Representation by Ternary Quadratic Forms

Edna Jones

Rose-Hulman Institute of Technology
Texas A&M Math REU

July 23, 2014

The Quadratic Forms of Interest

$Q(\vec{\mathbf{x}}) = ax^2 + by^2 + cz^2$, where

- a, b, c are positive integers
- $\gcd(a, b, c) = 1$
- $\vec{\mathbf{x}} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$

The Quadratic Forms of Interest

$Q(\vec{\mathbf{x}}) = ax^2 + by^2 + cz^2$, where

- a, b, c are positive integers
- $\gcd(a, b, c) = 1$
- $\vec{\mathbf{x}} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$

Examples:

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

Globally Represented

Definition

An integer m is *(globally) represented by* Q if there exists $\vec{\mathbf{x}} \in \mathbb{Z}^3$ such that $Q(\vec{\mathbf{x}}) = m$.

Globally Represented

Definition

An integer m is *(globally) represented by Q* if there exists $\vec{\mathbf{x}} \in \mathbb{Z}^3$ such that $Q(\vec{\mathbf{x}}) = m$.

Example

1 and 9 are globally represented by $Q(\vec{\mathbf{x}}) = x^2 + 5y^2 + 7z^2$, because

- $1 = 1^2 + 5 \cdot 0^2 + 7 \cdot 0^2$
- $9 = 2^2 + 5 \cdot 1^2 + 7 \cdot 0^2$

Locally Represented

Definition

Let p be a positive prime integer. 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

$$Q(\vec{\mathbf{x}}) \equiv m \pmod{p^k}.$$

Locally Represented

Definition

Let p be a positive prime integer. 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

$$Q(\vec{\mathbf{x}}) \equiv m \pmod{p^k}.$$

Definition

An integer m is *locally represented (everywhere) by Q* if m is locally represented at p for every prime p and there exists $\vec{\mathbf{x}} \in \mathbb{R}^3$ such that $Q(\vec{\mathbf{x}}) = m$.

Locally Represented Example

Example

1 and 3 are locally represented everywhere by
$Q(\vec{\mathbf{x}}) = x^2 + 5y^2 + 7z^2$.

Locally Represented Example

Example

1 and 3 are locally represented everywhere by $Q(\vec{\mathbf{x}}) = x^2 + 5y^2 + 7z^2$.

- $1^2 + 5 \cdot 0^2 + 7 \cdot 0^2 \equiv 1 \pmod{p^k}$ for any prime p and integer $k \geq 0$

Locally Represented Example

Example

1 and 3 are locally represented everywhere by $Q(\vec{\mathbf{x}}) = x^2 + 5y^2 + 7z^2$.

- $1^2 + 5 \cdot 0^2 + 7 \cdot 0^2 \equiv 1 \pmod{p^k}$ for any prime p and integer $k \geq 0$
- More difficult to see why 3 locally represented everywhere by Q, because 3 is not globally represented by Q

Difference between Globally and Locally Represented

- m is globally represented by Q
  $\implies$ m is locally represented everywhere by Q

Difference between Globally and Locally Represented

- m is globally represented by Q
  $\Longrightarrow$ m is locally represented everywhere by Q
- m is locally represented everywhere by Q
  $\not\Longrightarrow$ m is globally represented by Q

Difference between Globally and Locally Represented

- m is globally represented by Q
  $\implies$ m is locally represented everywhere by Q
- m is locally represented everywhere by Q
  $\not\Longrightarrow$ m is globally represented by Q
- However, for m square-free and sufficiently large, m is locally represented everywhere by Q
  $\implies$ m is globally represented by Q

Difference between Globally and Locally Represented

- m is globally represented by Q
  $\Longrightarrow$ m is locally represented everywhere by Q
- m is locally represented everywhere by Q
  $\not\Longrightarrow$ m is globally represented by Q
- However, for m square-free and sufficiently large, m is locally represented everywhere by Q
  $\Longrightarrow$ m is globally represented by Q
- How large is sufficiently large?

Questions that Arose

- How do you determine that m is locally represented everywhere by Q?

Questions that Arose

- How do you determine that m is locally represented everywhere by Q?
- How do you determine that m is locally represented by Q at a prime p?

Counting Solutions (mod p^k)

Let p be a positive prime integer and k a non-negative integer.

Definition

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

Counting Solutions (mod p^k)

Let p be a positive prime integer and k a non-negative integer.

Definition

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

m is locally represented by Q at a prime p if and only if $r_{p^k,Q}(m) > 0$ for every nonnegative integer k.

An Abbreviation and a Definition

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

An Abbreviation and a Definition

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

Definition

The *quadratic Gauss sum* $G\left(\frac{n}{q}\right)$ *over* $\mathbb{Z}/q\mathbb{Z}$ is defined by

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

An Abbreviation and a Definition

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

Definition

The *quadratic Gauss sum* $G\left(\frac{n}{q}\right)$ *over* $\mathbb{Z}/q\mathbb{Z}$ is defined by

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

I have explicit formulas for quadratic Gauss sums.

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

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

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

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

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

Counting Solutions (mod p^k)

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

Counting Solutions (mod p^k)

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

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

Counting Solutions (mod p^k)

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

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

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

Counting Solutions (mod p^k)

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

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

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

A Formula for $r_{p^k,Q}(m)$

Let $Q(\vec{\mathbf{x}}) = ax^2 + by^2 + cz^2$.
Let p be an odd prime such that $p \nmid abc$.
Let m be square-free.

A Formula for $r_{p^k,Q}(m)$

Let $Q(\vec{\mathbf{x}}) = ax^2 + by^2 + cz^2$.
Let p be an odd prime such that $p \nmid abc$.
Let m be square-free.

$$r_{p^k,Q}(m) = \begin{cases} 1, & \text{if } k = 0, \\ p^{2k}\left(1 + \dfrac{1}{p}\left(\dfrac{-abcm}{p}\right)\right), & \text{if } p \nmid m \text{ or } k = 1, \\ p^{2k}\left(1 - \dfrac{1}{p^2}\right), & \text{if } p \mid m \text{ and } k > 1, \end{cases}$$

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

A Formula for $r_{p^k,Q}(m)$

Let $Q(\vec{\mathbf{x}}) = ax^2 + by^2 + cz^2$.
Let p be an odd prime such that $p \nmid abc$.
Let m be square-free.

$$r_{p^k,Q}(m) = \begin{cases} 1, & \text{if } k = 0, \\ p^{2k}\left(1 + \frac{1}{p}\left(\frac{-abcm}{p}\right)\right), & \text{if } p \nmid m \text{ or } k = 1, \\ p^{2k}\left(1 - \frac{1}{p^2}\right), & \text{if } p \mid m \text{ and } k > 1, \end{cases}$$

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

Under the above conditions, $r_{p^k,Q}(m) > 0$ for every $k \geq 0$.

Back to an Example

m square-free, p odd, and $p \nmid abc$

$$\implies m \text{ is locally represented by } Q \text{ at the prime } p$$

Back to an Example

m square-free, p odd, and $p \nmid abc$

$\implies$ m is locally represented by Q at the prime p

Example

- $Q(\vec{\mathbf{x}}) = x^2 + 5y^2 + 7z^2$ and $m = 3$

Back to an Example

m square-free, p odd, and $p \nmid abc$
$\implies$ m is locally represented by Q at the prime p

Example

- $Q(\vec{\mathbf{x}}) = x^2 + 5y^2 + 7z^2$ and $m = 3$
- 3 is square-free

Back to an Example

m square-free, p odd, and $p \nmid abc$
$\implies$ m is locally represented by Q at the prime p

Example

- $Q(\vec{\mathbf{x}}) = x^2 + 5y^2 + 7z^2$ and $m = 3$
- 3 is square-free
- 5 and 7 are the only odd primes that divide $1 \cdot 5 \cdot 7$

Back to an Example

m square-free, p odd, and $p \nmid abc$
$\implies$ m is locally represented by Q at the prime p

Example

- $Q(\vec{\mathbf{x}}) = x^2 + 5y^2 + 7z^2$ and $m = 3$
- 3 is square-free
- 5 and 7 are the only odd primes that divide $1 \cdot 5 \cdot 7$
- Now only need to check if 3 is locally represented at the primes 2, 5, and 7

Another Formula for $r_{p^k,Q}(m)$

Let $Q(\vec{\mathbf{x}}) = ax^2 + by^2 + cz^2$.
Let p be an odd prime such that p divides exactly one of a, b, c.

Another Formula for $r_{p^k,Q}(m)$

Let $Q(\vec{\mathbf{x}}) = ax^2 + by^2 + cz^2$.
Let p be an odd prime such that p divides exactly one of a, b, c.
Without loss of generality, say $p \mid c$ but $p \nmid ab$.

Another Formula for $r_{p^k,Q}(m)$

Let $Q(\vec{\mathbf{x}}) = ax^2 + by^2 + cz^2$.
Let p be an odd prime such that p divides exactly one of a, b, c.
Without loss of generality, say $p \mid c$ but $p \nmid ab$.
If $p \nmid m$,

$$r_{p^k,Q}(m) = \begin{cases} 1, & k = 0, \\ p^{2k}\left(1 - \frac{1}{p}\left(\frac{-ab}{p}\right)\right), & k \geq 1, \end{cases}$$

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

Another Formula for $r_{p^k,Q}(m)$

Let $Q(\vec{\mathbf{x}}) = ax^2 + by^2 + cz^2$.
Let p be an odd prime such that p divides exactly one of a, b, c.
Without loss of generality, say $p \mid c$ but $p \nmid ab$.
If $p \nmid m$,

$$r_{p^k,Q}(m) = \begin{cases} 1, & k = 0, \\ p^{2k}\left(1 - \frac{1}{p}\left(\frac{-ab}{p}\right)\right), & k \geq 1, \end{cases}$$

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

Under the above conditions, $r_{p^k,Q}(m) > 0$ for every $k \geq 0$.

Back to an Example

p odd, $p \nmid m$, and p divides exactly one of a, b, c
$\implies$ m is locally represented by Q at the prime p

Back to an Example

p odd, $p \nmid m$, and p divides exactly one of a, b, c
$\implies$ m is locally represented by Q at the prime p

Example

- $Q(\vec{\mathbf{x}}) = x^2 + 5y^2 + 7z^2$ and $m = 3$

Back to an Example

p odd, $p \nmid m$, and p divides exactly one of a, b, c
$\implies$ m is locally represented by Q at the prime p

Example

- $Q(\vec{\mathbf{x}}) = x^2 + 5y^2 + 7z^2$ and $m = 3$
  - 5 divides exactly one of the coefficients of Q

Back to an Example

p odd, $p \nmid m$, and p divides exactly one of a, b, c
$\implies$ m is locally represented by Q at the prime p

Example

- $Q(\vec{\mathbf{x}}) = x^2 + 5y^2 + 7z^2$ and $m = 3$
  - 5 divides exactly one of the coefficients of Q
  - $5 \nmid 3$

Back to an Example

p odd, $p \nmid m$, and p divides exactly one of a, b, c
$\implies$ m is locally represented by Q at the prime p

Example

- $Q(\vec{\mathbf{x}}) = x^2 + 5y^2 + 7z^2$ and $m = 3$
  - 5 divides exactly one of the coefficients of Q
  - $5 \nmid 3$
  - 3 is locally represented at the prime 5

Back to an Example

p odd, $p \nmid m$, and p divides exactly one of a, b, c
$\implies$ m is locally represented by Q at the prime p

Example

- $Q(\vec{\mathbf{x}}) = x^2 + 5y^2 + 7z^2$ and $m = 3$
  - 5 divides exactly one of the coefficients of Q
  - $5 \nmid 3$
  - 3 is locally represented at the prime 5
- Similar case holds for the prime 7

Back to an Example

p odd, $p \nmid m$, and p divides exactly one of a, b, c
$\implies$ m is locally represented by Q at the prime p

Example

- $Q(\vec{\mathbf{x}}) = x^2 + 5y^2 + 7z^2$ and $m = 3$
    - 5 divides exactly one of the coefficients of Q
    - $5 \nmid 3$
    - 3 is locally represented at the prime 5
- Similar case holds for the prime 7
- Now only need to check if 3 is locally represented at the prime 2

Locally Represented at the Prime 2

Theorem

If $2 \nmid abcm$ and there exists a solution to

$$Q(\vec{\mathbf{x}}) = ax^2 + by^2 + cz^2 \equiv m \pmod{8},$$

then m is locally represented by Q at the prime 2.

Back to an Example

$2 \nmid abcm$ and solution to $Q(\vec{\mathbf{x}}) \equiv m \pmod 8$ exists
$\implies$ m is locally represented by Q at the prime 2

Example

- $Q(\vec{\mathbf{x}}) = x^2 + 5y^2 + 7z^2$ and $m = 3$

Back to an Example

$2 \nmid abcm$ and solution to $Q(\vec{\mathbf{x}}) \equiv m \pmod 8$ exists
$\implies$ m is locally represented by Q at the prime 2

Example

- $Q(\vec{\mathbf{x}}) = x^2 + 5y^2 + 7z^2$ and $m = 3$
- $2 \nmid (1 \cdot 5 \cdot 7 \cdot 3)$

Back to an Example

$2 \nmid abcm$ and solution to $Q(\vec{\mathbf{x}}) \equiv m \pmod 8$ exists
$\implies m$ is locally represented by Q at the prime 2

Example

- $Q(\vec{\mathbf{x}}) = x^2 + 5y^2 + 7z^2$ and $m = 3$
- $2 \nmid (1 \cdot 5 \cdot 7 \cdot 3)$
- $2^2 + 5 \cdot 0^2 + 7 \cdot 1^2 = 11 \equiv 3 \pmod 8$

Back to an Example

$2 \nmid abcm$ and solution to $Q(\vec{\mathbf{x}}) \equiv m \pmod 8$ exists
$\implies$ m is locally represented by Q at the prime 2

Example

- $Q(\vec{\mathbf{x}}) = x^2 + 5y^2 + 7z^2$ and $m = 3$
- $2 \nmid (1 \cdot 5 \cdot 7 \cdot 3)$
- $2^2 + 5 \cdot 0^2 + 7 \cdot 1^2 = 11 \equiv 3 \pmod 8$
- 3 is locally represented everywhere by Q

Future Work

Try to find a lower bound on the largest integer m that is locally but not globally represented by Q

Future Work

Try to find a lower bound on the largest integer m that is locally but not globally represented by Q

- computationally (using Sage)

Future Work

Try to find a lower bound on the largest integer m that is locally but not globally represented by Q

- computationally (using Sage)
- theoretically (using theta series, Eisenstein series, and cusp forms)

Thank you for listening!