GAUSS SUMS & REPRESENTATION BY TERNARY QUADRATIC FORMS

EDNA JONES

1. Background & Introduction

Mathematicians have been interested in the sum of squares for several centuries. The following historical background can be found in Grosswald's *Representations of Integers as Sums of Squares* [Gro85]. Diophantus (325–409 A.D.) discussed several problems connected with the Diophantine equation

$$x^2 + y^2 = n. \tag{1.1}$$

It appears that Girard (1595–1632) was the first to state the correct necessary and sufficient conditions on n for the solvability of (1.1) in the integers. Girard had the following conditions on n: n has to be a square, a prime $p \equiv 1 \pmod 4$, a product of such numbers, or the product of one of the preceding with a power of 2. There is no indication that Girard had (or even claimed to have) a proof for his statement.

Shortly afterward, Fermat (1601–1665), most likely independently, stated, as a condition on odd n, that $n \equiv 1 \pmod 4$ and that when n is divided by its largest square factor, the quotient should not contain any prime $q \equiv 3 \pmod 4$. In this statement, Fermat leaves out the even integers, but it appears from some of his other remarks that Fermat knew the complete theorem. Fermat claimed to have an "irrefutable proof" [Gro85, p. 14] of his statement. Although his proof was never made public, from Fermat's letters to Descartes and Mersenne, it seems that Fermat had a proof based on the method of descent.

However, according to Gauss, it was Euler (1707–1783) who gave the first known proof of a statement which is essentially equivalent to the following theorem.

Theorem 1.1. *The Diophantine equation* (1.1) *is solvable if and only if all prime divisors p of m with $p \equiv 3 \pmod 4$ occur in n to an even power.*

A proof of Theorem 1.1 can be found in Chapter 2 of Grosswald's *Representations of Integers as Sums of Squares* [Gro85].

Mathematicians have not been solely interested in the sum of two squares over the centuries; they have also been interested in the sum of three or more squares. However, for the remainder of this paper, we are primarily interested in the sum of three squares, with possibly some of the squares being multiplied by a positive integer before being added to the other squares. Before we state the general problem discussed in this paper, we discuss a well-known question related to a special case of the problem concerning the sum of three squares: What are the conditions on n if the Diophantine equation

$$x_1^2 + x_2^2 + x_3^2 = n \tag{1.2}$$

has solutions in integers x_i $(i = 1, 2, 3)$?

Diophantus gave a condition for the solvability of (1.2) if $n \equiv 1 \pmod 3$. Diophantus's condition for $n \equiv 1 \pmod 3$ is essentially equivalent to $n \neq 24k + 7$ for some integer k.

Bachet (1581–1638) found Diophantus's condition insufficient and added the condition that $n \neq 96k + 28$ some k. Fermat deemed that Bachet's conditions were insufficient and formulated the correct conditions. In a letter to Mersenne, Fermat stated that no integer of the form $8k + 7$ is the sum of three squares. Particular cases of representations as sums of three squares were considered by Descartes (1596–1650), Euler, Lagrange (1736–1813), Legendre (1752–1833), and others. In 1798, Legendre became the first person known to provide a proof of the following theorem which now bears his name.

Theorem 1.2 (Legendre's Three-Square Theorem)**.** *The Diophantine equation*

$$x_1^2 + x_2^2 + x_3^2 = n$$

has solutions in integers x_i ($i = 1, 2, 3$) if and and only if n is not of the form $4^a(8k + 7)$ with $a, k \in \mathbb{Z}$.

A proof of Legendre's Three-Square Theorem can be found in Chapter 4 of Grosswald's *Representations of Integers as Sums of Squares* [Gro85].

We consider a generalization of the sum of three squares problem involving positive definite ternary quadratic forms. Let $Q(\vec{\mathbf{x}}) = Q(x_1, x_2, x_3)$ be some positive definite ternary quadratic form with integral coefficients. We say that an integer m is *(globally) represented* by Q if there exists $\vec{\mathbf{x}} \in \mathbb{Z}^3$ such that $Q(\vec{\mathbf{x}}) = m$. As evidenced by the historical discussion, while attempting to answer the question of when is m is globally represented by an integral quadratic form Q, numerous mathematicians have considered the weaker condition of m being *locally represented (everywhere)* by Q, meaning that m is locally represented at p for every prime p and there exists $\vec{\mathbf{x}} \in \mathbb{R}^3$ such that $Q(\vec{\mathbf{x}}) = m$. An integer m is *locally represented by Q at the prime p* if for every nonnegative integer k there exists $\vec{\mathbf{x}} \in \mathbb{Z}^3$ such that $Q(\vec{\mathbf{x}}) \equiv m \pmod{p^k}$.

In 1988, Duke [Duk88] proved that every sufficiently large square-free integer that is locally represented everywhere by Q is globally represented by Q as an application of bounds for sums of Kloosterman sums given by Iwaniec [Iwa87]. In 2005, Duke quantified sufficiently large in terms of the determinant D of Q, where the determinant of Q is defined by the 3×3 determinant

$$D = \det(\partial^2 Q / \partial x_i \partial x_j).$$

Theorem 1.3 (W. Duke, [Duk05])**.** *There is an absolute constant $c > 0$ so that $Q(\vec{\mathbf{x}}) = m$ has integral solution provided that*

$$m > cD^{337}$$

is square-free and that the congruence $Q(\vec{\mathbf{x}}) \equiv m \pmod{8D^3}$ has a solution. The constant c is ineffective.

Let $S(Q)$ be the set of square-free integers that are locally represented everywhere by the quadratic form Q but are not globally represented by Q. Theorem 1.3 says the cardinality of $S(Q)$ is finite and gives an asymptotic bound on $\max(S(Q))$. Theorem 1.3 raises several questions: How sharp is this bound? Is D the best measure of this lower bound? This paper attempts to find a lower bound using computational methods. Let $S(Q, n)$ be the set of elements in $S(Q)$ that are less than n. Sage code that computes $S(Q, n)$ under certain conditions can be found in Appendix C.

A quadratic form Q is called *regular* if every integer locally represented everywhere by Q is globally represented by Q. We see from the definition of regular that if the quadratic form

Q is regular then $S(Q) = \emptyset$. In 1939, Jones and Pall [JP39, p. 190] provided a list of all primitive regular quadratic forms of the form $ax^2 + by^2 + cz^2$ with $0 < a \leq b \leq c$.

One of the most well-known regular positive definite ternary quadratic forms is $Q(\vec{\mathbf{x}}) = x_1^2 + x_2^2 + x_3^2$, the sum of three squares. The fact that this quadratic form is regular follows from Legendre's Three-Square Theorem.

We focus on the cases when Q is a positive definite diagonal integer-matrix ternary quadratic form, meaning that Q can written as $Q(\vec{\mathbf{v}}) = ax^2 + by^2 + cz^2$, where a, b, and c are positive integers and $\vec{\mathbf{v}} = (x, y, z)^T$. Under these conditions, the discriminant of Q is $D = 8abc$.

It is not immediately apparent how one can check that m is locally represented everywhere by Q, because it appears from the definition of locally represented everywhere that one would have to check if m is locally represented by Q at infinitely-many primes and that, for each prime p, one would need to check for infinitely-many $k \geq 0$ that there exists $\vec{\mathbf{v}} \in \mathbb{Z}^3$ such that $Q(\vec{\mathbf{v}}) \equiv m \pmod{p^k}$. This problem is partially addressed in Section 3.

The definition of local representation suggests that we should count the number of solutions to the congruence $Q(\vec{\mathbf{v}}) \equiv m \pmod{p^k}$ for $k \geq 0$, which we denote as $r_{p^k,Q}(m)$. For a positive integer n, we define $r_{n,Q}(m)$ as

$$r_{n,Q}(m) = \#\left\{\vec{\mathbf{v}} \in (\mathbb{Z}/n\mathbb{Z})^3 : Q(\vec{\mathbf{v}}) \equiv m \pmod{n}\right\}.$$

We note that an integer m is locally represented by Q at p if and only if $r_{p^k,Q}(m) > 0$ for every $k \geq 0$. Furthermore, if $r_{p^n,Q}(m) > 0$, then $r_{p^k,Q}(m) > 0$ for any $0 \leq k \leq n$.

To compute $r_{p^k,Q}(m)$, we use quadratic Gauss sums, $G\left(\frac{a}{q}\right)$. Unless otherwise specified, the term Gauss sum is taken to refer to a quadratic Gauss sum. Many Gauss sums have closed-form evaluations, some of which are found in Section 2.

In Section 3, we show that for the quadratic form $Q(\vec{\mathbf{v}}) = ax^2 + by^2 + cz^2$,

$$r_{p^k,Q}(m) = \frac{1}{p^k} \sum_{t=0}^{p^k-1} \mathrm{e}\left(\frac{-mt}{p^k}\right) G\left(\frac{at}{p^k}\right) G\left(\frac{bt}{p^k}\right) G\left(\frac{ct}{p^k}\right). \tag{1.3}$$

The form of (1.3) suggests that we can compute $r_{p^k,Q}(m)$ using the fast Fourier transform (FFT). We explain how this is possible in Section 3.1.

Although Section 3.1 describes how $r_{p^k,Q}(m)$ can be computed using the FFT, it does not say how large k must be to determine if an integer m is locally represented everywhere by Q. In Section 3.2, we use a version of Hensel's Lemma to determine how large k must be to decide local representation at a prime p.

In Section 3.2, we use Gauss sums and Hensel's Lemma to find some closed-form formulas for $r_{p^k,Q}(m)$. We start with when p is an odd prime. Theorem 3.6 says that if $p \nmid m$, then

$$r_{p^k,Q}(m) = \begin{cases} p^{2k}\left(1 + \frac{1}{p}\left(\frac{-abcm}{p}\right)\right), & \text{if } p \nmid abc, \\ p^{2k}\left(1 - \frac{1}{p}\left(\frac{-ab}{p}\right)\right), & \text{if } p \nmid ab \text{ and } p \mid c, \\ p^{2k}\left(1 + \left(\frac{am}{p}\right)\right), & \text{if } p \nmid a,\ p \mid b, \text{ and } p \mid c. \end{cases}$$

Theorem 3.10 states that if $p \nmid abc$ and $m = m_0 p$, where $\gcd(m_0, p) = 1$, then

$$r_{p^k,Q}(m) = \begin{cases} p^2 & \text{if } k = 1, \\ p^{2k}\left(1 - \dfrac{1}{p^2}\right), & \text{if } k \geq 2. \end{cases}$$

From Theorem 3.6 and Theorem 3.10, we can conclude that if p is an odd prime, $p \nmid abc$, and m is square-free, then $r_{p^k,Q}(m) > 0$ for all k. This implies that m is locally represented at the prime p if m is square-free and $p \nmid abc$.

Theorem 3.11 says that if $p \nmid ab$, $c = c_0 p$, $m = m_0 p$, and $k \geq 2$, where $\gcd(m_0, p) = 1$ and $c_0 \in \mathbb{Z}$, then

$$r_{p^k,Q}(m) = \begin{cases} p^{2k}\left(1 + \dfrac{1}{p}\left(\dfrac{c_0 m_0}{p}\right) + \left(\dfrac{-ab}{p}\right)\left(1 - \dfrac{1}{p}\right)\right), & \text{if } p \nmid ab \text{ and } p \parallel c, \\ p^{2k}\left(1 - \dfrac{1}{p}\right)\left(1 + \left(\dfrac{-ab}{p}\right)\right), & \text{if } p \nmid ab \text{ and } p^2 \mid c. \end{cases}$$

Combined with Theorems 3.6 and 3.10, Theorem 3.11 allows us to determine if a square-free integer m is locally represented at the odd prime p given that a, b, and c are pairwise coprime.

Theorem 3.16 states if $2 \nmid abc$ and $k \geq 3$, then

$$r_{2^k,Q}(m) = \begin{cases} 2^{2k}\left(1 + \dfrac{1}{16}\left(\dfrac{2}{abcm}\right)\left(\kappa_w + \lambda_w\left(\dfrac{-1}{m}\right)\right) + \dfrac{1}{8}\lambda_w\left(\dfrac{-1}{m}\right)\right), & \text{if } 2 \nmid m, \\ 2^{2k}\left(1 - \dfrac{1}{8}\kappa_w\right), & \text{if } 2 \parallel m, \end{cases}$$

where w is the number of elements in $\{a, b, c\}$ that are congruent to 3 (mod 4), $\kappa_w = 4(-w^2 + 3w - 1)$, and $\lambda_w = 4 \cdot (-1)^{\lfloor w/2 \rfloor}$. Theorem 3.16 allows us to determine if a square-free integer m is locally represented at the prime 2 given that a, b, and c are odd. Therefore, from Theorems 3.6, 3.10, 3.11, and 3.16, we can determine if a square-free integer m is locally represented everywhere by Q given that a, b, and c are odd and pairwise coprime.

In Section 4, we discuss patterns found in numerical computations done concerning the integers locally represented everywhere but not globally represented by certain quadratic forms. The numerical computations used some of the formulas found in Section 3. In Section 5, we summarize our results, describe open questions, and suggest areas for future research.

2. Formulas for Gauss Sums

Suppose $a, q \in \mathbb{Z}$ with $q > 0$. The *quadratic Gauss sum* $G\left(\dfrac{a}{q}\right)$ *over* $\mathbb{Z}/q\mathbb{Z}$ is defined by

$$G\left(\frac{a}{q}\right) := \sum_{j \pmod q} \mathrm{e}\left(\frac{aj^2}{q}\right) = \sum_{j \in \mathbb{Z}/q\mathbb{Z}} \mathrm{e}\left(\frac{aj^2}{q}\right) = \sum_{j=0}^{q-1} \mathrm{e}\left(\frac{aj^2}{q}\right),$$

where $\mathrm{e}(w) = e^{2\pi i w}$. Throughout this paper, we abbreviate $e^{2\pi i w}$ as $\mathrm{e}(w)$.

Throughout this section, take a to be an integer. The formulas in this section are useful in computing $r_{p^k,Q}(m)$. (See Section 3 to see how quadratic Gauss sums can be used to compute $r_{p^k,Q}(m)$.) Appendix A contains code written for Sage that can compute the quadratic Gauss sums mentioned in the current section.

This first sum is not a quadratic Gauss sum but is used to compute Gauss sums and $r_{p^k,Q}(m)$.

Lemma 2.1. *Let $a, q \in \mathbb{Z}$ and $q > 0$. Then*

$$\sum_{t=0}^{q-1} \mathrm{e}\left(\frac{at}{q}\right) = \begin{cases} q, & \text{if } a \equiv 0 \pmod{q}, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Since $\mathrm{e}\left(\frac{at}{q}\right)$ is a character of a group of order q, the lemma follows from the orthogonality of characters [Apo76, Theorem 6.10, p. 136]. □

The following lemma is a generalization of Lemma 2.1.

Lemma 2.2. *Let $a, n, q \in \mathbb{Z}$, $n > 0$, and $q > 0$. Then*

$$\sum_{t=0}^{nq-1} \mathrm{e}\left(\frac{at}{q}\right) = \begin{cases} nq, & \text{if } a \equiv 0 \pmod{q}, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Suppose $a \equiv 0 \pmod{q}$. Then there exists $\alpha \in \mathbb{Z}$ such that $a = \alpha q$. Therefore,

$$\sum_{t=0}^{nq-1} \mathrm{e}\left(\frac{at}{q}\right) = \sum_{t=0}^{nq-1} \mathrm{e}\left(\frac{\alpha q t}{q}\right) = \sum_{t=0}^{nq-1} \mathrm{e}(\alpha t) = \sum_{t=0}^{nq-1} e^{2\pi i \alpha t} = \sum_{t=0}^{nq-1} 1 = nq.$$

Suppose $a \not\equiv 0 \pmod{q}$. Note that $\mathrm{e}(0) = \mathrm{e}(an) = \mathrm{e}\left(\frac{anq}{q}\right)$. Thus,

$$\begin{aligned} \sum_{t=0}^{nq-1} \mathrm{e}\left(\frac{at}{q}\right) &= \mathrm{e}\left(\frac{a \cdot 0}{q}\right) + \sum_{t=1}^{nq-1} \mathrm{e}\left(\frac{at}{q}\right) \\ &= \mathrm{e}(0) + \sum_{t=1}^{nq-1} \mathrm{e}\left(\frac{at}{q}\right) \\ &= \mathrm{e}\left(\frac{anq}{q}\right) + \sum_{t=1}^{nq-1} \mathrm{e}\left(\frac{at}{q}\right) \\ &= \sum_{t=1}^{nq} \mathrm{e}\left(\frac{at}{q}\right). \end{aligned}$$

Mapping $t \mapsto t + 1$, we find that

$$\begin{aligned} \sum_{t=0}^{nq-1} \mathrm{e}\left(\frac{at}{q}\right) = \sum_{t=1}^{nq} \mathrm{e}\left(\frac{at}{q}\right) &= \sum_{t=0}^{nq-1} \mathrm{e}\left(\frac{a(t+1)}{q}\right) \\ &= \sum_{t=0}^{nq-1} \mathrm{e}\left(\frac{at}{q}\right) \mathrm{e}\left(\frac{a}{q}\right) \\ &= \mathrm{e}\left(\frac{a}{q}\right) \sum_{t=0}^{nq-1} \mathrm{e}\left(\frac{at}{q}\right). \end{aligned}$$

Because $a \not\equiv 0 \pmod{q}$, $\mathrm{e}\left(\frac{a}{q}\right) = e^{2\pi i a/q} \neq 1$. By subtracting $\mathrm{e}\left(\frac{a}{q}\right) \sum_{t=0}^{nq-1} \mathrm{e}\left(\frac{at}{q}\right)$ from both sides of previous equation, we get

$$\left(1 - \mathrm{e}\left(\frac{a}{q}\right)\right) \sum_{t=0}^{nq-1} \mathrm{e}\left(\frac{at}{q}\right) = 0.$$

Since $\mathrm{e}\left(\frac{a}{q}\right) \neq 1$, the last equation implies that $\sum_{t=0}^{nq-1} \mathrm{e}\left(\frac{at}{q}\right) = 0$. □

The next lemma follows immediately from Lemma 2.1. It gives the value of the exponential sum $\sum_{t=1}^{q-1} \mathrm{e}\left(\frac{at}{q}\right)$ if $a \not\equiv 0 \pmod{q}$.

Lemma 2.3. *Let $a, q \in \mathbb{Z}$ and $q > 0$. If $a \not\equiv 0 \pmod{q}$*

$$\sum_{t=1}^{q-1} \mathrm{e}\left(\frac{at}{q}\right) = -1.$$

Proof. By Lemma 2.1,

$$1 + \sum_{t=1}^{q-1} \mathrm{e}\left(\frac{at}{q}\right) = \mathrm{e}\left(\frac{a \cdot 0}{q}\right) + \sum_{t=1}^{q-1} \mathrm{e}\left(\frac{at}{q}\right) = \sum_{t=0}^{q-1} \mathrm{e}\left(\frac{at}{q}\right) = 0.$$

By rearranging terms in the last equation, we get the result of the lemma. □

We now provide a link between Gauss sums and exponential sums.

Lemma 2.4. *Suppose p is an odd prime and $a \in \mathbb{Z}$. Then*

$$G\left(\frac{a}{p}\right) = \sum_{t=0}^{p-1} \left(1 + \left(\frac{t}{p}\right)\right) \mathrm{e}\left(\frac{at}{p}\right), \tag{2.1}$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol.

If $a \not\equiv 0 \pmod{p}$, then

$$G\left(\frac{a}{p}\right) = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \mathrm{e}\left(\frac{at}{p}\right) = \sum_{t=1}^{p-1} \left(\frac{t}{p}\right) \mathrm{e}\left(\frac{at}{p}\right).$$

Proof. As noted by Cohen [Coh93, p. 27], the number of solutions modulo p of the congruence

$$j^2 \equiv t \pmod{p}$$

is $1 + \left(\frac{t}{p}\right)$. Therefore,

$$G\left(\frac{a}{p}\right) = \sum_{j=0}^{p-1} \mathrm{e}\left(\frac{aj^2}{p}\right) = \sum_{t=0}^{p-1} \left(1 + \left(\frac{t}{p}\right)\right) \mathrm{e}\left(\frac{at}{p}\right).$$

When $a \not\equiv 0 \pmod{p}$,

$$G\left(\frac{a}{p}\right) = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \mathrm{e}\left(\frac{at}{p}\right)$$

follows from (2.1) and Lemma 2.1.

Because $\left(\frac{0}{p}\right) = 0$,

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

□

We now begin to list the values of some Gauss sums. Lemma 2.5 can be used to compute $G\left(\frac{0}{q}\right)$ for any positive integer q.

Lemma 2.5. *Let q be a positive integer. Then*

$$G\left(\frac{0}{q}\right) = q.$$

Proof. By the definition of a quadratic Gauss sum,

$$G\left(\frac{0}{q}\right) = \sum_{j=0}^{q-1} \mathrm{e}\left(\frac{0j^2}{q}\right) = \sum_{j=0}^{q-1} 1 = q.$$

□

The next lemma gives us the value of $G\left(\frac{a}{1}\right)$ for any integer a.

Lemma 2.6. *For any $a \in \mathbb{Z}$,*

$$G\left(\frac{a}{1}\right) = 1.$$

Proof. By definition,

$$G\left(\frac{a}{1}\right) = \sum_{j=0}^{1-1} \mathrm{e}\left(\frac{aj^2}{1}\right) = \sum_{j=0}^{0} \mathrm{e}\left(aj^2\right) = \mathrm{e}\left(a \cdot 0^2\right) = 1.$$

□

Most formulas for a Gauss sum $G\left(\frac{a}{p^k}\right)$ assume that a is coprime to the prime p. The next lemma relates $G\left(\frac{a}{p^k}\right)$ to another Gauss sum $G\left(\frac{a_0}{p^k}\right)$ where a_0 is coprime to p.

Lemma 2.7. *Suppose k is a positive integer, p is a positive prime integer, and $a \neq 0$. Let ℓ be such that $p^\ell \parallel a$. Let $a = a_0 \cdot p^\ell$ so that $\gcd(a_0, p) = 1$. If $\ell \leq k$, then*

$$G\left(\frac{a}{p^k}\right) = p^\ell G\left(\frac{a_0}{p^{k-\ell}}\right). \tag{2.2}$$

Proof. By the definition of a quadratic Gauss sum,

$$G\left(\frac{a}{p^k}\right) = \sum_{j=0}^{p^k-1} \mathrm{e}\left(\frac{aj^2}{p^k}\right) = \sum_{j=0}^{p^k-1} \mathrm{e}\left(\frac{a_0 \cdot p^\ell j^2}{p^k}\right) = \sum_{j=0}^{p^k-1} \mathrm{e}\left(\frac{a_0 j^2}{p^{k-\ell}}\right)$$
$$= p^\ell \sum_{j=0}^{p^{k-\ell}-1} \mathrm{e}\left(\frac{a_0 j^2}{p^{k-\ell}}\right) = p^\ell G\left(\frac{a_0}{p^{k-\ell}}\right).$$

□

Before giving any more formulas for Gauss sums, we define ε_{p^k} and give some properties of ε_{p^k}. For the odd prime p and the positive integer k, define ε_{p^k} as

$$\varepsilon_{p^k} = \begin{cases} 1, & \text{if } p^k \equiv 1 \pmod 4, \\ i, & \text{if } p^k \equiv 3 \pmod 4. \end{cases}$$

Lemma 2.8. *Let p be an odd prime and k be a positive integer. Then $\varepsilon_{p^k}^2 = \left(\frac{-1}{p^k}\right)$ and $\varepsilon_{p^k}^4 = 1$, where $\left(\frac{\cdot}{p^k}\right)$ is the Jacobi symbol.*

Proof. Suppose that $p^k \equiv 1 \pmod 4$. Then $1 = \varepsilon_{p^k} = \varepsilon_{p^k}^2 = \varepsilon_{p^k}^4$. Because $p^k \equiv 1 \pmod 4$, we can write p^k as $p^k = 1 + 4j$. By Theorem 5.9 in LeVeque's *Fundamentals of Number Theory* [LeV96, p. 110],

$$\left(\frac{-1}{p^k}\right) = (-1)^{(p^k-1)/2} = (-1)^{(1+4j-1)/2} = (-1)^{2j} = 1.$$

□

The next lemma follows quickly from Lemma 2.8.

Lemma 2.9. *If p is an odd prime and k is a positive integer, then $\varepsilon_{p^{2k}} = 1$.*

Proof. By Lemma 2.8,

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

By the definition of the Jacobi symbol,

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

□

Now that we have defined ε_{p^k}, we can give a formula for $G\left(\frac{a}{p^k}\right)$ when a and the odd prime p are coprime.

Lemma 2.10. *Suppose k is a positive integer and p is an odd positive prime integer. Suppose $\gcd(a, p) = 1$. Then*

$$G\left(\frac{a}{p^k}\right) = p^{k/2} \left(\frac{a}{p^k}\right) \varepsilon_{p^k},$$

where $\left(\frac{\cdot}{p^k}\right)$ *is the Jacobi symbol.*

Proof. The lemma is a special case of Theorem 1.5.2 in Berndt's, Evans's, and Williams's *Gauss and Jacobi Sums* [BEW98, p. 26]. □

Using Lemmas 2.7 and 2.10, we develop Lemma 2.11 to compute $G\left(\frac{a}{p^k}\right)$ for the odd prime p.

Lemma 2.11. *Suppose k is a positive integer, p is an odd positive prime integer, and $a \neq 0$. Let ℓ be such that $p^\ell \parallel a$. Let $a = a_0 \cdot p^\ell$ so that $\gcd(a_0, p) = 1$. Then*

$$G\left(\frac{a}{p^k}\right) = \begin{cases} p^k, & \text{if } k \leq \ell, \\ p^{(k+\ell)/2}\left(\frac{a_0}{p^{k-\ell}}\right)\varepsilon_{p^{k-\ell}}, & \text{if } k > \ell. \end{cases}$$

Proof.
Suppose $k \leq \ell$. By the definition of a quadratic Gauss sum,

$$G\left(\frac{a}{p^k}\right) = \sum_{j=0}^{p^k-1} \mathrm{e}\left(\frac{aj^2}{p^k}\right) = \sum_{j=0}^{p^k-1} \mathrm{e}\left(\frac{a_0 p^\ell j^2}{p^k}\right) = \sum_{j=0}^{p^k-1} \mathrm{e}\big(a_0 p^{\ell-k} j^2\big) = \sum_{j=0}^{p^k-1} 1 = p^k.$$

Suppose $k > \ell$. By Lemma 2.7, $G\left(\frac{a}{p^k}\right) = p^\ell G\left(\frac{a_0}{p^{k-\ell}}\right)$. We apply Lemma 2.10 to see that

$$G\left(\frac{a}{p^k}\right) = p^\ell p^{(k-\ell)/2}\left(\frac{a_0}{p^{k-\ell}}\right)\varepsilon_{p^{k-\ell}} = p^{(k+\ell)/2}\left(\frac{a_0}{p^{k-\ell}}\right)\varepsilon_{p^{k-\ell}}.$$

□

So far we have mostly considered the Gauss sum $G\left(\frac{a}{q}\right)$ when q is an odd prime power. We would now like to consider $G\left(\frac{a}{q}\right)$ when q is an even prime power, i.e., $q = 2^k$ for some positive integer k. We first consider the value of $G\left(\frac{a}{2}\right)$.

Lemma 2.12.

$$G\left(\frac{a}{2}\right) = \begin{cases} 0, & \text{if } \gcd(a, 2) = 1, \\ 2, & \text{otherwise.} \end{cases}$$

Proof. Write $a = 2a_0 + r$, where $a_0 \in \mathbb{Z}$ and $r = 0$ or 1. By definition of quadratic Gauss sums,

$$\begin{aligned} G\Big(\frac{a}{2}\Big) &= \sum_{j=0}^{2-1} \mathrm{e}\Big(\frac{aj^2}{2}\Big) = \sum_{j=0}^{1} \mathrm{e}\Big(\frac{aj^2}{2}\Big) \\ &= \mathrm{e}\Big(\frac{a\cdot 0^2}{2}\Big) + \mathrm{e}\Big(\frac{a\cdot 1^2}{2}\Big) \\ &= \mathrm{e}(0) + \mathrm{e}\Big(\frac{a}{2}\Big) = 1 + \mathrm{e}\Big(\frac{2a_0+r}{2}\Big) = 1 + \mathrm{e}(a_0)\,\mathrm{e}\Big(\frac{r}{2}\Big) = 1 + \mathrm{e}\Big(\frac{r}{2}\Big) \\ &= 1 + (-1)^r. \end{aligned}$$

If a is odd, then $G\Big(\frac{a}{2}\Big) = 0$. If a is even, then $G\Big(\frac{a}{2}\Big) = 2$. □

Before we compute $G\Big(\frac{a}{2^k}\Big)$ for $k > 1$, we define ρ_a and state some of its properties. For the odd integer a,

$$\rho_a = 1 + i^a = \begin{cases} 1+i, & \text{if } a \equiv 1 \pmod 4, \\ 1-i, & \text{if } a \equiv 3 \pmod 4. \end{cases}$$

Lemma 2.13. *Let a and b be odd integers. If $b \equiv 1 \pmod 4$, then $\rho_{ab} = \rho_a$. If $b \equiv 3 \pmod 4$, then $\rho_{ab} = \bar{\rho}_a$.*

Proof. If $b \equiv 1 \pmod 4$, then

$$ab \equiv a \cdot 1 \equiv a \pmod 4,$$

so $\rho_{ab} = \rho_a$.

Suppose $b \equiv 3 \pmod 4$. If $a \equiv 1 \pmod 4$, then $\rho_a = 1 + i$ and

$$ab \equiv 1 \cdot 3 \equiv 3 \pmod 4.$$

Thus, $\rho_{ab} = 1 - i = \overline{1+i} = \rho_a$ if $a \equiv 1 \pmod 4$.

If $a \equiv 3 \pmod 4$, then $\rho_a = 1 - i$ and

$$ab \equiv 3 \cdot 3 \equiv 1 \pmod 4.$$

Thus, $\rho_{ab} = 1 + i = \overline{1-i} = \rho_a$ if $a \equiv 3 \pmod 4$. □

The next lemma computes $G\Big(\frac{a}{2^k}\Big)$ when a is odd and $k \geq 2$.

Lemma 2.14. *Suppose* $\gcd(a, 2) = 1$ *and* $k \geq 2$. *Then*

$$G\Big(\frac{a}{2^k}\Big) = 2^{k/2} \left(\frac{2^k}{a}\right) \rho_a.$$

Proof. The result follows from Equation 1.5.5 in Proposition 1.5.3 in Berndt's, Evans's, and Williams's *Gauss and Jacobi Sums* [BEW98, p. 26] . □

As seen in the next lemma, we can compute $G\Big(\frac{a}{2^k}\Big)$ using Lemmas 2.7 and 2.14.

Lemma 2.15. *Suppose $k \geq 2$ is an integer and $a \neq 0$. Let ℓ be such that $2^\ell \parallel a$. Let $a = a_0 \cdot 2^\ell$ so that $\gcd(a_0, 2) = 1$. Then*

$$G\Big(\frac{a}{2^k}\Big) = \begin{cases} 2^k, & \text{if } k \leq \ell, \\ 0, & \text{if } k = \ell + 1, \\ 2^{(k+\ell)/2} \left(\dfrac{2^{k-\ell}}{a_0}\right) \rho_{a_0}, & \text{if } k > \ell + 1. \end{cases}$$

Proof.

By definition of a quadratic Gauss sum,

$$G\Big(\frac{a}{2^k}\Big) = \sum_{j=0}^{2^k-1} \mathrm{e}\Big(\frac{aj^2}{2^k}\Big) = \sum_{j=0}^{2^k-1} \mathrm{e}\Big(\frac{a_0 \cdot 2^\ell j^2}{2^k}\Big).$$

If $k \leq \ell$, then

$$\sum_{j=0}^{2^k-1} \mathrm{e}\Big(\frac{a_0 \cdot 2^\ell j^2}{2^k}\Big) = \sum_{j=0}^{2^k-1} \mathrm{e}\big(a_0 \cdot 2^{\ell-k} j^2\big) = \sum_{j=0}^{p^k-1} 1 = 2^k.$$

Suppose that $k > \ell$. Then by Lemma 2.7, $G\Big(\frac{a}{2^k}\Big) = 2^\ell G\Big(\frac{a_0}{2^{k-\ell}}\Big)$. If $k = \ell + 1$, then by Lemma 2.12, $2^\ell G\Big(\frac{a_0}{2^{k-\ell}}\Big) = 2^\ell G\Big(\frac{a_0}{2}\Big) = 0$. If $k > \ell + 1$, then by Lemma 2.14,

$$2^\ell G\Big(\frac{a_0}{2^{k-\ell}}\Big) = 2^\ell 2^{(k-\ell)/2} \left(\frac{2^{k-\ell}}{a_0}\right) \rho_{a_0} = 2^{(k+\ell)/2} \left(\frac{2^{k-\ell}}{a_0}\right) \rho_{a_0}.$$

□

Now that we have some formulas for Gauss sums, we can develop formulas for $r_{p^k,Q}(m)$. Using Gauss sums, we begin to count the number of local solutions to $Q(\vec{\mathbf{v}}) = ax^2 + by^2 + cz^2$ in the next section.

3. Counting the Number of Local Solutions

Recall that $Q(\vec{\mathbf{v}})$ is a positive definite diagonal ternary quadratic form such that $Q(\vec{\mathbf{v}}) = ax^2 + by^2 + cz^2$, where a, b, and c are positive integers and $\vec{\mathbf{v}} = (x, y, z)^T$.

The definition of local representation suggests that we should calculate $r_{p^k,Q}(m)$, where p is a positive prime integer and k is a nonnegative integer. We note that m is locally represented by Q at p if and only if $r_{p^k,Q}(m) > 0$ for every $k \geq 0$. We restrict our attention to $m \geq 0$, because given the quadratic form $Q(\vec{\mathbf{v}}) = ax^2 + by^2 + cz^2$, where a, b, c are positive integers, there exists $\vec{\mathbf{v}} \in \mathbb{R}^3$ such that $Q(\vec{\mathbf{v}}) = m$ if and only if $m \geq 0$. The case in which $k = 0$ is trivial, because every integer m is congruent to 0 (mod 1), and $\mathbb{Z}/\mathbb{Z}$ contains exactly one element. Thus, $r_{1,Q} = 1$, and so we only consider $k \geq 1$ for the remainder of this paper.

We also only consider primitive quadratic forms so that $\gcd(a, b, c) = 1$. The reason for this is that if $\gcd(a, b, c) = d > 1$, then the primitive quadratic form $\frac{a}{d}x^2 + \frac{b}{d}y^2 + \frac{c}{d}z^2$ gives us enough information to determine which integers are (locally or globally) represented by the quadratic form $ax^2 + by^2 + cz^2$.

The first theorem of this section gives a general formula for $r_{n,Q}(m)$ in terms of Gauss sums.

Theorem 3.1. *Let a, b, c, and n be positive integers. Let $Q(\vec{\mathbf{v}}) = ax^2 + by^2 + cz^2$. Then*

$$r_{n,Q}(m) = \frac{1}{n}\sum_{t=0}^{n-1} \mathrm{e}\left(\frac{-mt}{n}\right) G\left(\frac{at}{n}\right) G\left(\frac{bt}{n}\right) G\left(\frac{ct}{n}\right).$$

Proof. By Lemma 2.1,

$$\frac{1}{n}\sum_{t=0}^{n-1} \mathrm{e}\left(\frac{(Q(\vec{\mathbf{v}})-m)t}{n}\right) = \begin{cases} 1, & \text{if } Q(\vec{\mathbf{v}}) \equiv m \pmod{n}, \\ 0, & \text{otherwise.} \end{cases}$$

Therefore,

$$\begin{aligned} r_{n,Q}(m) &= \sum_{\vec{\mathbf{v}}\in(\mathbb{Z}/n\mathbb{Z})^3} \frac{1}{n}\sum_{t=0}^{n-1} \mathrm{e}\left(\frac{(Q(\vec{\mathbf{v}})-m)t}{n}\right) \\ &= \sum_{x=0}^{n-1}\sum_{y=0}^{n-1}\sum_{z=0}^{n-1} \frac{1}{n}\sum_{t=0}^{n-1} \mathrm{e}\left(\frac{(ax^2+by^2+cz^2-m)t}{n}\right) \\ &= \sum_{x=0}^{n-1}\sum_{y=0}^{n-1}\sum_{z=0}^{n-1} \frac{1}{n}\sum_{t=0}^{n-1} \mathrm{e}\left(\frac{atx^2}{n}\right)\mathrm{e}\left(\frac{bty^2}{n}\right)\mathrm{e}\left(\frac{ctz^2}{n}\right)\mathrm{e}\left(\frac{-mt}{n}\right) \\ &= \frac{1}{n}\sum_{t=0}^{n-1} \mathrm{e}\left(\frac{-mt}{n}\right) \sum_{x=0}^{n-1} \mathrm{e}\left(\frac{atx^2}{n}\right) \sum_{y=0}^{n-1} \mathrm{e}\left(\frac{bty^2}{n}\right) \sum_{z=0}^{n-1} \mathrm{e}\left(\frac{ctz^2}{n}\right) \\ &= \frac{1}{n}\sum_{t=0}^{n-1} \mathrm{e}\left(\frac{-mt}{n}\right) G\left(\frac{at}{n}\right) G\left(\frac{bt}{n}\right) G\left(\frac{ct}{n}\right). \end{aligned}$$

□

The next result is a special case of Theorem 3.1, describing what happens when n is a prime power.

Corollary 3.2. *Let a, b, c, and k be positive integers, and let p be a prime. Let $Q(\vec{\mathbf{v}}) = ax^2 + by^2 + cz^2$. Then*

$$r_{p^k,Q}(m) = \frac{1}{p^k}\sum_{t=0}^{p^k-1} \mathrm{e}\left(\frac{-mt}{p^k}\right) G\left(\frac{at}{p^k}\right) G\left(\frac{bt}{p^k}\right) G\left(\frac{ct}{p^k}\right). \tag{3.1}$$

This may also be written as

$$r_{p^k,Q}(m) = p^{2k} + \frac{1}{p^k}\sum_{t=1}^{p^k-1} \mathrm{e}\left(\frac{-mt}{p^k}\right) G\left(\frac{at}{p^k}\right) G\left(\frac{bt}{p^k}\right) G\left(\frac{ct}{p^k}\right). \tag{3.2}$$

Proof. Take $n = p^k$ in Theorem 3.1 to get (3.1).

If $t = 0$, by Lemma 2.5,

$$\frac{1}{p^k}\mathrm{e}\left(\frac{-mt}{p^k}\right) G\left(\frac{at}{p^k}\right) G\left(\frac{bt}{p^k}\right) G\left(\frac{ct}{p^k}\right) = \frac{1}{p^k}\cdot 1 \cdot p^k \cdot p^k \cdot p^k = p^{2k}.$$

Substituting p^{2k} for the $t = 0$ term in (3.1), we get (3.2). □

Corollary 3.2 shows that quadratic Gauss sums can be used to calculate $r_{p^k,Q}(m)$. Methods involving the fast Fourier transform or Hensel's Lemma can be used to evaluate (3.1) explicitly. Section 3.1 shows how the fast Fourier transform can be used to compute $r_{p^k,Q}(m)$. Section 3.2 uses Hensel's Lemma to evaluate (3.1) explicitly.

3.1. **Using the Fast Fourier Transform.**

The fast Fourier transform (FFT) can be used to relatively quickly calculate $r_{p^k,Q}(m)$ for every $m \in \mathbb{Z}/p^k\mathbb{Z}$. The FFT is a discrete Fourier transform (DFT) algorithm. Let $f(t)$ be a function from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{C}$, where n is a positive integer. Then the DFT creates another function $\hat{f} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ in the following manner:

$$\hat{f}(m) = \sum_{t=0}^{n-1} f(t)\, \mathrm{e}\left(\frac{-mt}{n}\right).$$

Note that if $f : \mathbb{Z}/p^k\mathbb{Z} \to \mathbb{C}$ is defined by $f(t) = \dfrac{1}{p^k} G\left(\dfrac{at}{p^k}\right) G\left(\dfrac{bt}{p^k}\right) G\left(\dfrac{ct}{p^k}\right)$, then

$$r_{p^k,Q}(m) = \hat{f}(m) = \sum_{t=0}^{p^k-1} f(t)\, \mathrm{e}\left(\frac{-mt}{p^k}\right).$$

Therefore, the FFT can be used to calculate $r_{p^k,Q}(m)$ for every $m \in \mathbb{Z}/p^k\mathbb{Z}$. Appendix B contains code written for Sage that can be used to calculate $r_{p^k,Q}(m)$ for every $m \in \mathbb{Z}/p^k\mathbb{Z}$.

3.2. **Using Hensel's Lemma.**

The result of Section 3.1 allows $r_{p^k,Q}(m)$ to be computed for every $m \in \mathbb{Z}/p^k\mathbb{Z}$ using the FFT. However, it does not tell us how large k must be to determine whether an integer m is locally represented everywhere by Q. To help determine this, we use a version of Hensel's Lemma. The following theorem is a version of Hensel's Lemma specific to the quadratic forms being considered in this section.

Theorem 3.3 (Hensel's Lemma for odd prime powers)**.** *Let m be an integer and p be an odd positive prime integer. Suppose $\vec{\mathbf{v}}_0 = (x_0, y_0, z_0)^T$ is a solution to $Q(\vec{\mathbf{v}}) \equiv m \pmod{p^k}$ for some $k \geq 1$. If $p \nmid ax_0$, $p \nmid by_0$, or $p \nmid cz_0$, then there are exactly p^2 solutions to $Q(\vec{\mathbf{v}}) \equiv m \pmod{p^{k+1}}$ of the form $(x_0 + x_1p^k, y_0 + y_1p^k, z_0 + z_1p^k)^T$, where $x_1, y_1, z_1 \in \mathbb{Z}/p\mathbb{Z}$.*

Proof. Without loss of generality, assume that $p \nmid ax_0$.

We first prove that there exists a solution to $Q(\vec{\mathbf{v}}) \equiv m \pmod{p^{k+1}}$ of the form $(x_0 + x_1p^k, y_0 + y_1p^k, z_0 + z_1p^k)^T$. Because $Q(\vec{\mathbf{v}}_0) \equiv m \pmod{p^k}$, there exists $\ell \in \mathbb{Z}$ such that

$$ax_0^2 + by_0^2 + cz_0^2 = m + \ell p^k. \tag{3.3}$$

For any $x_1, y_1, z_1 \in \mathbb{Z}/p\mathbb{Z}$, we expand

$$a(x_0 + p^k x_1)^2 + b(y_0 + p^k y_1)^2 + c(z_0 + p^k z_1)^2 - m$$

to obtain

$$ax_0^2 + 2ax_0x_1p^k + ax_1^2p^{2k} + by_0^2 + 2by_0y_1p^k + by_1^2p^{2k} + cz_0^2 + 2cz_0z_1p^k + cz_1^2p^{2k} - m.$$

By rearranging terms in the last expression, we have

$$(ax_0^2 + by_0^2 + cz_0^2) - m + 2ax_0x_1p^k + 2by_0y_1p^k + 2cz_0z_1p^k + ax_1^2p^{2k} + by_1^2p^{2k} + cz_1^2p^{2k}.$$

We use (3.3) to rewrite this as

$$m + \ell p^k - m + (2ax_0x_1 + 2by_0y_1 + 2cz_0z_1)p^k + (ax_1^2 + by_1^2 + cz_1^2)p^{2k} \\ = (\ell + 2ax_0x_1 + 2by_0y_1 + 2cz_0z_1)p^k + (ax_1^2 + by_1^2 + cz_1^2)p^{2k}.$$

Take this modulo p^{k+1} to get that

$$a(x_0 + p^k x_1)^2 + b(y_0 + p^k y_1)^2 + c(z_0 + p^k z_1)^2 - m \\ \equiv (\ell + 2ax_0x_1 + 2by_0y_1 + 2cz_0z_1)p^k \pmod{p^{k+1}}. \tag{3.4}$$

Let

$$x_1 = (2ax_0)^{-1}(-\ell - 2by_0y_1 - 2cz_0z_1), \tag{3.5}$$

where $2ax_0(2ax_0)^{-1} \equiv 1 \pmod p$ if and only if $2ax_0(2ax_0)^{-1} = 1 + tp$ for some $t \in \mathbb{Z}$. Note that $(2ax_0)^{-1}$ exists since $p \nmid 2ax_0$. Then use (3.5) to substitute for x_1 in (3.4) to get

$$a(x_0 + p^k x_1)^2 + b(y_0 + p^k y_1)^2 + c(z_0 + p^k z_1)^2 - m \\ \equiv (\ell + 2ax_0(2ax_0)^{-1}(-\ell - 2by_0y_1 - 2cz_0z_1) + 2by_0y_1 + 2cz_0z_1)p^k \pmod{p^{k+1}}.$$

Replace $2ax_0(2ax_0)^{-1}$ by $1 + tp$ to see that

$$a(x_0 + p^k x_1)^2 + b(y_0 + p^k y_1)^2 + c(z_0 + p^k z_1)^2 - m \\ \equiv (\ell + (1 + tp)(-\ell - 2by_0y_1 - 2cz_0z_1) + 2by_0y_1 + 2cz_0z_1)p^k \pmod{p^{k+1}}.$$

Expand and cancel like terms to simplify the expression to

$$a(x_0 + p^k x_1)^2 + b(y_0 + p^k y_1)^2 + c(z_0 + p^k z_1)^2 - m \equiv t(-\ell - 2by_0y_1 - 2cz_0z_1)p^{k+1} \\ \equiv 0 \pmod{p^{k+1}}.$$

Thus, there exists a solution to $Q(\vec{\mathbf{v}}) \equiv m \pmod{p^{k+1}}$ of the form $(x_0 + x_1p^k, y_0 + y_1p^k, z_0 + z_1p^k)^T$.

Conversely, if $a(x_0 + p^k x_1)^2 + b(y_0 + p^k y_1)^2 + c(z_0 + p^k z_1)^2 \equiv m \pmod{p^{k+1}}$, then by (3.4), we see that

$$(\ell + 2ax_0x_1 + 2by_0y_1 + 2cz_0z_1)p^k \equiv 0 \pmod{p^{k+1}}$$

for some $\ell \in \mathbb{Z}$. We divide by p^k to see that this is equivalent to

$$\ell + 2ax_0x_1 + 2by_0y_1 + 2cz_0z_1 \equiv 0 \pmod p.$$

Solve this congruence for x_1 to get

$$x_1 \equiv (2ax_0)^{-1}(-\ell - 2by_0y_1 - 2cz_0z_1) \pmod p. \tag{3.6}$$

Congruence (3.6) shows that $x_1 \in \mathbb{Z}/p\mathbb{Z}$ is uniquely determined by the choices of y_1 and z_1. Because there are no restrictions on $y_1, z_1 \in \mathbb{Z}/p\mathbb{Z}$, there are p choices for y_1 and p choices for z_1. Therefore, there are exactly p^2 solutions to $Q(\vec{\mathbf{v}}) \equiv m \pmod{p^{k+1}}$ of the form $(x_0 + x_1p^k, y_0 + y_1p^k, z_0 + z_1p^k)^T$, where $x_1, y_1, z_1 \in \mathbb{Z}/p\mathbb{Z}$. □

The following corollary follows from an induction proof using Theorem 3.3. The corollary allows us under certain conditions to state how many solutions there are in $(\mathbb{Z}/p^{k+\ell}\mathbb{Z})^3$ to $Q(\vec{\mathbf{v}}) \equiv m \pmod{p^{k+\ell}}$ given the number of solutions in $(\mathbb{Z}/p^k\mathbb{Z})^3$ to $Q(\vec{\mathbf{v}}) \equiv m \pmod{p^k}$.

Corollary 3.4. *Let p be an odd positive prime integer. Suppose that $\{(x_1, y_1, z_1)^T, \ldots, (x_n, y_n, z_n)^T\}$ is the set of the $r_{p^k,Q}(m)$ solutions in $(\mathbb{Z}/p^k\mathbb{Z})^3$ to $Q(\vec{\mathbf{v}}) \equiv m \pmod{p^k}$, and suppose that $p \nmid ax_j$, $p \nmid by_j$, or $p \nmid cz_j$ for each $j \in \mathbb{Z}$, $1 \leq j \leq r_{p^k,Q}(m)$. Then there are exactly $r_{p^k,Q}(m) \cdot p^{2\ell}$ solutions in $(\mathbb{Z}/p^{k+\ell}\mathbb{Z})^3$ to $Q(\vec{\mathbf{v}}) \equiv m \pmod{p^{k+\ell}}$ for $\ell \geq 0$. Furthermore, each of the solutions $(x_0, y_0, z_0)^T$ in $(\mathbb{Z}/p^{k+\ell}\mathbb{Z})^3$ to $Q(\vec{\mathbf{v}}) \equiv m \pmod{p^{k+\ell}}$ satisfies the property that $p \nmid ax_0$, $p \nmid by_0$, or $p \nmid cz_0$.*

Proof. The corollary is clearly true when $\ell = 0$.

Let $n = r_{p^k,Q}(m)$. Assume that there are exactly $np^{2\ell}$ solutions in $(\mathbb{Z}/p^{k+\ell}\mathbb{Z})^3$ to $Q(\vec{\mathbf{v}}) \equiv m \pmod{p^{k+\ell}}$ for some $\ell \geq 0$. Let $\{(x_1, y_1, z_1)^T, \ldots, (x_{np^{2\ell}}, y_{np^{2\ell}}, z_{np^{2\ell}})^T\}$ be the set of the $np^{2\ell}$ solutions in $(\mathbb{Z}/p^{k+\ell}\mathbb{Z})^3$ to $Q(\vec{\mathbf{v}}) \equiv m \pmod{p^{k+\ell}}$. Assume that $p \nmid ax_j$, $p \nmid by_j$, or $p \nmid cz_j$ for each $j \in \mathbb{Z}$, $1 \leq j \leq np^{2\ell}$.

According to Theorem 3.3, for each solution $(x_j, y_j, z_j)^T$ in $\mathbb{Z}/p^{k+\ell}\mathbb{Z}$ to $Q(\vec{\mathbf{v}}) \equiv m \pmod{p^{k+\ell}}$, there exist p^2 solutions to $Q(\vec{\mathbf{v}}) \equiv m \pmod{p^{k+\ell+1}}$ of the form $(x_j + x'_j p^{k+\ell}, y_j + y'_j p^{k+\ell}, z_j + z'_j p^{k+\ell})^T$, where $x'_j, y'_j, z'_j \in \mathbb{Z}/p\mathbb{Z}$. Since $p \nmid ax_j$, $p \nmid by_j$, or $p \nmid cz_j$, we see that

$$\begin{aligned} p \nmid a(x_j + x'_j p^{k+\ell}) &= ax_j + ax'_j p^{k+\ell}, \\ p \nmid b(y_j + y'_j p^{k+\ell}) &= by_j + by'_j p^{k+\ell}, \text{ or} \\ p \nmid c(z_j + z'_j p^{k+\ell}) &= cz_j + cz'_j p^{k+\ell}. \end{aligned}$$

Let $S_{k+\ell+1,j}$ be the set of the p^2 solutions to $Q(\vec{\mathbf{v}}) \equiv m \pmod{p^{k+\ell+1}}$ of the form $(x_j + x'_j p^{k+\ell}, y_j + y'_j p^{k+\ell}, z_j + z'_j p^{k+\ell})^T$, $1 \leq j \leq np^{2\ell}$. Because

$$\begin{aligned} x_j + x'_j p^{k+\ell} &\equiv x_j \pmod{p^{k+\ell}}, \\ y_j + y'_j p^{k+\ell} &\equiv y_j \pmod{p^{k+\ell}}, \text{ and} \\ z_j + z'_j p^{k+\ell} k &\equiv z_j \pmod{p^{k+\ell}}, \end{aligned}$$

$S_{k+\ell+1,j_1} \cap S_{k+\ell+1,j_2} = \emptyset$ for $1 \leq j_1 < j_2 \leq np^{2\ell}$. Therefore, there are $np^{2\ell} \cdot p^2 = np^{2(\ell+1)}$ solutions to $Q(\vec{\mathbf{v}}) \equiv m \pmod{p^{k+\ell+1}}$. By the principle of mathematical induction, the corollary follows. □

Because the sum $\displaystyle\sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right) G\left(\frac{at}{p}\right) G\left(\frac{bt}{p}\right) G\left(\frac{ct}{p}\right)$ appears in the evaluation of $r_{p,Q}(m)$, we prove a lemma about the sum for several cases of the coefficients a, b, c.

Lemma 3.5. *If p is an odd prime, then*

$$\sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right) G\left(\frac{at}{p}\right) G\left(\frac{bt}{p}\right) G\left(\frac{ct}{p}\right) =$$

$$\begin{cases} \left(\dfrac{abc}{p}\right) \varepsilon_p^3 p^{3/2} \displaystyle\sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right) \left(\frac{t}{p}\right), & \text{if } p \nmid abc, \\ p^2 \left(\dfrac{-ab}{p}\right) \displaystyle\sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right), & \text{if } p \nmid ab \text{ and } p \mid c, \\ \left(\dfrac{a}{p}\right) p^{5/2} \varepsilon_p \displaystyle\sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right) \left(\frac{t}{p}\right), & \text{if } p \nmid a,\ p \mid b, \text{ and } p \mid c. \end{cases}$$

Proof. Because t ranges between 1 and $p-1$, p is coprime to t. Therefore, for any $n \in \mathbb{Z}$, p divides nt if and only if p divides n. By Lemma 2.11, for any $n \in \mathbb{Z}$ and $1 \leq t \leq p-1$, we have

$$G\left(\frac{nt}{p}\right) = \begin{cases} p, & \text{if } p \mid n, \\ p^{1/2}\left(\frac{nt}{p}\right)\varepsilon_p, & \text{if } p \nmid n. \end{cases} \tag{3.7}$$

Suppose p divides exactly r of a, b, c. Let q be the product of the numbers in the set $\{a, b, c\}$ that are not divisible by p. Using (3.7) and the multiplicative property of the Legendre symbol, we see that

$$\sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right) G\left(\frac{at}{p}\right) G\left(\frac{bt}{p}\right) G\left(\frac{ct}{p}\right) = \sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right)\left(\frac{q}{p}\right)\left(p^{1/2}\left(\frac{t}{p}\right)\varepsilon_p\right)^{3-r} p^r.$$

Suppose $p \nmid abc$. Then $q = abc$, $r = 0$, and

$$\begin{aligned} \sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right) G\left(\frac{at}{p}\right) G\left(\frac{bt}{p}\right) G\left(\frac{ct}{p}\right) &= \sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right)\left(\frac{abc}{p}\right)\left(p^{1/2}\left(\frac{t}{p}\right)\varepsilon_p\right)^3 \\ &= \left(\frac{abc}{p}\right)\varepsilon_p^3 p^{3/2} \sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right)\left(\frac{t}{p}\right)^2\left(\frac{t}{p}\right) \\ &= \left(\frac{abc}{p}\right)\varepsilon_p^3 p^{3/2} \sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right)\left(\frac{t}{p}\right) \end{aligned}$$

since $\left(\frac{t}{p}\right)^2 = 1$ if $p \nmid t$.

Now suppose that $p \nmid ab$ and $p \mid c$. Then $r = 1$, $q = ab$, and

$$\begin{aligned} \sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right) G\left(\frac{at}{p}\right) G\left(\frac{bt}{p}\right) G\left(\frac{ct}{p}\right) &= \sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right)\left(\frac{ab}{p}\right)\left(p^{1/2}\left(\frac{t}{p}\right)\varepsilon_p\right)^2 p \\ &= p^2\left(\frac{ab}{p}\right)\varepsilon_p^2 \sum_{t=1}^{p-1}\left(\frac{t}{p}\right)^2 \mathrm{e}\left(\frac{-mt}{p}\right) \\ &= p^2\left(\frac{ab}{p}\right)\varepsilon_p^2 \sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right) \end{aligned}$$

since $\left(\frac{t}{p}\right)^2 = 1$ if $t \not\equiv 0 \pmod{p}$. By Lemma 2.8,

$$p^2\left(\frac{ab}{p}\right)\varepsilon_p^2 \sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right) = p^2\left(\frac{ab}{p}\right)\left(\frac{-1}{p}\right) \sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right).$$

By the multiplicative property of the Legendre symbol,

$$p^2\left(\frac{ab}{p}\right)\left(\frac{-1}{p}\right) \sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right) = p^2\left(\frac{-ab}{p}\right) \sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right).$$

Now suppose that $p \nmid a$, $p \mid b$, and $p \mid c$. Then $r = 2$, $q = a$, and

$$\sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right) G\left(\frac{at}{p}\right) G\left(\frac{bt}{p}\right) G\left(\frac{ct}{p}\right) = \sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right) \left(\frac{a}{p}\right) p^{1/2} \left(\frac{t}{p}\right) \varepsilon_p p^2$$
$$= \left(\frac{a}{p}\right) p^{5/2} \varepsilon_p \sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right) \left(\frac{t}{p}\right).$$

□

We now use Gauss sums and Hensel's Lemma for odd primes to find some closed-form formulas for $r_{p^k,Q}(m)$. We start with when p is an odd prime and p does not divide m.

Theorem 3.6. *Let p be an odd prime. Suppose $p \nmid m$.*

$$r_{p^k,Q}(m) = \begin{cases} p^{2k}\left(1 + \frac{1}{p}\left(\frac{-abcm}{p}\right)\right), & \text{if } p \nmid abc, \\ p^{2k}\left(1 - \frac{1}{p}\left(\frac{-ab}{p}\right)\right), & \text{if } p \nmid ab \text{ and } p \mid c, \\ p^{2k}\left(1 + \left(\frac{am}{p}\right)\right), & \text{if } p \nmid a,\ p \mid b, \text{ and } p \mid c. \end{cases} \tag{3.8}$$

Proof. Because $p \nmid m$, any solution $(x_0, y_0, z_0)^T$ to $Q(\vec{\mathbf{v}}) \equiv m \pmod{p}$ has the property that $p \nmid ax_0$, $p \nmid by_0$, or $p \nmid cz_0$. Therefore, Corollary 3.4 can be used once $r_{p,Q}(m)$ is known.

Suppose $p \nmid abc$. By Lemma 3.5,

$$\sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right) G\left(\frac{at}{p}\right) G\left(\frac{bt}{p}\right) G\left(\frac{ct}{p}\right) = \left(\frac{abc}{p}\right) \varepsilon_p^3 p^{3/2} \sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right) \left(\frac{t}{p}\right).$$

By Lemma 2.4, because $m \not\equiv 0 \pmod{p}$,

$$\left(\frac{abc}{p}\right) \varepsilon_p^3 p^{3/2} \sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right) \left(\frac{t}{p}\right) = \left(\frac{abc}{p}\right) \varepsilon_p^3 p^{3/2} G\left(\frac{-m}{p}\right). \tag{3.9}$$

Since $p \nmid m$, we can apply Lemma 2.10 and see that

$$\left(\frac{abc}{p}\right) \varepsilon_p^3 p^{3/2} G\left(\frac{-m}{p}\right) = \left(\frac{abc}{p}\right) \varepsilon_p^3 p^{3/2} p^{1/2} \left(\frac{-m}{p}\right) \varepsilon_p = \left(\frac{abc}{p}\right) \left(\frac{-m}{p}\right) \varepsilon_p^4 p^2$$

By Lemma 2.8 and the multiplicative property of the Legendre symbol,

$$\left(\frac{abc}{p}\right) \left(\frac{-m}{p}\right) \varepsilon_p^4 p^2 = \left(\frac{-abcm}{p}\right) p^2.$$

Therefore, by Corollary 3.2,

$$r_{p,Q}(m) = p^2 + \frac{1}{p} \sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right) G\left(\frac{at}{p}\right) G\left(\frac{bt}{p}\right) G\left(\frac{ct}{p}\right)$$
$$= p^2 + \frac{1}{p}\left(\frac{-abcm}{p}\right) p^2 = p^2\left(1 + \frac{1}{p}\left(\frac{-abcm}{p}\right)\right).$$

The formula $r_{p^k,Q}(m) = p^{2k}\left(1 + \frac{1}{p}\left(\frac{-abcm}{p}\right)\right)$ follows from Corollary 3.4.

Now suppose that $p \nmid ab$ and $p \mid c$. By Lemma 3.5,

$$\sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right) G\left(\frac{at}{p}\right) G\left(\frac{bt}{p}\right) G\left(\frac{ct}{p}\right) = p^2 \left(\frac{-ab}{p}\right) \sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right).$$

By applying Lemmas 2.3, we have

$$p^2 \left(\frac{-ab}{p}\right) \sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right) = p^2 \left(\frac{-ab}{p}\right)(-1) = -p^2 \left(\frac{-ab}{p}\right).$$

Therefore, by Corollary 3.2,

$$\begin{aligned} r_{p,Q}(m) &= p^2 + \frac{1}{p} \sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right) G\left(\frac{at}{p}\right) G\left(\frac{bt}{p}\right) G\left(\frac{ct}{p}\right) \\ &= p^2 + \frac{1}{p}\left(-p^2 \left(\frac{-ab}{p}\right)\right) = p^2 \left(1 - \frac{1}{p}\left(\frac{-ab}{p}\right)\right). \end{aligned}$$

The formula $r_{p^k,Q}(m) = p^{2k}\left(1 - \frac{1}{p}\left(\frac{-ab}{p}\right)\right)$ follows from Corollary 3.4.

Now suppose that $p \nmid a$, $p \mid b$, and $p \mid c$. By Lemma 3.5,

$$\sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right) G\left(\frac{at}{p}\right) G\left(\frac{bt}{p}\right) G\left(\frac{ct}{p}\right) = \left(\frac{a}{p}\right) p^{5/2} \varepsilon_p \sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right)\left(\frac{t}{p}\right).$$

By Lemma 2.4,

$$\left(\frac{a}{p}\right) p^{5/2} \varepsilon_p \sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right)\left(\frac{t}{p}\right) = \left(\frac{a}{p}\right) p^{5/2} \varepsilon_p G\left(\frac{-m}{p}\right).$$

Since $p \nmid m$, we can apply Lemma 2.10 and see that

$$\left(\frac{a}{p}\right) p^{5/2} \varepsilon_p G\left(\frac{-m}{p}\right) = \left(\frac{a}{p}\right) p^{5/2} \varepsilon_p p^{1/2} \left(\frac{-m}{p}\right) \varepsilon_p = \left(\frac{a}{p}\right) p^3 \varepsilon_p^2 \left(\frac{-m}{p}\right).$$

By Lemma 2.8 and the multiplicative property of the Legendre symbol,

$$\left(\frac{a}{p}\right) p^3 \varepsilon_p^2 \left(\frac{-m}{p}\right) = \left(\frac{a}{p}\right) p^3 \left(\frac{-1}{p}\right)\left(\frac{-m}{p}\right) = \left(\frac{am}{p}\right) p^3.$$

Therefore, by Corollary 3.2,

$$\begin{aligned} r_{p,Q}(m) &= p^2 + \frac{1}{p} \sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right) G\left(\frac{at}{p}\right) G\left(\frac{bt}{p}\right) G\left(\frac{ct}{p}\right) \\ &= p^2 + \frac{1}{p}\left(\frac{am}{p}\right) p^3 = p^2 + p^2 \left(\frac{am}{p}\right) = p^2 \left(1 + \left(\frac{am}{p}\right)\right). \end{aligned}$$

The formula $r_{p^k,Q}(m) = p^{2k}\left(1 + \left(\frac{am}{p}\right)\right)$ follows from Corollary 3.4. □

Before state the value of $r_{p^k,Q}(m)$ when p is an odd prime and p divides m exactly, we compute a sum of Legendre symbols. This sum is used to compute $r_{p^k,Q}(m)$ when p is an odd prime and p divides m exactly.

Lemma 3.7. *Let p be an odd prime. Then*

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

Proof. Because $\left(\frac{0}{p}\right)=0$,

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

From Lemma 2.4 , we know that

$$G\left(\frac{0}{p}\right)=\sum_{t=0}^{p-1}\left(1+\left(\frac{t}{p}\right)\right)\mathrm{e}\left(\frac{0t}{p}\right)=\sum_{t=0}^{p-1}\left(1+\left(\frac{t}{p}\right)\right)=p+\sum_{t=0}^{p-1}\left(\frac{t}{p}\right). \tag{3.10}$$

On the other hand, from Lemma 2.5 we know that

$$G\left(\frac{0}{p}\right)=p. \tag{3.11}$$

By setting (3.10) equal to (3.11), we see that

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

which implies

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

□

For further computations, we are concerned about computing $r_{p^k,Q}(m)$ when $k>1$. To do this, we expand sums into sums involving $(\mathbb{Z}/p^\tau\mathbb{Z})^*$, where $(\mathbb{Z}/p^\tau\mathbb{Z})^*$ is the multiplicative group (mod p^τ). The next lemma allows us to do this expansion.

Lemma 3.8. *Let p be a prime and k be a positive integer. If $f:\mathbb{Z}\to\mathbb{C}$ is a periodic function with a period of p^k, then*

$$\sum_{t\in(\mathbb{Z}/p^k\mathbb{Z})\setminus\{\bar{0}\}}f(t)=\sum_{t=1}^{p^k-1}f(t)=\sum_{\tau=0}^{k-1}\sum_{t_0\in(\mathbb{Z}/p^{k-\tau}\mathbb{Z})^*}f(t_0p^\tau),$$

where $\bar{0}$ is the zero element of $\mathbb{Z}/p^k\mathbb{Z}$.

Proof. The first equality follows from choosing coset representatives of $(\mathbb{Z}/p^k\mathbb{Z})\setminus\{\bar{0}\}$. To prove the lemma, we prove that each element of $A=(\mathbb{Z}/p^k\mathbb{Z})\setminus\{\bar{0}\}$ can be written uniquely as an element of $B=\{t_0p^\tau\mid\tau\in\mathbb{Z},0\le\tau\le k-1,t_0\in(\mathbb{Z}/p^{k-\tau}\mathbb{Z})^*\}$ and that $B\subseteq A$.

Let $t\in A$. Let p^τ be the highest power of p that divides t. (Such a τ exists since $t\not\equiv 0$ (mod p^k) by the definition of A.) Since $t\not\equiv 0$ (mod p^k), we have $0\le\tau\le k-1$. Let $t_0=t/p^\tau$. Because p^τ is the highest power of p that divides t, we conclude that $p\nmid t_0$. This implies that $t_0\in(\mathbb{Z}/p^{k-\tau}\mathbb{Z})^*$. Therefore, $t=t_0p^\tau$, where $t_0p^\tau\in B$.

We need to show that $t_0 p^\tau \in B$ is unique given an element $t \in A$. Let s be a coset representative of t. Any coset representative of t can be written as $s + rp^k$ for some $r \in \mathbb{Z}$. Let s_1 and s_2 be coset representatives of t. Then $s_1 = s + r_1 p^k$ and $s_2 = s + r_2 p^k$. Suppose that p^{τ_1} is the highest power of p that divides s_1. (Since $p^k \nmid s_1$, such a τ_1 exists and is less that k.) Because p^{τ_1} divides s_1 and $r_1 p^k$, we see that p^{τ_1} divides s. Therefore, since p^{τ_1} divides $r_2 p^k$, we conclude p^{τ_1} divides $s + r_2 p^k = s_2$. A similar argument shows that the highest power of p that divides s_2 also divides s_1. Therefore, the highest power of p that divides t, called p^τ, is unique.

Let $t_1 = s_1/p^\tau$ and $t_2 = s_2/p^\tau$. We want to show that t_1 and t_2 are coset representatives of the same element in $(\mathbb{Z}/p^{k-\tau}\mathbb{Z})^*$. We do this by showing $p^{k-\tau}$ divides $t_1 - t_2$. Now

$$t_1 - t_2 = \frac{s_1}{p^\tau} - \frac{s_2}{p^\tau} = \frac{s + r_1 p^k}{p^\tau} - \frac{s + r_2 p^k}{p^\tau} = (r_1 - r_2) p^{k-\tau},$$

so t_1 and t_2 represent the same element in $(\mathbb{Z}/p^{k-\tau}\mathbb{Z})^*$.

The final piece of this proof is to show that $B \subseteq A$. For any $t_0 p^\tau \in B$ such that $t_0 \in (\mathbb{Z}/p^{k-\tau}\mathbb{Z})^*$ and $0 \le \tau \le k-1$, $t_0 p^\tau$ is a nonzero element of $\mathbb{Z}/p^k\mathbb{Z}$, so $B \subseteq A$. □

Now the sums involving $(\mathbb{Z}/p^\tau\mathbb{Z})^*$ will have to be evaluated. The following lemma allows us to evaluate these sums.

Lemma 3.9. *Let p, n, and τ be positive integers such that $n \le \tau$. If $f : \mathbb{Z}/p^\tau\mathbb{Z} \to \mathbb{C}$ is a character with a period of p^τ, then*

$$\sum_{t_0 \in (\mathbb{Z}/p^\tau\mathbb{Z})^*} f(t_0) = \sum_{t_1 \in (\mathbb{Z}/p^n\mathbb{Z})^*} f(t_1) \sum_{t_2=0}^{p^{\tau-n}-1} f(p^n t_2). \tag{3.12}$$

If f has a period of p, then

$$\sum_{t_0 \in (\mathbb{Z}/p^\tau\mathbb{Z})^*} f(t_0) = p^{\tau-n} \sum_{t_1 \in (\mathbb{Z}/p^n\mathbb{Z})^*} f(t_1). \tag{3.13}$$

If p is prime, then

$$\sum_{t_0 \in (\mathbb{Z}/p^\tau\mathbb{Z})^*} f(t_0) = \sum_{t_1=1}^{p-1} f(t_1) \sum_{t_2=0}^{p^{\tau-1}-1} f(pt_2). \tag{3.14}$$

If f has a period of p and p is prime, then

$$\sum_{t_0 \in (\mathbb{Z}/p^\tau\mathbb{Z})^*} f(t_0) = p^{\tau-1} \sum_{t_1=1}^{p-1} f(t_1). \tag{3.15}$$

Proof. Any $t_0 \in (\mathbb{Z}/p^\tau\mathbb{Z})^*$ can be uniquely written as $t_1 + p^n t_2$, where $t_1 \in (\mathbb{Z}/p^n\mathbb{Z})^*$ and $0 \le t_2 \le p^{\tau-n} - 1$. (This is because of the uniqueness of the base-p expansion of t_0.) Therefore,

$$\sum_{t_0 \in (\mathbb{Z}/p^\tau\mathbb{Z})^*} f(t_0) = \sum_{t_1 \in (\mathbb{Z}/p^n\mathbb{Z})^*} \sum_{t_2=0}^{p^{\tau-n}-1} f(t_1 + p^n t_2).$$

Because f is a character with a period of p^τ,

$$\sum_{t_1\in(\mathbb{Z}/p^n\mathbb{Z})^*}\sum_{t_2=0}^{p^{\tau-n}-1} f(t_1+p^nt_2)=\sum_{t_1\in(\mathbb{Z}/p^n\mathbb{Z})^*}\sum_{t_2=0}^{p^{\tau-n}-1} f(t_1)f(p^nt_2)=\sum_{t_1\in(\mathbb{Z}/p^n\mathbb{Z})^*} f(t_1)\sum_{t_2=0}^{p^{\tau-n}-1} f(p^nt_2).$$

Because $f:\mathbb{Z}/p^\tau\mathbb{Z}\to\mathbb{C}$ is a character, $f(0)=1$. If f has a period of p, then $f(tp)=f(0)=1$ for any $t\in\mathbb{Z}$. Thus, if f has a period of p, then

$$\sum_{t_2=0}^{p^{\tau-n}-1} f(pt_2)=\sum_{t_2=0}^{p^{\tau-n}-1} 1=p^{\tau-n}$$

and

$$\sum_{t_1\in(\mathbb{Z}/p^n\mathbb{Z})^*} f(t_1)\sum_{t_2=0}^{p^{\tau-n}-1} f(p^nt_2)=\sum_{t_1\in(\mathbb{Z}/p^n\mathbb{Z})^*} f(t_1)\cdot p^{\tau-n}=p^{\tau-n}\sum_{t_1\in(\mathbb{Z}/p^n\mathbb{Z})^*} f(t_1).$$

If p is prime, the elements of $(\mathbb{Z}/p\mathbb{Z})^*$ correspond to the elements in the set $\{t_1\in\mathbb{Z}\mid 1\le t_1\le p-1\}$, so (3.14) and (3.15) follow from (3.12) and (3.13), respectively, with $n=1$. □

Now that we have computed the sum of Legendre symbols and evaluated expanded sums, we can now compute $r_{p^k,Q}(m)$ when p is an odd prime and p divides m exactly.

Theorem 3.10. *Let p be an odd prime. Suppose $p\parallel m$ so that $m=m_0p$ for some $m_0\in\mathbb{Z}$ and $\gcd(m_0,p)=1$. Suppose that $p\nmid abc$. Then*

$$r_{p^k,Q}(m)=\begin{cases}p^2 & \text{if } k=1,\\ p^{2k}\left(1-\dfrac{1}{p^2}\right), & \text{if } k\ge 2.\end{cases}$$

Proof. For the case in which $k=1$, we can apply Lemma 3.5 and see that

$$\begin{aligned}\sum_{t=1}^{p-1}\mathrm{e}\left(\frac{-mt}{p}\right)G\left(\frac{at}{p}\right)G\left(\frac{bt}{p}\right)G\left(\frac{ct}{p}\right)&=\left(\frac{abc}{p}\right)\varepsilon_p^3p^{3/2}\sum_{t=1}^{p-1}\mathrm{e}\left(\frac{-mt}{p}\right)\left(\frac{t}{p}\right)\\&=\left(\frac{abc}{p}\right)\varepsilon_p^3p^{3/2}\sum_{t=1}^{p-1}\mathrm{e}\left(\frac{-m_0pt}{p}\right)\left(\frac{t}{p}\right)\\&=\left(\frac{abc}{p}\right)\varepsilon_p^3p^{3/2}\sum_{t=1}^{p-1}\mathrm{e}(-m_0t)\left(\frac{t}{p}\right)\\&=\left(\frac{abc}{p}\right)\varepsilon_p^3p^{3/2}\sum_{t=1}^{p-1}\left(\frac{t}{p}\right).\end{aligned}$$

By Lemma 3.7,

$$\left(\frac{abc}{p}\right)\varepsilon_p^3p^{3/2}\sum_{t=1}^{p-1}\left(\frac{t}{p}\right)=\left(\frac{abc}{p}\right)\varepsilon_p^3p^{3/2}\cdot 0=0.$$

By Corollary 3.2,

$$\begin{aligned} r_{p,Q}(m) &= p^2 + \frac{1}{p}\sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right) G\left(\frac{at}{p}\right) G\left(\frac{bt}{p}\right) G\left(\frac{ct}{p}\right) \\ &= p^2 + \frac{1}{p}\cdot 0 = p^2. \end{aligned}$$

Let $(x_0, y_0, z_0)^T$ be a solution to $Q(\vec{\mathbf{v}}) \equiv m \pmod{p^2}$. Toward contradiction, assume that $p \mid ax_0$, $p \mid by_0$, and $p \mid cz_0$. Since $p \nmid abc$, $x_0 = x_1 p$, $y_0 = y_1 p$, and $z_0 = z_1 p$ for some $x_1, y_1, z_1 \in \mathbb{Z}$. Thus,

$$\begin{aligned} ax_0^2 + by_0^2 + cz_0^2 &= a(x_1 p)^2 + b(y_1 p)^2 + c(z_1 p)^2 \\ &= ax_1^2 p^2 + by_1^2 p^2 + cz_1^2 p^2 \\ &\equiv 0 \pmod{p^2}. \end{aligned}$$

However, this contradicts the fact that $m \not\equiv 0 \pmod{p^2}$ since $p \parallel m$. Therefore, for any solution $(x_0, y_0, z_0)^T$ to $Q(\vec{\mathbf{v}}) \equiv m \pmod{p^2}$, $p \nmid ax_0$, $p \nmid by_0$, or $p \nmid cz_0$. Thus, Corollary 3.4 can be used once $r_{p^2,Q}(m)$ is known. In this case,

$$\begin{aligned} r_{p^2,Q}(m) &= p^4 + \frac{1}{p^2}\sum_{t=1}^{p^2-1} \mathrm{e}\left(\frac{-mt}{p^2}\right) G\left(\frac{at}{p^2}\right) G\left(\frac{bt}{p^2}\right) G\left(\frac{ct}{p^2}\right) \\ &= p^4 + \frac{1}{p^2}\sum_{t=1}^{p^2-1} \mathrm{e}\left(\frac{-m_0 t}{p}\right) G\left(\frac{at}{p^2}\right) G\left(\frac{bt}{p^2}\right) G\left(\frac{ct}{p^2}\right). \end{aligned}$$

By Lemma 3.8,

$$\begin{aligned} &\sum_{t=1}^{p^2-1} \mathrm{e}\left(\frac{-m_0 t}{p}\right) G\left(\frac{at}{p^2}\right) G\left(\frac{bt}{p^2}\right) G\left(\frac{ct}{p^2}\right) \\ &= \sum_{\tau=0}^{1} \sum_{t_0 \in (\mathbb{Z}/p^{2-\tau}\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0 t_0 p^\tau}{p}\right) G\left(\frac{at_0 p^\tau}{p^2}\right) G\left(\frac{bt_0 p^\tau}{p^2}\right) G\left(\frac{ct_0 p^\tau}{p^2}\right) \\ &= \sum_{t_0 \in (\mathbb{Z}/p^2\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0 t_0}{p}\right) G\left(\frac{at_0}{p^2}\right) G\left(\frac{bt_0}{p^2}\right) G\left(\frac{ct_0}{p^2}\right) \\ &\qquad + \sum_{t_0 \in (\mathbb{Z}/p\mathbb{Z})^*} \mathrm{e}(-m_0 t_0)\, G\left(\frac{at_0 p}{p^2}\right) G\left(\frac{bt_0 p}{p^2}\right) G\left(\frac{ct_0 p}{p^2}\right) \\ &= \sum_{t_0 \in (\mathbb{Z}/p^2\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0 t_0}{p}\right) G\left(\frac{at_0}{p^2}\right) G\left(\frac{bt_0}{p^2}\right) G\left(\frac{ct_0}{p^2}\right) + \sum_{t_0=1}^{p-1} G\left(\frac{at_0 p}{p^2}\right) G\left(\frac{bt_0 p}{p^2}\right) G\left(\frac{ct_0 p}{p^2}\right). \end{aligned}$$

We apply Lemma 2.10 to see that

$$\begin{aligned}
&\sum_{t_0\in(\mathbb{Z}/p^2\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0t_0}{p}\right) G\left(\frac{at_0}{p^2}\right) G\left(\frac{bt_0}{p^2}\right) G\left(\frac{ct_0}{p^2}\right)\\
&= \sum_{t_0\in(\mathbb{Z}/p^2\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0t_0}{p}\right) p\left(\frac{at_0}{p^2}\right)\varepsilon_{p^2} p\left(\frac{bt_0}{p^2}\right)\varepsilon_{p^2} p\left(\frac{ct_0}{p^2}\right)\varepsilon_{p^2}\\
&= p^3 \sum_{t_0\in(\mathbb{Z}/p^2\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0t_0}{p}\right)\left(\frac{at_0}{p^2}\right)\varepsilon_{p^2}\left(\frac{bt_0}{p^2}\right)\varepsilon_{p^2}\left(\frac{ct_0}{p^2}\right)\varepsilon_{p^2}.
\end{aligned}$$

By Lemma 2.9, we have $\varepsilon_{p^2}=1$. By the definition of the Jacobi symbol,

$$\left(\frac{at_0}{p^2}\right)=\left(\frac{at_0}{p}\right)^2=\left(\frac{bt_0}{p^2}\right)=\left(\frac{bt_0}{p}\right)^2=\left(\frac{ct_0}{p^2}\right)=\left(\frac{ct_0}{p}\right)^2=1.$$

Therefore,

$$\sum_{t_0\in(\mathbb{Z}/p^2\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0t_0}{p}\right)\left(\frac{at_0}{p^2}\right)\varepsilon_{p^2}\left(\frac{bt_0}{p^2}\right)\varepsilon_{p^2}\left(\frac{ct_0}{p^2}\right)\varepsilon_{p^2} = \sum_{t_0\in(\mathbb{Z}/p^2\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0t_0}{p}\right).$$

By Lemma 3.9,

$$\sum_{t_0\in(\mathbb{Z}/p^2\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0t_0}{p}\right) = p\sum_{t_1=1}^{p-1} \mathrm{e}\left(\frac{-m_0t_0}{p}\right).$$

By Lemma 2.3,

$$\sum_{t_1=1}^{p-1} \mathrm{e}\left(\frac{-m_0t_0}{p}\right) = -1.$$

By Lemma 2.11,

$$\begin{aligned}
\sum_{t_0=1}^{p-1} G\left(\frac{at_0p}{p^2}\right) G\left(\frac{bt_0p}{p^2}\right) G\left(\frac{ct_0p}{p^2}\right) &= \sum_{t_0=1}^{p-1} p^{3/2}\left(\frac{at_0}{p}\right)\varepsilon_p p^{3/2}\left(\frac{bt_0}{p}\right)\varepsilon_p p^{3/2}\left(\frac{ct_0}{p}\right)\varepsilon_p\\
&= p^{9/2}\varepsilon_p^3 \sum_{t_0=1}^{p-1}\left(\frac{at_0}{p}\right)\left(\frac{bt_0}{p}\right)\left(\frac{ct_0}{p}\right).
\end{aligned}$$

By the multiplicative property of the Legendre symbol,

$$p^{9/2}\varepsilon_p^3 \sum_{t_0=1}^{p-1}\left(\frac{at_0}{p}\right)\left(\frac{bt_0}{p}\right)\left(\frac{ct_0}{p}\right) = p^{9/2}\varepsilon_p^3\left(\frac{abc}{p}\right)\sum_{t_0=1}^{p-1}\left(\frac{t_0}{p}\right)^3.$$

Because $\left(\frac{t_0}{p}\right)^3=\left(\frac{t_0}{p}\right)$ for any t_0,

$$\sum_{t_0=1}^{p-1}\left(\frac{t_0}{p}\right)^3 = \sum_{t_0=1}^{p-1}\left(\frac{t_0}{p}\right).$$

By Lemma 3.7,

$$\sum_{t_0=1}^{p-1} \left(\frac{t_0}{p}\right) = 0.$$

After a number of substitutions, we see that

$$r_{p^2,Q}(m) = p^4 + \frac{1}{p^2}\left(p^3 \cdot p \cdot (-1) + p^{9/2}\varepsilon_p^3 \left(\frac{abc}{p}\right) \cdot 0\right) = p^4\left(1 - \frac{1}{p^2}\right).$$

The equation $r_{p^k,Q}(m) = p^{2k}\left(1 - \frac{1}{p^2}\right)$ for $k \geq 2$ follows from Corollary 3.4. □

From Theorem 3.6 and Theorem 3.10, we can conclude that if p is an odd prime, $p \nmid abc$, and m is square-free, then $r_{p^k,Q}(m) > 0$ for all k. This implies that m is locally represented at the prime p if m is square-free and $p \nmid abc$.

We now compute $r_{p^k,Q}(m)$ when p is an odd prime, p exactly divides m, p does not divide a or b, and p divides c.

Theorem 3.11. *Let p be an odd prime. Suppose that $p \parallel m$, $p \nmid ab$, and $p \mid c$. Let $m = m_0 p$ and $c = c_0 p$ for some $m_0, c_0 \in \mathbb{Z}$. Then*

$$r_{p,Q}(m) = p^2\left(1 + \left(\frac{-ab}{p}\right) - \frac{1}{p}\left(\frac{-ab}{p}\right)\right),$$

and for $k \geq 2$,

$$r_{p^k,Q}(m) = \begin{cases} p^{2k}\left(1 + \frac{1}{p}\left(\frac{c_0 m_0}{p}\right) + \left(\frac{-ab}{p}\right)\left(1 - \frac{1}{p}\right)\right), & \text{if } p \nmid ab \text{ and } p \parallel c, \\ p^{2k}\left(1 - \frac{1}{p}\right)\left(1 + \left(\frac{-ab}{p}\right)\right), & \text{if } p \nmid ab \text{ and } p^2 \mid c. \end{cases}$$

Proof. We apply Lemma 3.5 and see that

$$\begin{aligned} \sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right) G\left(\frac{at}{p}\right) G\left(\frac{bt}{p}\right) G\left(\frac{ct}{p}\right) &= p^2\left(\frac{-ab}{p}\right) \sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right) \\ &= p^2\left(\frac{-ab}{p}\right) \sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-m_0 pt}{p}\right) \\ &= p^2\left(\frac{-ab}{p}\right) \sum_{t=1}^{p-1} \mathrm{e}(-m_0 t) \\ &= p^2\left(\frac{-ab}{p}\right) \sum_{t=1}^{p-1} 1 \\ &= p^2\left(\frac{-ab}{p}\right)(p-1). \end{aligned}$$

By Corollary 3.2,

$$\begin{aligned} r_{p,Q}(m) &= p^2 + \frac{1}{p}\sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right) G\left(\frac{at}{p}\right) G\left(\frac{bt}{p}\right) G\left(\frac{ct}{p}\right) \\ &= p^2 + \frac{1}{p}\cdot p^2 \left(\frac{-ab}{p}\right)(p-1) = p^2\left(1 + \left(\frac{-ab}{p}\right) - \frac{1}{p}\left(\frac{-ab}{p}\right)\right). \end{aligned}$$

Now suppose $k \geq 2$, $p \nmid ab$, and $p \parallel c$. Then $\gcd(c_0, p) = 1$. By Corollary 3.2,

$$\begin{aligned} r_{p^k,Q}(m) &= p^{2k} + \frac{1}{p^k}\sum_{t=1}^{p^k-1} \mathrm{e}\left(\frac{-mt}{p^k}\right) G\left(\frac{at}{p^k}\right) G\left(\frac{bt}{p^k}\right) G\left(\frac{ct}{p^k}\right) \\ &= p^{2k} + \frac{1}{p^k}\sum_{t=1}^{p^k-1} \mathrm{e}\left(\frac{-m_0pt}{p^k}\right) G\left(\frac{at}{p^k}\right) G\left(\frac{bt}{p^k}\right) G\left(\frac{c_0pt}{p^k}\right) \\ &= p^{2k} + \frac{1}{p^k}\sum_{t=1}^{p^k-1} \mathrm{e}\left(\frac{-m_0t}{p^{k-1}}\right) G\left(\frac{at}{p^k}\right) G\left(\frac{bt}{p^k}\right) G\left(\frac{c_0pt}{p^k}\right). \end{aligned} \tag{3.16}$$

By Lemma 3.9,

$$\begin{aligned} &\sum_{t=1}^{p^k-1} \mathrm{e}\left(\frac{-m_0t}{p^{k-1}}\right) G\left(\frac{at}{p^k}\right) G\left(\frac{bt}{p^k}\right) G\left(\frac{c_0pt}{p^k}\right) \\ &= \sum_{\tau=0}^{k-1} \sum_{t_0 \in (\mathbb{Z}/p^{k-\tau}\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0t_0p^\tau}{p^{k-1}}\right) G\left(\frac{at_0p^\tau}{p^k}\right) G\left(\frac{bt_0p^\tau}{p^k}\right) G\left(\frac{c_0pt_0p^\tau}{p^k}\right) \\ &= \sum_{\tau=0}^{k-1} \sum_{t_0 \in (\mathbb{Z}/p^{k-\tau}\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0t_0}{p^{k-\tau-1}}\right) G\left(\frac{at_0p^\tau}{p^k}\right) G\left(\frac{bt_0p^\tau}{p^k}\right) G\left(\frac{c_0t_0p^{\tau+1}}{p^k}\right). \end{aligned} \tag{3.17}$$

Let

$$s_{k,\tau} = \sum_{t_0 \in (\mathbb{Z}/p^{k-\tau}\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0t_0}{p^{k-\tau-1}}\right) G\left(\frac{at_0p^\tau}{p^k}\right) G\left(\frac{bt_0p^\tau}{p^k}\right) G\left(\frac{c_0t_0p^{\tau+1}}{p^k}\right).$$

Using (3.17), substitute into (3.16) to see that

$$r_{p^k,Q}(m) = p^{2k} + \frac{1}{p^k}\sum_{\tau=0}^{k-1} s_{k,\tau}. \tag{3.18}$$

First suppose that $\tau = k-1$. Then

$$\begin{aligned} s_{k,\tau} &= \sum_{t_0 \in (\mathbb{Z}/p\mathbb{Z})^*} \mathrm{e}(-m_0t_0)\, G\left(\frac{at_0p^{k-1}}{p^k}\right) G\left(\frac{bt_0p^{k-1}}{p^k}\right) G\left(\frac{c_0t_0p^k}{p^k}\right) \\ &= \sum_{t_0=1}^{p-1} G\left(\frac{at_0p^{k-1}}{p^k}\right) G\left(\frac{bt_0p^{k-1}}{p^k}\right) G\left(\frac{c_0t_0p^k}{p^k}\right). \end{aligned}$$

By Lemma 2.11,

$$\sum_{t_0=1}^{p-1} G\left(\frac{at_0p^{k-1}}{p^k}\right) G\left(\frac{bt_0p^{k-1}}{p^k}\right) G\left(\frac{c_0t_0p^k}{p^k}\right) = \sum_{t_0=1}^{p-1} p^{(2k-1)/2} \left(\frac{at_0}{p}\right) \varepsilon_p p^{(2k-1)/2} \left(\frac{bt_0}{p}\right) \varepsilon_p p^k$$
$$= p^{3k-1}\varepsilon_p^2 \sum_{t_0=1}^{p-1} \left(\frac{at_0}{p}\right)\left(\frac{bt_0}{p}\right).$$

By Lemma 2.8 and the multiplicative property of the Legendre symbol,

$$p^{3k-1}\varepsilon_p^2 \sum_{t_0=1}^{p-1} \left(\frac{at_0}{p}\right)\left(\frac{bt_0}{p}\right) = p^{3k-1}\left(\frac{-1}{p}\right)\left(\frac{ab}{p}\right)\sum_{t_0=1}^{p-1}\left(\frac{t_0}{p}\right)^2 = p^{3k-1}\left(\frac{-ab}{p}\right)\sum_{t_0=1}^{p-1}\left(\frac{t_0}{p}\right)^2.$$

Since $\left(\frac{t_0}{p}\right)^2 = 1$ if $1 \le t_0 \le p-1$, we have

$$p^{3k-1}\left(\frac{-ab}{p}\right)\sum_{t_0=1}^{p-1}\left(\frac{t_0}{p}\right)^2 = p^{3k-1}\left(\frac{-ab}{p}\right)\sum_{t_0=1}^{p-1} 1 = p^{3k-1}\left(\frac{-ab}{p}\right)(p-1).$$

Therefore,

$$s_{k,k-1} = p^{3k-1}\left(\frac{-ab}{p}\right)(p-1). \tag{3.19}$$

Now suppose that $\tau = k-2$. Then

$$s_{k,\tau} = \sum_{t_0 \in (\mathbb{Z}/p^2\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0t_0}{p}\right) G\left(\frac{at_0p^{k-2}}{p^k}\right) G\left(\frac{bt_0p^{k-2}}{p^k}\right) G\left(\frac{c_0t_0p^{k-1}}{p^k}\right).$$

By Lemma 2.11,

$$\sum_{t_0 \in (\mathbb{Z}/p^2\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0t_0}{p}\right) G\left(\frac{at_0p^{k-2}}{p^k}\right) G\left(\frac{bt_0p^{k-2}}{p^k}\right) G\left(\frac{c_0t_0p^{k-1}}{p^k}\right)$$
$$= \sum_{t_0 \in (\mathbb{Z}/p^2\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0t_0}{p}\right) p^{(2k-2)/2}\left(\frac{at_0}{p^2}\right)\varepsilon_{p^2} p^{(2k-2)/2}\left(\frac{bt_0}{p^2}\right)\varepsilon_{p^2} p^{(2k-1)/2}\left(\frac{c_0t_0}{p}\right)\varepsilon_p$$
$$= p^{(6k-5)/2}\varepsilon_{p^2}^2\varepsilon_p \sum_{t_0 \in (\mathbb{Z}/p^2\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0t_0}{p}\right)\left(\frac{at_0}{p^2}\right)\left(\frac{bt_0}{p^2}\right)\left(\frac{c_0t_0}{p}\right).$$

By the definition of the Jacobi symbol, since $at_0 \not\equiv 0 \pmod p$ and $bt_0 \not\equiv 0 \pmod p$,

$$\left(\frac{at_0}{p^2}\right) = \left(\frac{at_0}{p}\right)^2 = \left(\frac{bt_0}{p^2}\right) = \left(\frac{bt_0}{p}\right)^2 = 1.$$

Therefore, by using the multiplicative property of the Legendre symbol, we see that

$$p^{(6k-5)/2}\varepsilon_{p^2}^2\varepsilon_p \sum_{t_0 \in (\mathbb{Z}/p^2\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0t_0}{p}\right)\left(\frac{at_0}{p^2}\right)\left(\frac{bt_0}{p^2}\right)\left(\frac{c_0t_0}{p}\right) =$$
$$p^{(6k-5)/2}\varepsilon_{p^2}^2\varepsilon_p\left(\frac{c_0}{p}\right) \sum_{t_0 \in (\mathbb{Z}/p^2\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0t_0}{p}\right)\left(\frac{t_0}{p}\right).$$

By Lemma 2.9, $\varepsilon_{p^2}=1$ and

$$p^{(6k-5)/2}\varepsilon_{p^2}^2\varepsilon_p\left(\frac{c_0}{p}\right)\sum_{t_0\in(\mathbb{Z}/p^2\mathbb{Z})^*}\mathrm{e}\left(\frac{-m_0t_0}{p}\right)\left(\frac{t_0}{p}\right)=p^{(6k-5)/2}\varepsilon_p\left(\frac{c_0}{p}\right)\sum_{t_0\in(\mathbb{Z}/p^2\mathbb{Z})^*}\mathrm{e}\left(\frac{-m_0t_0}{p}\right)\left(\frac{t_0}{p}\right).$$

By Lemma 3.9,

$$p^{(6k-5)/2}\varepsilon_p\left(\frac{c_0}{p}\right)\sum_{t_0\in(\mathbb{Z}/p^2\mathbb{Z})^*}\mathrm{e}\left(\frac{-m_0t_0}{p}\right)\left(\frac{t_0}{p}\right)=p^{(6k-3)/2}\varepsilon_p\left(\frac{c_0}{p}\right)\sum_{t_1=1}^{p-1}\mathrm{e}\left(\frac{-m_0t_1}{p}\right)\left(\frac{t_1}{p}\right).$$

By Lemma 2.4,

$$p^{(6k-3)/2}\varepsilon_p\left(\frac{c_0}{p}\right)\sum_{t_1=1}^{p-1}\mathrm{e}\left(\frac{-m_0t_1}{p}\right)\left(\frac{t_1}{p}\right)=p^{(6k-3)/2}\varepsilon_p\left(\frac{c_0}{p}\right)G\left(\frac{-m_0}{p}\right).$$

By Lemma 2.10,

$$\begin{aligned}p^{(6k-3)/2}\varepsilon_p\left(\frac{c_0}{p}\right)G\left(\frac{-m_0}{p}\right)&=p^{(6k-3)/2}\varepsilon_p\left(\frac{c_0}{p}\right)p^{1/2}\left(\frac{-m_0}{p}\right)\varepsilon_p\\&=p^{3k-1}\varepsilon_p^2\left(\frac{c_0}{p}\right)\left(\frac{-m_0}{p}\right).\end{aligned}$$

By Lemma 2.8 and the multiplicative property of the Legendre symbol,

$$p^{3k-1}\varepsilon_p^2\left(\frac{c_0}{p}\right)\left(\frac{-m_0}{p}\right)=p^{3k-1}\left(\frac{-1}{p}\right)\left(\frac{-c_0m_0}{p}\right)=p^{3k-1}\left(\frac{c_0m_0}{p}\right).$$

Therefore,

$$s_{k,k-2}=p^{3k-1}\left(\frac{c_0m_0}{p}\right). \tag{3.20}$$

Now suppose that $0\le\tau<k-2$. Then, by Lemma 2.11,

$$\begin{aligned}s_{k,\tau}&=\sum_{t_0\in(\mathbb{Z}/p^{k-\tau}\mathbb{Z})^*}\mathrm{e}\left(\frac{-m_0t_0}{p^{k-\tau-1}}\right)G\left(\frac{at_0p^\tau}{p^k}\right)G\left(\frac{bt_0p^\tau}{p^k}\right)G\left(\frac{c_0t_0p^{\tau+1}}{p^k}\right)\\&=\sum_{t_0\in(\mathbb{Z}/p^{k-\tau}\mathbb{Z})^*}\mathrm{e}\left(\frac{-m_0t_0}{p^{k-\tau-1}}\right)p^{k+\tau}\left(\frac{at_0}{p^{k-\tau}}\right)\varepsilon_{p^{k-\tau}}^2\left(\frac{bt_0}{p^{k-\tau}}\right)p^{(k+\tau+1)/2}\left(\frac{c_0t_0}{p^{k-\tau-1}}\right)\varepsilon_{p^{k-\tau-1}}\\&=p^{(3k+3\tau+1)/2}\varepsilon_{p^{k-\tau}}^2\varepsilon_{p^{k-\tau-1}}\sum_{t_0\in(\mathbb{Z}/p^{k-\tau}\mathbb{Z})^*}\mathrm{e}\left(\frac{-m_0t_0}{p^{k-\tau-1}}\right)\left(\frac{at_0}{p^{k-\tau}}\right)\left(\frac{bt_0}{p^{k-\tau}}\right)\left(\frac{c_0t_0}{p^{k-\tau-1}}\right).\end{aligned}$$

By Lemma 2.8 and the definition of the Jacobi symbol,

$$\begin{aligned}&p^{(3k+3\tau+1)/2}\varepsilon_{p^{k-\tau}}^2\varepsilon_{p^{k-\tau-1}}\sum_{t_0\in(\mathbb{Z}/p^{k-\tau}\mathbb{Z})^*}\mathrm{e}\left(\frac{-m_0t_0}{p^{k-\tau-1}}\right)\left(\frac{at_0}{p^{k-\tau}}\right)\left(\frac{bt_0}{p^{k-\tau}}\right)\left(\frac{c_0t_0}{p^{k-\tau-1}}\right)\\&=p^{(3k+3\tau+1)/2}\left(\frac{-1}{p^{k-\tau}}\right)\left(\frac{ab}{p^{k-\tau}}\right)\varepsilon_{p^{k-\tau-1}}\sum_{t_0\in(\mathbb{Z}/p^{k-\tau}\mathbb{Z})^*}\mathrm{e}\left(\frac{-m_0t_0}{p^{k-\tau-1}}\right)\left(\frac{t_0}{p^{k-\tau}}\right)^2\left(\frac{c_0t_0}{p^{k-\tau-1}}\right)\\&=p^{(3k+3\tau+1)/2}\left(\frac{-ab}{p^{k-\tau}}\right)\varepsilon_{p^{k-\tau-1}}\left(\frac{c_0}{p^{k-\tau-1}}\right)\sum_{t_0\in(\mathbb{Z}/p^{k-\tau}\mathbb{Z})^*}\mathrm{e}\left(\frac{-m_0t_0}{p^{k-\tau-1}}\right)\left(\frac{t_0}{p^{k-\tau}}\right)^2\left(\frac{t_0}{p}\right)^{k-\tau-1}.\end{aligned}$$

Because $t_0 \in (\mathbb{Z}/p^{k-\tau}\mathbb{Z})^*$, $\left(\frac{t_0}{p^{k-\tau}}\right)^2 = 1$ and

$$\sum_{t_0 \in (\mathbb{Z}/p^{k-\tau}\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0 t_0}{p^{k-\tau-1}}\right)\left(\frac{t_0}{p^{k-\tau}}\right)^2\left(\frac{t_0}{p}\right)^{k-\tau-1} = \sum_{t_0 \in (\mathbb{Z}/p^{k-\tau}\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0 t_0}{p^{k-\tau-1}}\right)\left(\frac{t_0}{p}\right)^{k-\tau-1}.$$

By Lemma 3.9,

$$\sum_{t_0 \in (\mathbb{Z}/p^{k-\tau}\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0 t_0}{p^{k-\tau-1}}\right)\left(\frac{t_0}{p}\right)^{k-\tau-1}$$
$$= \sum_{t_1=1}^{p-1} \mathrm{e}\left(\frac{-m_0 t_1}{p^{k-\tau-1}}\right)\left(\frac{t_1}{p}\right)^{k-\tau-1} \sum_{t_2=0}^{p^{\tau-1}-1} \mathrm{e}\left(\frac{-m_0 t_2 p}{p^{k-\tau-1}}\right)\left(\frac{t_2 p}{p}\right)^{k-\tau-1}.$$

Because $\left(\frac{t_2 p}{p}\right) = 0$ for any $t_2 \in \mathbb{Z}$,

$$\sum_{t_1=1}^{p-1} \mathrm{e}\left(\frac{-m_0 t_1}{p^{k-\tau-1}}\right)\left(\frac{t_1}{p}\right)^{k-\tau-1} \sum_{t_2=0}^{p^{\tau-1}-1} \mathrm{e}\left(\frac{-m_0 t_2 p}{p^{k-\tau-1}}\right)\left(\frac{t_2 p}{p}\right)^{k-\tau-1}$$
$$= \sum_{t_1=1}^{p-1} \mathrm{e}\left(\frac{-m_0 t_1}{p^{k-\tau-1}}\right)\left(\frac{t_1}{p}\right)^{k-\tau-1} \sum_{t_2=0}^{p^{\tau-1}-1} \mathrm{e}\left(\frac{-m_0 t_2 p}{p^{k-\tau-1}}\right) \cdot 0^{k-\tau-1} = 0.$$

Therefore, if $0 \le \tau < k-2$, then

$$s_{k,\tau} = p^{(3k+3\tau+1)/2}\left(\frac{-ab}{p^{k-\tau}}\right)\varepsilon_{p^{k-\tau-1}}\left(\frac{c_0}{p^{k-\tau-1}}\right) \cdot 0 = 0. \tag{3.21}$$

Using (3.19), (3.20), and (3.21), substitute into (3.18) to find that

$$\begin{aligned} r_{p^k,Q}(m) &= p^{2k} + \frac{1}{p^k}\left(s_{k,k-1} + s_{k,k-2} + \sum_{\tau=0}^{k-3} s_{k,\tau}\right) \\ &= p^{2k} + \frac{1}{p^k}\left(p^{3k-1}\left(\frac{-ab}{p}\right)(p-1) + p^{3k-1}\left(\frac{c_0 m_0}{p}\right) + \sum_{\tau=0}^{k-3} 0\right) \\ &= p^{2k}\left(1 + \frac{1}{p}\left(\frac{c_0 m_0}{p}\right) + \left(\frac{-ab}{p}\right)\left(1 - \frac{1}{p}\right)\right). \end{aligned}$$

Now suppose $k \ge 2$, $p \nmid ab$, and $p^2 \mid c$. Let $(x_0, y_0, z_0)^T$ be a solution to $Q(\vec{\mathbf{x}}) \equiv m \pmod{p^2}$. Let $c = c_1 p^2$ for some $c_1 \in \mathbb{Z}$. Toward contradiction, assume that $p \mid ax_0$, $p \mid by_0$, and $p \mid cz_0$. Since $p \nmid ab$, $x_0 = x_1 p$ and $y_0 = y_1 p$ for some $x_1, y_1, \in \mathbb{Z}$. Thus,

$$\begin{aligned} ax_0^2 + by_0^2 + cz_0^2 &= a(x_1 p)^2 + b(y_1 p)^2 + c_1 p^2 z_0^2 \\ &= ax_1^2 p^2 + by_1^2 p^2 + cz_0^2 p^2 \\ &\equiv 0 \pmod{p^2}. \end{aligned}$$

However, this contradicts the fact that $m \not\equiv 0 \pmod{p^2}$ since $p \parallel m$. Therefore, for any solution $(x_0, y_0, z_0)^T$ to $Q(\vec{\mathbf{x}}) \equiv m \pmod{p^2}$, $p \nmid ax_0$, $p \nmid by_0$, or $p \nmid cz_0$. Thus, Corollary 3.4

can be used once $r_{p^2,Q}(m)$ is known. In this case, by Corollary 3.2,

$$\begin{aligned} r_{p^2,Q}(m) &= p^4 + \frac{1}{p^2}\sum_{t=1}^{p^2-1} \mathrm{e}\left(\frac{-mt}{p^2}\right) G\left(\frac{at}{p^2}\right) G\left(\frac{bt}{p^2}\right) G\left(\frac{ct}{p^2}\right) \\ &= p^4 + \frac{1}{p^2}\sum_{t=1}^{p^2-1} \mathrm{e}\left(\frac{-m_0 t}{p}\right) G\left(\frac{at}{p^2}\right) G\left(\frac{bt}{p^2}\right) G\left(\frac{c_1 p^2 t}{p^2}\right). \end{aligned} \tag{3.22}$$

By Lemma 2.11,

$$\begin{aligned} \sum_{t=1}^{p^2-1} \mathrm{e}\left(\frac{-m_0 t}{p}\right) G\left(\frac{at}{p^2}\right) G\left(\frac{bt}{p^2}\right) G\left(\frac{c_1 p^2 t}{p^2}\right) &= \sum_{t=1}^{p^2-1} \mathrm{e}\left(\frac{-m_0 t}{p}\right) G\left(\frac{at}{p^2}\right) G\left(\frac{bt}{p^2}\right) p^2 \\ &= p^2 \sum_{t=1}^{p^2-1} \mathrm{e}\left(\frac{-m_0 t}{p}\right) G\left(\frac{at}{p^2}\right) G\left(\frac{bt}{p^2}\right). \end{aligned} \tag{3.23}$$

By Lemma 3.8,

$$\begin{aligned} &\sum_{t=1}^{p^2-1} \mathrm{e}\left(\frac{-m_0 t}{p}\right) G\left(\frac{at}{p^2}\right) G\left(\frac{bt}{p^2}\right) \\ &\qquad = \sum_{\tau=0}^{1} \sum_{t_0 \in (\mathbb{Z}/p^{2-\tau}\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0 t_0 p^\tau}{p}\right) G\left(\frac{at_0 p^\tau}{p^2}\right) G\left(\frac{bt_0 p^\tau}{p^2}\right). \end{aligned} \tag{3.24}$$

Suppose that $\tau = 0$. Then

$$\sum_{t_0 \in (\mathbb{Z}/p^{2-\tau}\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0 t_0 p^\tau}{p}\right) G\left(\frac{at_0 p^\tau}{p^2}\right) G\left(\frac{bt_0 p^\tau}{p^2}\right) = \sum_{t_0 \in (\mathbb{Z}/p^2\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0 t_0}{p}\right) G\left(\frac{at_0}{p^2}\right) G\left(\frac{bt_0}{p^2}\right).$$

By Lemma 2.10,

$$\begin{aligned} \sum_{t_0 \in (\mathbb{Z}/p^2\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0 t_0}{p}\right) G\left(\frac{at_0}{p^2}\right) G\left(\frac{bt_0}{p^2}\right) &= \sum_{t_0 \in (\mathbb{Z}/p^2\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0 t_0}{p}\right) p \left(\frac{at_0}{p^2}\right) \varepsilon_{p^2} p \left(\frac{bt_0}{p^2}\right) \varepsilon_{p^2} \\ &= p^2 \varepsilon_{p^2}^2 \sum_{t_0 \in (\mathbb{Z}/p^2\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0 t_0}{p}\right) \left(\frac{at_0}{p^2}\right) \left(\frac{bt_0}{p^2}\right). \end{aligned}$$

By Lemma 2.9, $\varepsilon_{p^2} = 1$, so

$$p^2 \varepsilon_{p^2}^2 \sum_{t_0 \in (\mathbb{Z}/p^2\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0 t_0}{p}\right) \left(\frac{at_0}{p^2}\right) \left(\frac{bt_0}{p^2}\right) = p^2 \sum_{t_0 \in (\mathbb{Z}/p^2\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0 t_0}{p}\right) \left(\frac{at_0}{p^2}\right) \left(\frac{bt_0}{p^2}\right).$$

By the definition of the Jacobi symbol,

$$p^2 \sum_{t_0 \in (\mathbb{Z}/p^2\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0 t_0}{p}\right) \left(\frac{at_0}{p^2}\right) \left(\frac{bt_0}{p^2}\right) = p^2 \sum_{t_0 \in (\mathbb{Z}/p^2\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0 t_0}{p}\right) \left(\frac{at_0}{p}\right)^2 \left(\frac{bt_0}{p}\right)^2.$$

Since $p \nmid at_0$ and $p \nmid bt_0$, $\left(\frac{at_0}{p}\right)^2 = \left(\frac{bt_0}{p}\right)^2 = 1$, so

$$p^2 \sum_{t_0 \in (\mathbb{Z}/p^2\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0 t_0}{p}\right) \left(\frac{at_0}{p}\right)^2 \left(\frac{bt_0}{p}\right)^2 = p^2 \sum_{t_0 \in (\mathbb{Z}/p^2\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0 t_0}{p}\right).$$

By Lemma 3.9,

$$p^2 \sum_{t_0 \in (\mathbb{Z}/p^2\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0 t_0}{p}\right) = p^3 \sum_{t_1=1}^{p-1} \mathrm{e}\left(\frac{-m_0 t_1}{p}\right).$$

By Lemma 2.3,

$$p^3 \sum_{t_1=1}^{p-1} \mathrm{e}\left(\frac{-m_0 t_1}{p}\right) = -p^3.$$

Therefore, if $\tau = 0$, then

$$\sum_{t_0 \in (\mathbb{Z}/p^{2-\tau}\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0 t_0 p^\tau}{p}\right) G\left(\frac{at_0 p^\tau}{p^2}\right) G\left(\frac{bt_0 p^\tau}{p^2}\right) = -p^3. \tag{3.25}$$

Suppose $\tau = 1$. Then

$$\begin{aligned}\sum_{t_0 \in (\mathbb{Z}/p^{2-\tau}\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0 t_0 p^\tau}{p}\right) G\left(\frac{at_0 p^\tau}{p^2}\right) G\left(\frac{bt_0 p^\tau}{p^2}\right) &= \sum_{t_0 \in (\mathbb{Z}/p\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0 t_0 p}{p}\right) G\left(\frac{at_0 p}{p^2}\right) G\left(\frac{bt_0 p}{p^2}\right) \\ &= \sum_{t_0=1}^{p-1} \mathrm{e}(-m_0 t_0)\, G\left(\frac{at_0 p}{p^2}\right) G\left(\frac{bt_0 p}{p^2}\right) \\ &= \sum_{t_0=1}^{p-1} G\left(\frac{at_0 p}{p^2}\right) G\left(\frac{bt_0 p}{p^2}\right).\end{aligned}$$

By Lemma 2.11,

$$\begin{aligned}\sum_{t_0=1}^{p-1} G\left(\frac{at_0 p}{p^2}\right) G\left(\frac{bt_0 p}{p^2}\right) &= \sum_{t_0=1}^{p-1} p^{3/2} \left(\frac{at_0}{p}\right) \varepsilon_p p^{3/2} \left(\frac{bt_0}{p}\right) \varepsilon_p \\ &= p^3 \varepsilon_p^2 \sum_{t_0=1}^{p-1} \left(\frac{at_0}{p}\right) \left(\frac{bt_0}{p}\right).\end{aligned}$$

By applying Lemma 2.8 and the multiplicative property of the Legendre symbol, we have

$$p^3 \varepsilon_p^2 \sum_{t_0=1}^{p-1} \left(\frac{at_0}{p}\right) \left(\frac{bt_0}{p}\right) = p^3 \left(\frac{-1}{p}\right) \left(\frac{ab}{p}\right) \sum_{t_0=1}^{p-1} \left(\frac{t_0}{p}\right)^2 = p^3 \left(\frac{-ab}{p}\right) \sum_{t_0=1}^{p-1} \left(\frac{t_0}{p}\right)^2.$$

Since $t_0 \not\equiv 0 \pmod{p}$ if $1 \le t_0 \le p-1$, $\left(\frac{t_0}{p}\right)^2 = 1$ and

$$p^3 \left(\frac{-ab}{p}\right) \sum_{t_0=1}^{p-1} \left(\frac{t_0}{p}\right)^2 = p^3 \left(\frac{-ab}{p}\right) \sum_{t_0=1}^{p-1} 1 = p^3 \left(\frac{-ab}{p}\right) (p-1).$$

Thus, if $\tau = 1$, then

$$\sum_{t_0 \in (\mathbb{Z}/p^{2-\tau}\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0 t_0 p^\tau}{p}\right) G\left(\frac{a t_0 p^\tau}{p^2}\right) G\left(\frac{b t_0 p^\tau}{p^2}\right) = p^3 \left(\frac{-ab}{p}\right)(p-1). \tag{3.26}$$

After using (3.23), (3.24), (3.25), and (3.26) to substitute into (3.22), we see that

$$\begin{aligned} r_{p^2,Q}(m) &= p^4 + \frac{1}{p^2} p^2 \left(-p^3 + p^3 \left(\frac{-ab}{p}\right)(p-1)\right) \\ &= p^4 \left(1 - \frac{1}{p}\right)\left(1 + \left(\frac{-ab}{p}\right)\right). \end{aligned}$$

Therefore, if $k \geq 2$, $p \nmid ab$, and $p^2 \mid c$, we apply Corollary 3.4 and see that

$$r_{p^k,Q}(m) = p^{2k} \left(1 - \frac{1}{p}\right)\left(1 + \left(\frac{-ab}{p}\right)\right).$$

□

Combined with Theorems 3.6 and 3.10, Theorem 3.11 allows us to determine if a square-free integer m is locally represented at the odd prime p given that a, b, and c are pairwise coprime.

The next formula we have for $r_{p^k,Q}(m)$ concerns the case in which p exactly divides m, p does not divide a, and p^2 divides b and c.

Theorem 3.12. *Let p be a prime. If $p \parallel m$, $p \nmid a$, $p^2 \mid b$ and $p^2 \mid c$, then*

$$r_{p^k,Q}(m) = \begin{cases} p^2 & \text{if } k = 1, \\ 0, & \text{if } k \geq 2. \end{cases}$$

Proof. Because p divides b, c, and m, a solution to the congruence $Q(\vec{\mathbf{v}}) = ax^2 + by^2 + cz^2 \equiv m \pmod{p}$ would satisfy $ax^2 \equiv 0 \pmod{p}$. Since $a \not\equiv 0 \pmod{p}$, this implies $x^2 \equiv 0 \pmod{p}$. Because p is prime, we see that p divides x, i.e., $x = x_0 p$ for some $x_0 \in \mathbb{Z}$ and $x \equiv 0 \pmod{p}$. Therefore, at $k = 1$, x must be congruent to $0 \pmod{p}$, and y and z are free to be anything in $\mathbb{Z}/p\mathbb{Z}$. This gives p^2 solutions to $Q(\vec{\mathbf{v}}) \equiv m \pmod{p}$, where $\vec{\mathbf{v}} \in (\mathbb{Z}/p\mathbb{Z})^3$.

Furthermore, because $p^2 \mid b$ and $p^2 \mid c$,

$$Q(\vec{\mathbf{v}}) = ax^2 + by^2 + cz^2 = a(x_0 p)^2 + by^2 + cz^2 \equiv 0 \pmod{p^2}.$$

However, since $p \parallel m$, $m \not\equiv 0 \pmod{p^2}$. Therefore, there are no solutions to $Q(\vec{\mathbf{v}}) \equiv m \pmod{p^2}$ if $p^2 \mid b$ and $p^2 \mid c$. This makes it impossible to have solutions for $Q(\vec{\mathbf{v}}) \equiv m \pmod{p^k}$ for $k \geq 2$ if $p^2 \mid b$ and $p^2 \mid c$, so $r_{p^k,Q}(m) = 0$ for $k \geq 2$ if $p^2 \mid b$ and $p^2 \mid c$. □

So far in this section we have focused on computing $r_{p^k,Q}(m)$ when p is an odd prime. For the remainder of this section we consider $r_{p^k,Q}(m)$ when $p = 2$. Before we can develop closed-form formulas for $r_{2^k,Q}(m)$. We state a theorem similar to Theorem 3.3 that is applicable to powers of 2.

Theorem 3.13 (Hensel's Lemma for powers of 2)**.** *Let m be an integer. Suppose $\vec{\mathbf{v}}_0 = (x_0, y_0, z_0)^T$ is a solution to $Q(\vec{\mathbf{v}}) \equiv m \pmod{2^k}$ for some $k \geq 3$. If $2 \nmid ax_0$, $2 \nmid by_0$, or $2 \nmid cz_0$, then there are exactly 32 solutions to $Q(\vec{\mathbf{v}}) \equiv m \pmod{2^{k+1}}$ of the form $(x_0 + 2^{k-1}x_1, y_0 + 2^{k-1}y_1, z_0 + 2^{k-1}z_1)^T$, where $x_1, y_1, z_1 \in \mathbb{Z}/4\mathbb{Z}$.*

Proof. Without loss of generality, assume that $2 \nmid ax_0$.

We first prove that there exists a solution to $Q(\vec{\mathbf{v}}) \equiv m \pmod{2^{k+1}}$ of the form $(x_0 + x_1 2^{k-1}, y_0 + y_1 2^{k-1}, z_0 + z_1 2^{k-1})^T$. Because $Q(\vec{\mathbf{v}}_0) \equiv m \pmod{2^k}$, there exists $\ell \in \mathbb{Z}$ such that

$$ax_0^2 + by_0^2 + cz_0^2 = m + 2^k \ell. \tag{3.27}$$

For any $x_1, y_1, z_1 \in \mathbb{Z}/4\mathbb{Z}$, we expand

$$a(x_0 + 2^{k-1}x_1)^2 + b(y_0 + 2^{k-1}y_1)^2 + c(z_0 + 2^{k-1}z_1)^2 - m$$

to obtain

$$ax_0^2 + 2^k ax_0x_1 + 2^{2k-2}ax_1^2 + by_0^2 + 2^k by_0y_1 + 2^{2k-2}by_1^2 + cz_0^2 + 2^k cz_0z_1 + 2^{2k-2}cz_1^2 - m.$$

By rearranging terms in the last expression, we have

$$(ax_0^2 + by_0^2 + cz_0^2) - m + 2^k ax_0x_1 + 2^k by_0y_1 + 2^k cz_0z_1 + 2^{2k-2}ax_1^2 + 2^{2k-2}by_1^2 + 2^{2k-2}cz_1^2.$$

We use (3.27) to rewrite this as

$$\begin{aligned} m + 2^k\ell - m + 2^k ax_0x_1 + 2^k by_0y_1 + 2^k cz_0z_1 + 2^{2k-2}ax_1^2 + 2^{2k-2}by_1^2 + 2^{2k-2}cz_1^2 \\ = 2^k(\ell + ax_0x_1 + by_0y_1 + cz_0z_1) + 2^{2k-2}(ax_1^2 + by_1^2 + cz_1^2). \end{aligned} \tag{3.28}$$

Because $k \geq 3$, $2^{2k-2} \geq 2^{k+1}$, so when we take (3.28) modulo 2^{k+1}, we get

$$\begin{aligned} a(x_0 + 2^{k-1}x_1)^2 + b(y_0 + 2^{k-1}y_1)^2 + c(z_0 + 2^{k-1}z_1)^2 - m \\ \equiv 2^k(\ell + ax_0x_1 + by_0y_1 + cz_0z_1) \pmod{2^{k+1}}. \end{aligned} \tag{3.29}$$

Let

$$x_1 = (ax_0)^{-1}(-\ell - by_0y_1 - cz_0z_1), \tag{3.30}$$

where $ax_0(ax_0)^{-1} \equiv 1 \pmod 2$ if and only if $2ax_0(2ax_0)^{-1} = 1 + 2t$ for some $t \in \mathbb{Z}$. Note that $(ax_0)^{-1}$ exists since $2 \nmid ax_0$. Then use (3.30) to substitute for x_1 in (3.29) to get

$$\begin{aligned} a(x_0 + 2^{k-1}x_1)^2 + b(y_0 + 2^{k-1}y_1)^2 + c(z_0 + 2^{k-1}z_1)^2 - m \\ \equiv 2^k(\ell + ax_0(ax_0)^{-1}(-\ell - by_0y_1 - cz_0z_1) + by_0y_1 + cz_0z_1) \pmod{2^{k+1}}. \end{aligned}$$

Replace $ax_0(ax_0)^{-1}$ by $1 + 2t$ to see that

$$\begin{aligned} a(x_0 + 2^{k-1}x_1)^2 + b(y_0 + 2^{k-1}y_1)^2 + c(z_0 + 2^{k-1}z_1)^2 - m \\ \equiv 2^k(\ell + (1 + 2t)(-\ell - by_0y_1 - cz_0z_1) + by_0y_1 + cz_0z_1) \pmod{2^{k+1}}. \end{aligned}$$

Expand and cancel like terms to simplify the expression to

$$\begin{aligned} a(x_0 + 2^{k-1}x_1)^2 + b(y_0 + 2^{k-1}y_1)^2 + c(z_0 + 2^{k-1}z_1)^2 - m &\equiv 2^{k+1}t(-\ell - 2by_0y_1 - 2cz_0z_1) \\ &\equiv 0 \pmod{2^{k+1}}. \end{aligned}$$

Thus, there exists a solution to $Q(\vec{\mathbf{v}}) \equiv m \pmod{2^{k+1}}$ of the form $(x_0 + x_1 2^{k-1}, y_0 + y_1 2^{k-1}, z_0 + z_1 2^{k-1})^T$.

Conversely, if $a(x_0 + 2^{k-1}x_1)^2 + b(y_0 + 2^{k-1}y_1)^2 + c(z_0 + 2^{k-1}z_1)^2 \equiv m \pmod{2^{k+1}}$, then by using (3.29), we see that

$$2^k(\ell + ax_0x_1 + by_0y_1 + cz_0z_1) \equiv 0 \pmod{2^{k+1}}$$

for some $\ell \in \mathbb{Z}$. We divide by 2^k to see that this is equivalent to

$$\ell + ax_0x_1 + by_0y_1 + cz_0z_1 \equiv 0 \pmod 2.$$

Solve this congruence for x_1 to get

$$x_1 \equiv (ax_0)^{-1}(-\ell - by_0y_1 - cz_0z_1) \pmod 2. \tag{3.31}$$

Congruence (3.31) shows that $x_1 \in \mathbb{Z}/4\mathbb{Z}$ is determined (mod 2) by the choices of y_1 and z_1. Since $x_1 \in \mathbb{Z}/4\mathbb{Z}$, there are exactly 2 choices for x_1 once y_1 and z_1 have been chosen. Because there are no restrictions on $y_1, z_1 \in \mathbb{Z}/4\mathbb{Z}$, there are 4 choices for y_1 and 4 choices for z_1. Therefore, there are exactly 32 solutions to $Q(\vec{\mathbf{v}}) \equiv m \pmod{2^{k+1}}$ of the form $(x_0 + 2^{k-1}x_1, y_0 + 2^{k-1}y_1, z_0 + 2^{k-1}z_1)^T$, where $x_1, y_1, z_1 \in \mathbb{Z}/4\mathbb{Z}$. □

The next corollary is similar to Corollary 3.4. The corollary allows us under certain conditions to state how many solutions there are in $(\mathbb{Z}/2^{k+\ell}\mathbb{Z})^3$ to $Q(\vec{\mathbf{v}}) \equiv m \pmod{2^{k+\ell}}$ given the number of solutions in $(\mathbb{Z}/2^k\mathbb{Z})^3$ to $Q(\vec{\mathbf{v}}) \equiv m \pmod{2^k}$.

Corollary 3.14. *Let $k \geq 3$. Suppose that $\{(x_1, y_1, z_1)^T, \ldots, (x_n, y_n, z_n)^T\}$ is the set of the $n = r_{2^k,Q}(m)$ solutions in $(\mathbb{Z}/2^k\mathbb{Z})^3$ to $Q(\vec{\mathbf{v}}) \equiv m \pmod{2^k}$, and suppose that $2 \nmid ax_j$, $2 \nmid by_j$, or $2 \nmid cz_j$ for each $j \in \mathbb{Z}$, $1 \leq j \leq r_{2^k,Q}(m)$. Then there are exactly $r_{2^k,Q}(m) \cdot 2^{2\ell}$ solutions in $(\mathbb{Z}/2^{k+\ell}\mathbb{Z})^3$ to $Q(\vec{\mathbf{v}}) \equiv m \pmod{2^{k+\ell}}$ for $\ell \geq 0$. Furthermore, each of the solutions $(x_0, y_0, z_0)^T$ in $(\mathbb{Z}/2^{k+\ell}\mathbb{Z})^3$ to $Q(\vec{\mathbf{v}}) \equiv m \pmod{2^{k+\ell}}$ satisfies the property that $2 \nmid ax_0$, $2 \nmid by_0$, or $2 \nmid cz_0$.*

Proof. The corollary is clearly true when $\ell = 0$.

Let $n = r_{2^k,Q}(m)$. Assume that there are exactly $2^{2\ell}n$ solutions in $(\mathbb{Z}/2^{k+\ell}\mathbb{Z})^3$ to $Q(\vec{\mathbf{v}}) \equiv m \pmod{2^{k+\ell}}$ for some $\ell \geq 0$. Let $\{(x_1, y_1, z_1)^T, \ldots, (x_{2^{2\ell}n}, y_{2^{2\ell}n}, z_{2^{2\ell}n})^T\}$ be the set of the $2^{2\ell}n$ solutions in $(\mathbb{Z}/2^{k+\ell}\mathbb{Z})^3$ to $Q(\vec{\mathbf{v}}) \equiv m \pmod{2^{k+\ell}}$. Assume that $p \nmid ax_j$, $p \nmid by_j$, or $p \nmid cz_j$ for each $j \in \mathbb{Z}$, $1 \leq j \leq 2^{2\ell}n$.

According to Theorem 3.13, for each solution $(x_j, y_j, z_j)^T$ in $\mathbb{Z}/2^{k+\ell}\mathbb{Z}$ to $Q(\vec{\mathbf{v}}) \equiv m \pmod{2^{k+\ell}}$, there exist 32 solutions to $Q(\vec{\mathbf{v}}) \equiv m \pmod{2^{k+\ell+1}}$ of the form $(x_j + 2^{k+\ell-1}x'_j, y_j + 2^{k+\ell-1}y'_j, z_j + 2^{k+\ell-1}z'_j)^T$, where $x'_j, y'_j, z'_j \in \mathbb{Z}/4\mathbb{Z}$. Since $2 \nmid ax_j$, $2 \nmid by_j$, or $2 \nmid cz_j$, we see that

$$\begin{aligned} 2 &\nmid a(x_j + 2^{k+\ell-1}x'_j) = ax_j + 2^{k+\ell}ax'_j, \\ 2 &\nmid b(y_j + 2^{k+\ell-1}y'_j) = by_j + 2^{k+\ell}by'_j, \text{ or} \\ 2 &\nmid c(z_j + 2^{k+\ell-1}z'_j) = cz_j + 2^{k+\ell}cz'_j. \end{aligned}$$

Let $1 \leq j_1, j_2 \leq 2^{2\ell}n$. Suppose that

$$\begin{aligned} x_{j_1} + 2^{k+\ell-1}x'_{j_1} &\equiv x_{j_2} + 2^{k+\ell-1}x'_{j_2} \pmod{2^{k+\ell+1}}, \\ y_{j_1} + 2^{k+\ell-1}y'_{j_1} &\equiv y_{j_2} + 2^{k+\ell-1}y'_{j_2} \pmod{2^{k+\ell+1}}, \text{ and} \\ z_{j_1} + 2^{k+\ell-1}z'_{j_1} &\equiv z_{j_2} + 2^{k+\ell-1}z'_{j_2} \pmod{2^{k+\ell+1}}. \end{aligned} \tag{3.32}$$

Congruence (3.32) implies that

$$(x_{j_1} - x_{j_2}) + 2^{k+\ell-1}(x'_{j_1} - x'_{j_2}) \equiv 0 \pmod{2^{k+\ell+1}},$$

which is equivalent to saying that

$$(x_{j_1} - x_{j_2}) + 2^{k+\ell-1}(x'_{j_1} - x'_{j_2}) = 2^{k+\ell+1}t$$

for some $t \in \mathbb{Z}$. Since $2^{k+\ell-1}$ divides $2^{k+\ell-1}(x'_{j_1} - x'_{j_2})$ and $2^{k+\ell+1}t$, we have $2^{k+\ell-1}$ divides $x_{j_1} - x_{j_2}$ and

$$x_{j_1} \equiv x_{j_2} \pmod{2^{k+\ell-1}}.$$

As shown in a similar manner, $y_{j_1} \equiv y_{j_2} \pmod{2^{k+\ell-1}}$ and $z_{j_1} \equiv z_{j_2} \pmod{2^{k+\ell-1}}$.

Conversely, suppose that

$$\begin{aligned} x_{j_1} &\equiv x_{j_2} \pmod{2^{k+\ell-1}}, \\ y_{j_1} &\equiv y_{j_2} \pmod{2^{k+\ell-1}}, \text{ and} \\ z_{j_1} &\equiv z_{j_2} \pmod{2^{k+\ell-1}}. \end{aligned}$$

Then there exists $t_x, t_y, t_z \in \mathbb{Z}$ so that

$$\begin{aligned} x_{j_1} &= x_{j_2} + 2^{k+\ell-1}t_x, \\ y_{j_1} &= y_{j_2} + 2^{k+\ell-1}t_y, \text{ and} \\ z_{j_1} &= z_{j_2} + 2^{k+\ell-1}t_z. \end{aligned}$$

Let $S_{k+\ell+1,j}$ be the set of the 32 solutions to $Q(\vec{\mathbf{v}}) \equiv m \pmod{p^{k+\ell+1}}$ of the form $(x_j + 2^{k+\ell-1}x'_j, y_j + 2^{k+\ell-1}y'_j, z_j + 2^{k+\ell-1}z'_j)^T$, $1 \leq j \leq 2^{2\ell}n$. Let $(x_{j_1} + 2^{k+\ell-1}x'_{j_1}, y_{j_1} + 2^{k+\ell-1}y'_{j_1}, z_{j_1} + 2^{k+\ell-1}z'_{j_1})^T \in S_{k+\ell+1,j_1}$. Observe that

$$\begin{aligned} x_{j_1} + 2^{k+\ell-1}x'_{j_1} &= x_{j_2} + 2^{k+\ell-1}t_x + 2^{k+\ell-1}x'_{j_1} = x_{j_2} + 2^{k+\ell-1}(t_x + x'_{j_1}), \\ y_{j_1} + 2^{k+\ell-1}y'_{j_1} &= y_{j_2} + 2^{k+\ell-1}t_y + 2^{k+\ell-1}y'_{j_1} = y_{j_2} + 2^{k+\ell-1}(t_y + y'_{j_1}), \text{ and} \\ z_{j_1} + 2^{k+\ell-1}z'_{j_1} &= z_{j_2} + 2^{k+\ell-1}t_z + 2^{k+\ell-1}z'_{j_1} = z_{j_2} + 2^{k+\ell-1}(t_z + z'_{j_1}). \end{aligned}$$

Therefore, $(x_{j_1} + 2^{k+\ell-1}x'_{j_1}, y_{j_1} + 2^{k+\ell-1}y'_{j_1}, z_{j_1} + 2^{k+\ell-1}z'_{j_1})^T \in S_{k+\ell+1,j_2}$, and $S_{k+\ell+1,j_1} \subseteq S_{k+\ell+1,j_2}$. It can be shown in a similar manner that $S_{k+\ell+1,j_2} \subseteq S_{k+\ell+1,j_1}$, so $S_{k+\ell+1,j_1} = S_{k+\ell+1,j_2}$.

To summarize, if $1 \leq j_1, j_2 \leq 2^{2\ell}n$, then

$$S_{k+\ell+1,j_1} \cap S_{k+\ell+1,j_2} = \begin{cases} S_{k+\ell+1,j_1} = S_{k+\ell+1,j_2}, & \text{if } x_{j_1} - x_{j_2} \equiv y_{j_1} - y_{j_2} \equiv z_{j_1} - z_{j_2} \equiv 0 \pmod{2^{k+\ell-1}}, \\ \emptyset, & \text{otherwise.} \end{cases}$$

Given a solution in $(x_{j_1}, y_{j_1}, z_{j_1})^T$ in $(\mathbb{Z}/2^{k+\ell}\mathbb{Z})^3$, there are only 2 choices for in $x_{j_2} \in \mathbb{Z}/2^{k+\ell}\mathbb{Z}$ where $x_{j_2} \equiv x_{j_1} \pmod{2^{k+\ell-1}}$, only 2 choices for in $y_{j_2} \in \mathbb{Z}/2^{k+\ell}\mathbb{Z}$ where $y_{j_2} \equiv y_{j_1} \pmod{2^{k+\ell-1}}$, and only 2 choices for in $z_{j_2} \in \mathbb{Z}/2^{k+\ell}\mathbb{Z}$ where $z_{j_2} \equiv z_{j_1} \pmod{2^{k+\ell-1}}$. Thus, there are 8 solutions in $(\mathbb{Z}/2^{k+\ell}\mathbb{Z})^3$ of the form $(x_j, y_j, z_j)^T$ such that $S_{k+\ell+1,j} = S_{k+\ell+1,j_1}$. This means that every solution to $Q(\vec{\mathbf{v}}) \equiv m \pmod{2^{k+1}}$ of the form $(x_j + 2^{k-1}x'_j, y_j + 2^{k-1}y'_j, z_j + 2^{k-1}z'_j)^T$ is counted 8 times. Therefore, there are $2^{2\ell}n \cdot \frac{32}{8} = 2^{2\ell}n \cdot 2^2 = 2^{2(\ell+1)}n$ solutions to $Q(\vec{\mathbf{v}}) \equiv m \pmod{2^{k+\ell+1}}$. By the principle of mathematical induction, the corollary follows. □

Before computing $r_{2^k,Q}(m)$, we define w, κ_w, and λ_w for the quadratic form $Q(\vec{\mathbf{v}}) = ax^2 + by^2 + cz^2$. Define w to be the number of elements in $\{a, b, c\}$ that are congruent to 3 (mod 4), $\kappa_w = 4(-w^2 + 3w - 1)$, and $\lambda_w = 4 \cdot (-1)^{\lfloor w/2 \rfloor}$. The next lemma relates κ_w and λ_w to ρ_a, ρ_b, and ρ_c.

Lemma 3.15. *For the quadratic form* $Q(\vec{\mathbf{v}}) = ax^2 + by^2 + cz^2$,

$$\kappa_w = 2\mathrm{Re}(\rho_a\rho_b\rho_c) = \rho_a\rho_b\rho_c + \bar{\rho}_a\bar{\rho}_b\bar{\rho}_c$$

and

$$\lambda_w = 2\mathrm{Im}(\rho_a\rho_b\rho_c) = -i\rho_a\rho_b\rho_c + i\bar{\rho}_a\bar{\rho}_b\bar{\rho}_c.$$

Proof. We begin this proof by computing products of $1+i$ and $1-i$. We have

$$(1+i)^2 = 1 + 2i + i^2 = 1 + 2i + (-1) = 2i, \text{ and} \tag{3.33}$$

$$(1-i)^2 = 1 - 2i + i^2 = 1 - 2i + (-1) = -2i. \tag{3.34}$$

We also notice that $\overline{\rho_a\rho_b\rho_c} = \bar{\rho}_a\bar{\rho}_b\bar{\rho}_c$. Furthermore, for any $u \in \mathbb{C}$,

$$u + \bar{u} = (\mathrm{Re}(u) + i\mathrm{Im}(u)) + (\mathrm{Re}(u) - i\mathrm{Im}(u)) = 2\mathrm{Re}(u),$$

so $2\mathrm{Re}(\rho_a\rho_b\rho_c) = \rho_a\rho_b\rho_c + \bar{\rho}_a\bar{\rho}_b\bar{\rho}_c$. Also, for any $u \in \mathbb{C}$,

$$\begin{aligned} -iu + i\bar{u} &= -i(\mathrm{Re}(u) + i\mathrm{Im}(u)) + i(\mathrm{Re}(u) - i\mathrm{Im}(u)) \\ &= -i\mathrm{Re}(u) - i^2\mathrm{Im}(u) + i\mathrm{Re}(u) - i^2\mathrm{Im}(u) = 2\mathrm{Im}(u), \end{aligned}$$

so $2\mathrm{Im}(\rho_a\rho_b\rho_c) = -i\rho_a\rho_b\rho_c + i\bar{\rho}_a\bar{\rho}_b\bar{\rho}_c$.

For any odd integer q,

$$\rho_q = \begin{cases} 1+i, & \text{if } q \equiv 1 \pmod 4, \\ 1-i, & \text{if } q \equiv 3 \pmod 4, \end{cases}$$

so

$$\rho_a\rho_b\rho_c = (1+i)^{3-w}(1-i)^w.$$

Suppose that $w = 0$. Then $\kappa_w = 4(-0^2 + 3\cdot 0 - 1) = -4$ and $\lambda_w = 4\cdot(-1)^{\lfloor 0/2\rfloor} = 4$. Furthermore,

$$\rho_a\rho_b\rho_c = (1+i)^{3-0}(1-i)^0 = (1+i)^3 = (1+i)^2(1+i).$$

Use (3.33) to substitute into the last equation to see that

$$\rho_a\rho_b\rho_c = 2i(1+i) = 2i + 2i^2 = -2 + 2i,$$

so $2\mathrm{Re}(\rho_a\rho_b\rho_c) = -4$ and $2\mathrm{Im}(\rho_a\rho_b\rho_c) = 4$. Therefore, if $w = 0$, $\kappa_w = 2\mathrm{Re}(\rho_a\rho_b\rho_c)$ and $\lambda_w = 2\mathrm{Im}(\rho_a\rho_b\rho_c)$.

Suppose that $w = 1$. Then $\kappa_w = 4(-1^2 + 3\cdot 1 - 1) = 4$ and $\lambda_w = 4\cdot(-1)^{\lfloor 1/2\rfloor} = 4$. Furthermore,

$$\rho_a\rho_b\rho_c = (1+i)^{3-1}(1-i)^1 = (1+i)^2(1-i).$$

Use (3.33) to substitute into the last equation to see that

$$\rho_a\rho_b\rho_c = 2i(1-i) = 2i - 2i^2 = 2 + 2i,$$

so $2\mathrm{Re}(\rho_a\rho_b\rho_c) = 4$ and $2\mathrm{Im}(\rho_a\rho_b\rho_c) = 4$. Therefore, if $w = 1$, $\kappa_w = 2\mathrm{Re}(\rho_a\rho_b\rho_c)$ and $\lambda_w = 2\mathrm{Im}(\rho_a\rho_b\rho_c)$.

Suppose that $w = 2$. Then $\kappa_w = 4(-2^2 + 3\cdot 2 - 1) = 4$ and $\lambda_w = 4\cdot(-1)^{\lfloor 2/2\rfloor} = -4$. Furthermore,

$$\rho_a\rho_b\rho_c = (1+i)^{3-2}(1-i)^2 = (1+i)(1-i)^2.$$

Use (3.34) to substitute into the last equation to see that

$$\rho_a\rho_b\rho_c = (1+i)(-2i) = -2i - 2i^2 = 2 - 2i,$$

so $2\mathrm{Re}(\rho_a\rho_b\rho_c) = 4$ and $2\mathrm{Im}(\rho_a\rho_b\rho_c) = -4$. Therefore, if $w = 2$, $\kappa_w = 2\mathrm{Re}(\rho_a\rho_b\rho_c)$ and $\lambda_w = 2\mathrm{Im}(\rho_a\rho_b\rho_c)$.

Suppose that $w = 3$. Then $\kappa_w = 4(-3^2 + 3\cdot 3 - 1) = -4$ and $\lambda_w = 4\cdot(-1)^{\lfloor 3/2\rfloor} = -4$. Furthermore,

$$\rho_a\rho_b\rho_c = (1+i)^{3-3}(1-i)^3 = (1-i)^3 = (1-i)^2(1-i).$$

Use (3.34) to substitute into the last equation to see that

$$\rho_a\rho_b\rho_c = (-2i)(1-i) = -2i + 2i^2 = -2 - 2i,$$

so $2\mathrm{Re}(\rho_a\rho_b\rho_c) = -4$ and $2\mathrm{Im}(\rho_a\rho_b\rho_c) = -4$. Therefore, if $w = 3$, $\kappa_w = 2\mathrm{Re}(\rho_a\rho_b\rho_c)$ and $\lambda_w = 2\mathrm{Im}(\rho_a\rho_b\rho_c)$. □

Using κ_w and λ_w, the next theorem computes $r_{2^k,Q}(m)$ when m is square-free and a, b, and c are odd.

Theorem 3.16. *Suppose $2 \nmid abc$. Then*

$$r_{2,Q}(m) = 4$$

and

$$r_{2^2,Q}(m) = \begin{cases} 2^4 + 2(-1)^{\lfloor m/2\rfloor}\kappa_w, & \text{if } m \equiv 0 \pmod 2, \\ 2^4 + 2(-1)^{\lfloor m/2\rfloor}\lambda_w, & \text{otherwise.} \end{cases}$$

If $k \geq 3$,

$$r_{2^k,Q}(m) = \begin{cases} 2^{2k}\left(1 + \dfrac{1}{16}\left(\dfrac{2}{abcm}\right)\left(\kappa_w + \lambda_w\left(\dfrac{-1}{m}\right)\right) + \dfrac{1}{8}\lambda_w\left(\dfrac{-1}{m}\right)\right), & \text{if } 2 \nmid m, \\ 2^{2k}\left(1 - \dfrac{1}{8}\kappa_w\right), & \text{if } 2 \parallel m. \end{cases}$$

Proof. For any $k \geq 1$, by Corollary 3.2, we have

$$r_{2^k,Q}(m) = 2^{2k} + \frac{1}{2^k}\sum_{t=1}^{2^k-1} \mathrm{e}\left(\frac{-mt}{2^k}\right) G\left(\frac{at}{2^k}\right) G\left(\frac{bt}{2^k}\right) G\left(\frac{ct}{2^k}\right). \tag{3.35}$$

By Lemma 2.12, $G\left(\frac{a}{2}\right) = G\left(\frac{b}{2}\right) = G\left(\frac{c}{2}\right) = 0$, so by (3.35),

$$\begin{aligned} r_{2,Q}(m) = r_{2^1,Q}(m) &= 2^2 + \frac{1}{2}\sum_{t=1}^{2-1} \mathrm{e}\left(\frac{-mt}{2}\right) G\left(\frac{at}{2}\right) G\left(\frac{bt}{2}\right) G\left(\frac{ct}{2}\right) \\ &= 4 + \frac{1}{2}\sum_{t=1}^{2-1} \mathrm{e}\left(\frac{-mt}{2}\right)\cdot 0\cdot 0\cdot 0 = 4. \end{aligned}$$

Now suppose that $k \geq 2$. Using Lemma 3.8, (3.35) is equivalent to

$$r_{2^k,Q}(m) = 2^{2k} + \frac{1}{2^k}\sum_{\tau=0}^{k-1} \sum_{t_0 \in (\mathbb{Z}/2^{k-\tau}\mathbb{Z})^*} \mathrm{e}\left(\frac{-mt_0 2^\tau}{2^k}\right) G\left(\frac{at_0 2^\tau}{2^k}\right) G\left(\frac{bt_0 2^\tau}{2^k}\right) G\left(\frac{ct_0 2^\tau}{2^k}\right).$$

Let

$$s_{k,\tau} = \sum_{t_0 \in (\mathbb{Z}/2^{k-\tau}\mathbb{Z})^*} \mathrm{e}\left(\frac{-mt_0 2^\tau}{2^k}\right) G\left(\frac{at_0 2^\tau}{2^k}\right) G\left(\frac{bt_0 2^\tau}{2^k}\right) G\left(\frac{ct_0 2^\tau}{2^k}\right)$$

so that

$$r_{2^k,Q}(m) = 2^{2k} + \frac{1}{2^k} \sum_{\tau=0}^{k-1} s_{k,\tau}. \tag{3.36}$$

Suppose that $\tau = k-1$. Then

$$s_{k,\tau} = \sum_{t_0 \in (\mathbb{Z}/2^{k-\tau}\mathbb{Z})^*} \mathrm{e}\left(\frac{-mt_0 2^{k-1}}{2^k}\right) G\left(\frac{at_0 2^{k-1}}{2^k}\right) G\left(\frac{bt_0 2^{k-1}}{2^k}\right) G\left(\frac{ct_0 2^{k-1}}{2^k}\right).$$

By Lemma 2.15, $G\left(\frac{at_0 2^{k-1}}{2^k}\right) = G\left(\frac{bt_0 2^{k-1}}{2^k}\right) = G\left(\frac{ct_0 2^{k-1}}{2^k}\right) = 0$, so

$$s_{k,k-1} = \sum_{t_0 \in (\mathbb{Z}/p^{k-\tau}\mathbb{Z})^*} \mathrm{e}\left(\frac{-mt_0 2^{k-1}}{2^k}\right) \cdot 0 \cdot 0 \cdot 0 = 0. \tag{3.37}$$

Suppose $\tau \leq k-2$. Because $\tau \leq k-2$, we apply Lemma 2.15 and see that

$$\begin{aligned} s_{k,\tau} &= \sum_{t_0 \in (\mathbb{Z}/2^{k-\tau}\mathbb{Z})^*} \mathrm{e}\left(\frac{-mt_0}{2^{k-\tau}}\right) 2^{(k+\tau)/2} \left(\frac{2^{k-\tau}}{at_0}\right) \rho_{at_0} 2^{(k+\tau)/2} \left(\frac{2^{k-\tau}}{bt_0}\right) \rho_{bt_0} 2^{(k+\tau)/2} \left(\frac{2^{k-\tau}}{ct_0}\right) \rho_{ct_0} \\ &= 2^{3(k+\tau)/2} \sum_{t_0 \in (\mathbb{Z}/2^{k-\tau}\mathbb{Z})^*} \mathrm{e}\left(\frac{-mt_0}{2^{k-\tau}}\right) \left(\frac{2^{k-\tau}}{at_0}\right) \rho_{at_0} \left(\frac{2^{k-\tau}}{bt_0}\right) \rho_{bt_0} \left(\frac{2^{k-\tau}}{ct_0}\right) \rho_{ct_0}. \end{aligned}$$

By the definition of the Jacobi symbol,

$$s_{k,\tau} = 2^{3(k+\tau)/2} \left(\frac{2^{k-\tau}}{abc}\right) \sum_{t_0 \in (\mathbb{Z}/2^{k-\tau}\mathbb{Z})^*} \mathrm{e}\left(\frac{-mt_0}{2^{k-\tau}}\right) \left(\frac{2^{k-\tau}}{t_0}\right)^3 \rho_{at_0}\rho_{bt_0}\rho_{ct_0}.$$

Because $2 \nmid t_0$, $\left(\frac{2^{k-\tau}}{t_0}\right)^3 = \left(\frac{2^{k-\tau}}{t_0}\right)$ and

$$s_{k,\tau} = 2^{3(k+\tau)/2} \left(\frac{2^{k-\tau}}{abc}\right) \sum_{t_0 \in (\mathbb{Z}/2^{k-\tau}\mathbb{Z})^*} \mathrm{e}\left(\frac{-mt_0}{2^{k-\tau}}\right) \left(\frac{2^{k-\tau}}{t_0}\right) \rho_{at_0}\rho_{bt_0}\rho_{ct_0}.$$

Let $t_0 = t_1 + 4t_2$, where $t_1 \in \{1,3\}$ and $0 \leq t_2 \leq 2^{k-\tau-2} - 1$. Then

$$\begin{aligned} s_{k,\tau} &= 2^{3(k+\tau)/2} \left(\frac{2^{k-\tau}}{abc}\right) \sum_{t_1 \in \{1,3\}} \sum_{t_2=0}^{2^{k-\tau-2}-1} \mathrm{e}\left(\frac{-m(t_1+4t_2)}{2^{k-\tau}}\right) \left(\frac{2^{k-\tau}}{t_1+4t_2}\right) \rho_{a(t_1+4t_2)}\rho_{b(t_1+4t_2)}\rho_{c(t_1+4t_2)} \\ &= 2^{3(k+\tau)/2} \left(\frac{2^{k-\tau}}{abc}\right) \sum_{t_2=0}^{2^{k-\tau-2}-1} \left[\mathrm{e}\left(\frac{-m}{2^{k-\tau}}\right) \mathrm{e}\left(\frac{-4mt_2}{2^{k-\tau}}\right) \left(\frac{2^{k-\tau}}{1+4t_2}\right) \rho_{a(1+4t_2)}\rho_{b(1+4t_2)}\rho_{c(1+4t_2)} \right. \\ &\quad \left. + \mathrm{e}\left(\frac{-3m}{2^{k-\tau}}\right) \mathrm{e}\left(\frac{-4mt_2}{2^{k-\tau}}\right) \left(\frac{2^{k-\tau}}{3+4t_2}\right) \rho_{a(3+4t_2)}\rho_{b(3+4t_2)}\rho_{c(3+4t_2)} \right]. \end{aligned}$$

By Lemma 2.13 and some rearranging of terms,

$$s_{k,\tau} = 2^{3(k+\tau)/2}\left(\frac{2^{k-\tau}}{abc}\right)\sum_{t_2=0}^{2^{k-\tau-2}-1}\mathrm{e}\left(\frac{-4mt_2}{2^{k-\tau}}\right)\left[\mathrm{e}\left(\frac{-m}{2^{k-\tau}}\right)\left(\frac{2^{k-\tau}}{1+4t_2}\right)\rho_a\rho_b\rho_c + \mathrm{e}\left(\frac{-3m}{2^{k-\tau}}\right)\left(\frac{2^{k-\tau}}{3+4t_2}\right)\bar{\rho}_a\bar{\rho}_b\bar{\rho}_c\right]. \tag{3.38}$$

When $k-\tau=2$ (i.e., $\tau=k-2$),

$$\begin{aligned} s_{k,\tau} &= 2^{3k-3}\left(\frac{2^2}{abc}\right)\mathrm{e}\left(\frac{-4mt_2}{2^2}\right)\left[\mathrm{e}\left(\frac{-m}{2^2}\right)\left(\frac{2^2}{1+4t_2}\right)\rho_a\rho_b\rho_c \right.\\ &\qquad \left. + \mathrm{e}\left(\frac{-3m}{2^2}\right)\left(\frac{2^2}{3+4t_2}\right)\bar{\rho}_a\bar{\rho}_b\bar{\rho}_c\right]. \\ &= 2^{3k-3}\left(\frac{2^2}{abc}\right)\left[\mathrm{e}\left(\frac{-m}{4}\right)\left(\frac{2^2}{1+4t_2}\right)\rho_a\rho_b\rho_c + \mathrm{e}\left(\frac{-3m}{4}\right)\left(\frac{2^2}{3+4t_2}\right)\bar{\rho}_a\bar{\rho}_b\bar{\rho}_c\right]. \end{aligned}$$

By the multiplicative property of the Jacobi symbol,

$$\left(\frac{2^2}{abc}\right) = \left(\frac{2}{abc}\right)^2 = \left(\frac{2^2}{1+4t_2}\right) = \left(\frac{2}{1+4t_2}\right)^2 = \left(\frac{2^2}{3+4t_2}\right) = \left(\frac{2}{3+4t_2}\right)^2 = 1,$$

so

$$s_{k,k-2} = 2^{3k-3}\left[\mathrm{e}\left(\frac{-m}{4}\right)\rho_a\rho_b\rho_c + \mathrm{e}\left(\frac{-3m}{4}\right)\bar{\rho}_a\bar{\rho}_b\bar{\rho}_c\right].$$

If $m\equiv 0 \pmod 4$, then

$$\begin{aligned} s_{k,k-2} &= 2^{3k-3}\left[\mathrm{e}\left(\frac{-0}{4}\right)\rho_a\rho_b\rho_c + \mathrm{e}\left(\frac{-3\cdot 0}{4}\right)\bar{\rho}_a\bar{\rho}_b\bar{\rho}_c\right] \\ &= 2^{3k-3}\cdot 1\cdot[\rho_a\rho_b\rho_c + \bar{\rho}_a\bar{\rho}_b\bar{\rho}_c] \\ &= 2^{3k-3}(-1)^{\lfloor m/2\rfloor}\kappa_w. \end{aligned}$$

If $m\equiv 1 \pmod 4$, then

$$\begin{aligned} s_{k,k-2} &= 2^{3k-3}\left[\mathrm{e}\left(\frac{-1}{4}\right)\rho_a\rho_b\rho_c + \mathrm{e}\left(\frac{-3\cdot 1}{4}\right)\bar{\rho}_a\bar{\rho}_b\bar{\rho}_c\right] \\ &= 2^{3k-3}\cdot 1\cdot[-i\rho_a\rho_b\rho_c + i\bar{\rho}_a\bar{\rho}_b\bar{\rho}_c] \\ &= 2^{3k-3}(-1)^{\lfloor m/2\rfloor}\lambda_w. \end{aligned}$$

If $m\equiv 2 \pmod 4$, then

$$\begin{aligned} s_{k,k-2} &= 2^{3k-3}\left[\mathrm{e}\left(\frac{-2}{4}\right)\rho_a\rho_b\rho_c + \mathrm{e}\left(\frac{-3\cdot 2}{4}\right)\bar{\rho}_a\bar{\rho}_b\bar{\rho}_c\right] \\ &= 2^{3k-3}\left[-\rho_a\rho_b\rho_c - \bar{\rho}_a\bar{\rho}_b\bar{\rho}_c\right] = 2^{3k-3}\cdot(-1)\cdot\kappa_w \\ &= 2^{3k-3}(-1)^{\lfloor m/2\rfloor}\kappa_w. \end{aligned}$$

If $m \equiv 3 \pmod 4$, then

$$\begin{aligned} s_{k,k-2} &= 2^{3k-3}\left[\mathrm{e}\left(\frac{-3}{4}\right)\rho_a\rho_b\rho_c + \mathrm{e}\left(\frac{-3\cdot 3}{4}\right)\bar{\rho}_a\bar{\rho}_b\bar{\rho}_c\right] \\ &= 2^{3k-3}\cdot 1\cdot[i\rho_a\rho_b\rho_c - i\bar{\rho}_a\bar{\rho}_b\bar{\rho}_c] = 2^{3k-3}\cdot(-1)\cdot\lambda_w \\ &= 2^{3k-3}(-1)^{\lfloor m/2\rfloor}\lambda_w. \end{aligned}$$

Therefore,

$$s_{k,k-2} = \begin{cases} 2^{3k-3}(-1)^{\lfloor m/2\rfloor}\kappa_w, & \text{if } m \equiv 0 \pmod 2. \\ 2^{3k-3}(-1)^{\lfloor m/2\rfloor}\lambda_w, & \text{otherwise.} \end{cases} \tag{3.39}$$

When $k = 2$, using (3.37) and (3.39) to substitute into (3.36), we see that

$$\begin{aligned} r_{2^2,Q}(m) &= 2^4 + \frac{1}{4}\sum_{\tau=0}^{1} s_{2,\tau} = 2^4 + \frac{1}{4}(s_{2,0} + 0) \\ &= \begin{cases} 2^4 + \frac{1}{4}2^{3\cdot 2-3}(-1)^{\lfloor m/2\rfloor}\kappa_w, & \text{if } m \equiv 0 \pmod 2, \\ 2^4 + \frac{1}{4}2^{3\cdot 2-3}(-1)^{\lfloor m/2\rfloor}\lambda_w, & \text{otherwise,} \end{cases} \\ &= \begin{cases} 2^4 + 2(-1)^{\lfloor m/2\rfloor}\kappa_w, & \text{if } m \equiv 0 \pmod 2, \\ 2^4 + 2(-1)^{\lfloor m/2\rfloor}\lambda_w, & \text{otherwise.} \end{cases} \end{aligned}$$

When $k - \tau = 3$ (i.e., $\tau = k - 3$), the equation (3.38) becomes

$$\begin{aligned} s_{k,\tau} &= 2^{3(2k-3)/2}\left(\frac{2^3}{abc}\right)\sum_{t_2=0}^{2^{3-2}-1}\mathrm{e}\left(\frac{-4mt_2}{2^3}\right)\left[\mathrm{e}\left(\frac{-m}{2^3}\right)\left(\frac{2^3}{1+4t_2}\right)\rho_a\rho_b\rho_c\right. \\ &\qquad \left. + \mathrm{e}\left(\frac{-3m}{2^3}\right)\left(\frac{2^3}{3+4t_2}\right)\bar{\rho}_a\bar{\rho}_b\bar{\rho}_c\right] \\ &= 2^{3(2k-3)/2}\left(\frac{2^3}{abc}\right)\sum_{t_2=0}^{1}\mathrm{e}\left(\frac{mt_2}{2}\right)\left[\mathrm{e}\left(\frac{-m}{8}\right)\left(\frac{2^3}{1+4t_2}\right)\rho_a\rho_b\rho_c\right. \\ &\qquad \left. + \mathrm{e}\left(\frac{-3m}{8}\right)\left(\frac{2^3}{3+4t_2}\right)\bar{\rho}_a\bar{\rho}_b\bar{\rho}_c\right]. \end{aligned}$$

By the multiplicative property of the Jacobi symbol,

$$\begin{aligned} &\left(\frac{2^3}{abc}\right) = \left(\frac{2}{abc}\right)^3 = \left(\frac{2}{abc}\right)^2\left(\frac{2}{abc}\right) = \left(\frac{2}{abc}\right), \\ &\left(\frac{2^3}{1+4t_2}\right) = \left(\frac{2}{1+4t_2}\right)^3 = \left(\frac{2}{1+4t_2}\right)^2\left(\frac{2}{1+4t_2}\right) = \left(\frac{2}{1+4t_2}\right), \text{ and} \\ &\left(\frac{2^3}{3+4t_2}\right) = \left(\frac{2}{3+4t_2}\right)^3 = \left(\frac{2}{3+4t_2}\right)^2\left(\frac{2}{3+4t_2}\right) = \left(\frac{2}{3+4t_2}\right), \end{aligned}$$

so

$$\begin{aligned}
s_{k,k-3} &= 2^{3(2k-3)/2}\left(\frac{2}{abc}\right)\sum_{t_2=0}^{1}\mathrm{e}\left(\frac{mt_2}{2}\right)\left[\mathrm{e}\left(\frac{-m}{8}\right)\left(\frac{2}{1+4t_2}\right)\rho_a\rho_b\rho_c\right.\\
&\qquad\left.+\,\mathrm{e}\left(\frac{-3m}{8}\right)\left(\frac{2}{3+4t_2}\right)\bar\rho_a\bar\rho_b\bar\rho_c\right]\\
&= 2^{3(2k-3)/2}\left(\frac{2}{abc}\right)\left(\mathrm{e}\left(\frac{m\cdot 0}{2}\right)\left[\mathrm{e}\left(\frac{-m}{8}\right)\left(\frac{2}{1+4\cdot 0}\right)\rho_a\rho_b\rho_c\right.\right.\\
&\qquad\left.+\,\mathrm{e}\left(\frac{-3m}{8}\right)\left(\frac{2}{3+4\cdot 0}\right)\bar\rho_a\bar\rho_b\bar\rho_c\right]\\
&\qquad\left.+\,\mathrm{e}\left(\frac{m\cdot 1}{2}\right)\left[\mathrm{e}\left(\frac{-m}{8}\right)\left(\frac{2}{1+4\cdot 1}\right)\rho_a\rho_b\rho_c+\,\mathrm{e}\left(\frac{-3m}{8}\right)\left(\frac{2}{3+4\cdot 1}\right)\bar\rho_a\bar\rho_b\bar\rho_c\right]\right)\\
&= 2^{3(2k-3)/2}\left(\frac{2}{abc}\right)\left(\mathrm{e}\left(\frac{-m}{8}\right)\cdot 1\cdot\rho_a\rho_b\rho_c+\,\mathrm{e}\left(\frac{-3m}{8}\right)\cdot(-1)\cdot\bar\rho_a\bar\rho_b\bar\rho_c\right.\\
&\qquad\left.+\,\mathrm{e}\left(\frac{3m}{8}\right)\cdot(-1)\cdot\rho_a\rho_b\rho_c+\,\mathrm{e}\left(\frac{m}{8}\right)\cdot 1\cdot\bar\rho_a\bar\rho_b\bar\rho_c\right)\\
&= 2^{3(2k-3)/2}\left(\frac{2}{abc}\right)\left(\mathrm{e}\left(\frac{-m}{8}\right)\rho_a\rho_b\rho_c-\,\mathrm{e}\left(\frac{-3m}{8}\right)\bar\rho_a\bar\rho_b\bar\rho_c\right.\\
&\qquad\left.-\,\mathrm{e}\left(\frac{3m}{8}\right)\rho_a\rho_b\rho_c+\,\mathrm{e}\left(\frac{m}{8}\right)\bar\rho_a\bar\rho_b\bar\rho_c\right).
\end{aligned}$$

If $m\equiv 1 \pmod 8$, then

$$\begin{aligned}
s_{k,k-3} &= 2^{3(2k-3)/2}\left(\frac{2}{abc}\right)\left(\mathrm{e}\left(\frac{-1}{8}\right)\rho_a\rho_b\rho_c-\,\mathrm{e}\left(\frac{-3\cdot 1}{8}\right)\bar\rho_a\bar\rho_b\bar\rho_c\right.\\
&\qquad\left.-\,\mathrm{e}\left(\frac{3\cdot 1}{8}\right)\rho_a\rho_b\rho_c+\,\mathrm{e}\left(\frac{1}{8}\right)\bar\rho_a\bar\rho_b\bar\rho_c\right)\\
&= 2^{3(2k-3)/2}\left(\frac{2}{abc}\right)\left(2\mathrm{e}\left(\frac{-1}{8}\right)\rho_a\rho_b\rho_c-2\mathrm{e}\left(\frac{-3\cdot 1}{8}\right)\bar\rho_a\bar\rho_b\bar\rho_c\right)\\
&= 2^{(6k-9)/2}\left(\frac{2}{abc}\right)\left(2^{1/2}(1-i)\rho_a\rho_b\rho_c-2^{1/2}(-1-i)\bar\rho_a\bar\rho_b\bar\rho_c\right)\\
&= 2^{3k-4}\left(\frac{2}{abc}\right)\left((1-i)\rho_a\rho_b\rho_c-(-1-i)\bar\rho_a\bar\rho_b\bar\rho_c\right)=2^{3k-4}\left(\frac{2}{abc}\right)\left(\kappa_w+\lambda_w\right).
\end{aligned}$$

Since $m\equiv 1 \pmod 8$, by Theorem 5.9 in LeVeque's *Fundamentals of Number Theory* [LeV96, p. 110],

$$\left(\frac{2}{abcm}\right)=\left(\frac{2}{abc}\right)\ \text{and}\ \left(\frac{-1}{m}\right)=1,$$

so

$$s_{k,k-3}=2^{3k-4}\left(\frac{2}{abcm}\right)\left(\kappa_w+\lambda_w\left(\frac{-1}{m}\right)\right)$$

if $m\equiv 1 \pmod 8$.

If $m \equiv 3 \pmod 8$, then

$$\begin{aligned} s_{k,k-3} &= 2^{3(2k-3)/2}\left(\frac{2}{abc}\right)\left(\mathrm{e}\left(\frac{-3}{8}\right)\rho_a\rho_b\rho_c - \mathrm{e}\left(\frac{-3\cdot 3}{8}\right)\bar\rho_a\bar\rho_b\bar\rho_c \right. \\ &\qquad \left. - \mathrm{e}\left(\frac{3\cdot 3}{8}\right)\rho_a\rho_b\rho_c + \mathrm{e}\left(\frac{3}{8}\right)\bar\rho_a\bar\rho_b\bar\rho_c\right) \\ &= 2^{3(2k-3)/2}\left(\frac{2}{abc}\right)\left(2\mathrm{e}\left(\frac{-3}{8}\right)\rho_a\rho_b\rho_c - 2\mathrm{e}\left(\frac{-3\cdot 3}{8}\right)\bar\rho_a\bar\rho_b\bar\rho_c\right) \\ &= 2^{(6k-9)/2}\left(\frac{2}{abc}\right)\left(2^{1/2}(-1-i)\rho_a\rho_b\rho_c - 2^{1/2}(1-i)\bar\rho_a\bar\rho_b\bar\rho_c\right) \\ &= 2^{3k-4}\left(\frac{2}{abc}\right)\left((-1-i)\rho_a\rho_b\rho_c - (1-i)\bar\rho_a\bar\rho_b\bar\rho_c\right) = 2^{3k-4}\left(\frac{2}{abc}\right)\left(-\kappa_w + \lambda_w\right). \end{aligned}$$

Since $m \equiv 3 \pmod 8$, by Theorem 5.9 in LeVeque's *Fundamentals of Number Theory* [LeV96, p. 110],

$$\left(\frac{2}{abcm}\right) = -\left(\frac{2}{abc}\right) \text{ and } \left(\frac{-1}{m}\right) = -1,$$

so

$$s_{k,k-3} = 2^{3k-4}\left(\frac{2}{abcm}\right)\left(\kappa_w + \lambda_w\left(\frac{-1}{m}\right)\right)$$

if $m \equiv 3 \pmod 8$.

If $m \equiv 5 \pmod 8$, then

$$\begin{aligned} s_{k,k-3} &= 2^{3(2k-3)/2}\left(\frac{2}{abc}\right)\left(\mathrm{e}\left(\frac{-5}{8}\right)\rho_a\rho_b\rho_c - \mathrm{e}\left(\frac{-3\cdot 5}{8}\right)\bar\rho_a\bar\rho_b\bar\rho_c \right. \\ &\qquad \left. - \mathrm{e}\left(\frac{3\cdot 5}{8}\right)\rho_a\rho_b\rho_c + \mathrm{e}\left(\frac{5}{8}\right)\bar\rho_a\bar\rho_b\bar\rho_c\right) \\ &= 2^{3(2k-3)/2}\left(\frac{2}{abc}\right)\left(2\mathrm{e}\left(\frac{-5}{8}\right)\rho_a\rho_b\rho_c - 2\mathrm{e}\left(\frac{-3\cdot 5}{8}\right)\bar\rho_a\bar\rho_b\bar\rho_c\right) \\ &= 2^{(6k-9)/2}\left(\frac{2}{abc}\right)\left(2^{1/2}(-1+i)\rho_a\rho_b\rho_c - 2^{1/2}(1+i)\bar\rho_a\bar\rho_b\bar\rho_c\right) \\ &= 2^{3k-4}\left(\frac{2}{abc}\right)\left((-1+i)\rho_a\rho_b\rho_c - (1+i)\bar\rho_a\bar\rho_b\bar\rho_c\right) = 2^{3k-4}\left(\frac{2}{abc}\right)\left(-\kappa_w - \lambda_w\right). \end{aligned}$$

Since $m \equiv 5 \pmod 8$, by Theorem 5.9 in LeVeque's *Fundamentals of Number Theory* [LeV96, p. 110],

$$\left(\frac{2}{abcm}\right) = -\left(\frac{2}{abc}\right) \text{ and } \left(\frac{-1}{m}\right) = 1,$$

so

$$s_{k,k-3} = 2^{3k-4}\left(\frac{2}{abcm}\right)\left(\kappa_w + \lambda_w\left(\frac{-1}{m}\right)\right)$$

if $m \equiv 5 \pmod 8$.

If $m \equiv 7 \pmod 8$, then

$$\begin{aligned} s_{k,k-3} &= 2^{3(2k-3)/2} \left(\frac{2}{abc}\right) \left(\mathrm{e}\left(\frac{-7}{8}\right) \rho_a\rho_b\rho_c - \mathrm{e}\left(\frac{-3\cdot 7}{8}\right) \bar\rho_a\bar\rho_b\bar\rho_c \right. \\ &\qquad \left. - \mathrm{e}\left(\frac{3\cdot 7}{8}\right) \rho_a\rho_b\rho_c + \mathrm{e}\left(\frac{7}{8}\right) \bar\rho_a\bar\rho_b\bar\rho_c \right) \\ &= 2^{3(2k-3)/2} \left(\frac{2}{abc}\right) \left(2\mathrm{e}\left(\frac{-7}{8}\right) \rho_a\rho_b\rho_c - 2\mathrm{e}\left(\frac{-3\cdot 7}{8}\right) \bar\rho_a\bar\rho_b\bar\rho_c \right) \\ &= 2^{(6k-9)/2} \left(\frac{2}{abc}\right) \left(2^{1/2}(1+i)\rho_a\rho_b\rho_c - 2^{1/2}(-1+i)\bar\rho_a\bar\rho_b\bar\rho_c \right) \\ &= 2^{3k-4} \left(\frac{2}{abc}\right) \left((1+i)\rho_a\rho_b\rho_c - (-1+i)\bar\rho_a\bar\rho_b\bar\rho_c \right) = 2^{3k-4} \left(\frac{2}{abc}\right) \left(\kappa_w - \lambda_w\right). \end{aligned}$$

Since $m \equiv 7 \pmod 8$, by Theorem 5.9 in LeVeque's *Fundamentals of Number Theory* [LeV96, p. 110],

$$\left(\frac{2}{abcm}\right) = \left(\frac{2}{abc}\right) \text{ and } \left(\frac{-1}{m}\right) = -1,$$

so

$$s_{k,k-3} = 2^{3k-4} \left(\frac{2}{abcm}\right) \left(\kappa_w + \lambda_w \left(\frac{-1}{m}\right)\right)$$

if $m \equiv 7 \pmod 8$.

Therefore, for any odd integer m,

$$s_{k,k-3} = 2^{3k-4} \left(\frac{2}{abcm}\right) \left(\kappa_w + \lambda_w \left(\frac{-1}{m}\right)\right). \tag{3.40}$$

If $m \equiv 2 \pmod 8$, then

$$\begin{aligned} s_{k,k-3} &= 2^{3(2k-3)/2} \left(\frac{2}{abc}\right) \left(\mathrm{e}\left(\frac{-2}{8}\right) \rho_a\rho_b\rho_c - \mathrm{e}\left(\frac{-3\cdot 2}{8}\right) \bar\rho_a\bar\rho_b\bar\rho_c \right. \\ &\qquad \left. - \mathrm{e}\left(\frac{3\cdot 2}{8}\right) \rho_a\rho_b\rho_c + \mathrm{e}\left(\frac{2}{8}\right) \bar\rho_a\bar\rho_b\bar\rho_c \right) \\ &= 2^{3(2k-3)/2} \left(\frac{2}{abc}\right) \left(-i\rho_a\rho_b\rho_c - i\bar\rho_a\bar\rho_b\bar\rho_c + i\rho_a\rho_b\rho_c + i\bar\rho_a\bar\rho_b\bar\rho_c \right) = 0. \end{aligned}$$

If $m \equiv 6 \pmod 8$, then

$$\begin{aligned} s_{k,k-3} &= 2^{3(2k-3)/2} \left(\frac{2}{abc}\right) \left(\mathrm{e}\left(\frac{-6}{8}\right) \rho_a\rho_b\rho_c - \mathrm{e}\left(\frac{-3\cdot 6}{8}\right) \bar\rho_a\bar\rho_b\bar\rho_c \right. \\ &\qquad \left. - \mathrm{e}\left(\frac{3\cdot 6}{8}\right) \rho_a\rho_b\rho_c + \mathrm{e}\left(\frac{6}{8}\right) \bar\rho_a\bar\rho_b\bar\rho_c \right) \\ &= 2^{3(2k-3)/2} \left(\frac{2}{abc}\right) \left(i\rho_a\rho_b\rho_c + i\bar\rho_a\bar\rho_b\bar\rho_c - i\rho_a\rho_b\rho_c - i\bar\rho_a\bar\rho_b\bar\rho_c \right) = 0. \end{aligned}$$

Thus, if $2 \parallel m$,

$$s_{k,k-3} = 0. \tag{3.41}$$

When $k = 3$, using (3.37), (3.39), (3.40), and (3.41) to substitute into (3.36), we see that

$$\begin{aligned}
r_{2^3,Q}(m) &= 2^{2\cdot 3} + \frac{1}{2^3}\sum_{\tau=0}^{3-1} s_{k,\tau} \\
&= 2^6 + \frac{1}{8}\left(s_{3,0} + s_{3,1} + s_{3,2}\right) \\
&= 2^6 + \frac{1}{8}\left(s_{3,0} + s_{3,1} + 0\right) = 2^6 + \frac{1}{8}\left(s_{3,0} + s_{3,1}\right) \\
&= \begin{cases} 2^6 + \frac{1}{8}\left(2^{3\cdot 3-4}\left(\frac{2}{abcm}\right)\left(\kappa_w + \lambda_w\left(\frac{-1}{m}\right)\right) + 2^{3\cdot 3-3}(-1)^{\lfloor m/2\rfloor}\lambda_w\right), & \text{if } 2 \nmid m, \\ 2^6 + \frac{1}{8}\left(0 + 2^{3\cdot 3-3}(-1)^{\lfloor m/2\rfloor}\kappa_w\right), & \text{if } 2 \parallel m, \end{cases} \\
&= \begin{cases} 2^6 + \frac{1}{8}\left(2^5\left(\frac{2}{abcm}\right)\left(\kappa_w + \lambda_w\left(\frac{-1}{m}\right)\right) + 2^6\lambda_w(-1)^{\lfloor m/2\rfloor}\right), & \text{if } 2 \nmid m, \\ 2^6 + \frac{1}{8}\left(2^6(-1)^{\lfloor m/2\rfloor}\kappa_w\right), & \text{if } 2 \parallel m, \end{cases} \\
&= \begin{cases} 2^6\left(1 + \frac{1}{16}\left(\frac{2}{abcm}\right)\left(\kappa_w + \lambda_w\left(\frac{-1}{m}\right)\right) + \frac{1}{8}\lambda_w(-1)^{\lfloor m/2\rfloor}\right), & \text{if } 2 \nmid m, \\ 2^6\left(1 - \frac{1}{8}\kappa_w\right), & \text{if } 2 \parallel m. \end{cases}
\end{aligned}$$

If m is odd (i.e., $2 \nmid m$), then, by Theorem 5.9 in LeVeque's *Fundamentals of Number Theory* [LeV96, p. 110],

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

so

$$r_{2^3,Q}(m) = \begin{cases} 2^6\left(1 + \frac{1}{16}\left(\frac{2}{abcm}\right)\left(\kappa_w + \lambda_w\left(\frac{-1}{m}\right)\right) + \frac{1}{8}\lambda_w\left(\frac{-1}{m}\right)\right), & \text{if } 2 \nmid m, \\ 2^6\left(1 - \frac{1}{8}\kappa_w\right), & \text{if } 2 \parallel m. \end{cases}$$

Let $\vec{\mathbf{v}}_0 = (x_0, y_0, z_0)^T$ be a solution to $Q(\vec{\mathbf{v}}) \equiv m \pmod{2^3}$. Toward contradiction, assume that $2 \mid ax_0$, $2 \mid by_0$, and $2 \mid cz_0$. Since $2 \nmid abc$, $x_0 = 2x_1$, $y_0 = 2y_1$, and $z_0 = 2z_1$ for some $x_1, y_1, z_1 \in \mathbb{Z}$. Thus,

$$\begin{aligned}
Q(\vec{\mathbf{v}}_0) = ax_0^2 + by_0^2 + cz_0^2 &= a(2x_1)^2 + b(2y_1)^2 + c(2z_1)^2 \\
&= 4ax_1^2 + 4by_1^2 + 4cz_1^2 \\
&\equiv 0 \pmod 4.
\end{aligned}$$

However, we assumed that $2^2 \nmid m$, so $m \not\equiv 0 \equiv Q(\vec{\mathbf{v}}_0) \pmod 4$. Because $Q(\vec{\mathbf{v}}_0) \not\equiv m \pmod{2^2}$, it is impossible for $Q(\vec{\mathbf{v}}_0) \equiv m \pmod{2^3}$, producing a contradiction. Thus, $2 \nmid ax_0$, $2 \nmid by_0$, or $2 \nmid cz_0$ for any solution $\vec{\mathbf{v}}_0 = (x_0, y_0, z_0)^T$ to $Q(\vec{\mathbf{v}}) \equiv m \pmod{2^3}$. By

Corollary 3.14, for $k \geq 3$,

$$r_{2^k,Q}(m) = \begin{cases} 2^{2k}\left(1 + \frac{1}{16}\left(\frac{2}{abcm}\right)\left(\kappa_w + \lambda_w\left(\frac{-1}{m}\right)\right) + \frac{1}{8}\lambda_w\left(\frac{-1}{m}\right)\right), & \text{if } 2 \nmid m, \\ 2^{2k}\left(1 - \frac{1}{8}\kappa_w\right), & \text{if } 2 \parallel m. \end{cases}$$

□

With Theorems 3.6, 3.10, 3.11, and 3.16, we can determine if a square-free integer m is locally represented everywhere by Q given that a, b, and c are odd and pairwise coprime. The formulas found in this section can be used to write a program to find $S(Q, n)$ for some integer n. In the next section, we discuss some results of some numerical computations made by a program using the formulas for $r_{p^k,Q}(m)$ found in this section.

4. Observations about Data

We analyzed $S(Q, 2000000)$ for Q such that $a, b, c < 30$ are odd and pairwise coprime. Out of the 322 quadratic forms examined, only 46 had $\max(S(Q, 2000000)) < 500000$, 54 had $\max(S(Q, 2000000)) < 1000000$, and 65 had $\max(S(Q, 2000000)) < 1500000$. Therefore, it is unreasonable to say that $S(Q, 2000000) = S(Q)$ for many of quadratic forms examined. The data collected suggests that $\max(S(Q))$ grows rapidly compared to any of the measures used for Q. These measures include the determinant of Q (denoted $\det(Q)$), the level of Q (denoted $\text{level}(Q)$), the maximum of a, b, and c (denoted $\max(a, b, c)$), and $\sqrt{a^2 + b^2 + c^2}$. Furthermore, it appears that the upper bound on the size of $S(Q)$ grows as the measure of Q grows. Appendix D lists $S(Q, 2000000)$ if $S(Q, 2000000)$ is empty or $\max(S(Q, 2000000)) < 15000$. Appendix E contains plots concerning $\max(S(Q, 2000000))$ and $|S(Q, 2000000)|$.

It appears that the lower bound on the maximum of $S(Q)$ increases as the size of $S(Q)$ increases. This is expected since the size of $S(Q)$ automatically creates a lower bound of $|S(Q)|$ for the maximum of $S(Q)$. From the data collected, it seems that $\max(S(Q)) \geq 55|S(Q)|$. This estimate was found by dividing $\max(S(Q, 2000000))$ by $|S(Q, 2000000)|$ if $0 < |S(Q, 2000000)| < 1800000$. Let $sl(Q, n) = \max(S(Q, n))/|S(Q, n)|$ for Q such that $|S(Q, n)| < \frac{9}{10}n$. The minimum value of $sl(Q, 2000000)$ for the considered quadratic forms is $721/13 \approx 55.46$. This value is achieved by the quadratic form $Q(\vec{\mathbf{v}}) = x^2 + 9y^2 + 13z^2$. Appendix F lists the 25 smallest values of $sl(Q, 2000000)$ found and their corresponding quadratic forms.

5. Future Directions

Section 3 lists formulas for $r_{p^k,Q}(m)$ under particular divisibility conditions on the coefficients of a positive definite diagonal integer-matrix ternary quadratic form. The formulas for $r_{p^k,Q}(m)$ can be used to determine if a square-free integer m is locally represented everywhere by Q given that a, b, and c are odd and pairwise coprime. The author of this paper has written a program in Sage to compute which square-free integers are locally represented everywhere but are not globally represented by such quadratic forms. Some observations about the data generated by this program are found in Section 4.

More formulas for $r_{p^k,Q}(m)$ can be developed. For example, what is $r_{p^k,Q}(m)$ when p is an odd prime, m is square-free, $p \nmid a$, $p \parallel b$, and $p \mid c$? What is $r_{2^k,Q}(m)$ if m is square-free and

at least one of a, b, c is even? By answering these questions, we could write programs that could compute $S(Q, n)$ for any quadratic form.

Out of the 322 quadratic forms examined, only 46 had $\max(S(Q, 2000000)) < 500000$, 54 had $\max(S(Q, 2000000)) < 1000000$, and 65 had $\max(S(Q, 2000000)) < 1500000$. Therefore, it is unreasonable to say that $S(Q, 2000000) = S(Q)$ for many of quadratic forms examined. Thus, it would be nice to compute $S(Q, n)$ for $n > 2000000$ and collect more computational data about these quadratic forms.

From the data collected, it seems that $\max(S(Q)) \geq 55|S(Q)|$. However, this bound was found computationally, so it would be nice to determine a lower bound for $\max(S(Q))$ in terms of $|S(Q)|$ theoretically.

Only 5 of the 322 quadratic forms examined are regular quadratic forms. They are $x^2 + y^2 + z^2$, $x^2 + y^2 + 3z^2$, $x^2 + y^2 + 5z^2$, $x^2 + y^2 + 9z^2$, and $x^2 + y^2 + 21z^2$. These were the only quadratic forms examined in which $S(Q, 2000000)$ was computed to be the empty set. This raises the question: If $S(Q)$ is nonempty, how large can the minimum element of $S(Q)$ be?

Appendix A. Sage Code for Quadratic Gauss Sums

The following function written for Sage returns the quadratic Gauss sum $G\left(\frac{(num)}{p^k}\right)$.

```
def quadratic_Gauss_sum(num, p, k):
    """
    Returns the quadratic Gauss sum $G \left( \frac{(num)}{p^k} \right)$.

    INPUT:
        ‘num‘ -- an integer
        ‘p‘ -- a positive prime integer
        ‘k‘ -- a non-negative integer

    OUTPUT:
        Integer
    """

    if num not in ZZ:
        raise TypeError("num = " + str(num) + " is not an integer!")
    if p not in ZZ:
        raise TypeError("p = " + str(p) + " is not an integer!")
    if p <= 0:
        raise TypeError("p = " + str(p) + " is not positive!")
    if not is_prime(p):
        raise TypeError("p = " + str(p) + " is not prime!")
    if k not in ZZ:
        raise TypeError("k = " + str(k) + " is not an integer!")
    if k < 0:
        raise TypeError("k = " + str(k) + " is not non-negative!")

    if num == 0:
        return p**k
    if k == 0:
    # k == 0, so p**k == 1
        return 1
    elif p == 2:
    # p == 2
        val = valuation(num, p)
        if k == 1:
        # p**k == 2
            if val > 0:
                return 2
            else:
                return 0
        else:
        # p**k == 2**k, k >= 2
            if k == val + 1:
```

```
        # k == val + 1
            return 0
        elif k <= val:
        # k < val + 1
            return p**k
        else:
        # k > val + 1
            num2 = num / (p**val)

            # Calculates enum2
            if num2 % 4 == 1:
                enum2 = 1 + i
            elif num2 % 4 == 3:
                enum2 = 1 - i
            else:
                raise ArithmeticError('This shouldn\'t happen')

            # Calculates the Gauss sum
            return (p**((k+val)/2) * kronecker_symbol(p**(k-val), num2) *
                enum2)

else:
# p >= 3, a.k.a. p is a prime odd
    val = valuation(num, p)
    if k <= val:
    # k <= val, the Gauss sum equals p**k
        return p**k
    else:
    # k > val
        diff = k - val

        # Calculates eppow
        ppow = p**diff
        if ppow % 4 == 1:
            eppow = 1
        elif ppow % 4 == 3:
            eppow = i
        else:
            raise ArithmeticError('This shouldn\'t happen')

        # Calculates the Gauss sum
        num2 = num / (p**val)
        return kronecker_symbol(num2, ppow) * eppow * p**((k+val)/2)
```

Appendix B. Sage Code for Computing $r_{p^k,Q}(m)$ Using the Fast Fourier Transform

The following function written for Sage returns a list of length p^k whose mth entry is $r_{p^k,Q}(m)$. The `representation_list_mod_p_to_k_fft()` function uses the `quadratic_Gauss_sum()` function mentioned in Appendix A.

```
def representation_list_mod_p_to_k_fft(a, b, c, p, k):
    """
    Returns a list of length $p^k$ whose $m$th entry is $r_{p^k , Q}(m)$.
    This method uses the fast Fourier transform.

    INPUT:
        ‘a‘ -- a positive integer
        ‘b‘ -- a positive integer
        ‘c‘ -- a positive integer
        ‘p‘ -- a positive prime integer
        ‘k‘ -- a non-negative integer

    OUTPUT:
        list
    """

    tol = 10**(-6)
    pk = p**k
    rpkQmsFFT = FastFourierTransform(pk)
    for m in IntegerRange(pk):
        fpkm = (quadratic_Gauss_sum(a*m, p, k) *
            quadratic_Gauss_sum(b*m, p, k) *
            quadratic_Gauss_sum(c*m, p, k) / pk)
        rpkQmsFFT[m] = (fpkm.real(), fpkm.imag())
    rpkQmsFFT.forward_transform()

    # rpkQms is the list that will only contain the real part
    # of the entries in rpkQmsFFT (once the real part has been
    # rounded to the appropriate integer)
    rpkQms = [0]*pk
    for m in IntegerRange(pk):
        if abs(rpkQmsFFT[m][1]) > tol:
            raise ArithmeticError('This shouldn\'t happen')
        rpkQms[m] = round(rpkQmsFFT[m][0])

    return rpkQms
```

Appendix C. Sage Code for Computing a List of Square-Free Non-Negative Integers That Are Represented Locally But Not Represented Globally by a Quadratic Form

The following function written for Sage returns a list of square-free non-negative integers less than n that are represented locally but not represented globally by a given quadratic form Q. The function `get_locally_not_globally_represented_list_odd(Q,n)` uses the `representation_list_mod_p_to_k_fft()` function mentioned in Appendix B.

```
def get_locally_not_globally_represented_list_odd(Q,n):
    """
    Returns $S(Q)$, a list of non-negative square-free integers less
    than n that are represented locally but not represented globally
    by the quadratic form Q.

    INPUT:
        ‘Q‘ -- a diagonal ternary quadratic form with the diagonal
                elements being pairwise coprime positive odd integers
        ‘n‘ -- an integer

    OUTPUT:
        list
    """
    if not n in ZZ:
        raise TypeError, "n = " + str(n) + " is not an integer!"

    tol = 10**(-6)

    # thetaCoeffs stores the first n coefficients of the theta series
    # associated with Q
    thetaCoeffs = Q.theta_series(n).polynomial().list()
    thetaCoeffsLen = len(thetaCoeffs)
    if thetaCoeffsLen < n:
        numOfAddedZeros = n - thetaCoeffsLen
        thetaCoeffs.extend([0]*numOfAddedZeros)

    # Gets the prime divisors of the discriminant of Q
    primes = prime_divisors(Q[0,0]*Q[1,1]*Q[2,2])
    repListsModPrimesDict = {2 : representation_list_mod_p_to_k_fft(Q[0,0], \
        Q[1,1], Q[2,2], 2, 3)}
    for p in primes:
        repListsModPrimesDict[p] = representation_list_mod_p_to_k_fft(Q[0,0], \
            Q[1,1], Q[2,2], p, 2)
    primes.append(2)

    # Creates the desired list of numbers
    repList = []
    for j in IntegerRange(n):
```

```
        if thetaCoeffs[j] < 1:
            if j.is_squarefree():
                isLocallyRep = True
                for p in primes:
                    pRepList = repListsModPrimesDict[p]
                    if pRepList[j%len(pRepList)] < tol:
                        isLocallyRep = False
                if isLocallyRep:
                    repList.append(j)
    return repList
```

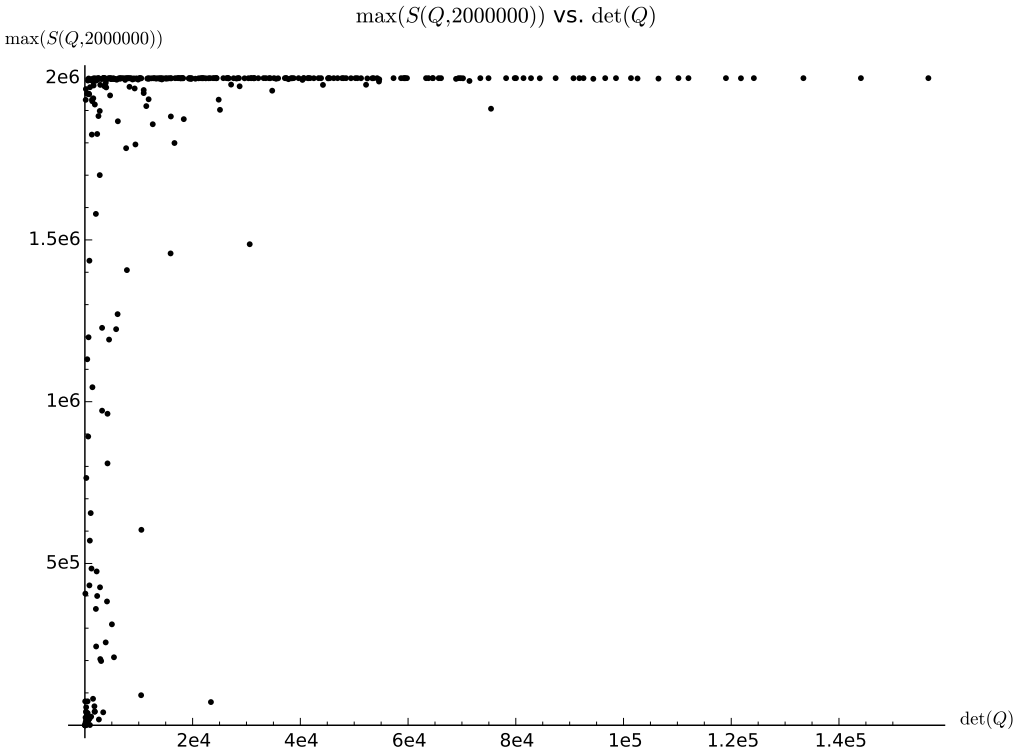
Appendix D. $S(Q, 2000000)$ for Some Quadratic Forms

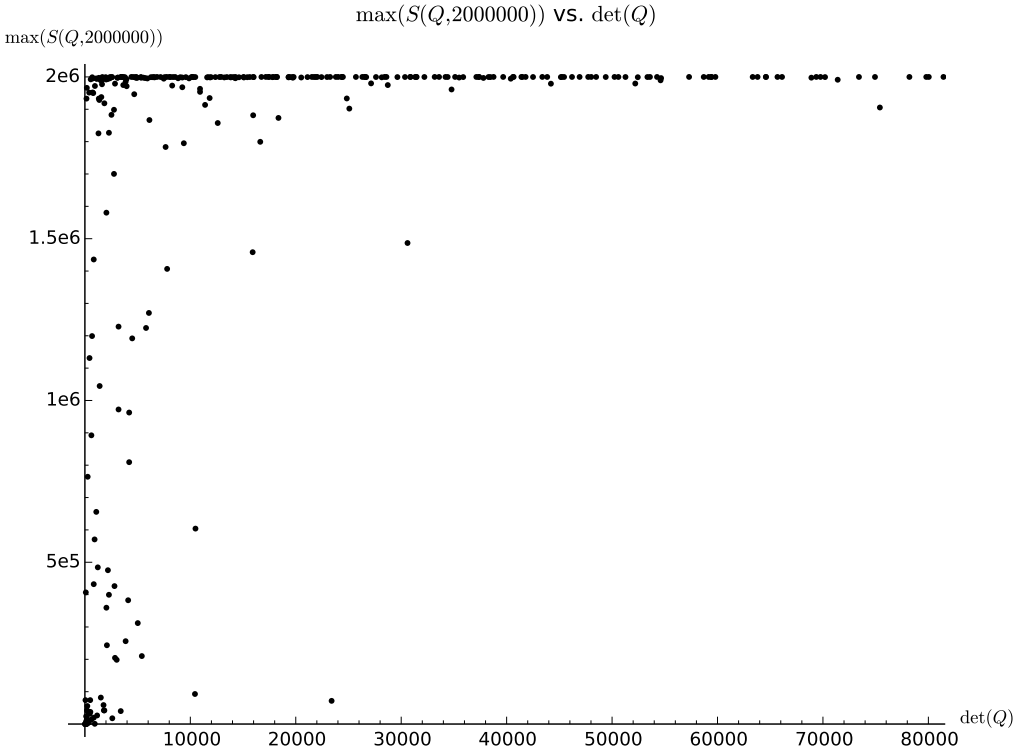
The following table lists $S(Q, 2000000)$ for the quadratic form $Q(\vec{\mathbf{v}}) = ax^2+by^2+cz^2$ (where $a, b, c < 30$ are odd and pairwise coprime) if $S(Q, 2000000)$ is empty or $\max(S(Q, 2000000)) < 15000$. The first column of the table contains the coefficients of a quadratic form Q in the form (a, b, c). The second column states $S(Q, 2000000)$.

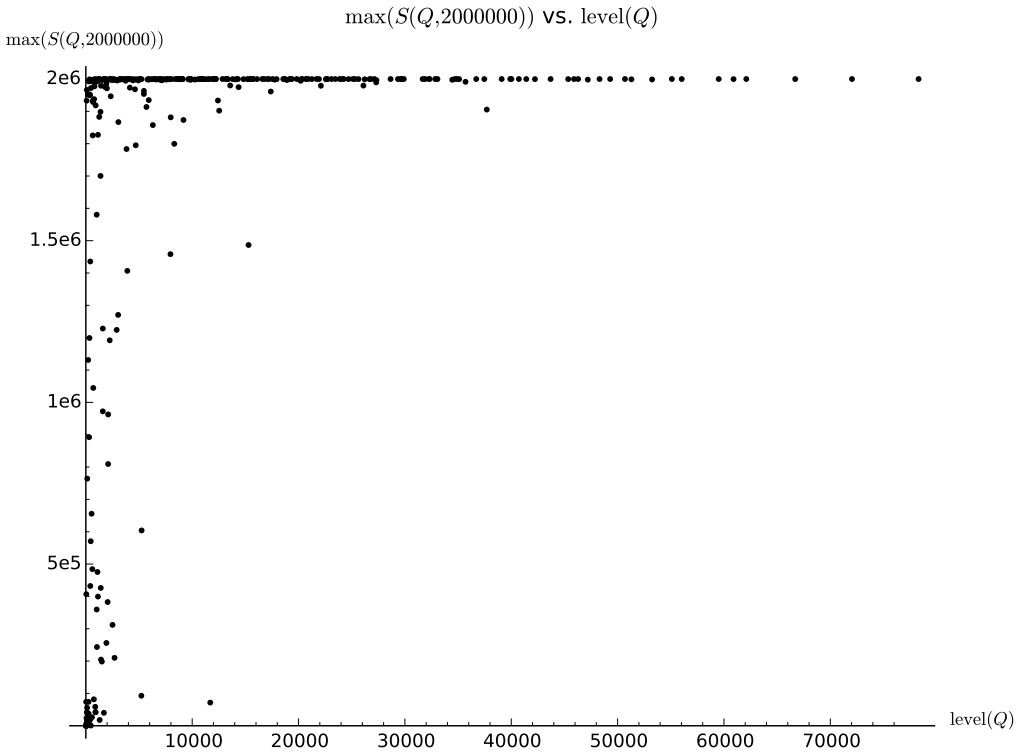
(a, b, c)	$S(Q, 2000000)$
$(1, 1, 1)$	$\{\}$
$(1, 1, 3)$	$\{\}$
$(1, 1, 5)$	$\{\}$
$(1, 1, 9)$	$\{\}$
$(1, 1, 21)$	$\{\}$
$(1, 1, 13)$	$\{6, 7, 46, 55, 79, 271, 439, 721\}$
$(1, 9, 13)$	$\{2, 5, 7, 41, 46, 55, 79, 146, 167, 185, 271, 439, 721\}$
$(1, 3, 7)$	$\{2, 5, 17, 22, 30, 58, 62, 122, 165, 318, 498, 822, 957, 1193\}$
$(1, 1, 17)$	$\{3, 6, 11, 14, 38, 59, 83, 110, 131, 201, 209, 339, 419, 581, 1046, 1259, 2315, 2726, 2819\}$
$(1, 3, 13)$	$\{2, 5, 10, 11, 23, 30, 35, 46, 47, 58, 66, 82, 85, 102, 107, 158, 167, 187, 197, 218, 255, 262, 266, 278, 282, 370, 435, 443, 462, 503, 530, 583, 622, 678, 802, 822, 898, 1002, 1030, 1173, 1187, 1415, 2118, 2543, 2802, 3882\}$
$(1, 5, 9)$	$\{2, 7, 17, 22, 26, 31, 47, 53, 62, 71, 74, 113, 119, 133, 146, 191, 194, 199, 209, 218, 221, 257, 302, 367, 377, 383, 422, 434, 503, 599, 638, 698, 719, 727, 1013, 1031, 1247, 1391, 1631, 1673, 1973, 2006, 2519, 3722, 3953, 4031, 4697\}$
$(1, 1, 15)$	$\{6, 7, 11, 14, 22, 38, 42, 43, 46, 59, 71, 91, 103, 107, 114, 123, 127, 154, 186, 191, 214, 231, 267, 319, 323, 326, 359, 382, 438, 478, 487, 494, 506, 547, 618, 654, 658, 659, 834, 1079, 1086, 1131, 1222, 1302, 1446, 1486, 1563, 1743, 2123, 2326, 2634, 2787, 4047, 6378, 8394\}$
$(1, 3, 25)$	$\{2, 11, 14, 17, 22, 23, 47, 58, 59, 66, 71, 83, 94, 102, 138, 166, 174, 178, 187, 202, 278, 287, 353, 518, 542, 759, 786, 922, 1182, 1343, 1398, 1511, 1578, 1582, 1974, 3243, 3503, 3562, 5358, 12423, 13422\}$
$(1, 1, 27)$	$\{7, 11, 14, 19, 22, 23, 38, 46, 55, 62, 70, 71, 83, 86, 94, 103, 115, 119, 139, 151, 154, 167, 179, 199, 203, 211, 215, 262, 266, 322, 331, 335, 374, 395, 418, 430, 467, 523, 526, 542, 551, 559, 587, 595, 614, 671, 710, 766, 790, 851, 863, 878, 895, 934, 938, 979, 1034, 1039, 1231, 1235, 1291, 1406, 1426, 1610, 1742, 1846, 1991, 2270, 2446, 2567, 2659, 2674, 3083, 3107, 3514, 3799, 4262, 4486, 5855, 6719, 8627, 8858, 13711, 14986\}$

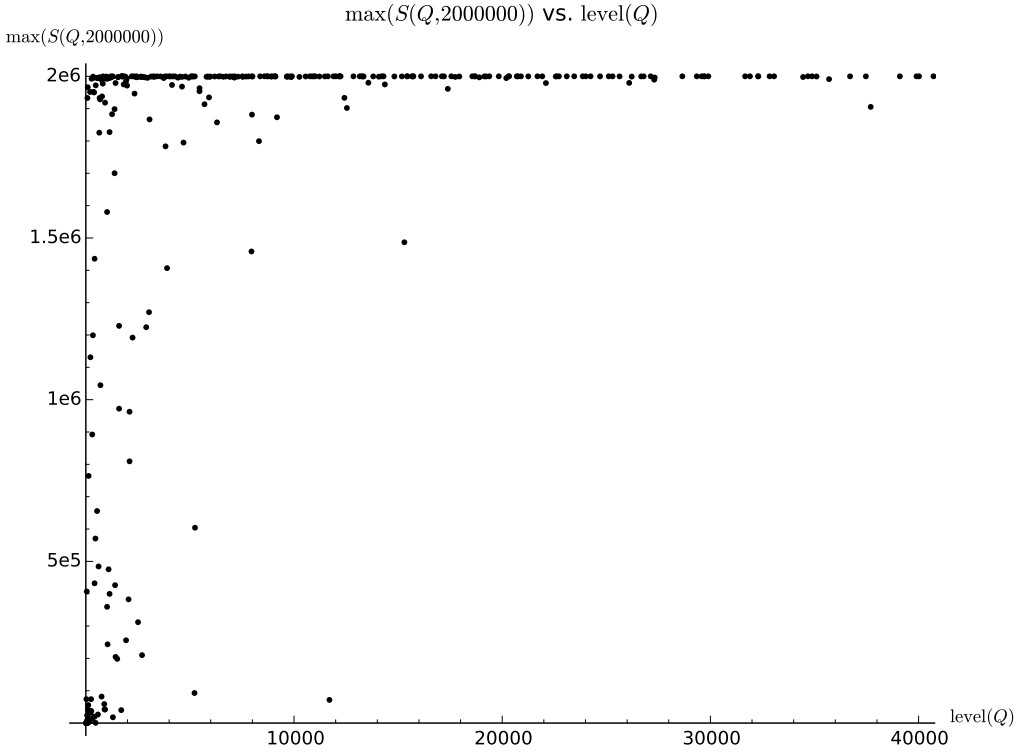
Appendix E. Plots About $S(Q, 2000000)$

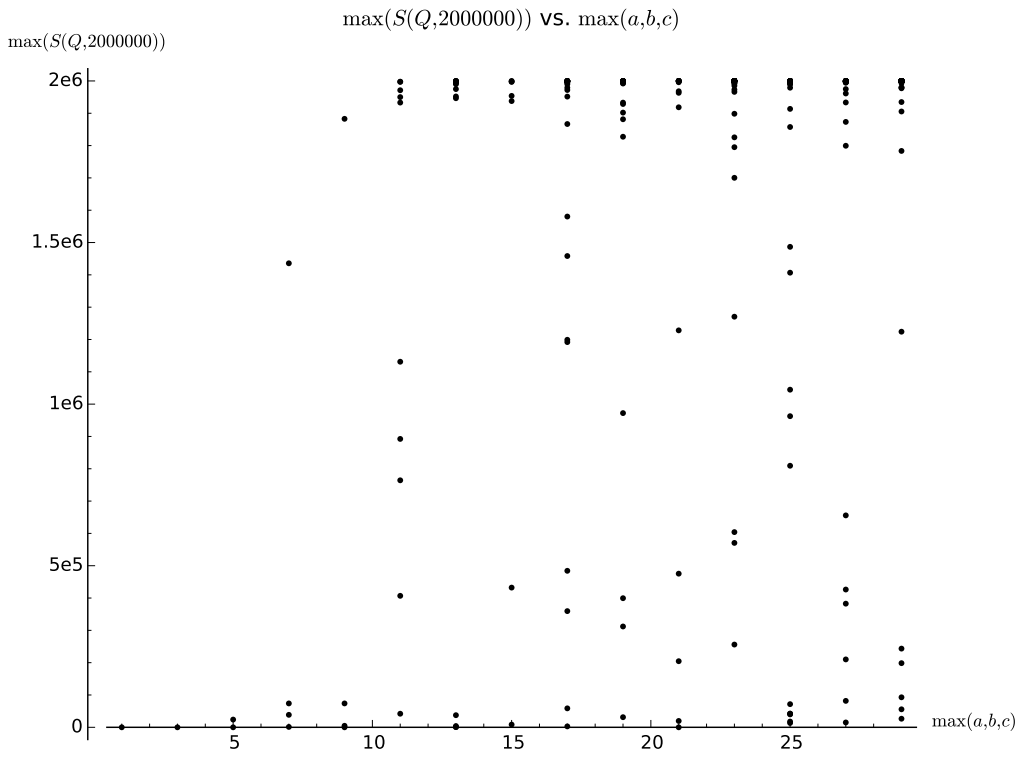
The following plots were made using the `get_locally_not_globally_represented_list_odd()` function to find all the elements of $S(Q, 2000000)$ for Q such that $a, b, c < 30$ are odd and pairwise coprime.

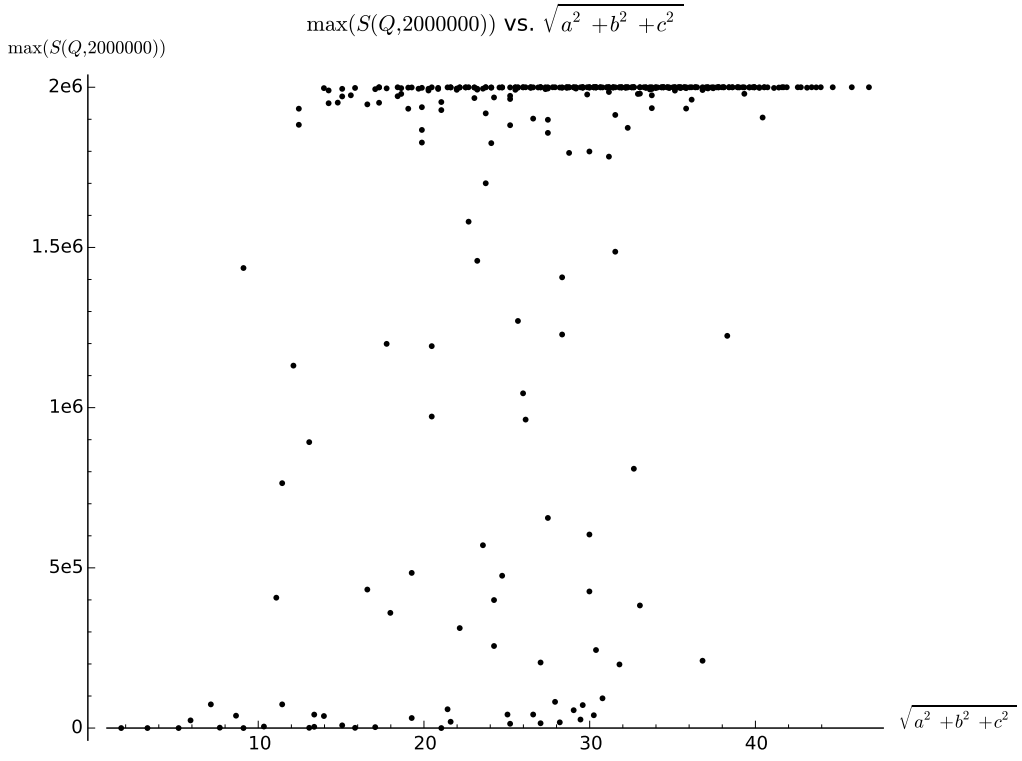


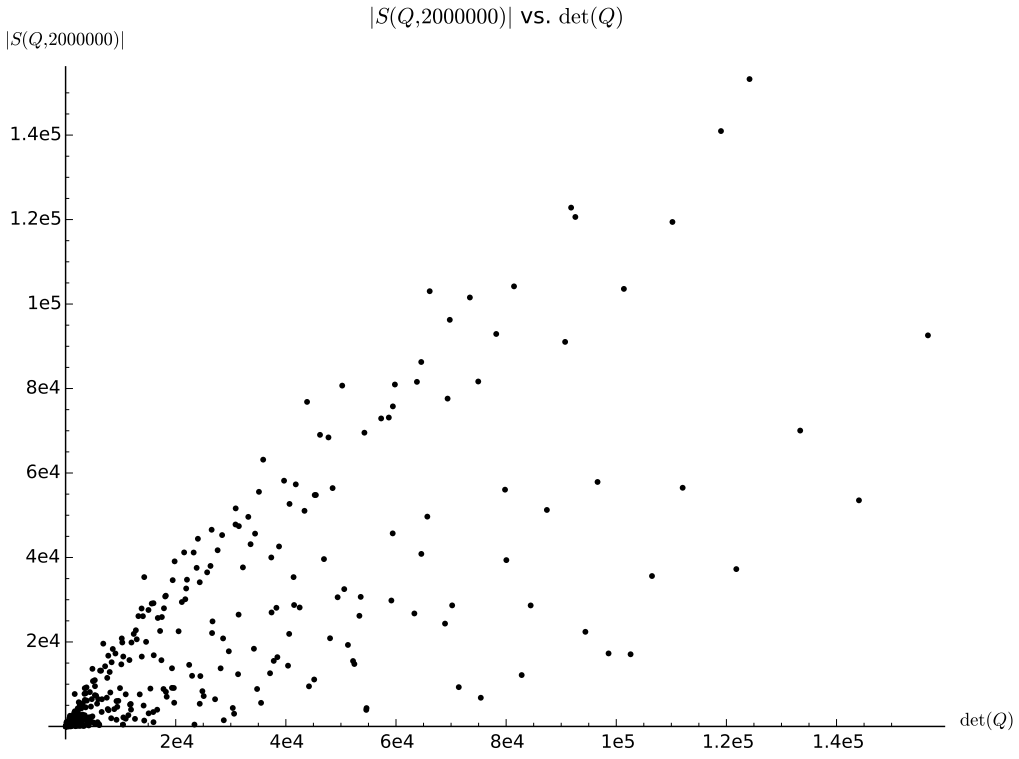


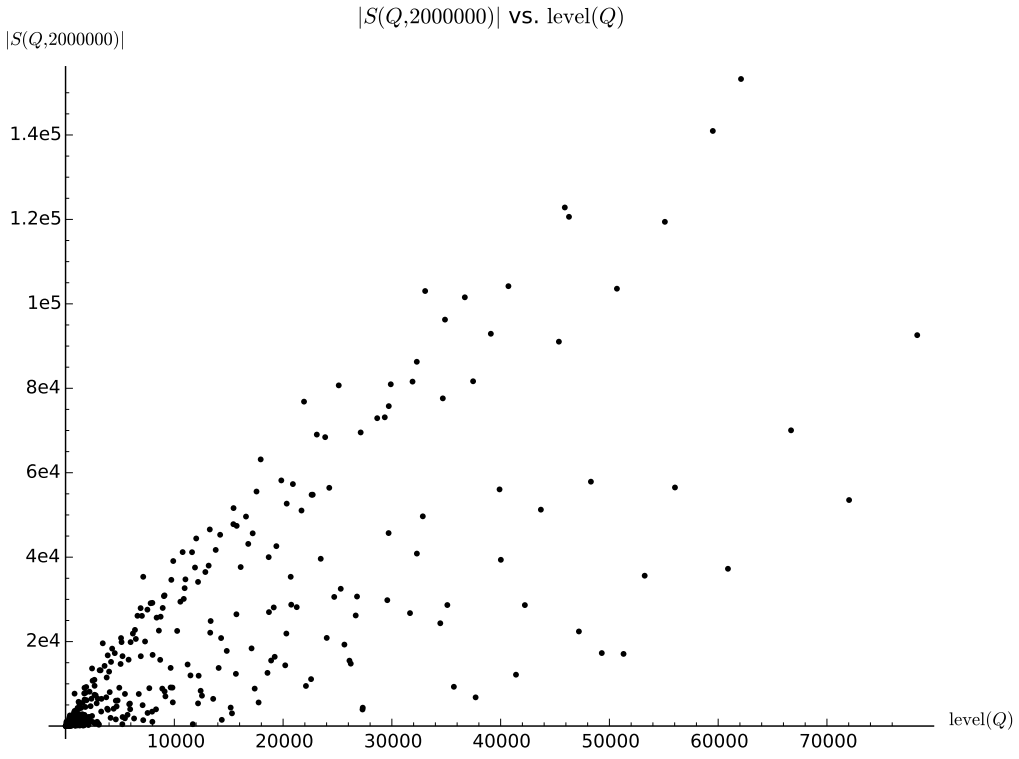

max(S(Q,2000000)) vs. level(Q)
max(S(Q,2000000))
2e6
1.5e6
1e6
5e5
level(Q)
10000
20000
30000
40000
50000
60000
70000

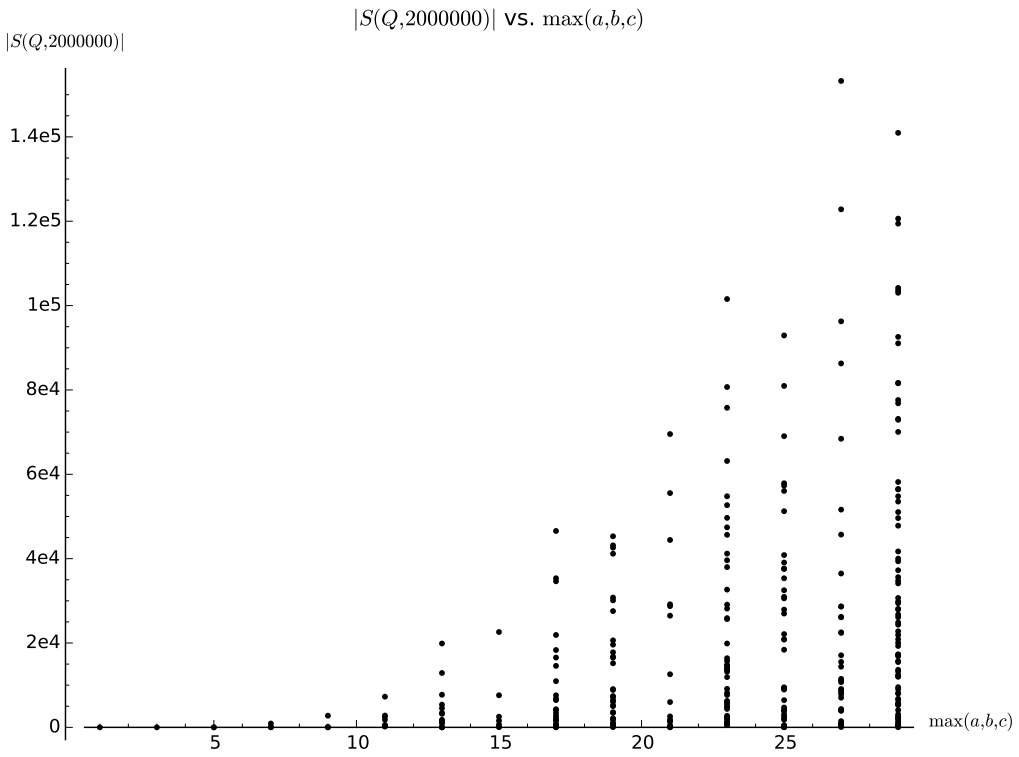

max(S(Q,2000000)) vs. level(Q)
max(S(Q,2000000))
2e6
1.5e6
1e6
5e5
level(Q)
10000
20000
30000
40000

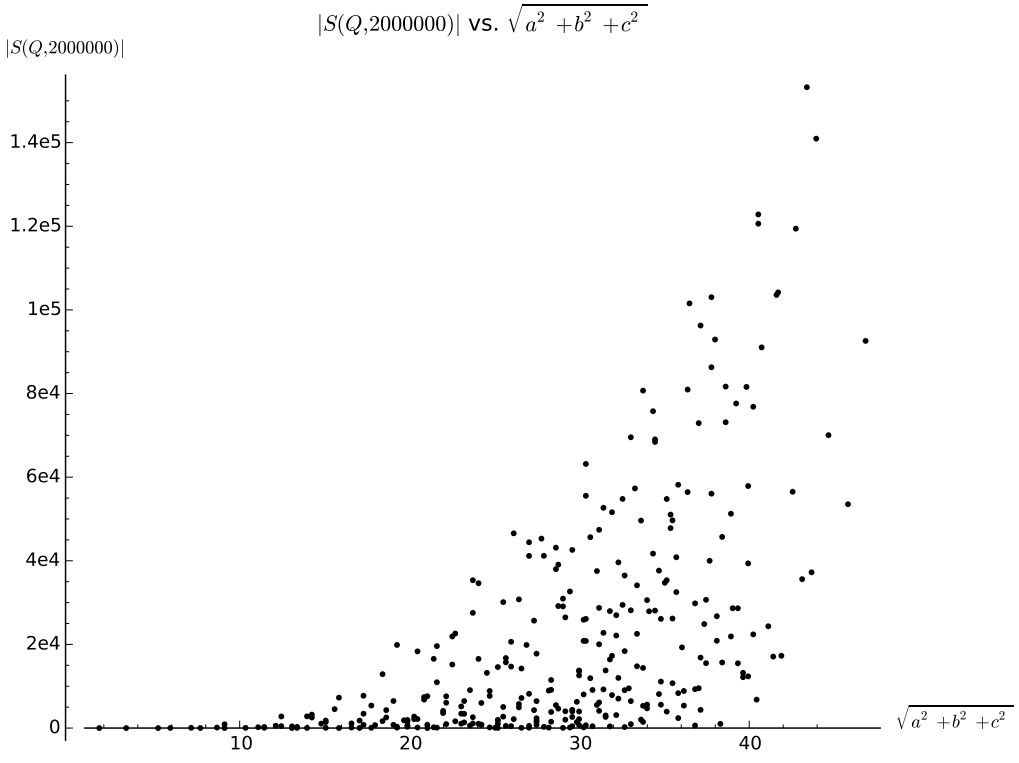

max(S(Q,2000000)) vs. max(a,b,c)
max(S(Q,2000000))
2e6
1.5e6
1e6
5e5
0
5
10
15
20
25
max(a,b,c)

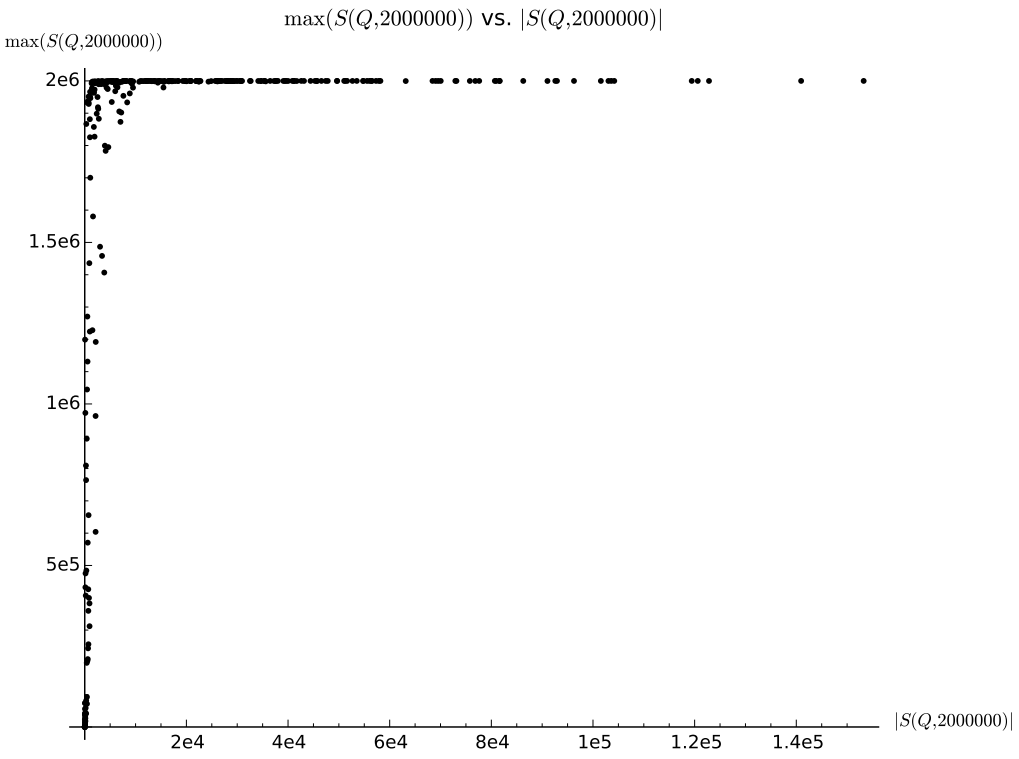

max(S(Q,2000000)) vs. √(a² +b² +c²)
max(S(Q,2000000))
2e6
1.5e6
1e6
5e5
0
10
20
30
40
√(a² +b² +c²)

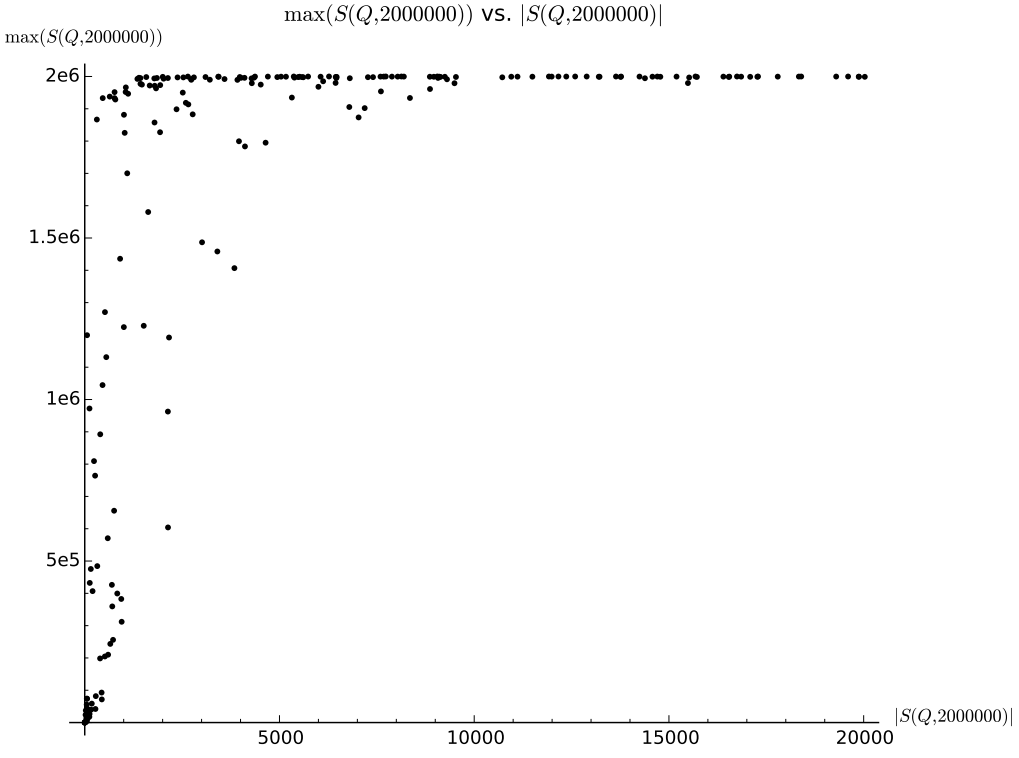

|S(Q,2000000)| vs. det(Q)
|S(Q,2000000)|
1.4e5
1.2e5
1e5
8e4
6e4
4e4
2e4
2e4
4e4
6e4
8e4
1e5
1.2e5
1.4e5
det(Q)


|S(Q,2000000)| vs. level(Q)
|S(Q,2000000)|
1.4e5
1.2e5
1e5
8e4
6e4
4e4
2e4
10000
20000
30000
40000
50000
60000
70000
level(Q)


$|S(Q,2000000)|$ vs. $\max(a,b,c)$
$|S(Q,2000000)|$
1.4e5
1.2e5
1e5
8e4
6e4
4e4
2e4
0
5
10
15
20
25
$\max(a,b,c)$


$|S(Q,2000000)|$ vs. $\sqrt{a^2+b^2+c^2}$
$|S(Q,2000000)|$
1.4e5
1.2e5
1e5
8e4
6e4
4e4
2e4
0
10
20
30
40
$\sqrt{a^2+b^2+c^2}$


max(S(Q,2000000)) vs. |S(Q,2000000)|
max(S(Q,2000000))
2e6
1.5e6
1e6
5e5
2e4
4e4
6e4
8e4
1e5
1.2e5
1.4e5
|S(Q,2000000)|


max(S(Q,2000000)) vs. |S(Q,2000000)|
max(S(Q,2000000))
2e6
1.5e6
1e6
5e5
5000
10000
15000
20000
|S(Q,2000000)|

Appendix F. Smallest Values of $\max(S(Q, 2000000))/|S(Q, 2000000)|$

Let $sl(Q, n) = \max(S(Q, n))/|S(Q, n)|$ for Q such that $|S(Q, n)| < \frac{9}{10}n$. The following table lists the 25 smallest values of $sl(Q, 2000000)$ found and their corresponding quadratic forms. The first column of the table contains $sl(Q, 2000000)$. The second column contains the coefficients of the corresponding quadratic form Q in the form (a, b, c), where $Q(\vec{\mathbf{v}}) = ax^2 + by^2 + cz^2$. The last column contains a decimal approximation of $sl(Q, 2000000)$. Note that $a, b, c < 30$ are odd and pairwise coprime.

$sl(Q, 2000000)$	(a, b, c)	Approximation of $sl(Q, 2000000)$
721/13	(1, 9, 13)	55.4615384615385
1941/23	(1, 3, 13)	84.3913043478261
1193/14	(1, 3, 7)	85.2142857142857
721/8	(1, 1, 13)	90.1250000000000
4697/47	(1, 5, 9)	99.9361702127660
2819/19	(1, 1, 17)	148.368421052632
17818/119	(1, 13, 25)	149.731092436975
8394/55	(1, 1, 15)	152.618181818182
42037/275	(3, 7, 11)	152.861818181818
35831/219	(9, 13, 25)	163.611872146119
7493/42	(1, 1, 27)	178.404761904762
19651/96	(1, 5, 21)	204.697916666667
26547/124	(1, 5, 29)	214.088709677419
92842/433	(5, 9, 29)	214.415704387991
19999/82	(1, 17, 25)	243.890243902439
604013/2138	(3, 19, 23)	282.513096351731
81797/284	(1, 7, 27)	288.017605633803
58647/181	(1, 13, 17)	324.016574585635
13422/41	(1, 3, 25)	327.365853658537
311969/948	(3, 11, 19)	329.081223628692
7719/23	(1, 5, 7)	335.608695652174
105041/300	(1, 25, 27)	350.136666666667
31305/89	(1, 3, 19)	351.741573033708
256057/727	(3, 7, 23)	352.210453920220
468901/1281	(3, 13, 25)	366.042935206870

References

[Apo76] Tom M. Apostol, *Introduction to analytic number theory*, Springer-Verlag, 1976.

[BEW98] Bruce C. Berndt, Ronald J. Evans, and Kenneth S. Williams, *Gauss and Jacobi sums*, John Wiley & Sons, 1998.

[Coh93] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, pp. 27 – 28, Springer-Verlag, 1993.

[Duk88] W. Duke, *Lattice points on ellipsoids*, Séminaire de Théorie des Nombres **16** (1987-1988).

[Duk05] ———, *On ternary quadratic forms*, Journal of Number Theory **110** (2005), no. 1, 37 – 43, available on web, accessed 19 Nov. 2014, `http://www.sciencedirect.com/science/article/pii/S0022314X04001404#`.

[Gro85] Emil Grosswald, *Representations of integers as sums of squares*, Springer-Verlag, 1985.

[Iwa87] Henryk Iwaniec, *Fourier coefficients of modular forms of half-integral weight*, Inventiones mathematicae **87** (1987), no. 2, 385 – 401.

[JP39] Burton W. Jones and Gordon Pall, *Regular and semi-regular positive ternary quadratic forms*, Acta Mathematica **70** (1939), no. 1, 165 – 191.

[LeV96] William J. LeVeque, *Fundamentals of number theory*, Dover, 1996, originally published by Addison-Wesley, c. 1977.

CM 3204, Rose-Hulman Institute of Technology, 5500 Wabash Ave., Terre Haute, IN 47803, U.S.A.

E-mail address: `jonesel@rose-hulman.edu`