [8] used the quadratic residues of the field with prime order $p \equiv 3 \pmod 4$ to construct Hadamard matrices of order $p+1$. While Paley passed away that same year, his results spurred a great deal of interest.

One person that took notice of Paley's achievements was Horst Sachs [12]. Sachs defined the appropriately named Paley graphs with vertices given by elements of $\mathbb{F}_p$, where p is a prime power congruent to 1 mod 4, and an edge ab exists in the graph if and only if $a-b$ is a quadratic residue. The reasoning behind Sachs requirement for $p \equiv 1 \bmod 4$ instead of $p \equiv 3 \bmod 4$ becomes clear after recalling the first supplementary law to the law of quadratic reciprocity stating

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

from which we find that -1 is a quadratic residue if and only if $p \equiv 1 \bmod 4$. This allows us to notice the importance of $p \equiv 1 \bmod 4$ in Sachs construction since ab being an edge gives both $a-b$ and $b-a$ are quadratic residues of p. From the study of Paley graphs came a larger class of self-complementary graphs allowing for convenient lower bounds in Ramsey theory. Paley graphs also have a natural counterpart, Paley digraphs, which call upon the experience of their originator Paley by considering a digraph with vertices given by $\mathbb{F}_p$, where $p \equiv 3 \bmod 4$, and an arc from a to b is formed if $b-a$ is a quadratic residue of p [4]. The construction of tournaments became an immediate consequence of the Paley digraphs, which led to many mathematicians looking for more ties between quadratic residues and graphs.

Bommireddy Maheswari and Madhavi Lavaku have been the most recent addition to the long list of mathematicians looking for such ties. In a recent paper [7], the aforementioned authors considered quadratic residue graphs, which strongly resemble the ideas behind Paley graphs and digraphs. Quadratic residue graphs are defined as having vertices that coincide with elements of $\mathbb{F}_p$ where p is an odd prime and the vertices a and b are adjacent if and only if either $a-b$ or $b-a$ is a quadratic residue of p. This leads to the quadratic residue graph, which we shall denote by $G_2(p)$, coinciding with a Paley graph when $p \equiv 1 \bmod 4$ and a complete graph when $p \equiv 3 \bmod 4$ (which also happens to be the underlying graph of a Paley digraph). The beauty behind Maheswari and Lavaku's article is the ability to make a connection between the pairs of consecutive quadratic residues in $\mathbb{F}_p$ and the number of triangles in $G_2(p)$ when $p \equiv 1 \pmod 4$.

We wish to expand upon Maheswari and Lavaku's results on quadratic residue graphs by considering the quartic analogues of their work. However, before we proceed, we must introduce some notation and recall some of the facts surrounding quadratic and quartic residuacity. It is well-known that for an odd prime p the multiplicative group $\mathbb{F}_p^\times$ is cyclic. Thus, $\mathbb{F}_p^\times$ has a unique subgroup of order $\frac{p-1}{2}$ consisting of the quadratic residues modulo p (i.e., the squares in $\mathbb{F}_p^\times$). We shall denote this subgroup by $\mathbb{F}_p^{\times 2}$. Similarly, if we assume that $p \equiv 1 \pmod 4$, there exists a unique subgroup of order $\frac{p-1}{4}$ consisting of the quartic residues (i.e., the

fourth powers in $\mathbb{F}_p^\times$), which we denote by $\mathbb{F}_p^{\times 4}$. Since every fourth power is a square, it follows that $\mathbb{F}_p^{\times 4} \subset \mathbb{F}_p^{\times 2}$.

Thus, if p is an odd prime, then the vertex set of $G_2(p)$ is $V(G_2(p)) = \mathbb{F}_p$ and the edge set is given by

$$E(G_2(p)) = \{ab \mid a - b \in \mathbb{F}_p^{\times 2} \text{ or } b - a \in \mathbb{F}_p^{\times 2}\}.$$

An immediate consequence of the definition of $G_2(p)$ is that when $p \equiv 1 \pmod 4$, the graph $G_2(p)$ has exactly $\frac{p(p-1)}{4}$ edges. A natural extension from this class of quadratic residue graphs is the quartic residue graph. If we assume that $p \equiv 1 \pmod 4$, then the quartic residue graph $G_4(p)$ is defined to have vertex set $V(G_4(p)) = \mathbb{F}_p$ and edge set

$$E(G_4(p)) = \{ab \mid a - b \in \mathbb{F}_p^{\times 4} \text{ or } b - a \in \mathbb{F}_p^{\times 4}\}.$$

These quartic residue graphs provide us with an example of an infinite class of circulant graphs. Analogous to the quadratic case, we see that $G_4(p)$ is isomorphic to $G_2(p)$ if and only if $p \equiv 5 \pmod 8$. In the case where $p \equiv 1 \pmod 8$, $G_4(p)$ creates a new class of graphs with $\frac{p(p-1)}{8}$ edges (for example, Figure 1 provides the graph $G_4(17)$). Such graphs shall be the focal point of this article.

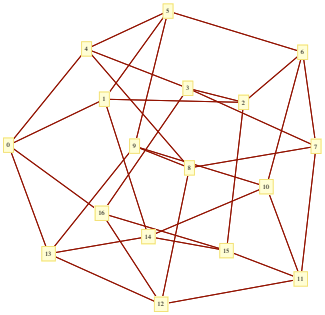

Figure 1: The quartic residue graph for the prime 17.

In Section 2, we will extend the work of Maheswari and Lavaku [7] to compute the number of triangles in $G_4(p)$ when $p \equiv 1 \pmod 4$. We find that if $p \equiv 1 \pmod 8$, then the number of triangles depends upon the number of pairs of consecutive quartic residues of p, which we denote by $N_4(p)$. In Sections 3, 4, and 5, our focus will turn to an explicit evaluation of $N_4(p)$, relying on an explicit evaluation of a certain quartic Jacobi sum. The final section provides a few examples demonstrating the utility of our results.

2. Counting Triangles

Prior to providing an explicit enumeration of triangles in quartic residue graphs, we summarize Maheswari and Lavaku's results [7] for resolving the corresponding problem for quadratic residue graphs. For an odd prime p, let $T(G_2(p))$ denote the number of triangles in the quadratic residue graph $G_2(p)$. Then

$$T(G_2(p)) = \begin{cases} \frac{p(p-1)}{12} N_2(p) & \text{if } p \equiv 1 \pmod 4 \\ \\ \frac{p(p-1)(p-2)}{6} & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

where $N_2(p)$ denotes the number of pairs of consecutive quadratic residues of p. This result does not provide a closed-form for the number of triangles when $p \equiv 1 \pmod 4$ since it depends on $N_2(p)$. However, one can find a closed-form for $N_2(p)$ in Section 10.1 of Andrews' book [1], where it is proved that for any odd prime p,

$$N_2(p) = \frac{1}{4}(p - 4 - (-1)^{(p-1)/2}).$$

Thus, when $p \equiv 1 \pmod 4$, we have

$$T(G_2(p)) = \frac{1}{48} p(p-1)(p-5).$$

Now assume $p \equiv 1 \pmod 4$ and let $T(G_4(p))$ denote the number of triangles in $G_4(p)$. We noted in Section 1 that $p \equiv 5 \pmod 8$ leads to $G_4(p) = G_2(p)$ and the problem of counting triangles is reduced to the result just described. The case $p \equiv 1 \pmod 8$ is addressed by the following theorem.

Theorem 1. *If $p \equiv 1 \pmod 8$ is a prime, then the number of triangles in the quartic residue graph $G_4(p)$ is given by*

$$T(G_4(p)) = \frac{p(p-1)}{24} N_4(p),$$

where $N_4(p)$ denotes the number of pairs of consecutive quartic residues of p.

Proof. We refer to a triangle in $G_4(p)$ as a *fundamental triangle* if it has 0 and 1 included in its vertices. Then the set of fundamental triangles is given by

$$\Delta_1 := \{(0, 1, b) \mid b, b-1 \in \mathbb{F}_p^{\times 4}\}.$$

It follows that a 3-tuple $(0, 1, b)$ is a fundamental triangle if and only if $b-1$ and b are a pair of consecutive quartic residues. Thus,

$$|\Delta_1| = N_4(p).$$

Now for each $a \in \mathbb{F}_p^{\times 4}$, we define the set of triangles

$$\Delta_a := \{(0, a, b) \mid b, b - a \in \mathbb{F}_p^{\times 4}\}.$$

Let $f : \Delta_1 \longrightarrow \Delta_a$ be the map given by

$$f(0, 1, b) \longrightarrow (0, a, ab).$$

To see that f is one-to-one, suppose that

$$f(0, 1, b_1) = f(0, 1, b_2), \qquad \text{for } b_1, b_2 \in \mathbb{F}_p^{\times 4}.$$

Then $(0, a, ab_1) = (0, a, ab_2)$, which gives $ab_1 = ab_2$. Since $\mathbb{F}_p^{\times 4}$ is a group, a has a multiplicative inverse, implying $b_1 = b_2$. We also note that f is onto since an arbitrary triangle $(0, a, b) \in \Delta_a$ satisfies

$$f(0, 1, a^{-1}b) = (0, a, b).$$

Again, we are using the fact that $\mathbb{F}_p^{\times 4}$ is a multiplicative group to justify the existence of a^{-1} and the fact that $a^{-1}b \in \mathbb{F}_p^{\times 4}$. Thus, we have shown that

$$|\Delta_a| = |\Delta_1| = N_4(p)$$

for all $a \in \mathbb{F}_p^{\times 4}$. If we wish to count all of the triangles that have 0 as a vertex, we consider the union

$$\bigcup_{a \in \mathbb{F}_p^{\times 4}} \Delta_a,$$

which is not disjoint. In fact, $(0, a, b)$ and $(0, b, a)$ represent the same triangle, from which we conclude that each triangle is counted twice in this union. Hence,

$$\left| \bigcup_{a \in \mathbb{F}_p^{\times 4}} \Delta_a \right| = \frac{p-1}{8} N_4(p).$$

Now recall that $G_4(p)$ is a regular graph. Thus, every one of the p vertices has the same number of triangles containing that vertex. After accounting for all of the vertices in $G_4(p)$, we notice that each triangle has been counted three times. Thus,

$$T(G_4(p)) = \frac{p(p-1)}{24} N_4(p)$$

gives the total number of triangles when $p \equiv 1 \pmod 8$. □

An immediate consequence of Theorem 5 worth noting is what occurs when $p \not\equiv 1 \pmod 3$. We see that if $p \equiv 2 \pmod 3$ (still assuming that $p \equiv 1 \pmod 8$), then $N_4(p)$ is necessarily divisible by 3 (otherwise, $T(G_4(p))$ would not be an integer).

3. Pairs of Consecutive Quartic Residues

In this section, we begin with the calculation of $N_4(p)$ following the ideas behind Andrews' approach in Section 10.1 of [1]. Since our focus has shifted to quartic residues, we must define the quartic residue symbol. Like the Legendre symbol, which we denote by $\left(\frac{\cdot}{p}\right)$, the quartic residue symbol will tell us when a nonzero element in $\mathbb{Z}/p\mathbb{Z}$ is a fourth power. However, unlike the Legendre symbol (which only takes on the values ± 1), the quartic residue symbol takes on values in the fourth roots of unity. As a result, the majority of our work must be done within the ring of Gaussian Integers $\mathbb{Z}[i]$. The reader is referred to Sections 9.7 and 9.8 in Ireland and Rosen's book [5] for a more thorough introduction to the quartic residue symbol.

Unless otherwise stated, we assume that $p \equiv 1 \pmod 4$ is a prime. In this case, p splits in $\mathbb{Z}[i]$ as $p = \pi\overline{\pi} = (a+bi)(a-bi)$ for some $a, b \in \mathbb{Z}$. Since $\mathbb{Z}[i]$ is a unique factorization domain, this description is unique up to associates and we may single out a particular associate by requiring that π be primary (i.e., $\pi \equiv 1 \pmod{2+2i}$). However, this designation of prime will not be necessary until Section 4. In order to enumerate the consecutive quartic residues in $(\mathbb{Z}/p\mathbb{Z})^\times$, our work shall begin in $\mathbb{Z}[i]$ and be completed in $\mathbb{Z}$ via the isomorphism

$$\mathbb{Z}[i]/\pi\mathbb{Z}[i] \cong \mathbb{Z}/p\mathbb{Z}.$$

This isomorphism is made explicit by noting that $0, 1, \ldots, p-1$ are incongruent modulo π and may be used as the distinct coset representatives in $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$. Similar to $\mathbb{Z}/p\mathbb{Z}$, we will often just use $0, 1, \ldots, p-1$ when referring to the left cosets of $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ containing these elements.

For the prime $\pi \in \mathbb{Z}[i]$ (subject to the above constraints) and an element $\alpha \in \mathbb{Z}[i]$ relatively prime to π, the quartic residue symbol is defined by

$$\left(\frac{\alpha}{\pi}\right)_4 \equiv \alpha^{(p-1)/4} \pmod{\pi}.$$

It defines a group homomorphism

$$\left(\frac{\cdot}{\pi}\right)_4 : (\mathbb{Z}[i]/\pi\mathbb{Z}[i])^\times \longrightarrow \{\pm 1, \pm i\}$$

and may be extended to all of $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ by setting $\left(\frac{\alpha}{\pi}\right)_4 = 0$ whenever α is not relatively prime to π. In order to further familiarize ourselves with the quartic residue symbol we list the following well-known properties below (cf., [5]) which will be used throughout the remainder of this paper.

Properties of the Quartic Residue Symbol. *Let $p \equiv 1 \pmod 4$ be a prime that factors as $p = \pi\overline{\pi}$ in $\mathbb{Z}[i]$ and let $a \in \mathbb{Z}$ be relatively prime to p. If $\alpha \in \mathbb{Z}[i]$ is relatively prime to p, then the quartic residue symbol satisfies the following properties:*

1. $\left(\frac{\alpha}{\pi}\right)_4 = 1$ *if and only if* $x^4 \equiv \alpha \pmod{\pi}$ *is solvable;*
2. $\left(\frac{a}{\pi}\right)_4^2 = \left(\frac{a}{p}\right)$*;*
3. *If* $\left(\frac{a}{p}\right) = 1$*, then* $\left(\frac{a}{\pi}\right)_4 = \pm 1$*;*
4. *If* $\left(\frac{a}{p}\right) = -1$*, then* $\left(\frac{a}{\pi}\right)_4 = \pm i$*;*
5. $\left(\frac{\cdot}{\pi}\right)_4 : (\mathbb{Z}[i]/\pi\mathbb{Z}[i])^\times \longrightarrow \{\pm 1, \pm i\}$ *is a* $\frac{p-1}{4}$*-to-one mapping;*
6. $\left(\frac{-1}{\pi}\right)_4 = (-1)^{(p-1)/4}$.

We begin our evaluation of $N_4(p)$ by considering the expression

$$c_p(n) = \left(1 + \left(\frac{n-1}{\pi}\right)_4\right)\left(1 + \left(\frac{n-1}{\pi}\right)_4^2\right)\left(1 + \left(\frac{n}{\pi}\right)_4\right)\left(1 + \left(\frac{n}{\pi}\right)_4^2\right),$$

which takes on the value 0 unless $n-1$ and n are both quartic residues of p, in which case it takes on the value 16. An immediate consequence of this observation gives

$$N_4(p) = \frac{1}{16}\sum_{n=2}^{p-1} c_p(n).$$

Expanding $c_p(n)$ results in sixteen different sums, many of which are straightforward to evaluate. The first sum is the simplest:

$$\sum_{n=2}^{p-1} 1 = p - 2. \tag{1}$$

Next, we note that the quartic residue symbol (and some of its powers) are nontrivial characters on $(\mathbb{Z}[i]/\pi\mathbb{Z}[i])^\times$ and are subject to the orthogonality relations for characters (see Section 21.1 of [11]). In particular, whenever $\chi : G \longrightarrow \mathbb{C}^\times$ is a nontrivial character of a finite group G, we have

$$\sum_{n \in G} \chi(n) = 0. \tag{2}$$

Applying (2) to the quartic residue symbol yields

$$\sum_{n=2}^{p-1}\left(\frac{n-1}{\pi}\right)_4 = -\left(\frac{-1}{\pi}\right)_4 = -(-1)^{(p-1)/4} \tag{3}$$

and

$$\sum_{n=2}^{p-1}\left(\frac{n}{\pi}\right)_4 = -\left(\frac{1}{\pi}\right)_4 = -1. \tag{4}$$

A similar computation also gives

$$\sum_{n=2}^{p-1}\left(\frac{n-1}{\pi}\right)_4^3 = -(-1)^{(p-1)/4} \tag{5}$$

and

$$\sum_{n=2}^{p-1}\left(\frac{n}{\pi}\right)_4^2 = \sum_{n=2}^{p-1}\left(\frac{n}{\pi}\right)_4^3 = \sum_{n=2}^{p-1}\left(\frac{n-1}{\pi}\right)_4^2 = -1. \tag{6}$$

The remaining sums all involve characters of both $n-1$ and n. For $1 \le i \le 3$ and $1 \le j \le 3$, define

$$S_{i,j} := \sum_{n=2}^{p-1}\left(\frac{n-1}{\pi}\right)_4^i\left(\frac{n}{\pi}\right)_4^j.$$

In the special cases where $i+j=4$, the sums can be evaluated in the following way:

$$\begin{aligned} S_{i,4-i} &= \sum_{n=2}^{p-1}\left(\frac{n-1}{\pi}\right)_4^i\left(\frac{n}{\pi}\right)_4^{4-i}\left(\frac{n^{-1}}{\pi}\right)_4^4 \\ &= \sum_{n=2}^{p-1}\left(\frac{1-n^{-1}}{\pi}\right)_4^i. \end{aligned}$$

As n runs through the interval $2 \le n \le p-1$, so does n^{-1} so that the sum can be written as

$$\begin{aligned} S_{i,4-i} &= \sum_{n=2}^{p-1}\left(\frac{1-n}{\pi}\right)_4^i \\ &= \left(\frac{-1}{\pi}\right)_4^i\sum_{n=2}^{p-1}\left(\frac{n-1}{\pi}\right)_4^i. \end{aligned}$$

Hence, we obtain the sums

$$S_{1,3} = S_{2,3} = S_{3,1} = -1. \tag{7}$$

At this point, we have computed 10 of the 16 sums in the expansion of $N_4(p)$. The six remaining sums are $S_{1,1}$, $S_{1,2}$, $S_{2,1}$, $S_{2,3}$, $S_{3,2}$, and $S_{3,3}$. Instead of evaluating each of these sums individually, we concern ourselves with the evaluation of the sum

$$S := S_{1,1} + S_{1,2} + S_{2,1} + S_{2,3} + S_{3,2} + S_{3,3}.$$

The following theorem reduces the problem of evaluating S to just the evaluation of (the real part of) $S_{1,1}$.

Theorem 2. *Assuming that $p \equiv 1 \pmod 4$ and $S_{i,j}$ and S are defined as above, we have*

$$S = (2 + (-1)^{(p-1)/4})2Re(S_{1,1}),$$

where $Re(z)$ denotes the real part of the complex number z.

Proof. Since the quartic residue symbol is a character of a finite group, we note that $\left(\frac{\cdot}{\pi}\right)_4^{-1} = \overline{\left(\frac{\cdot}{\pi}\right)_4}$, from which it follows that

$$S_{1,1} = \overline{S_{3,3}}, \quad S_{1,2} = \overline{S_{3,2}}, \quad \text{and} \quad S_{2,1} = \overline{S_{2,3}}.$$

Applying the technique that we used to evaluate $S_{i,4-i}$ to $S_{1,1}$ gives

$$\begin{aligned} S_{1,1} &= \sum_{n=2}^{p-1} \left(\frac{n-1}{\pi}\right)_4 \left(\frac{n}{\pi}\right)_4 \left(\frac{n^{-1}}{\pi}\right)_4^4 \\ &= \sum_{n=2}^{p-1} \left(\frac{1-n^{-1}}{\pi}\right)_4 \left(\frac{n^{-1}}{\pi}\right)_4^2 \\ &= \left(\frac{-1}{\pi}\right)_4 \sum_{n=2}^{p-1} \left(\frac{n-1}{\pi}\right)_4 \left(\frac{n}{\pi}\right)_4^2 \\ &= (-1)^{(p-1)/4} S_{1,2}. \end{aligned}$$

Similarly, we also have $S_{3,3} = (-1)^{(p-1)/4} S_{3,2}$. Upon expanding the sum $S_{1,2}$, we find

$$\begin{aligned} S_{1,2} &= \left(\frac{1}{\pi}\right)_4 \left(\frac{2}{\pi}\right)_4^2 + \cdots + \left(\frac{p-2}{\pi}\right)_4 \left(\frac{p-1}{\pi}\right)_4^2 \\ &= \left(\frac{-(p-1)}{\pi}\right)_4 \left(\frac{-(p-2)}{\pi}\right)_4^2 + \cdots + \left(\frac{-2}{\pi}\right)_4 \left(\frac{-1}{\pi}\right)_4^2 \\ &= (-1)^{(p-1)/4} S_{2,1}. \end{aligned}$$

Similarly, we also have $S_{3,2} = (-1)^{(p-1)/4} S_{2,3}$. This yields

$$\begin{aligned} S &= (2 + (-1)^{(p-1)/4})(S_{1,1} + S_{3,3}) \\ &= (2 + (-1)^{(p-1)/4})2Re(S_{1,1}), \end{aligned}$$

which completes the proof of Theorem 2. □

Theorem 2 reduces the evaluation of $N_4(p)$ to the problem of determining the real part of $S_{1,1}$. We will accomplish this task by identifying $S_{1,1}$ with a quartic Jacobi Sum. This computation is the focus of the next section, as it requires us to develop the relevant theory of Gauss and Jacobi Sums.

4. Quartic Gauss and Jacobi Sums

In order to make our notations more consistent with standard treatments on Gauss and Jacobi sums, we will denote the quartic residue symbol modulo π by χ_4, and note that this character defines a Dirichlet character modulo p of order 4 in a natural way. Likewise, we will denote the Legendre symbol modulo p by χ_2 so that $\chi_4^2 = \chi_2$. We find that

$$S_{1,1} = (-1)^{(p-1)/4} \sum_{n=2}^{p-1} \chi_4(n)\chi_4(1-n).$$

This new sum is an example of a Jacobi sum and although the method employed to evaluate it is well-known (cf., Sections 8.3 and 9.9 of [5]), we include it here for completeness.

In general, suppose that $\chi : \mathbb{F}_p^\times \longrightarrow \mathbb{C}^\times$ is a nontrivial (and necessarily primitive) character of order r and define the *Gauss sum* of χ by

$$G(\chi) := \sum_{n=1}^{p-1} \chi(n)\zeta^n,$$

where ζ is the primitive p^{th} root of unity $e^{2\pi i/p}$. For any $m \in \mathbb{F}_p^\times$, the m^{th} *variant Gauss sum* is defined by

$$G_m(\chi) := \sum_{n=1}^{p-1} \chi(n)\zeta^{mn}.$$

By definition, note that $G_m(\chi) \in \mathbb{Z}[\zeta_p, \zeta_r]$.

The connection between $G_m(\chi)$ and $G(\chi)$ is made explicit by

$$\begin{aligned} G_m(\chi) &= \sum_{n=1}^{p-1} \chi(n)\zeta^{mn} \\ &= \overline{\chi}(m) \sum_{n=1}^{p-1} \chi(mn)\zeta^{mn} \\ &= \overline{\chi}(m) \sum_{n'=1}^{p-1} \chi(n')\zeta^{n'} \qquad \text{(letting } \ n' = mn) \\ &= \overline{\chi}(m)G(\chi). \end{aligned}$$

From this, we may compute the product

$$\begin{aligned} G(\chi)\overline{G(\chi)} &= \sum_{m=1}^{p-1} \overline{\chi}(m) G(\chi)\zeta^{-m} \\ &= \sum_{m=1}^{p-1}\sum_{n=1}^{p-1} \chi(n)\zeta^{mn}\zeta^{-m} \\ &= \sum_{n=1}^{p-1} \chi(n) \sum_{m=1}^{p-1} \zeta^{(n-1)m}. \end{aligned}$$

Since the inner sum is given by

$$\sum_{m=1}^{p-1} \zeta^{(n-1)m} = \begin{cases} p & \text{if } n = 1 \\ 0 & \text{if } n \neq 1, \end{cases}$$

we obtain

$$G(\chi)\overline{G(\chi)} = \chi(1)p = p. \tag{8}$$

It is important to note that this relation holds for any nontrivial character of $\mathbb{F}_p^\times$ as we will apply it to both the Legendre and quartic residue symbols.

Now suppose that $\chi, \psi : \mathbb{F}_p^\times \longrightarrow \mathbb{C}^\times$ are any two nontrivial characters. Then the *Jacobi sum* $J(\chi, \psi)$ is defined to be

$$J(\chi, \psi) := \sum_{n=2}^{p-1} \chi(n)\psi(1-n),$$

which is an element of $\mathbb{Z}[\zeta_r]$ where r is the least common multiple of the orders of χ and ψ. We note that some authors define Gauss and Jacobi sums to be the negatives of our definitions (eg., see Section 4.6 of [6]) as this minor modification simplifies the statement of the Davenport-Hasse Theorem on lifted Gauss sums [3]. Since we are only working over $\mathbb{F}_p$ and not over its finite extensions, this modification is omitted from our definitions. The particular Jacobi sum that we need to evaluate in order to complete the evaluation of $S_{1,1}$ is $J(\chi_4, \chi_4)$, and this is the content of the following theorem (cf., Propositions 9.9.3 and 9.9.4 of [5]).

Theorem 3. *Let $p \equiv 1 \pmod 4$ be a prime. If π is the primary prime above p in $\mathbb{Z}[i]$ that is associated with χ_4, then*

$$J(\chi_4, \chi_4) = -\chi_4(-1)\pi.$$

Proof. As χ_4 takes on its values in $\mathbb{Z}[i]$, it is clear that $J(\chi_4,\chi_4)=a+bi$, for some $a,b\in\mathbb{Z}$. Consider the expression

$$\begin{aligned}G(\chi_4)^2 &= \sum_{\substack{1\le m\le p-1\\ 1\le n\le p-1}} \chi_4(m)\chi_4(n)\zeta^{m+n}\\ &= \sum_{\substack{1\le m\le p-1\\ 0\le r\le p-1}} \chi_4(m)\chi_4(r-m)\zeta^{r} \qquad \text{(substituting } r=m+n)\\ &= \sum_{m=1}^{p-1}\chi_4(m)\chi_4(-m)+\sum_{\substack{1\le m\le p-1\\ 1\le r\le p-1}}\chi_4(m)\chi_4(r-m)\zeta^r.\end{aligned}$$

The first sum becomes

$$\sum_{m=1}^{p-1}\chi_4(-1)\chi_4(m)^2=\chi_4(-1)\sum_{m=1}^{p-1}\chi_2(m)=0$$

by the orthogonality relation (2). In the second sum, we make the substitution $t=mr^{-1}$ (which is only possible since $r\in\mathbb{F}_p^\times$):

$$\begin{aligned}\sum_{\substack{2\le t\le p-1\\ 1\le r\le p-1}}\chi_4(tr)\chi_4(r-tr)\zeta^r &= \sum_{\substack{2\le t\le p-1\\ 1\le r\le p-1}}\chi_4(t)\chi_4(r)\chi_4(r)\chi_4(1-t)\zeta^r\\ &= \left(\sum_{r=1}^{p-1}\chi_2(r)\zeta^r\right)\left(\sum_{t=2}^{p-1}\chi_4(t)\chi_4(1-t)\right)\\ &= G(\chi_2)J(\chi_4,\chi_4).\end{aligned}$$

So we have shown that $J(\chi_4,\chi_4)=\frac{G(\chi_4)^2}{G(\chi_2)}$. Then

$$J(\chi_4,\chi_4)\overline{J(\chi_4,\chi_4)}=\frac{\left(G(\chi_4)\overline{G(\chi_4)}\right)^2}{G(\chi_2)\overline{G(\chi_2)}}=p$$

by (8). Thus, $J(\chi_4,\chi_4)\in\mathbb{Z}[i]$ is equal to one of the associates of the primary prime π in $\mathbb{Z}[i]$. In order to determine which one, write

$$\begin{aligned}J(\chi_4,\chi_4) &= \sum_{t=2}^{p-1}\chi_4(t)\chi_4(1-t)\\ &= \sum_{t=2}^{(p-1)/2}\chi_4(t)\chi_4(1-t)+\chi_4\left(\frac{p+1}{2}\right)^2+\sum_{t=(p+3)/2}^{p-1}\chi_4(t)\chi_4(1-t)\\ &= \chi_4\left(\frac{p+1}{2}\right)^2+2\sum_{t=2}^{(p-1)/2}\chi_4(t)\chi_4(1-t).\end{aligned}$$

It can be checked directly that $\chi_4(t) \equiv 1 \pmod{1+i}$ since $\chi_4(t) \in \{\pm 1, \pm i\}$ for any $t \in \mathbb{F}_p^\times$. From this observation, it follows that

$$2 \sum_{t=2}^{(p-1)/2} \chi_4(t)\chi_4(1-t) \equiv 2\left(\frac{p-3}{2}\right) \equiv p-3 \equiv -2 \pmod{2+2i},$$

since $-4 = (2+2i)(-1+i)$ and $p-1$ is divisible by 4. Using the fact that $(p+1)/2$ and 2 are inverses modulo p along with elementary properties of the Legendre and quartic residue symbols, we deduce that $\chi_4\left(\frac{p+1}{2}\right)^2 = \chi_4(2)^2 = \chi_4(-1)$. Thus,

$$J(\chi_4, \chi_4) \equiv \chi_4(-1) - 2 \pmod{2+2i}.$$

Finally, we see that

$$\begin{aligned} -\chi_4(-1)J(\chi_4,\chi_4) &\equiv 2\chi_4(-1) - 1 \pmod{2+2i} \\ &\equiv 1 \pmod{2+2i} \end{aligned}$$

since $\chi_4(-1) = (-1)^{(p-1)/4} = \pm 1$. So, $-\chi_4(-1)J(\chi_4,\chi_4)$ is the primary prime above p in $\mathbb{Z}[i]$ and noting that $\chi_4(-1) = \pm 1$ results in the statement of Theorem 3. □

Now that we have evaluated $J(\chi_4, \chi_4)$, we are in a position to compile all of our results to give an explicit evaluation of $N_4(p)$, and subsequently, $T(G_4(p))$. The next section brings together all of our work.

5. Main Results

The evaluation of $J(\chi_4, \chi_4)$ in Section 4 has provided us with the ability to evaluate $S_{1,1}$. So, we may combine (1), (3), (4), (5), (6), (7), Theorem 2, and Theorem 3 to obtain the following.

Theorem 4. *Let $p \equiv 1 \pmod 4$ be a prime. If $\pi = a+bi$ is a primary prime above p in $\mathbb{Z}[i]$, then the number of pairs of consecutive quartic residues modulo p is given by*

$$N_4(p) = \frac{1}{16}\left(p - 9 - 4a - 2(1+a)(-1)^{(p-1)/4}\right).$$

Applying Theorem 4 to the enumeration of triangles in quartic residue graphs, we deduce our final theorem:

Theorem 5. *Let $p \equiv 1 \pmod 4$ be a prime. If $\pi = a+bi$ is a primary prime above p in $\mathbb{Z}[i]$, then the number of triangles in the quartic residue graph $G_4(p)$ is given by*

$$T(G_4(p)) = \begin{cases} \frac{p(p-1)(p-11-6a)}{384} & \text{if } p \equiv 1 \pmod 8 \\ \\ \frac{p(p-1)(p-5)}{48} & \text{if } p \equiv 5 \pmod 8. \end{cases}$$

6. Examples

When applying Theorems 4 or 5 to specific values of $p \equiv 1 \pmod 4$, it is often simpler to identify a primary prime π above p in $\mathbb{Z}[i]$ by using the fact (see Lemma 6, Section 9.7 of [5]) that $\pi = a + bi$ is primary if any only if

$$a \equiv 1 \pmod 4 \quad \text{and} \quad b \equiv 0 \pmod 4$$

or

$$a \equiv 3 \pmod 4 \quad \text{and} \quad b \equiv 2 \pmod 4.$$

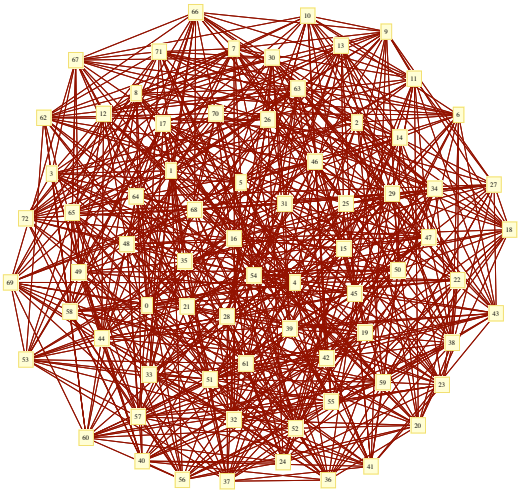

Figure 2: The quartic residue graph $G_4(73)$, demonstrating the difficulty in counting triangles.

Example 6. Consider the prime $p = 73$. When determining the quartic residues by hand, we find the pairs of consecutive quartic residues to be 1 and 2, 8 and 9, 36 and 37, 64 and 65, along with 71 and 72. In this case, $73 = 3^2 + 8^2$ which means that $a = \pm 3$. The associates of $3 + 8i$ are $3 + 8i$, $-3 - 8i$, $-8 + 3i$, and $8 - 3i$. The primary prime in this list is $-3 - 8i$ (since $-3 \equiv 1 \pmod 4$ and $-8 \equiv 0 \pmod 4$). Thus, we take $a = -3$ and apply Theorem 4 to obtain

$$N_4(73) = \frac{1}{16}\left(73 - 9 - 2(1) - (-3)(4 + 2(1))\right) = 5,$$

which agrees with our expected number.

In order to further illustrate the importance of our calculation, we observe Figure 2 and notice the difficulty in determining the number of triangles. With the assistance of Theorem 5, we find there should exist $\frac{73(73-1)5}{24} = 1095$ triangles in $G_4(73)$.

While the previous example may shed some light on the importance of counting the consecutive pairs of quartic residues, our ideas become more prevalent when considering the simpler graph $G_4(41)$.

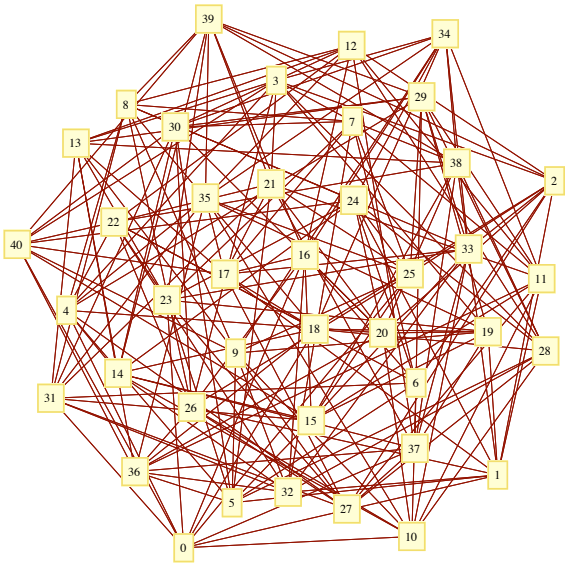

Figure 3: The quartic residue graph $G_4(41)$.

Example 7. We begin by drawing our attention to Figure 3, which shows the graph of $G_4(41)$. Although this graph is relatively small, counting the number of triangles in such a graph is still a daunting task. However, we notice that $41 = 5^2 + 4^2$, which gives us a primary prime of $5 + 4i$. Therefore $a = 5$ and our number of consecutive pairs of quartic residues becomes

$$N_4(41) = \frac{1}{16}\left(41 - 9 - 2(1) - (5)(4 + 2(1))\right) = 0.$$

This immediately tells us that no triangles exist in $G_4(41)$, which is not obvious from our initial observations of the graph.

In this paper, we have merely extended the results of Maheswari and Lavaku [7] to the quartic setting. However, the real significance of this work is the underlying relationship between quadratic and quartic residues and the number of triangles in the relevant graphs. We have appealed to classical methods in number theory to answer a graph-theoretic question. Perhaps it will be possible to take the opposite approach and utilize quadratic and quartic residue graphs to gain some insight into classical problems in number theory.

References

[1] G. Andrews, Number Theory, Dover Publications, Inc., 1971.

[2] B. Bollobás, Random Graphs, Cambridge University Press, 2001.

[3] H. Davenport and H. Hasse, Die nullstellen der kongruenzzetafunktionen in gewissen zyklischen fällen, *J. Reine Angew. Math.* **172** (1934), 151-182.

[4] R. Graham and J. Spencer, A constructive solution to a tournament problem, *Canad. Math. Bull.* **14** (1971), 45-48.

[5] K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory, 2nd edition, Springer-Verlag, 1990.

[6] F. Lemmermeyer, Reciprocity Laws, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000.

[7] B. Maheswari and M. Lavaku, Enumeration of triangles and Hamilton cycles in quadratic residue Cayley graphs, *Chamchuri Journal of Math.* **1** (2009), 95-103.

[8] R. E. A. C. Paley, On orthogonal matrices, *J. Math. Phys.* **12** (1933), 311-320.

[9] R. E. A. C. Paley and A. Zygmund, On some series of functions, *Proc. Camb. Phil. Soc.* **28** (1932), 190-205.

[10] R. E. A. C. Paley, N. Wiener, and A. Zygmund, Notes on random functions, *Math. Zeitschrift* **37** (1932), 647-668.

[11] P. Ribenboim, Classical Theory of Algebraic Numbers, Universitext, Springer-Verlag, New York, 2001.

[12] H. Sachs, Über selbstkomplementäre graphen, *Publicationes Math.* **9** (1962), 270-288.