GAUSS SUMS & REPRESENTATION BY TERNARY QUADRATIC FORMS

EDNA JONES

ABSTRACT. This paper specifies some conditions as to when an integer m is locally represented by a positive definite diagonal integer-matrix ternary quadratic form Q at a prime p. We use quadratic Gauss sums and a version of Hensel's Lemma to count how many solutions there are to the equivalence $Q(\vec{\mathbf{x}}) \equiv m \pmod{p^k}$ for any $k \geq 0$. Given that m is coprime to the determinant of the Hessian matrix of Q, we can determine if m is locally represented everywhere by Q in finitely many steps.

1. INTRODUCTION

One of the oldest questions in number theory is the question of when is an integer m is globally represented by an integral quadratic form Q. In this paper, we focus on when Q is a positive definite diagonal integer-matrix ternary quadratic form, meaning that Q can written as $Q(\vec{\mathbf{x}}) = ax^2 + by^2 + cz^2$, where a, b, and c are positive integers and $\vec{\mathbf{x}} = (x, y, z)^T$. We say that m is *(globally) represented* by Q if there exists $\vec{\mathbf{x}} \in \mathbb{Z}^3$ such that $Q(\vec{\mathbf{x}}) = m$.

In attempting to answer the question of when is m is globally represented by an integral quadratic form Q, people 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 $Q(\vec{\mathbf{x}}) \equiv m \pmod{p^k}$.

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. Actually, it is not immediately apparent how to check if m is locally represented by Q at a given prime p, because it appears from the definition of locally represented at p that one would need to check for infinitely-many $k \geq 0$ that there exists $\vec{\mathbf{x}} \in \mathbb{Z}^3$ such that $Q(\vec{\mathbf{x}}) \equiv m \pmod{p^k}$.

The definition of an integer m being locally represented by Q at a prime p suggests that we should count how many solutions there are to the equivalence $Q(\vec{\mathbf{x}}) \equiv m \pmod{p^k}$ for $k \geq 0$. We use $r_{p^k,Q}(m)$ to do this counting. For a positive integer n, we define $r_{n,Q}(m)$ as

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

Clearly, m is locally represented by Q at p if and only if $r_{p^k,Q}(m) > 0$ for every $k \geq 0$.

To compute $r_{p^k,Q}(m)$, we use quadratic Gauss sums. Suppose $a, q \in \mathbb{Z}$ with $q > 0$. The *quadratic Gauss sum $G\left(\frac{a}{q}\right)$ 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 $\mathrm{e}(w)$. Unless otherwise specified, in this paper, the term Gauss sum will be taken to refer to a quadratic Gauss sum. Many Gauss sums have closed-form evaluations. Some of these formulas can be found in Section 2.

In Section 3, we show that

$$r_{p^k,Q}(m) = \frac{1}{p^k} \sum_{t=0}^{p^k-1} \mathrm{e}\left(\frac{-mt}{p^k}\right) G\left(\frac{at}{p^k}\right) G\left(\frac{bt}{p^k}\right) G\left(\frac{ct}{p^k}\right). \tag{1.1}$$

Given certain conditions on a, b, c, and m, we can find closed-form formulas for $r_{p^k,Q}(m)$. As an example, if p is an odd prime, $p \nmid abcm$, and $k \geq 1$, we can explicitly evaluate (1.1) and get

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

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol. Other explicit formulas for $r_{p^k,Q}(m)$ appear in Section 3.

2. Formulas for Gauss Sums

For all of the formulas in 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 $r_{p^k,Q}(m)$.)

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. The lemma follows from the orthogonality of characters. $\square$

Lemma 2.2. *Suppose p is an odd prime and $a \in \mathbb{Z}$. Then*

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

If $p \nmid a$, then

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

Proof. 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 $p \nmid a$,

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

follows from (2.1) and Lemma 2.1. ☐

Let q be a positive integer. Equations (2.2),(2.3), and (2.4) follow from the definition of quadratic Gauss sums.

$$G\left(\frac{0}{q}\right) = q. \tag{2.2}$$

$$G\left(\frac{a}{1}\right) = 1. \tag{2.3}$$

$$G\left(\frac{a}{2}\right) = \begin{cases} 0, & \text{if } \gcd(a,2) = 1, \\ 2, & \text{otherwise.} \end{cases} \tag{2.4}$$

Lemma 2.3. *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*

$$G\left(\frac{a}{p^k}\right) = p^\ell G\left(\frac{a_0}{p^{k-\ell}}\right). \tag{2.5}$$

Proof. By the definition of a quadratic Gauss sum,

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

☐

Lemma 2.4. *Suppose $k \geq 1$ and p is an odd prime. 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 and

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

Proof. The lemma is a special case of Theorem 1.5.2 in [BEW98] on page 26. ☐

Lemma 2.5. *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. If $k \leq \ell$, then the result follows from the definition of a quadratic Gauss sum.

Suppose $k > \ell$. Using the definition of a quadratic Gauss sum and Lemmas 2.3 and 2.4,

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

Lemma 2.6. *Suppose* $\gcd(a, 2) = 1$ *and* $k \geq 2$. *Then*

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

where $\left(\frac{\cdot}{a}\right)$ *is the Jacobi symbol and*

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

Proof. See Equation 1.5.5 in Proposition 1.5.3 of [BEW98] on page 26. $\square$

Lemma 2.7. *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*

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

Proof. If $k \leq \ell$, then the result follows from the definition of a quadratic Gauss sum.

Suppose $k = \ell + 1$, so $k - \ell = 1$ and $\ell = k - 1$. Using the definition of a quadratic Gauss sum and Lemmas 2.3 and 2.6,

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

Suppose $k > \ell + 1$, so $k - \ell \geq 2$. Using the definition of a quadratic Gauss sum and Lemmas 2.3 and 2.6,

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

3. Counting the Number of Local Solutions

Throughout this paper, $Q(\vec{\mathbf{x}})$ is a positive definite diagonal ternary quadratic form such that $Q(\vec{\mathbf{x}}) = ax^2 + by^2 + cz^2$, where a, b, and c are positive integers and $\vec{\mathbf{x}} = (x, y, z)^T$. Recall that the definition of an integer m being locally represented everywhere by Q suggests that we should calculate $r_{p^k,Q}(m)$, where p is a positive prime integer and k is a nonnegative integer. Clearly, 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 $Q(\vec{\mathbf{x}}) = ax^2 + by^2 + cz^2$, where a, b, c are positive integers, there exists $\vec{\mathbf{x}} \in \mathbb{R}^3$ such that $Q(\vec{\mathbf{x}}) = m$ 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, $r_{1,Q}(m) = 1$, 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 $ax^2+by^2+cz^2$.

By Lemma 2.1,

$$\frac{1}{p^k}\sum_{t=0}^{p^k-1}\mathrm{e}\left(\frac{(Q(\vec{\mathbf{x}})-m)t}{p^k}\right)=\begin{cases}1, & \text{if } Q(\vec{\mathbf{x}})\equiv m \pmod{p^k},\\ 0, & \text{otherwise.}\end{cases} \tag{3.1}$$

Therefore,

$$r_{p^k,Q}(m)=\sum_{\vec{\mathbf{x}}\in(\mathbb{Z}/p^k\mathbb{Z})^3}\frac{1}{p^k}\sum_{t=0}^{p^k-1}\mathrm{e}\left(\frac{(Q(\vec{\mathbf{x}})-m)t}{p^k}\right) \tag{3.2}$$

$$=\sum_{x=0}^{p^k-1}\sum_{y=0}^{p^k-1}\sum_{z=0}^{p^k-1}\frac{1}{p^k}\sum_{t=0}^{p^k-1}\mathrm{e}\left(\frac{(ax^2+by^2+cz^2-m)t}{p^k}\right) \tag{3.3}$$

$$=\frac{1}{p^k}\sum_{t=0}^{p^k-1}\mathrm{e}\left(\frac{-mt}{p^k}\right)G\left(\frac{at}{p^k}\right)G\left(\frac{bt}{p^k}\right)G\left(\frac{ct}{p^k}\right). \tag{3.4}$$

Equation (3.4) 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 equation (3.4) explicitly.

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

The fast Fourier transform (FFT) can be used to relative 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 $f(t)=\frac{1}{p^k}G\left(\frac{at}{p^k}\right)G\left(\frac{bt}{p^k}\right)G\left(\frac{ct}{p^k}\right)$, 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 $m\in\mathbb{Z}/p^k\mathbb{Z}$.

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

The following theorem is essentially a version of Hensel's lemma specific to the quadratic forms being considered in this paper.

Theorem 3.1. *Let m be an integer and p be an odd positive prime integer. Suppose $\vec{\mathbf{x}}_0=(x_0,y_0,z_0)^T\in\mathbb{Z}^3$ is a solution to $Q(\vec{\mathbf{x}})\equiv m \pmod{p^k}$ for some $k\geq 1$. If $p\nmid ax_0$, $p\nmid by_0$, or $p\nmid cz_0$, then $\vec{\mathbf{x}}_0=(x_0,y_0,z_0)^T$ lifts to exactly p^2 solutions to $Q(\vec{\mathbf{x}})\equiv m \pmod{p^{k+1}}$. That is,* *there are exactly* p^2 *solutions to* $Q(\vec{\mathbf{x}}) \equiv m \pmod{p^{k+1}}$ *of the form* $(x_0 + x_1 p^k, y_0 + y_1 p^k, z_0 + z_1 p^k)^T$*, 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 $Q(\vec{\mathbf{x}}) \equiv m \pmod{p^{k+1}}$ of the form $(x_0 + x_1 p^k, y_0 + y_1 p^k, z_0 + z_1 p^k)^T$. Because $Q(\vec{\mathbf{x}}_0) \equiv m \pmod{p^k}$, there exists $\ell \in \mathbb{Z}$ such that $ax_0^2 + by_0^2 + cz_0^2 = m + \ell p^k$. For some $x_1, y_1, z_1 \in \mathbb{Z}/p\mathbb{Z}$, observe that

$$a(x_0 + p^k x_1)^2 + b(y_0 + p^k y_1)^2 + c(z_0 + p^k z_1)^2 - m \tag{3.5}$$

$$= (\ell + 2ax_0x_1 + 2by_0y_1 + 2cz_0z_1)p^k + (ax_1^2 + by_1^2 + cz_1^2)p^{2k} \tag{3.6}$$

$$\equiv (\ell + 2ax_0x_1 + 2by_0y_1 + 2cz_0z_1)p^k \pmod{p^{k+1}}. \tag{3.7}$$

Let

$$x_1 = (2ax_0)^{-1}(-\ell - 2by_0y_1 - 2cz_0z_1), \tag{3.8}$$

where $2ax_0(2ax_0)^{-1} \equiv 1 \pmod{p} \iff 2ax_0(2ax_0)^{-1} = 1 + tp$ for some $t \in \mathbb{Z}$. (Note that $(2ax_0)^{-1}$ exists since $p \nmid 2ax_0$.) Then

$$a(x_0 + p^k x_1)^2 + b(y_0 + p^k y_1)^2 + c(z_0 + p^k z_1)^2 - m \tag{3.9}$$

$$\equiv (\ell + 2ax_0x_1 + 2by_0y_1 + 2cz_0z_1)p^k \pmod{p^{k+1}} \tag{3.10}$$

$$= (\ell + 2ax_0(2ax_0)^{-1}(-\ell - 2by_0y_1 - 2cz_0z_1) + 2by_0y_1 + 2cz_0z_1)p^k \pmod{p^{k+1}} \tag{3.11}$$

$$= (\ell + (1 + tp)(-\ell - 2by_0y_1 - 2cz_0z_1) + 2by_0y_1 + 2cz_0z_1)p^k \pmod{p^{k+1}} \tag{3.12}$$

$$= t(-\ell - 2by_0y_1 - 2cz_0z_1)p^{k+1} \pmod{p^{k+1}} \tag{3.13}$$

$$\equiv 0 \pmod{p^{k+1}} \tag{3.14}$$

$$\iff a(x_0 + p^k x_1)^2 + b(y_0 + p^k y_1)^2 + c(z_0 + p^k z_1)^2 \equiv m \pmod{p^{k+1}}. \tag{3.15}$$

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

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 using (3.7), we see that

$$(\ell + 2ax_0x_1 + 2by_0y_1 + 2cz_0z_1)p^k \equiv 0 \pmod{p^{k+1}} \tag{3.16}$$

$$\iff \ell + 2ax_0x_1 + 2by_0y_1 + 2cz_0z_1 \equiv 0 \pmod{p} \tag{3.17}$$

$$\iff 2ax_0x_1 \equiv -\ell - 2by_0y_1 - 2cz_0z_1 \pmod{p} \tag{3.18}$$

$$\iff x_1 \equiv (2ax_0)^{-1}(-\ell - 2by_0y_1 - 2cz_0z_1) \pmod{p}. \tag{3.19}$$

From (3.19), we see 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 $Q(\vec{\mathbf{x}}) \equiv m \pmod{p^{k+1}}$ of the form $(x_0 + x_1 p^k, y_0 + y_1 p^k, z_0 + z_1 p^k)^T$, where $x_1, y_1, z_1 \in \mathbb{Z}/p\mathbb{Z}$. □

Corollary 3.2. *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* $n = r_{p^k,Q}(m)$ *solutions in* $(\mathbb{Z}/p^k\mathbb{Z})^3$ *to* $Q(\vec{\mathbf{x}}) \equiv m \pmod{p^k}$*, 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* $Q(\vec{\mathbf{x}}) \equiv m \pmod{p^{k+\ell}}$ *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* $Q(\vec{\mathbf{x}}) \equiv m \pmod{p^{k+\ell}}$ *satisfies the property that* $p \nmid ax_0$*,* $p \nmid by_0$*, or* $p \nmid cz_0$*.*

Proof. The corollary follows from a simple induction proof using Theorem 3.1. ☐

Theorem 3.3. *Let p be an odd prime. Suppose $p \nmid m$. Since $Q(\vec{\mathbf{x}})$ is a primitive quadratic form, p divides exactly none, one, or two of a, b, c. If p divides exactly one of a, b, c, rename a, b, c to a', b', c' so that $p \nmid a'b'$ and $p \mid c'$. If p divides exactly two of a, b, c, rename a, b, c to a', b', c' so that $p \nmid a'$, $p \mid b'$, and $p \mid c'$. Then*

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

Proof.

Because $p \nmid m$, any solution $(x_0, y_0, z_0)^T$ to $Q(\vec{\mathbf{x}}) \equiv m \pmod p$ has the property that $p \nmid ax_0$, $p \nmid by_0$, or $p \nmid cz_0$. Therefore, Corollary 3.2 can be used once $r_{p,Q}(m)$ is known.

Case 1 ($p \nmid abc$):

Using (3.4), we get

$$r_{p,Q}(m) = \frac{1}{p}\sum_{t=0}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right) G\left(\frac{at}{p}\right) G\left(\frac{bt}{p}\right) G\left(\frac{ct}{p}\right) \tag{3.20}$$

$$= p^2 + \frac{1}{p}\sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right) G\left(\frac{at}{p}\right) G\left(\frac{bt}{p}\right) G\left(\frac{ct}{p}\right) \tag{3.21}$$

$$= p^2 + \frac{1}{p}\sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right) p^{1/2}\left(\frac{at}{p}\right)\varepsilon_p p^{1/2}\left(\frac{bt}{p}\right)\varepsilon_p p^{1/2}\left(\frac{ct}{p}\right)\varepsilon_p \tag{3.22}$$

$$= p^2 + p^{1/2}(\varepsilon_p)^3\left(\frac{abc}{p}\right)\sum_{t=1}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right)\left(\frac{t}{p}\right) \tag{3.23}$$

$$= p^2 + p^{1/2}(\varepsilon_p)^3\left(\frac{abc}{p}\right)\sum_{t=0}^{p-1} \mathrm{e}\left(\frac{-mt}{p}\right)\left(\frac{t}{p}\right) \qquad \left(\text{since } \left(\frac{0}{p}\right) = 0\right) \tag{3.24}$$

$$= p^2 + p^{1/2}(\varepsilon_p)^3\left(\frac{abc}{p}\right) G\left(\frac{-m}{p}\right) \qquad (\text{by Lemma 2.2}) \tag{3.25}$$

$$= p^2 + p^{1/2}(\varepsilon_p)^3\left(\frac{abc}{p}\right) p^{1/2}\left(\frac{-m}{p}\right)\varepsilon_p \tag{3.26}$$

$$= p^2 + p\left(\frac{-abcm}{p}\right) = p^2\left(1 + \frac{1}{p}\left(\frac{-abcm}{p}\right)\right) \qquad (\text{since } (\varepsilon_p)^4 = 1). \tag{3.27}$$

The formula $r_{p^k,Q} = p^{2k}\left(1 + \frac{1}{p}\left(\frac{-abcm}{p}\right)\right)$ follows from Corollary 3.2.

Case 2 ($p \nmid a'b'$ and $p \mid c'$):
Using (3.4), we get

$$\begin{aligned}
r_{p,Q}(m) &= \frac{1}{p}\sum_{t=0}^{p-1} \mathrm{e}\!\left(\frac{-mt}{p}\right) G\!\left(\frac{a't}{p}\right) G\!\left(\frac{b't}{p}\right) G\!\left(\frac{c't}{p}\right) \\
&= p^2 + \frac{1}{p}\sum_{t=1}^{p-1} \mathrm{e}\!\left(\frac{-mt}{p}\right) G\!\left(\frac{a't}{p}\right) G\!\left(\frac{b't}{p}\right) \cdot p \\
&= p^2 + \sum_{t=1}^{p-1} \mathrm{e}\!\left(\frac{-mt}{p}\right) p^{1/2} \left(\frac{a't}{p}\right) \varepsilon_p p^{1/2} \left(\frac{b't}{p}\right) \varepsilon_p \\
&= p^2 + p \cdot (\varepsilon_p)^2 \left(\frac{a'b'}{p}\right) \sum_{t=1}^{p-1} \mathrm{e}\!\left(\frac{-mt}{p}\right) \\
&= p^2 + p \left(\frac{-a'b'}{p}\right) \left(\sum_{t=0}^{p-1} \mathrm{e}\!\left(\frac{-mt}{p}\right) - 1\right) && \left(\text{since } (\varepsilon_p)^2 = \left(\frac{-1}{p}\right)\right) \\
&= p^2 - p \left(\frac{-a'b'}{p}\right) = p^2 \left(1 - \frac{1}{p}\left(\frac{-a'b'}{p}\right)\right) && \text{(by Lemma 2.1).}
\end{aligned}$$

The formula $r_{p^k,Q} = p^{2k}\left(1 - \frac{1}{p}\left(\frac{-a'b'}{p}\right)\right)$ follows from Corollary 3.2.

Case 3 ($p \nmid a'$, $p \mid b'$, and $p \mid c'$):
Using (3.4), we get

$$\begin{aligned}
r_{p,Q}(m) &= \frac{1}{p}\sum_{t=0}^{p-1} \mathrm{e}\!\left(\frac{-mt}{p}\right) G\!\left(\frac{a't}{p}\right) G\!\left(\frac{b't}{p}\right) G\!\left(\frac{c't}{p}\right) \\
&= p^2 + \frac{1}{p}\sum_{t=1}^{p-1} \mathrm{e}\!\left(\frac{-mt}{p}\right) p^{1/2} \left(\frac{a't}{p}\right) \varepsilon_p \cdot p^2 \\
&= p^2 + p^{3/2}\varepsilon_p \left(\frac{a'}{p}\right) \sum_{t=1}^{p-1} \mathrm{e}\!\left(\frac{-mt}{p}\right) \left(\frac{t}{p}\right) \\
&= p^2 + p^{3/2}\varepsilon_p \left(\frac{a'}{p}\right) \sum_{t=0}^{p-1} \mathrm{e}\!\left(\frac{-mt}{p}\right) \left(\frac{t}{p}\right) && \left(\text{since } \left(\frac{0}{p}\right) = 0\right) \\
&= p^2 + p^{3/2}\varepsilon_p \left(\frac{a'}{p}\right) G\!\left(\frac{-m}{p}\right) \\
&= p^2 + p^{3/2}\varepsilon_p \left(\frac{a'}{p}\right) p^{1/2} \left(\frac{-m}{p}\right) \varepsilon_p \\
&= p^2 + p^2(\varepsilon_p)^2 \left(\frac{-a'm}{p}\right) \\
&= p^2 + p^2 \left(\frac{a'm}{p}\right) = p^2\left(1 + \left(\frac{a'm}{p}\right)\right) && \left(\text{since } (\varepsilon_p)^2 = \left(\frac{-1}{p}\right)\right).
\end{aligned}$$

The formula $r_{p^k,Q} = p^{2k}\left(1+\left(\frac{a'm}{p}\right)\right)$ follows from Corollary 3.2. □

Lemma 3.4. *Let p is 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. Since $\left(\frac{0}{p}\right) = 0$, $\sum_{t=0}^{p-1}\left(\frac{t}{p}\right) = \sum_{t=1}^{p-1}\left(\frac{t}{p}\right)$.

From Lemma 2.2 , we know that

$$G\left(\frac{0}{p}\right) = \sum_{t=0}^{p-1}\left(1+\left(\frac{t}{p}\right)\right)\mathrm{e}\left(\frac{0t}{p}\right) = \sum_{t=0}^{p-1}\left(1+\left(\frac{t}{p}\right)\right) = p+\sum_{t=0}^{p-1}\left(\frac{t}{p}\right). \tag{3.28}$$

On the other hand, from (2.2) we know that

$$G\left(\frac{0}{p}\right) = p. \tag{3.29}$$

By setting (3.28) equal to (3.29), we get

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

□

Theorem 3.5. *Let p be an odd prime. Suppose that $p \parallel m$ and $p \nmid abc$. Then*

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

Proof. Let $m = m'p$ for some $m' \in \mathbb{Z}$ so that $\gcd(m', p) = 1$.

For the case in which $k = 1$, the proof is somewhat the same as in the proof of Case 1 of Theorem 3.3. Equation (3.24) still holds when $p \mid m$. Therefore,

$$\begin{aligned} r_{p,Q}(m) &= p^2 + p^{1/2}(\varepsilon_p)^3\left(\frac{abc}{p}\right)\sum_{t=0}^{p-1}\mathrm{e}\left(\frac{-mt}{p}\right)\left(\frac{t}{p}\right) \\ &= p^2 + p^{1/2}(\varepsilon_p)^3\left(\frac{abc}{p}\right)\sum_{t=0}^{p-1}\mathrm{e}(-m't)\left(\frac{t}{p}\right) \\ &= p^2 + p^{1/2}(\varepsilon_p)^3\left(\frac{abc}{p}\right)\sum_{t=0}^{p-1}\left(\frac{t}{p}\right) = p^2 \qquad \text{(by Lemma 3.4).} \end{aligned}$$

Let $(x_0, y_0, z_0)^T$ be a solution to $Q(\vec{\mathbf{x}}) \equiv m \pmod{p^2}$. Toward contradiction, assume that $p \mid ax_0$, $p \mid by_0$, and $p \mid cz_0$. Since $p \nmid abc$, $x_0 = x_1p$, $y_0 = y_1p$, and $z_0 = z_1p$ for some

$x_1, y_1, z_1 \in \mathbb{Z}$. Thus,

$$\begin{aligned} ax_0^2 + by_0^2 + cz_0^2 &= a(x_1p)^2 + b(y_1p)^2 + c(z_1p)^2 \\ &= ax_1^2p^2 + by_1^2p^2 + cz_1^2p^2 \\ &\equiv 0 \pmod{p^2}. \end{aligned}$$

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

$$\begin{aligned} r_{p^2,Q}(m) &= \frac{1}{p^2} \sum_{t=0}^{p^2-1} \mathrm{e}\left(\frac{-mt}{p^2}\right) G\left(\frac{at}{p^2}\right) G\left(\frac{bt}{p^2}\right) G\left(\frac{ct}{p^2}\right) \\ &= p^4 + \frac{1}{p^2} \sum_{t=1}^{p^2-1} \mathrm{e}\left(\frac{-mt}{p^2}\right) G\left(\frac{at}{p^2}\right) G\left(\frac{bt}{p^2}\right) G\left(\frac{ct}{p^2}\right) \\ &= p^4 + \frac{1}{p^2} \sum_{t=1}^{p^2-1} \mathrm{e}\left(\frac{-m't}{p}\right) G\left(\frac{at}{p^2}\right) G\left(\frac{bt}{p^2}\right) G\left(\frac{ct}{p^2}\right). \end{aligned}$$

Let $t = t_0p^\tau$, where $\tau \in \{0, 1\}$ and $t_0 \in (\mathbb{Z}/p^{2-\tau}\mathbb{Z})^*$.

$$\begin{aligned} r_{p^2,Q}(m) &= p^4 + \frac{1}{p^2} \sum_{\tau=0}^{1} \sum_{t_0 \in (\mathbb{Z}/p^{2-\tau}\mathbb{Z})^*} \mathrm{e}\left(\frac{-m't_0p^\tau}{p}\right) G\left(\frac{at_0p^\tau}{p^2}\right) G\left(\frac{bt_0p^\tau}{p^2}\right) G\left(\frac{ct_0p^\tau}{p^2}\right) \\ &= p^4 + \frac{1}{p^2} \sum_{t_0 \in (\mathbb{Z}/p^2\mathbb{Z})^*} \mathrm{e}\left(\frac{-m't_0}{p}\right) G\left(\frac{at_0}{p^2}\right) G\left(\frac{bt_0}{p^2}\right) G\left(\frac{ct_0}{p^2}\right) \\ &\quad + \frac{1}{p^2} \sum_{t_0=1}^{p-1} \mathrm{e}\left(\frac{-m't_0p}{p}\right) G\left(\frac{at_0p}{p^2}\right) G\left(\frac{bt_0p}{p^2}\right) G\left(\frac{ct_0p}{p^2}\right) \\ &= p^4 + \frac{1}{p^2} \sum_{t_0 \in (\mathbb{Z}/p^2\mathbb{Z})^*} \mathrm{e}\left(\frac{-m't_0}{p}\right) p \left(\frac{at_0}{p^2}\right) \varepsilon_{p^2} p \left(\frac{bt_0}{p^2}\right) \varepsilon_{p^2} p \left(\frac{ct_0}{p^2}\right) \varepsilon_{p^2} \\ &\quad + \frac{1}{p^2} \sum_{t_0=1}^{p-1} \mathrm{e}(-m't_0)\, p^{3/2} \left(\frac{at_0}{p}\right) \varepsilon_p p^{3/2} \left(\frac{bt_0}{p}\right) \varepsilon_p p^{3/2} \left(\frac{ct_0}{p}\right) \varepsilon_p \\ &= p^4 + p \sum_{t_0 \in (\mathbb{Z}/p^2\mathbb{Z})^*} \mathrm{e}\left(\frac{-m't_0}{p}\right) + p^{5/2} \left(\frac{abc}{p}\right) (\varepsilon_p)^3 \sum_{t_0=1}^{p-1} \left(\frac{t_0}{p}\right) \\ &= p^4 + p \sum_{t_0 \in (\mathbb{Z}/p^2\mathbb{Z})^*} \mathrm{e}\left(\frac{-m't_0}{p}\right) \qquad \text{(by Lemma 3.4).} \end{aligned}$$

Now t_0 can be rewritten as $t_0 = t_1 + t_2 p$, where $1 \leq t_1 \leq p-1$ and $0 \leq t_2 \leq p-1$. Thus,

$$\begin{aligned}
r_{p^2,Q}(m) &= p^4 + p \sum_{t_1=1}^{p-1} \sum_{t_2=0}^{p-1} \mathrm{e}\left(\frac{-m'(t_1+t_2 p)}{p}\right) \\
&= p^4 + p \sum_{t_1=1}^{p-1} \mathrm{e}\left(\frac{-m't_1}{p}\right) \sum_{t_2=0}^{p-1} \mathrm{e}(-m't_2) \\
&= p^4 + p^2 \left(\sum_{t_1=0}^{p-1} \mathrm{e}\left(\frac{-m't_1}{p}\right) - 1 \right) \\
&= p^4 - p^2 && \text{(by Lemma 2.1)} \\
&= p^4 \left(1 - \frac{1}{p^2}\right).
\end{aligned}$$

The equation $r_{p^k,Q}(m) = p^{2k}\left(1 - \frac{1}{p^2}\right)$ for $k \geq 2$ follows from Corollary 3.2. □

Theorem 3.6. *Let m be an integer. Suppose $\vec{\mathbf{x}}_0 = (x_0, y_0, z_0)^T \in \mathbb{Z}^3$ is a solution to $Q(\vec{\mathbf{x}}) \equiv m \pmod{2^k}$ 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 $Q(\vec{\mathbf{x}}) \equiv m \pmod{2^{k+1}}$ 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 prove that there exists a solution to $Q(\vec{\mathbf{x}}) \equiv m \pmod{2^{k+1}}$ of the form $(x_0+2^{k-1}x_1, y_0+2^{k-1}y_1, z_0+2^{k-1}z_1)^T$. Because $Q(\vec{\mathbf{x}}_0) \equiv m \pmod{2^k}$, there exists $\ell \in \mathbb{Z}$ such that $ax_0^2 + by_0^2 + cz_0^2 = m + 2^k\ell$. For some $x_1, y_1, z_1 \in \mathbb{Z}/4\mathbb{Z}$, observe that

$$\begin{aligned}
&a(x_0 + 2^{k-1}x_1)^2 + b(y_0 + 2^{k-1}y_1)^2 + c(z_0 + 2^{k-1}z_1)^2 - m && (3.30)\\
&\quad = 2^k(\ell + ax_0x_1 + by_0y_1 + cz_0z_1) + 2^{2k-2}(ax_1^2 + by_1^2 + cz_1^2) && (3.31)\\
&\quad \equiv 2^k(\ell + ax_0x_1 + by_0y_1 + cz_0z_1) \pmod{2^{k+1}}, && (3.32)
\end{aligned}$$

since $k \geq 3$.

Let

$$x_1 = (ax_0)^{-1}(-\ell - by_0y_1 - cz_0z_1), \tag{3.33}$$

where $ax_0(ax_0)^{-1} \equiv 1 \pmod{p} \iff ax_0(ax_0)^{-1} = 1+2t$ for some $t \in \mathbb{Z}$. (Note that $(ax_0)^{-1}$ exists since $2 \nmid ax_0$.) Then

$$\begin{aligned}
&a(x_0 + 2^{k-1}x_1)^2 + b(y_0 + 2^{k-1}y_1)^2 + c(z_0 + 2^{k-1}z_1)^2 - m && (3.34)\\
&\quad \equiv 2^k(\ell + ax_0x_1 + by_0y_1 + cz_0z_1) \pmod{2^{k+1}} && (3.35)\\
&\quad \equiv 2^k(\ell + ax_0(ax_0)^{-1}(-\ell - by_0y_1 - cz_0z_1) + by_0y_1 + cz_0z_1) \pmod{2^{k+1}} && (3.36)\\
&\quad \equiv 2^k(\ell + (1+2t)(-\ell - by_0y_1 - cz_0z_1) + by_0y_1 + cz_0z_1) \pmod{2^{k+1}} && (3.37)\\
&\quad \equiv 2^{k+1}t(-\ell - by_0y_1 - cz_0z_1) \pmod{2^{k+1}} && (3.38)\\
&\quad \equiv 0 \pmod{2^{k+1}} && (3.39)\\
&\iff a(x_0 + 2^{k-1}x_1)^2 + b(y_0 + 2^{k-1}y_1)^2 + c(z_0 + 2^{k-1}z_1)^2 \equiv m \pmod{2^{k+1}}. && (3.40)
\end{aligned}$$

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

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 (3.32), we see that

$$2^k(\ell + ax_0x_1 + by_0y_1 + cz_0z_1) \equiv 0 \pmod{2^{k+1}} \tag{3.41}$$

$$\iff \ell + ax_0x_1 + by_0y_1 + cz_0z_1 \equiv 0 \pmod{2} \tag{3.42}$$

$$\iff ax_0x_1 \equiv -\ell - by_0y_1 - cz_0z_1 \pmod{2} \tag{3.43}$$

$$\iff x_1 \equiv (ax_0)^{-1}(-\ell - by_0y_1 - cz_0z_1) \pmod{2} \tag{3.44}$$

From (3.44), we see that $x_1 \in \mathbb{Z}/p\mathbb{Z}$ is uniquely determined $\pmod{2}$ by the choices of y_1 and z_1. However, $x_1 \in \mathbb{Z}/4\mathbb{Z}$, so 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 $Q(\vec{\mathbf{x}}) \equiv m \pmod{2^{k+1}}$ 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 $x_1, y_1, z_1 \in \mathbb{Z}/4\mathbb{Z}$. ☐

Corollary 3.7. *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 $Q(\vec{\mathbf{x}}) \equiv m \pmod{2^k}$, 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 $Q(\vec{\mathbf{x}}) \equiv m \pmod{2^{k+\ell}}$ 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 $Q(\vec{\mathbf{x}}) \equiv m \pmod{2^{k+\ell}}$ 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 $n = r_{2^k,Q}(m)$. Assume that there are exactly $2^{2\ell}n$ solutions in $(\mathbb{Z}/2^{k+\ell}\mathbb{Z})^3$ to $Q(\vec{\mathbf{x}}) \equiv m \pmod{2^{k+\ell}}$ 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 $Q(\vec{\mathbf{x}}) \equiv m \pmod{2^{k+\ell}}$. 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 3.6, for each solution $(x_j,y_j,z_j)^T$ in $\mathbb{Z}/2^{k+\ell}\mathbb{Z}$ to $Q(\vec{\mathbf{x}}) \equiv m \pmod{2^{k+\ell}}$, there exist 32 solutions to $Q(\vec{\mathbf{x}}) \equiv m \pmod{2^{k+\ell+1}}$ 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 $2 \nmid cz_j$, clearly

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

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

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

Then

$$\begin{aligned}
&x_{j_1} + 2^{k+\ell-1}x'_{j_1} \equiv x_{j_2} + 2^{k+\ell-1}x'_{j_2} \pmod{2^{k+\ell+1}} \\
&\iff (x_{j_1} - x_{j_2}) + 2^{k+\ell-1}(x'_{j_1} - x'_{j_2}) \equiv 0 \pmod{2^{k+\ell+1}} \\
&\iff (x_{j_1} - x_{j_2}) + 2^{k+\ell-1}(x'_{j_1} - x'_{j_2}) = 2^{k+\ell+1}t \quad \text{for some } t \in \mathbb{Z} \\
&\implies 2^{k+\ell-1} \mid (x_{j_1} - x_{j_2}) \iff x_{j_1} \equiv x_{j_2} \pmod{2^{k+\ell-1}}.
\end{aligned}$$

As shown 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 $Q(\vec{\mathbf{x}}) \equiv m \pmod{p^{k+\ell+1}}$ 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 $S_{k+\ell+1,j_1} = S_{k+\ell+1,j_2}$.

In short, 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 $Q(\vec{\mathbf{x}}) \equiv m \pmod{2^{k+1}}$ 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 $Q(\vec{\mathbf{x}}) \equiv m \pmod{2^{k+\ell+1}}$. By the principle of mathematical induction, the corollary follows. $\square$

4. Acknowledgments

I would like to acknowledge and to thank Matthew Young for his guidance, support, and advice throughout this project. This work was completed during the 2014 REU in Number Theory at Texas A&M University. I also thank the National Science Foundation for its generous support for this REU.

References

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

CM 2223, Rose-Hulman Institute of Technology, 5500 Wabash Ave., Terre Haute, IN 47803, U.S.A.

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