A Generalization of Mordell to Ternary Quadratic Forms

Sarah Blackwell, Gabe Durham, Tiffany Treece

The Wake Forest/Davidson Experience in Number Theory Research

July 29, 2015
Acknowledgements

Thanks to UGA and to the organizers.
Special thanks to Dr. Jeremy Rouse, Dr. Paul Pollack, and to the National Science Foundation for making this research possible (NSF grant DMS-1461189).
Outline

- Introduction and History
- Outline of Mordell’s Argument
- Generalization of Mordell
- Future Projects
Diophantus asked for a given $m \in \mathbb{Z}$, when do there exist $a, x, y, z \in \mathbb{Z}$ such that $m = x + y + z$ and $x + a, y + a$ and $z + a$ are all perfect squares.

The case where $a = 0$ eventually became of special interest to number theorists; i.e., when is a number the sum of three squares?
History of the Sum of Three Squares

- In 1636 Fermat stated that no integer of the form $8k + 7$ is a sum of three squares.
- In 1798 Legendre announced a proof of the theorem.
- As a result the statement is known as: “Legendre’s Three Squares Theorem.”
- The theorem states that if $m \in \mathbb{Z}$ and $m$ is not of the form $4^k(8\ell + 7)$ with $k, \ell \in \mathbb{Z}$, then there exists $x, y, z \in \mathbb{Z}$ such that $m = x^2 + y^2 + z^2$. 
In 1801 Gauss provided a proof of the theorem in his famous work *Disquisitiones Arithmeticae*.

He did so by giving a formula for the number of representations of an integer as a sum of three squares.
History of the Sum of Three Squares

Other proofs given for the theorem:

- 1850 - Dirichlet - Uses his theorem of primes in an arithmetic progression.
- 1957 - Ankeny - Uses Geometry of Numbers.
- 1960 - Mordell - Refines Ankeny’s techniques.
Mordell’s proof of the three squares theorem begins by introducing a polynomial $f(x, y, z)$ with integer coefficients given by:

$$mf(x, y, z) = (Ax + By + mz)^2 + (ax^2 + 2hxy + by^2).$$

The proof then uses a GoN result of Gauss to show that there are integers $x, y, z$ such that $f(x, y, z) = 1$.

Because of this result and because all the cross terms of the polynomial are even, he is able to complete the square and use a change of variables to conclude that $f(x, y, z)$ equals the sum of three squares.

By construction, there exist $x, y, z$ such that $f(x, y, z) = m$. 
Mordell’s Proof - Sum of Three Squares

- We can show what integers $m$ can be written as the sum of three squares as long as all of $A, B, a, b,$ and $h$ exist.
- The selection must satisfy the conditions: $A^2 + a \equiv 0$, $B^2 + b \equiv 0$, $2AB + 2h \equiv 0 \pmod{m}$ set by the construction of the polynomial.
- Additionally, we must satisfy the condition $ab - h^2 = m$.
- The proof uses quadratic reciprocity and Dirichlet’s theorem of primes in an arithmetic progression to achieve this.
The question regarding the sum of three squares is a special case of a much broader class of problems.
Definitions

- In our research we only considered integral positive definite ternary quadratic forms.
- An **integral ternary quadratic form** $Q$ is a homogeneous polynomial of degree 2, where:

$$Q : \mathbb{Z}^3 \rightarrow \mathbb{Z}$$

$$(x_1, x_2, x_3) \mapsto \sum_{1 \leq i \leq j \leq 3} a_{ij}x_i x_j$$

where $a_{ij} \in \mathbb{Z}$ $\forall i, j$.
- If we represent the quadratic form $Q$ by a symmetric matrix $M$, then the **determinant** of the form $Q$ is the determinant of the matrix $M$. 
A quadratic form $Q$ is **positive definite** if:

(i) $Q(\vec{x}) = 0 \iff \vec{x} = \vec{0}$
(ii) $\forall \vec{x} \neq \vec{0}, Q(\vec{x}) > 0$.

We say that an integer $m$ is represented by a ternary quadratic form, $Q$, if $\exists \vec{x} \in \mathbb{Z}^3$ such that $Q(\vec{x}) = m$.

Given two forms $Q$ and $P$ with their associated matrices $M_Q$ and $M_P$, we say $Q \sim P$ if $\exists A \in GL_n(\mathbb{Z})$ with $A^t M_Q A = M_P$. 
We wanted to see if Mordell’s argument could generalize to quadratic forms other than just the sum of three squares. We first chose to study the Ramanujan-Dickson forms.

In the early 20th century Ramanujan wanted to classify the universal diagonal quaternary quadratic forms, using the technique of escalation.

Dickson proved exactly which numbers were represented by these escalators in 1927 by using reduction theory.
Our Results

Theorem

(a) A positive integer \( m \) is represented by \( x^2 + y^2 + 2z^2 \) if and only if \( m \neq 4^k(16\ell + 14) \).

(b) A positive integer \( m \) is represented by \( x^2 + y^2 + 3z^2 \) if and only if \( m \neq 9^k(9\ell + 6) \).

(c) A positive integer \( m \) is represented by \( x^2 + 2y^2 + 2z^2 \) if and only if \( m \neq 4^k(8\ell + 7) \).

(d) A positive integer \( m \) is represented by \( x^2 + 2y^2 + 3z^2 \) if and only if \( m \neq 4^k(16\ell + 10) \).

(e) A positive integer \( m \) is represented by \( x^2 + 2y^2 + 4z^2 \) if and only if \( m \neq 4^k(16\ell + 14) \).

(f) A positive integer \( m \) is represented by \( x^2 + 2y^2 + 5z^2 \) if and only if \( m \neq 25^k(25\ell \pm 10) \).
Our Results

Additionally we used our method on forms of determinants 5 and 6:

**Theorem**

(a) A positive integer $m$ is represented by $x^2 + y^2 + 5z^2$ if and only if $m \neq 4^k(8\ell + 3)$.

(b) A positive integer $m$ is represented by $x^2 + 2y^2 + 2yz + 3z^2$ if and only if $m \neq 25^k(25\ell \pm 5)$.

**Theorem**

A positive integer $m$ is represented by $x^2 + y^2 + 6z^2$ if and only if $m \neq 9^k(9\ell + 3)$. 
Our Generalization

- We wish to examine the representation of an integer $m$ by a form $Q$, where $Q$ has determinant $D$.
- We begin by introducing a ternary quadratic form $f(x, y, z)$ with determinant $D$ given by:

\[ mf(x, y, z) = (Ax + By + mz)^2 + (ax^2 + 2hxy + by^2) \]

- Note that by construction $f(x, y, z)$ represents $m$.
- Instead of using Gauss’s result, we examine all forms of determinant $D$ with all even cross terms.
- We identify an equivalence class that is not represented by all other forms with the same determinant but is represented by $Q$.
- $f(x, y, z)$ has determinant $D \Leftrightarrow ab - h^2 = Dm$. 
Now we show how to select the constants $A, B, a, b$ and $h$.

First, we need the coefficients of $mf(x, y, z)$ to be divisible by $m$.

We need the following equivalences to hold:

$$A^2 + a \equiv 0, \quad B^2 + b \equiv 0, \quad 2AB + 2h \equiv 0 \pmod{m}$$

The last two equivalences hold if we set $B \equiv b \equiv h \equiv 0 \pmod{m}$. 
Our Generalization

- So we still need to satisfy $A^2 + a \equiv 0 \pmod{m}$ and $ab - h^2 = Dm$.
- In addition we construct $\frac{A^2 + a}{m}$ to represent the equivalence class we identified earlier.
- If we can achieve this, we have shown that $f(x, y, z)$ represents $m$ and some element of the equivalence class not represented by the non-$Q$ forms of determinant $D$.
- Thus $f(x, y, z) \sim Q$. 
Our Generalization

- Next we show that it is possible to choose an $a$ and $A$ fulfilling $A^2 + a \equiv 0 \pmod{m}$ and $ab - h^2 = Dm$.
- Note that $-a \equiv A^2 \pmod{m}$ and $-Dm \equiv h^2 \pmod{a}$.
- Let $a$ be a prime, $a \nmid m$, such that $\left(\frac{-a}{p}\right) = 1$ for all primes $p$ dividing $m$.
- Hence $\left(\frac{-a}{m}\right) = 1$ by properties of Jacobi symbol.
- Now we need to check that $\left(\frac{-a}{m}\right) = 1$ and $\left(\frac{-Dm}{a}\right) = 1$ are guaranteed to hold simultaneously. We will put certain restrictions on $a$ so these are guaranteed to hold.
The quadratic form $x^2 + 2y^2 + 4z^2$ represents all integers not of the form $4^k(16\ell + 14)$ with $k, \ell \in \mathbb{Z}$. 
Proof Outline for $x^2 + 2y^2 + 4z^2$

Positive definite quadratic forms with determinant $8$ and even cross terms:

- $Q_1 : x^2 + 2y^2 + 4z^2$
- $Q_2 : x^2 + y^2 + 8z^2$
- $Q_3 : x^2 + 3y^2 + 3z^2 + 2yz$
- $Q_4 : 2x^2 + 2y^2 + 3z^2 + 2yz + 2xz$

How can we tell these forms apart?

**Claim 1**: If $m \equiv 6 \pmod{16}$, then $m$ is not represented by $Q_2, Q_3,$ or $Q_4$.

**Claim 2**: Let $m \in \mathbb{Z}$. If $m \equiv 14 \pmod{16}$, then $m$ is not represented by $Q_1$.

**Claim 3**: If $Q_1$ represents $4m$, then $m \not\equiv 14 \pmod{16}$.
Positive definite quadratic forms with determinant 8 and even cross terms:

- $Q_1 : x^2 + 2y^2 + 4z^2$
- $Q_2 : x^2 + y^2 + 8z^2$
- $Q_3 : x^2 + 3y^2 + 3z^2 + 2yz$
- $Q_4 : 2x^2 + 2y^2 + 3z^2 + 2yz + 2xz$

How can we tell these forms apart?

**Claim 1:** If $m \equiv 6 \pmod{16}$, then $m$ is not represented by $Q_2, Q_3,$ or $Q_4$.

**Claim 2:** Let $m \in \mathbb{Z}$. If $m \equiv 14 \pmod{16}$, then $m$ is not represented by $Q_1$.

**Claim 3:** If $Q_1$ represents $4m$, then $m \not\equiv 14 \pmod{16}$.
Proof Outline for $x^2 + 2y^2 + 4z^2$

Positive definite quadratic forms with determinant 8 and even cross terms:

- $Q_1 : x^2 + 2y^2 + 4z^2$
- $Q_2 : x^2 + y^2 + 8z^2$
- $Q_3 : x^2 + 3y^2 + 3z^2 + 2yz$
- $Q_4 : 2x^2 + 2y^2 + 3z^2 + 2yz + 2xz$

How can we tell these forms apart?

**Claim 1:** If $m \equiv 6 \pmod{16}$, then $m$ is not represented by $Q_2$, $Q_3$, or $Q_4$.

**Claim 2:** Let $m \in \mathbb{Z}$. If $m \equiv 14 \pmod{16}$, then $m$ is not represented by $Q_1$.

**Claim 3:** If $Q_1$ represents $4m$, then $m \not\equiv 14 \pmod{16}$.
Proof Outline for $x^2 + 2y^2 + 4z^2$

Positive definite quadratic forms with determinant 8 and even cross terms:

- $Q_1 : x^2 + 2y^2 + 4z^2$
- $Q_2 : x^2 + y^2 + 8z^2$
- $Q_3 : x^2 + 3y^2 + 3z^2 + 2yz$
- $Q_4 : 2x^2 + 2y^2 + 3z^2 + 2yz + 2xz$

How can we tell these forms apart?

**Claim 1**: If $m \equiv 6 \pmod{16}$, then $m$ is not represented by $Q_2, Q_3,$ or $Q_4$.

**Claim 2**: Let $m \in \mathbb{Z}$. If $m \equiv 14 \pmod{16}$, then $m$ is not represented by $Q_1$.

**Claim 3**: If $Q_1$ represents $4m$, then $m \not\equiv 14 \pmod{16}$. 
Proof Outline for $x^2 + 2y^2 + 4z^2$

Let $m \in \mathbb{Z}$ and not of the form $4^k(16l + 14)$. Consider the ternary quadratic form $f(x, y, z)$ of determinant $D = 8$ given by

$$mf(x, y, z) = (Ax + By + mz)^2 + (ax^2 + 2hxy + by^2)$$

with the determinant condition

$$ab - h^2 = 8m$$

and integers $A, B$ such that $f(x, y, z)$ has integer coefficients and even cross terms. Note that $f(x, y, z)$ represents $m$. 
Choosing constants $A, B, a, b,$ and $h$:

Let $a$ be an odd prime with $a 
mid m$ so that $\left( \frac{-8m}{a} \right) = 1$.

Consider

\[
A^2 + a \equiv 0 \\
B^2 + b \equiv 0 \\
2AB + 2h \equiv 0 \pmod{m}.
\]

The second and third congruence conditions are satisfied if we choose $B \equiv b \equiv h \equiv 0 \pmod{m}$. The first condition is met if we choose

\[
\left( \frac{-a}{p} \right) = 1 \ \forall p \mid m.
\]
Proof Outline for $x^2 + 2y^2 + 4z^2$

Now we must check the consistency of

$$\left( \frac{-8m}{a} \right) = \left( \frac{-a}{m} \right) = 1.$$ 

In addition, we would like to construct each case so that

$$\frac{A^2 + a}{m} \equiv 6 \pmod{16}.$$ 

We have 11 congruences to check:

$m \equiv 1, 2, 3, 5, 6, 7, 9, 10, 11, 13, 15 \pmod{16}.$
Case $m \equiv 1, 9 \pmod{16}$

Let $a = 2a_1$ where $a_1$ is an odd prime, $a_1 \nmid m$, so $\left( \frac{-8m}{a_1} \right) = 1$. Additionally let $a_1 \equiv 3 \pmod{16}$. Now we must examine the consistency of $\left( \frac{-a}{m} \right) = 1$ and $\left( \frac{-8m}{a_1} \right) = 1$:

$$1 = \left( \frac{-8m}{a_1} \right) = \left( \frac{-1}{a_1} \right) \left( \frac{2}{a_1} \right) \left( \frac{m}{a_1} \right) = \prod_{p | m} \left( \frac{p}{a_1} \right)$$

$$= \prod_{p | m} \left( \frac{a_1}{p} \right) = \prod_{p | m} \left( \frac{-a_1}{p} \right) = \left( \frac{-2a_1}{m} \right) = \left( \frac{-a}{m} \right)$$

as needed.
Case $m \equiv 1, 9 \pmod{16}$

Now consider $A$. Since $a = 2a_1$ and $a_1 \equiv 3 \pmod{16}$, we have $a \equiv 6 \pmod{16}$.

\[
\frac{A^2 + a}{m} \equiv 6 \pmod{16}
\]

\[
A^2 + a \equiv 6 \pmod{16}
\]

\[
A^2 \equiv 0 \pmod{16}
\]

So choose $A \equiv 0 \pmod{4}$. 
Numerical Example Using the Form $x^2 + 2y^2 + 4z^2$

**Example:** Let $m = 17$.
Take $a = 38$, $b = 34$, $h = 34$, $B = 17$, $A = 8$.

So $17f(x, y, z) = (8x + 17y + 17z)^2 + (38x^2 + 68xy + 34y^2)$.

Dividing by $m$ and using a change of variables, we arrive at our desired form:

\[
\begin{align*}
  f(x, y, z) &= 6x^2 + 19y^2 + 17z^2 + 20xy + 16xz + 34yz \\
  &= (y + z)^2 + 2(x + y)^2 + 4(x + 2y + 2z)^2 \\
  &\sim X^2 + 2Y^2 + 4Z^2
\end{align*}
\]
Future Projects

Forms within the same genus:

- It is very difficult to distinguish two forms within the same genus as they represent the same equivalence classes.
- For instance, $x^2 + y^2 + 16z^2$ and $2x^2 + 2y^2 + 5z^2 + 2yz + 2xz$ are in the same genus. This makes it difficult to use our current method on $x^2 + y^2 + 16z^2$. 
Odd cross terms:

- The current method requires that all cross terms of the form have even coefficients. Another extension would be to alter the approach so that one could look at various forms with odd cross terms.
Questions?

Thank you for your attention!