Local Densities of Diagonal Integral Ternary Quadratic Forms at Odd Primes

Edna Jones

Rutgers, The State University of New Jersey

Study Group in Number Theory Seminar
The Graduate Center, CUNY
February 28, 2020

Quadratic Forms $Q(\mathbf{v}) = ax^2 + by^2 + cz^2$

$$Q(\mathbf{v}) = ax^2 + by^2 + cz^2$$

$a, b, c \in \mathbb{Z}$
$\gcd(a, b, c) = 1$

$$\mathbf{v} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

Examples

- $Q(\mathbf{v}) = x^2 + 3y^2 + 5z^2$
- $Q(\mathbf{v}) = x^2 + 4y^2 + 4z^2$
- $Q(\mathbf{v}) = 3x^2 + 4y^2 + 5z^2$
- $Q(\mathbf{v}) = x^2 + 5y^2 + 7z^2$

Quadratic Forms $Q(\mathbf{v}) = ax^2 + by^2 + cz^2$

$$Q(\mathbf{v}) = ax^2 + by^2 + cz^2$$

$a, b, c \in \mathbb{Z}$
$\gcd(a, b, c) = 1$

$$\mathbf{v} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

Examples

- $Q(\mathbf{v}) = x^2 + 3y^2 + 5z^2$
- $Q(\mathbf{v}) = x^2 + 4y^2 + 4z^2$
- $Q(\mathbf{v}) = 3x^2 + 4y^2 + 5z^2$
- $Q(\mathbf{v}) = x^2 + 5y^2 + 7z^2$

Let m be an integer. We would like to know when

$$Q(\mathbf{v}) = m$$

has an integer solution.

Easier Problem: Look (mod n)

Definition (Local representation number)

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

Easier Problem: Look $\pmod{n}$

Definition (Local representation number)

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

Because of Chinese Remainder Theorem, only need to look at $r_{p^k}(m, Q)$, p prime.

Local (representation) density or p-adic density

Let p be a prime. Let $\mathbb{Z}_p$ denote the set of p-adic integers with the usual Haar measure.

Definition (Local (representation) density or p-adic density)

$$\alpha_p(m, Q) = \lim_{U \to \{m\}} \frac{\mathrm{Vol}_{\mathbb{Z}_p^3}(Q^{-1}(U))}{\mathrm{Vol}_{\mathbb{Z}_p}(U)},$$

where U is an open set in $\mathbb{Z}_p$ containing m, $\mathrm{Vol}_{\mathbb{Z}_p^3}(Q^{-1}(U))$ is the volume of $Q^{-1}(U)$ in $\mathbb{Z}_p^3$, and $\mathrm{Vol}_{\mathbb{Z}_p}(U)$ is the volume of U in $\mathbb{Z}_p$.

Local (representation) density or p-adic density

Let p be a prime. Let $\mathbb{Z}_p$ denote the set of p-adic integers with the usual Haar measure.

Definition (Local (representation) density or p-adic density)

$$\alpha_p(m, Q) = \lim_{U \to \{m\}} \frac{\mathrm{Vol}_{\mathbb{Z}_p^3}(Q^{-1}(U))}{\mathrm{Vol}_{\mathbb{Z}_p}(U)},$$

where U is an open set in $\mathbb{Z}_p$ containing m, $\mathrm{Vol}_{\mathbb{Z}_p^3}(Q^{-1}(U))$ is the volume of $Q^{-1}(U)$ in $\mathbb{Z}_p^3$, and $\mathrm{Vol}_{\mathbb{Z}_p}(U)$ is the volume of U in $\mathbb{Z}_p$.

It can be shown that

$$\alpha_p(m, Q) = \lim_{k \to \infty} \frac{r_{p^k}(m, Q)}{p^{2k}}.$$

Why do we care about local densities?

Definition (Representation number)

$$r(m, Q) = \#\left\{\mathbf{v} \in \mathbb{Z}^3 : Q(\mathbf{v}) = m\right\}$$

Why do we care about local densities?

Definition (Representation number)

$$r(m, Q) = \# \left\{ \mathbf{v} \in \mathbb{Z}^3 : Q(\mathbf{v}) = m \right\}$$

The $\alpha_p(m, Q)$'s give us local information.

If $m \neq 0$, Hensel's lemma shows that

$$\alpha_p(m, Q) = 0 \iff r_{p^k}(m, Q) = 0 \text{ for some } k.$$

This implies that $r(m, Q) = 0$ if $\alpha_p(m, Q) = 0$ for some prime p. (Converse does not hold.)

Theorem (Siegel, 1935)

Let m be an integer and Q be a positive definite quadratic form of rank 3. Let $\{Q_j\}$ be a complete set representatives for classes in the same genus as Q. Then

$$\frac{\sum_j \frac{r(m,Q_j)}{\#O(Q_j)}}{\sum_j \frac{1}{\#O(Q_j)}} = \alpha_{\mathbb{R}}(m,Q) \prod_{p \text{ prime}} \alpha_p(m,Q),$$

where $O(Q_j)$ is the orthogonal group of Q_j over $\mathbb{Z}$,

$\alpha_{\mathbb{R}}(m,Q) = \lim_{U \to \{m\}} \frac{\mathrm{Vol}_{\mathbb{R}^3}(Q^{-1}(U))}{\mathrm{Vol}_{\mathbb{R}}(U)}$*, U is an open set in $\mathbb{R}$ containing m, $\mathrm{Vol}_{\mathbb{R}^3}(Q^{-1}(U))$ is the volume of $Q^{-1}(U)$ in $\mathbb{R}^3$, and $\mathrm{Vol}_{\mathbb{R}}(U)$ is the volume of U in $\mathbb{R}$.*

Corollary (Specialized Version of Siegel's Mass Formula)

Let m be an integer and Q be a positive definite quadratic form of rank 3. If Q is in a genus containing only one class, then

$$r(m, Q) = \alpha_{\mathbb{R}}(m, Q) \prod_{p \text{ prime}} \alpha_p(m, Q).$$

Specialized Version of Siegel's Mass Formula

Corollary (Specialized Version of Siegel's Mass Formula)

Let m be an integer and Q be a positive definite quadratic form of rank 3. If Q is in a genus containing only one class, then

$$r(m, Q) = \alpha_{\mathbb{R}}(m, Q) \prod_{p \text{ prime}} \alpha_p(m, Q).$$

- Jones and Pall (1939) proved that there are 82 primitive quadratic forms of the form $ax^2 + by^2 + cz^2$ with $0 < a \leq b \leq c$ such that each is in a genus containing only one class.

Specialized Version of Siegel's Mass Formula

Corollary (Specialized Version of Siegel's Mass Formula)

Let m be an integer and Q be a positive definite quadratic form of rank 3. If Q is in a genus containing only one class, then

$$r(m, Q) = \alpha_{\mathbb{R}}(m, Q) \prod_{p \text{ prime}} \alpha_p(m, Q).$$

- Jones and Pall (1939) proved that there are 82 primitive quadratic forms of the form $ax^2 + by^2 + cz^2$ with $0 < a \leq b \leq c$ such that each is in a genus containing only one class.
- Lomadze (1971) computed the representation numbers for these 82 quadratic forms.

Past Results on Local Densities

Complicated formulas (hard to tell when $\alpha_p(m, Q)$ is equal to zero):

- Yang (1998)
- Hanke (2004)

Past Results on Local Densities

Complicated formulas (hard to tell when $\alpha_p(m, Q)$ is equal to zero):

- Yang (1998)
- Hanke (2004)

Not in full generality:

- Siegel (1935): If $p \nmid 2abcm$, then

$$\alpha_p(m, Q) = 1 + \frac{1}{p}\left(\frac{-abcm}{p}\right),$$

  where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol.
- Berkovich and Jagy (2012)

Theorem (Berkovich and Jagy, 2012)

Let p be an odd prime and u be any integer with $\left(\frac{-u}{p}\right) = -1$. Let $Q(\mathbf{v}) = ux^2 + py^2 + upz^2$. Suppose m is a nonzero integer and $m = m_0 p^{m_1}$, where $\gcd(m_0, p) = 1$. Then

$$\alpha_p(m, Q) = \begin{cases} p^{-m_1/2}\left(1 - \left(\frac{-m_0}{p}\right)\right), & \text{if } m_1 \text{ is even,} \\ p^{(-m_1+1)/2}\left(1 + \frac{1}{p}\right), & \text{if } m_1 \text{ is odd.} \end{cases}$$

Formulas for Local Densities at Odd Primes

Theorem (J., 2020)

Let p be an odd prime. Suppose $p \nmid a$, $b = b_0 p^{b_1}$, and $c = c_0 p^{c_1}$, where $b_1 \leq c_1$, $\gcd(b_0, p) = 1$, and $\gcd(c_0, p) = 1$.
Suppose m is a nonzero integer and $m = m_0 p^{m_1}$, where $\gcd(m_0, p) = 1$.
$\alpha_p(m, Q)$ is easily computable using rational functions and Legendre symbols. Depends on a, b_0, b_1, c_0, c_1, m_0, m_1, and p.

Formulas for Local Densities at Odd Primes

Theorem (J., 2020)

Let p be an odd prime. Suppose $p \nmid a$, $b = b_0 p^{b_1}$, and $c = c_0 p^{c_1}$, where $b_1 \leq c_1$, $\gcd(b_0, p) = 1$, and $\gcd(c_0, p) = 1$.
Suppose m is a nonzero integer and $m = m_0 p^{m_1}$, where $\gcd(m_0, p) = 1$.
$\alpha_p(m, Q)$ is easily computable using rational functions and Legendre symbols. Depends on a, b_0, b_1, c_0, c_1, m_0, m_1, and p.

Multiple cases:

- $m_1 < b_1$ *and depends on parity of* m_1
- $b_1 \leq m_1 < c_1$ *and depends on parity of* b_1
- $m_1 \geq c_1$ *and depends on parities of* b_1, c_1, *and* m_1

Formulas for Local Densities at Odd Primes

Theorem (J., 2020)

Let p be an odd prime. Suppose $p \nmid a$, $b = b_0 p^{b_1}$, and $c = c_0 p^{c_1}$, where $b_1 \leq c_1$, $\gcd(b_0, p) = 1$, and $\gcd(c_0, p) = 1$.
Suppose m is a nonzero integer and $m = m_0 p^{m_1}$, where $\gcd(m_0, p) = 1$.
$\alpha_p(m, Q)$ is easily computable using rational functions and Legendre symbols. Depends on a, b_0, b_1, c_0, c_1, m_0, m_1, and p.

Multiple cases:

- $m_1 < b_1$ *and depends on parity of* m_1
- $b_1 \leq m_1 < c_1$ *and depends on parity of* b_1
- $m_1 \geq c_1$ *and depends on parities of* b_1, c_1, *and* m_1

Also $\alpha_p(0, Q)$ is computable. Multiple cases dependent on parities b_1 and c_1.

Main Theorem when $m_1 < c_1$

Theorem (J., 2020)

If $m_1 < b_1$, then

$$\alpha_p(m,Q) = \begin{cases} p^{m_1/2}\left(1 + \left(\frac{am_0}{p}\right)\right), & \text{if } m_1 \text{ is even,} \\ 0, & \text{if } m_1 \text{ is odd.} \end{cases}$$

If $b_1 \leq m_1 < c_1$, then $\alpha_p(m,Q) =$

$$\begin{cases} p^{b_1/2}\left(1 - \frac{1}{p}\left(\frac{-ab_0}{p}\right)^{m_1+1} + \left(1 - \frac{1}{p}\right)\left(\frac{m_1 - b_1}{2} \right.\right. \\ \qquad \left.\left. + \frac{(-1)^{m_1} - 1}{4} + \left(\frac{-ab_0}{p}\right)\left(\frac{m_1 - b_1}{2} + \frac{1 - (-1)^{m_1}}{4}\right)\right)\right), \\ \qquad\qquad \text{if } b_1 \text{ is even,} \\ p^{(b_1-1)/2}\left(1 + \left(\frac{a}{p}\right)^{m_1+1}\left(\frac{b_0}{p}\right)^{m_1}\left(\frac{m_0}{p}\right)\right), \text{if } b_1 \text{ is odd.} \end{cases}$$

Proof Sketch

1. Use exponential sums and quadratic Gauss sums to compute $r_{p^k}(m, Q)$.
2. Divide by p^{2k} and take a limit.

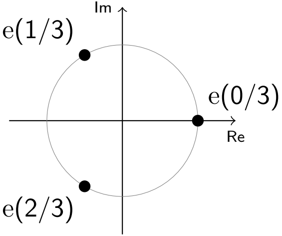
Abbreviate $\mathrm{e}(w) = e^{2\pi i w}$.

Definition

The *quadratic Gauss sum* $g(n;q)$ *over* $\mathbb{Z}/q\mathbb{Z}$ is defined by

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

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



A Sum Containing $\mathrm{e}(w)$

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

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

A Sum Containing $\mathrm{e}(w)$

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

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

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

Counting Solutions (mod p^k)

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

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

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

Counting Solutions (mod p^k)

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

Counting Solutions (mod p^k)

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

Counting Solutions (mod p^k)

$$
\begin{aligned}
&r_{p^k}(m, Q)\\
&= \frac{1}{p^k} \sum_{t=0}^{p^k-1} \mathrm{e}\left(\frac{-mt}{p^k}\right) g\left(at; p^k\right) g\left(bt; p^k\right) g\left(ct; p^k\right)\\
&= \frac{1}{p^k} \left(g\left(0; p^k\right)\right)^3 + \frac{1}{p^k} \sum_{t=1}^{p^k-1} \mathrm{e}\left(\frac{-mt}{p^k}\right) g\left(at; p^k\right) g\left(bt; p^k\right) g\left(ct; p^k\right).
\end{aligned}
$$

Counting Solutions (mod p^k)

$$
\begin{aligned}
&r_{p^k}(m, Q) \\
&= \frac{1}{p^k} \sum_{t=0}^{p^k-1} \mathrm{e}\left(\frac{-mt}{p^k}\right) g\left(at; p^k\right) g\left(bt; p^k\right) g\left(ct; p^k\right) \\
&= \frac{1}{p^k} \left(g\left(0; p^k\right)\right)^3 + \frac{1}{p^k} \sum_{t=1}^{p^k-1} \mathrm{e}\left(\frac{-mt}{p^k}\right) g\left(at; p^k\right) g\left(bt; p^k\right) g\left(ct; p^k\right).
\end{aligned}
$$

Since $g\left(0; p^k\right) = p^k$,

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

Formulas for Quadratic Gauss Sums

Lemma

Suppose k is a positive integer, p is an odd prime, and $n \neq 0$. Let $n = n_0 p^\ell$ so that $\gcd(n_0, p) = 1$. Then

$$g\left(n; p^k\right) = \begin{cases} p^k, & \text{if } \ell \geq k, \\ p^{(k+\ell)/2} \left(\frac{n_0}{p^{k-\ell}}\right) \varepsilon_{p^{k-\ell}}, & \text{if } \ell < k, \end{cases}$$

where

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

and $\left(\frac{\cdot}{p^{k-\ell}}\right)$ is the Jacobi symbol.

Formulas for Quadratic Gauss Sums

Lemma

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

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

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

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

Proof for the previous lemma.

Let t be an integer. The number of solutions modulo p of the congruence

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

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

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

Proof for the previous lemma.

Let t be an integer. The number of solutions modulo p of the congruence

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

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

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

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

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

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

Counting Solutions (mod p^k)

$$
\begin{aligned}
&r_{p^k}(m, Q) \\
&= p^{2k} + \frac{1}{p^k} \sum_{t=1}^{p^k-1} \mathrm{e}\left(\frac{-mt}{p^k}\right) g\left(at; p^k\right) g\left(bt; p^k\right) g\left(ct; p^k\right) \\
&= p^{2k} + \frac{1}{p^k} \sum_{t=1}^{p^k-1} \mathrm{e}\left(\frac{-m_0 p^{m_1} t}{p^k}\right) g\left(at; p^k\right) g\left(b_0 p^{b_1} t; p^k\right) g\left(c_0 p^{c_1} t; p^k\right).
\end{aligned}
$$

$$
\begin{aligned}
&r_{p^k}(m, Q) \\
&= p^{2k} + \frac{1}{p^k} \sum_{t=1}^{p^k-1} \mathrm{e}\left(\frac{-mt}{p^k}\right) g\left(at; p^k\right) g\left(bt; p^k\right) g\left(ct; p^k\right) \\
&= p^{2k} + \frac{1}{p^k} \sum_{t=1}^{p^k-1} \mathrm{e}\left(\frac{-m_0 p^{m_1} t}{p^k}\right) g\left(at; p^k\right) g\left(b_0 p^{b_1} t; p^k\right) g\left(c_0 p^{c_1} t; p^k\right).
\end{aligned}
$$

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

$$
\begin{aligned}
r_{p^k}(m, Q) = p^{2k} + \frac{1}{p^k} \sum_{\tau=0}^{k-1} \sum_{t_0 \in (\mathbb{Z}/p^{k-\tau}\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0 t_0 p^{m_1+\tau}}{p^k}\right) g\left(a t_0 p^\tau; p^k\right) \\
\cdot g\left(b_1 t_0 p^{b_1+\tau}; p^k\right) g\left(c_0 t_0 p^{c_1+\tau}; p^k\right).
\end{aligned}
$$

Counting Solutions (mod p^k)

Let

$$s_{k,\tau} = \sum_{t_0 \in (\mathbb{Z}/p^{k-\tau}\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0 t_0 p^{m_1+\tau}}{p^k}\right) g\left(a t_0 p^{\tau}; p^k\right) \cdot g\left(b_1 t_0 p^{b_1+\tau}; p^k\right) g\left(c_0 t_0 p^{c_1+\tau}; p^k\right)$$

so that

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

Counting Solutions (mod p^k)

Let

$$s_{k,\tau} = \sum_{t_0 \in (\mathbb{Z}/p^{k-\tau}\mathbb{Z})^*} \mathrm{e}\left(\frac{-m_0 t_0 p^{m_1+\tau}}{p^k}\right) g\left(a t_0 p^{\tau}; p^k\right) \cdot g\left(b_1 t_0 p^{b_1+\tau}; p^k\right) g\left(c_0 t_0 p^{c_1+\tau}; p^k\right)$$

so that

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

Compute $s_{k,\tau}$ under different conditions depending on b_1, c_1, m_1, k, and τ. Then compute $r_{p^k}(m, Q)$ and $\alpha_p(m, Q)$.

Computing $s_{k,\tau}$ when $0 \leq \tau \leq k - m_1 - 2$

Lemma

For $0 \leq \tau \leq k - m_1 - 2$, $s_{k,\tau} = 0$.

Lemma

For $0 \leq \tau \leq k - m_1 - 2$, $s_{k,\tau} = 0$.

Proof.

Suppose that $0 \leq \tau \leq k - m_1 - 2$. Then let $t_0 = t_1 + t_2 p$, where $1 \leq t_1 \leq p - 1$ and $0 \leq t_2 \leq p^{k-\tau-1} - 1$, so

$$s_{k,\tau} = \sum_{t_1=1}^{p-1} \sum_{t_2=0}^{p^{k-\tau-1}-1} \mathrm{e}\left(\frac{-m_0(t_1 + t_2 p)p^{m_1+\tau}}{p^k}\right) g\left(a(t_1 + t_2 p)p^{\tau}; p^k\right) \cdot g\left(b_1(t_1 + t_2 p)p^{b_1+\tau}; p^k\right) g\left(c_0(t_1 + t_2 p)p^{c_1+\tau}; p^k\right)$$

$$= \sum_{t_1=1}^{p-1} \sum_{t_2=0}^{p^{k-\tau-1}-1} \mathrm{e}\left(\frac{-m_0 t_1}{p^{k-m_1-\tau}}\right) \mathrm{e}\left(\frac{-m_0 t_2}{p^{k-m_1-1-\tau}}\right) g\left(a t_1 p^{\tau}; p^k\right) \cdot g\left(b_1 t_1 p^{b_1+\tau}; p^k\right) g\left(c_0 t_1 p^{c_1+\tau}; p^k\right)$$

Computing $s_{k,\tau}$ when $0 \leq \tau \leq k - m_1 - 2$

Lemma

For $0 \leq \tau \leq k - m_1 - 2$, $s_{k,\tau} = 0$.

Proof (continued).

$$s_{k,\tau} = \sum_{t_1=1}^{p-1} \mathrm{e}\left(\frac{-m_0 t_1}{p^{k-m_1-\tau}}\right) g\left(a t_1 p^{\tau}; p^k\right) g\left(b_1 t_1 p^{b_1+\tau}; p^k\right)$$

$$\cdot\, g\left(c_0 t_1 p^{c_1+\tau}; p^k\right) \sum_{t_2=0}^{p^{k-\tau-1}-1} \mathrm{e}\left(\frac{-m_0 t_2}{p^{k-m_1-1-\tau}}\right).$$

Computing $s_{k,\tau}$ when $0 \leq \tau \leq k - m_1 - 2$

Lemma

For $0 \leq \tau \leq k - m_1 - 2$, $s_{k,\tau} = 0$.

Proof (continued).

$$s_{k,\tau} = \sum_{t_1=1}^{p-1} \mathrm{e}\left(\frac{-m_0 t_1}{p^{k-m_1-\tau}}\right) g\left(a t_1 p^{\tau}; p^k\right) g\left(b_1 t_1 p^{b_1+\tau}; p^k\right) \cdot g\left(c_0 t_1 p^{c_1+\tau}; p^k\right) \sum_{t_2=0}^{p^{k-\tau-1}-1} \mathrm{e}\left(\frac{-m_0 t_2}{p^{k-m_1-1-\tau}}\right).$$

Now

$$\sum_{t_2=0}^{p^{k-\tau-1}-1} \mathrm{e}\left(\frac{-m_0 t_2}{p^{k-m_1-1-\tau}}\right) = p^{m_1} \sum_{t_2=0}^{p^{k-m_1-\tau-1}-1} \mathrm{e}\left(\frac{-m_0 t_2}{p^{k-m_1-1-\tau}}\right) = p^{m_1} \cdot 0 = 0.$$

□

Computing $s_{k,\tau}$ when $k - \min(m_1, b_1) \le \tau \le k - 1$

Lemma

For $k - \min(m_1, b_1) \le \tau \le k - 1$*,*

$$s_{k,\tau} = \begin{cases} p^{3k+(k-\tau)/2}\left(1 - \dfrac{1}{p}\right), & \text{if } k - \tau \text{ is even,} \\ 0, & \text{if } k - \tau \text{ is odd.} \end{cases}$$

Computing $s_{k,\tau}$ when $k - \min(m_1, b_1) \leq \tau \leq k - 1$

Lemma

For $k - \min(m_1, b_1) \leq \tau \leq k - 1$,

$$s_{k,\tau} = \begin{cases} p^{3k+(k-\tau)/2}\left(1 - \frac{1}{p}\right), & \text{if } k - \tau \text{ is even,} \\ 0, & \text{if } k - \tau \text{ is odd.} \end{cases}$$

Proof.

Suppose that $k - \min(m_1, b_1) \leq \tau \leq k - 1$. Then

$$s_{k,\tau} = \sum_{t_0 \in (\mathbb{Z}/p^{k-\tau}\mathbb{Z})^*} p^{(k+\tau)/2} \left(\frac{at_0}{p^{k-\tau}}\right) \varepsilon_{p^{k-\tau}} p^{2k}$$

$$= \varepsilon_{p^{k-\tau}} p^{5k/2+\tau/2} \left(\frac{a}{p}\right)^{k-\tau} \sum_{t_0 \in (\mathbb{Z}/p^{k-\tau}\mathbb{Z})^*} \left(\frac{t_0}{p}\right)^{k-\tau}.$$

Computing $s_{k,\tau}$ when $k - \min(m_1, b_1) \leq \tau \leq k-1$

Lemma

For $k - \min(m_1, b_1) \leq \tau \leq k-1$,

$$s_{k,\tau} = \begin{cases} p^{3k+(k-\tau)/2}\left(1 - \frac{1}{p}\right), & \text{if } k-\tau \text{ is even,} \\ 0, & \text{if } k-\tau \text{ is odd.} \end{cases}$$

Proof (continued).

$$s_{k,\tau} = \varepsilon_{p^{k-\tau}} p^{5k/2+\tau/2} \left(\frac{a}{p}\right)^{k-\tau} \sum_{t_0 \in (\mathbb{Z}/p^{k-\tau}\mathbb{Z})^*} \left(\frac{t_0}{p}\right)^{k-\tau}$$

$$= \begin{cases} p^{5k/2+\tau/2} p^{k-\tau}\left(1 - \frac{1}{p}\right), & \text{if } k-\tau \text{ is even,} \\ 0, & \text{if } k-\tau \text{ is odd.} \end{cases}$$

□

Computing $\sum_{\tau=k-\min(m_1,b_1)}^{k-1} s_{k,\tau}$

Lemma

Let $n_1 = \min(m_1, b_1)$. *Then*

$$\sum_{\tau=k-n_1}^{k-1} s_{k,\tau} = \sum_{\substack{\tau=k-n_1 \\ k-\tau \text{ is even}}}^{k-1} p^{3k+(k-\tau)/2}\left(1-\frac{1}{p}\right) = p^{3k}(p^{\lfloor n_1/2 \rfloor} - 1),$$

where $\lfloor x \rfloor$ *is the greatest integer less than or equal to* x.

Lemma

Let $n_1 = \min(m_1, b_1)$. *Then*

$$\sum_{\tau=k-n_1}^{k-1} s_{k,\tau} = \sum_{\substack{\tau=k-n_1 \\ k-\tau \text{ is even}}}^{k-1} p^{3k+(k-\tau)/2}\left(1-\frac{1}{p}\right) = p^{3k}(p^{\lfloor n_1/2 \rfloor} - 1),$$

where $\lfloor x \rfloor$ *is the greatest integer less than or equal to* x.

Proof sketch:

1. Let $\tau_1 = \frac{k-\tau}{2}$.
2. Apply formulas for geometric sums.

Thank you for listening!

Formulas for Local Densities at Odd Primes

Theorem (J., 2020)

Let Q be the integral quadratic form $ax^2 + by^2 + cz^2$, where a, b, and c are integers. Let p be an odd prime. Suppose $p \nmid a$, $b = b_0 p^{b_1}$, and $c = c_0 p^{c_1}$, where $b_1 \leq c_1$, $\gcd(b_0, p) = 1$, and $\gcd(c_0, p) = 1$.
Suppose m is a nonzero integer and $m = m_0 p^{m_1}$, where $\gcd(m_0, p) = 1$.
If $m_1 < b_1$, then

$$\alpha_p(m, Q) = \begin{cases} p^{m_1/2}\left(1 + \left(\frac{am_0}{p}\right)\right), & \text{if } m_1 \text{ is even}, \\ 0, & \text{if } m_1 \text{ is odd}. \end{cases}$$

Formulas for Local Densities at Odd Primes

Theorem (J., 2020, continued)

If $b_1 \leq m_1 < c_1$, then

$$\alpha_p(m, Q) = \begin{cases} p^{b_1/2}\left(1 - \frac{1}{p}\left(\frac{-ab_0}{p}\right)^{m_1+1} \right. \\ \qquad + \left(1-\frac{1}{p}\right)\left(\frac{m_1-b_1}{2} + \frac{(-1)^{m_1}-1}{4}\right. \\ \qquad \left.\left. + \left(\frac{-ab_0}{p}\right)\left(\frac{m_1-b_1}{2} + \frac{1-(-1)^{m_1}}{4}\right)\right)\right), \\ \qquad \text{if } b_1 \text{ is even,} \\ p^{(b_1-1)/2}\left(1 + \left(\frac{a}{p}\right)^{m_1+1}\left(\frac{b_0}{p}\right)^{m_1}\left(\frac{m_0}{p}\right)\right), \\ \qquad \text{if } b_1 \text{ is odd.} \end{cases}$$

Formulas for Local Densities at Odd Primes

Theorem (J., 2020, continued)

If $m_1 \geq c_1$ and b_1 and c_1 are even, then

$$\alpha_p(m, Q) = \begin{cases} p^{b_1/2}\left(1 + \frac{1}{p} + p^{-m_1/2 + c_1/2 - 1}\left(\left(\left(\frac{-ab_0c_0m_0}{p}\right) - 1\right) \right.\right. \\ \qquad \left.\left. + \left(1 - \frac{1}{p}\right)\left(\frac{c_1 - b_1}{2} + \left(\frac{-ab_0}{p}\right)\frac{c_1 - b_1}{2}\right)\right)\right), \\ \qquad \text{if } m_1 \text{ is even}, \\ p^{b_1/2}\left(\left(1 + \frac{1}{p}\right)\left(1 - p^{-(m_1+1)/2 + c_1/2}\right) \right. \\ \qquad \left. + \left(1 - \frac{1}{p}\right)\left(\frac{c_1 - b_1}{2} + \left(\frac{-ab_0}{p}\right)\frac{c_1 - b_1}{2}\right)\right), \\ \qquad \text{if } m_1 \text{ is odd}. \end{cases}$$

Formulas for Local Densities at Odd Primes

Theorem (J., 2020, continued)

If $m_1 \geq c_1$, b_1 is even, and c_1 is odd, then

$$\alpha_p(m, Q) =$$

$$\begin{cases} p^{b_1/2}\left(1 - p^{-m_1/2+(c_1-1)/2}\left(\frac{-ab_0}{p}\right)\left(1+\frac{1}{p}\right) + \frac{1}{p}\left(\frac{-ab_0}{p}\right) \right. \\ \qquad \left. + \left(1-\frac{1}{p}\right)\left(\frac{c_1-b_1-1}{2} + \left(\frac{-ab_0}{p}\right)\frac{c_1-b_1+1}{2}\right)\right), \\ \qquad\qquad \text{if } m_1 \text{ is even,} \\ p^{b_1/2}\left(1 + p^{-(m_1+1)/2+(c_1-1)/2}\left(\left(\frac{c_0 m_0}{p}\right) - \left(\frac{-ab_0}{p}\right)\right) \right. \\ \qquad + \frac{1}{p}\left(\frac{-ab_0}{p}\right) \\ \qquad \left. + \left(1-\frac{1}{p}\right)\left(\frac{c_1-b_1-1}{2} + \left(\frac{-ab_0}{p}\right)\frac{c_1-b_1+1}{2}\right)\right), \\ \qquad\qquad \text{if } m_1 \text{ is odd.} \end{cases}$$

Formulas for Local Densities at Odd Primes

Theorem (J., 2020, continued)

If $m_1 \geq c_1$, b_1 is odd, and c_1 is even, then

$$\alpha_p(m, Q) = \begin{cases} p^{(b_1-1)/2} \left(1 + \left(\frac{-ac_0}{p}\right) \right. \\ \qquad \left. -p^{-m_1/2+c_1/2} \left(1 + \frac{1}{p}\right) \left(\frac{-ac_0}{p}\right)\right), \\ \qquad \text{if } m_1 \text{ is even,} \\ p^{(b_1-1)/2} \left(1 + \left(\frac{-ac_0}{p}\right) \right. \\ \qquad \left. +p^{-(m_1+1)/2+c_1/2} \left(\left(\frac{b_0 m_0}{p}\right) - \left(\frac{-ac_0}{p}\right)\right)\right), \\ \qquad \text{if } m_1 \text{ is odd.} \end{cases}$$

Theorem (J., 2020, continued)

If $m_1 \geq c_1$ and b_1 and c_1 are odd, then

$$\alpha_p(m, Q) = \begin{cases} p^{(b_1-1)/2}\left(1 + \left(\frac{-b_0 c_0}{p}\right)\right. \\ \qquad \left.+ p^{-m_1/2+(c_1-1)/2}\left(\left(\frac{a m_0}{p}\right) - \left(\frac{-b_0 c_0}{p}\right)\right)\right), \\ \qquad \text{if } m_1 \text{ is even,} \\ p^{(b_1-1)/2}\left(1 + \left(\frac{-b_0 c_0}{p}\right)\right. \\ \qquad \left.- p^{(-m_1+c_1)/2}\left(1 + \frac{1}{p}\right)\left(\frac{-b_0 c_0}{p}\right)\right), \\ \qquad \text{if } m_1 \text{ is odd.} \end{cases}$$

Formulas for Local Densities at Odd Primes

Theorem (J., 2020, continued)

Furthermore,

$$\alpha_p(0, Q) =$$

$$\begin{cases} p^{b_1/2}\left(1 + \frac{1}{p} + \left(1 - \frac{1}{p}\right)\left(\frac{c_1 - b_1}{2} + \left(\frac{-ab_0}{p}\right)\frac{c_1 - b_1}{2}\right)\right), & \text{if } b_1 \text{ and } c_1 \text{ are even,} \\ p^{b_1/2}\left(1 + \frac{1}{p}\left(\frac{-ab_0}{p}\right) + \left(1 - \frac{1}{p}\right)\left(\frac{c_1 - b_1 - 1}{2} + \left(\frac{-ab_0}{p}\right)\frac{c_1 - b_1 + 1}{2}\right)\right), & \text{if } b_1 \text{ is even and } c_1 \text{ is odd,} \\ p^{(b_1-1)/2}\left(1 + \left(\frac{-ac_0}{p}\right)\right), & \text{if } b_1 \text{ is odd and } c_1 \text{ is even,} \\ p^{(b_1-1)/2}\left(1 + \left(\frac{-b_0 c_0}{p}\right)\right), & \text{if } b_1 \text{ and } c_1 \text{ are odd.} \end{cases}$$