Sums of Three Squares

Philippe Michaud-Rodgers

University of Warwick

09.03.2019

The Three-Square Theorem

Theorem (Legendre's Three-Square Theorem)

A positive integer n can be expressed as a sum of three squares if and only if n is not of the form $4^k(8m+7)$, $(k, m \geq 0)$.

Aim: Give a detailed outline of the proof.

- Binary Quadratic Forms
- Gauss' Class Number Problem
- Ternary Quadratic Forms

A Little History

- Integers of the form $3n + 1$ as sums of three squares studied by Diophantus (200-300 AD).
- Fermat, Euler, Lagrange, Legendre, and Dirichlet all studied the problem.
- First proof of the three-square theorem published by Legendre in 1798.
- Clearer proof presented by Dirichlet in 1850 based on the theory of binary and ternary quadratic forms.

The Two- and Four-Square Theorems

Theorem (Lagrange's Four-Square Theorem)

Every positive integer n can be expressed as a sum of four squares.

Theorem (Two-Square Theorem)

A positive integer n can be written as a sum of two squares if and only if in the prime factorisation of n every prime $q \equiv 3 \pmod 4$ appears with an even exponent.

Why is the three-square theorem much **harder** to prove?

No composition law. **Answering the question for primes is not enough**.

$$3 = 1^2 + 1^2 + 1^2, 5 = 1^2 + 2^2 + 0^2, \text{ but } 3 \times 5 = 15 \neq \text{ S3S}$$

Composition law for two squares:

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

One Direction of the Proof

Proposition

If $n = 4^k(8m+7)$ $(k, m \geq 0)$, then n is **not** *a sum of three squares.*

Proof.

- If $n = 8m + 7 = x^2 + y^2 + z^2$, then reduce modulo 8 to get

$$x^2 + y^2 + z^2 \equiv 7 \pmod 8.$$

- If $n = x^2 + y^2 + z^2$ is a sum of three square and $n = 4n'$, then x, y, z are even (reduce modulo 4), so

$$n' = \left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2 + \left(\frac{z}{2}\right)^2.$$

Binary Quadratic Forms - First Definitions

Definition

A **binary quadratic form over** $\mathbb{Z}$ is a polynomial of the form

$$f(x, y) = ax^2 + bxy + cy^2,$$

where $a, b, c \in \mathbb{Z}$. The matrix of f is

$$M_f = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}.$$

We choose this matrix because $f(x, y) = \begin{pmatrix} x & y \end{pmatrix} M_f \begin{pmatrix} x \\ y \end{pmatrix}$.

Note: Forms = Binary Forms = Binary Quadratic Forms = Binary Quadratic Forms over $\mathbb{Z}$.

Definition

An integer n is said to be **represented** by a given form f if there exist $x, y \in \mathbb{Z}$ such that $f(x, y) = n$.

Binary Quadratic Forms - Equivalence

Definition

Let f and g be two binary quadratic forms. We say that f **is equivalent to** g, and write $f \sim g$, if there exists a matrix $P \in \mathrm{SL}_2(\mathbb{Z})$ such that

$$M_g = P^T M_f P.$$

If two forms are equivalent then we say that they belong to the same **class**.

This is an **equivalence relation**.

Proposition

Equivalent forms represent the same integers.

Binary Quadratic Forms - Positive Definiteness and the Discriminant

Definition

Let $f(x, y) = ax^2 + bxy + cy^2$ be a binary quadratic form. The **discriminant** of f is $D(f) = b^2 - 4ac$.

Definition

A binary quadratic form f is **positive definite** if $f(x, y) \geqslant 0$ for all integers x and y, and $f(x, y) = 0$ if and only if $x = y = 0$.

Proposition

A binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ is positive definite if and only if $D < 0$ and $a > 0$.

Proposition

Suppose $f \sim g$. Then $D(f) = D(g)$, and f is positive definite if and only if g is positive definite.

Binary Quadratic Forms - An Example

Example

Let $f(x, y) = 13x^2 - 36xy + 25y^2$.

- $M_f = \left(\begin{smallmatrix} 13 & -18 \\ -18 & 25 \end{smallmatrix}\right)$.
- $D(f) = (-36)^2 - 4(13)(25) = -4$, so f is positive definite.
- $f(-4, 6) = \left(\begin{smallmatrix} -4 & 6 \end{smallmatrix}\right) M_f \left(\begin{smallmatrix} -4 \\ 6 \end{smallmatrix}\right) = 1972$, so 1972 is represented by f.
- $f \sim x^2 + y^2$ using $\left(\begin{smallmatrix} 3 & 4 \\ 2 & 3 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, that is $I_2 = \left(\begin{smallmatrix} 3 & 2 \\ 4 & 3 \end{smallmatrix}\right) M_f \left(\begin{smallmatrix} 3 & 4 \\ 2 & 3 \end{smallmatrix}\right)$.
- So $x^2 + y^2$ must represent 1972 too: 1972 is a sum of two squares!
- $1972 = \left(\begin{smallmatrix} -4 & 6 \end{smallmatrix}\right) M_f \left(\begin{smallmatrix} -4 \\ 6 \end{smallmatrix}\right) = \left(\begin{smallmatrix} -4 & 6 \end{smallmatrix}\right) \left(\begin{smallmatrix} 3 & 2 \\ 4 & 3 \end{smallmatrix}\right)^{-1} I_2 \left(\begin{smallmatrix} 3 & 4 \\ 2 & 3 \end{smallmatrix}\right)^{-1} \left(\begin{smallmatrix} -4 \\ 6 \end{smallmatrix}\right) = \left(\begin{smallmatrix} -36 & 0 \\ 0 & 26 \end{smallmatrix}\right) = \left(\begin{smallmatrix} -36 & 26 \end{smallmatrix}\right) I_2 \left(\begin{smallmatrix} -36 \\ 26 \end{smallmatrix}\right)$
- So $1972 = (-36)^2 + 26^2 = 36^2 + 26^2$.

Binary Quadratic Forms - Reduced Forms

We have classes of positive definite binary quadratic forms with discriminant D. We want to find (unique) **representatives** for these classes.

Definition

A positive definite binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ is said to be **reduced** if $|b| \leq a \leq c$, and $b \geq 0$ if either $|b| = a$ or $a = c$.

Theorem

Any positive definite binary quadratic form is equivalent to a unique reduced form.

To prove existence we use the **reduction algorithm**. Uniqueness comes from the condition $b \geq 0$ if either $|b| = a$ or $a = c$.

Binary Quadratic Forms - The Reduction Algorithm

- Let $f_0(x, y) = a_0x^2 + b_0xy + a_1y^2$ be a positive definite binary quadratic form.
- Find integers q_1 and b_1 such that

$$b_0 = 2a_1q_1 - b_1 \quad \text{and} \quad -a_1 < b_1 \leqslant a_1$$

(by reducing b_0 modulo $2a_1$).

- Transform f_0 to f_1 using $\left(\begin{smallmatrix} 0 & 1 \\ -1 & -q_1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ to obtain

$$f_1(x, y) = a_1x^2 + b_1xy + a_2y,$$

where $a_2 := a_0 - b_0q_1 + a_1q_1^2$.

- If $a_2 \geqslant a_1$, stop; otherwise repeat the process.

The process must terminate as $a_1 > a_2 > \cdots > 0$. Each form is equivalent to the next and once we stop the form is (almost) reduced.

Binary Quadratic Forms - Finiteness

Lemma

If $f(x, y) = ax^2 + bxy + cy^2$ is a reduced positive definite quadratic form with discriminant D, then

$$0 < a \leq \sqrt{\frac{-D}{3}}.$$

Proof.

- f is positive definite, so $a > 0$ and $D < 0$.
- $ac \geq a^2$ because $c \geq a$,
- $b^2 \leq a^2$ because $|b| \leq a$.

So

$$-D = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2.$$

□

Consequence: the number of classes of positive definite binary forms of a given discriminant D is finite.

Binary Quadratic Forms - Discriminant -4

Theorem

Every positive definite binary quadratic form with discriminant $D = -4$ is equivalent to a sum of two squares.

Proof.

Suppose $D(f) = -4$. Then $f \sim g(x, y) = ax^2 + bxy + cy^2$, with discriminant $D(g) = -4$ and

$$a \leq \sqrt{\frac{-D(g)}{3}} = \frac{2}{\sqrt{3}} < 2.$$

Since $a > 0$, $a = 1$. Then $b = 0$ or 1 since $|b| \leq a$.

Since $b^2 \equiv D \equiv 0 \pmod 4$, $b = 0$.

From $D(g) = b^2 - 4ac$, $c = 1$, so $g(x, y) = x^2 + y^2$. □

This is a powerful result!

Class Numbers - Primitivity

Definition

A binary form $f(x, y) = ax^2 + bxy + cy^2$ is *primitive* if a, b, and c are coprime.

Primitivity is preserved by equivalence.

Definition

Given some integer $D < 0$, the number of classes of primitive positive definite quadratic forms with discriminant D is denoted $h(D)$, this is the **class number of** D.

Definition

Let $D < 0$ such that $D \equiv 0$ or $1 \pmod 4$.

- If $D \equiv 0 \pmod 4$, then $x^2 - (D/4)y^2$ is the **principal form of discriminant** D.
- If $D \equiv 1 \pmod 4$, then $x^2 + xy - ((D-1)/4)y^2$ is the **principal form of discriminant** D.

So if $D \equiv 0$ or $1 \pmod 4$ then $h(D) \geq 1$.

Class Numbers - Class Number One

Theorem

If $n \in \mathbb{N}$, *then* $h(-4n) = 1$ *if and only if* $n \in \{1, 2, 3, 4, 7\}$.

Sketch Proof.

- If $n \in \{1, 2, 3, 4, 7\}$ use inequalities to show that the principal form is the only reduced form.
- If $n \notin \{1, 2, 3, 4, 7\}$, construct a primitive positive definite reduced form not equal to the principal form.

□

Theorem

We have that $h(D) = 1$ *if and only if*
$D = -3, -4, -7, -8, -11, -19, -43, -67,$ *or* -163, *where* D *is a negative fundamental discriminant (meaning that* $D \neq 1$ *is an integer such that* $D \equiv 1 \pmod 4$ *and* D *is square-free, or* $D = 4m$ *where* $m \equiv 2$ *or* $3 \pmod 4$ *and* m *is square-free.)*

This was proven by Heegner in 1952 and formally corrected by Stark in 1969.

Class Numbers - Primes of the form $x^2 + ny^2$

Theorem

Let p be a prime number. Then

- $p = x^2 + y^2$ *if and only if* $p \equiv 1 \pmod 4$ *or* $p = 2$
- $p = x^2 + 2y^2$ *if and only if* $p \equiv 1, 3 \pmod 8$ *or* $p = 2$
- $p = x^2 + 3y^2$ *if and only if* $p \equiv 1 \pmod 3$ *or* $p = 3$
- $p = x^2 + 4y^2$ *if and only if* $p \equiv 1 \pmod 4$
- $p = x^2 + 7y^2$ *if and only if* $p \equiv 1, 2, 4 \pmod 7$ *or* $p = 7$, *and* $p \neq 2$.

For '$\Rightarrow$' Consider the equation modulo 3, and use that squares modulo 3 are 1 and 0.

For the converse, first discard $p = 3$. Then use $\left(\frac{-3}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 3$. **So we need to show that $\left(\frac{-3}{p}\right) = 1 \Rightarrow p = x^2 + 3y^2$.**

Class Numbers - Primes $p = x^2 + 3y^2$

$\left(\frac{-3}{p}\right) = 1 \Rightarrow p = x^2 + 3y^2$.

Since $\left(\frac{-3}{p}\right) = 1$, choose $t \in \mathbb{Z}$ such that $t^2 \equiv -3 \pmod{p}$. So $t^2 = -3 + kp$, where $k \in \mathbb{Z}$. So

$$\det \begin{pmatrix} k & t \\ t & p \end{pmatrix} = 3.$$

Set $f(x, y) = kx^2 + 2txy + py^2$. So $D(f) = -12$.

- f is positive definite.
- f is primitive.

So $f \sim x^2 + 3y^2$, the principal form of discriminant -12, because $h(-12) = 1$.

Moreover, $f(0, 1) = p$, so f represents p. So $x^2 + 3y^2$ represents p. □

Bye-Bye Binary

There is a composition law for binary quadratic forms. The set of primitive classes forms a finite abelian group, the **Class Group**.

This composition law recently revolutionised by Fields medallist Manjul Bharagava who invented **Bhargava Cubes** as a way of studying this law.

Bhargava and Hanke recently (2014) proved the following long-standing conjecture.

Theorem (The 290-Theorem)

If a positive definite binary quadratic form represents all positive integers up to 290 *(in fact even a certain subset will do), then it represents all positive integers!*

Ternary Quadratic Forms - First Definitions

Definition

An **integral ternary quadratic form** is a polynomial

$$f(x_1, x_2, x_3) = \sum_{i,j=1}^{3} a_{ij} x_i x_j,$$

where $a_{ij} \in \mathbb{Z}$ and $a_{ij} = a_{ji}$ for all $i, j \in \{1, 2, 3\}$. The **matrix of** f is

$$(a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{pmatrix}.$$

The **determinant** of f is $d_3(f) = \det(a_{ij})$.

Over $\mathbb{Z}$ vs. integral

- The polynomial $3x_1^2 - 4x_1x_2 + 2x_2^2 + 7x_2x_3 + x_3^2$ is not an integral ternary form.
- The polynomial $3x_1^2 - 4x_1x_2 + 2x_2^2 + 6x_2x_3 + x_3^2$ is an integral ternary form.

Ternary Forms - Similarites and Differences to Binary Forms

- Definitions of **represented by**, **equivalence**, and **positive definite** are the 'same'.
- Equivalence preserves the determinant, positive definiteness and representation of integers.
  - The classification of positive definite forms.
  - The existence of a 'reduced' representative (not unique) for positive definite ternary forms.
  - A positive definite form with determinant 1 is equivalent to a sum of three squares.

Ternary Forms - Three Technical Theorems

Theorem

A ternary quadratic form $f(x_1, x_2, x_3) = \sum_{i,j=1}^{3} a_{ij} x_i x_j$ *is positive definite if and only if:*

$$a_{11} > 0, \qquad b := \begin{vmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{vmatrix} > 0, \qquad d_3 > 0.$$

Theorem

Every positive definite ternary quadratic form, with determinant d_3*, is equivalent to a form* $h(x_1, x_2, x_3) = \sum_{i,j=1}^{3} a_{ij} x_i x_j$*, satisfying:*

$$0 < a_{11} \leqslant \frac{4}{3} \sqrt[3]{d_3}, \qquad 2|a_{12}| \leqslant a_{11}, \qquad 2|a_{13}| \leqslant a_{11}.$$

Theorem

Every positive definite ternary quadratic form with determinant 1 *is equivalent to a sum of three squares.*

The Three Square-Theorem - Outline of Proof I

Theorem (Legendre's Three-Square Theorem)

A positive integer n can be expressed as a sum of three squares if and only if n is not of the form $4^k(8m+7)$, $(k, m \geq 0)$.

We have seen '$\Rightarrow$' already.

If $n = x^2 + y^2 + z^2$, then $4n = (2x)^2 + (2y)^2 + (2z)^2$. So enough to show that if $n \equiv 1, 2, 3, 5, 6 \pmod 8$, then n is a sum of three squares.

Main Idea

Construct a positive definite ternary quadratic form of determinant 1 that represents n.
If we can do this, then n can be expressed as a sum of three squares.

The Three Square-Theorem - Outline of Proof II

Constructing such a ternary form boils down to the following problem: **Find an integer $b > 0$ such that $-b$ is a square modulo $bn - 1$.**

Given such a b:

- Choose a_{12} such that $-b \equiv a_{12}^2 \pmod{bn-1}$.
- Set $a_{22} = bn - 1$.
- Set $a_{11} = \frac{b + a_{12}^2}{a_{22}}$.
- Set $a_{13} = 1, a_{23} = 0, a_{33} = n$
- Set $f(x_1, x_2, x_3) = \sum_{i,j=1}^{3} a_{ij} x_i x_j$.

Then f is a positive definite ternary form, has determinant 1, and $f(0, 0, 1) = n$.

How do we find such an integer b?

The Three Square-Theorem - Outline of Proof III

We need a $b > 0$ such that $-b$ is a square modulo $bn - 1$.

Two main ingredients

- **Jacobi Symbols**: A generalisation of the Legendre Symbol. Let $b = \prod_{r=1}^{k} p_r$ be an odd integer. Let $a \in \mathbb{Z}$. We define the *Jacobi symbol* $\left(\frac{a}{b}\right)$ as

$$\left(\frac{a}{b}\right) = \prod_{r=1}^{k} \left(\frac{a}{p_r}\right),$$

  where $\left(\frac{a}{p_r}\right)$ is the usual Legendre symbol.

  Warning: $\left(\frac{a}{b}\right) = +1 \not\Rightarrow a$ is a quadratic residue modulo b.
- **Dirichlet's Theorem on Primes in Arithmetic Progressions**: Let a and d be positive coprime integers. Then there are infinitely many primes congruent to a modulo d.

The Three Square-Theorem - Consequences I

Theorem (Gauss)

Every positive integer n can be expressed as the sum of three triangular numbers.

Proof.

Write $8n + 3 = x^2 + y^2 + z^2$. By considering this equation modulo 8, x, y, and z are all odd.
Write $x = 2r + 1, y = 2s + 1, z = 2t + 1$. Substituting in and rearranging gives

$$n = \frac{r(r+1)}{2} + \frac{s(s+1)}{2} + \frac{t(t+1)}{2}.$$

□

Gauss famously wrote in his diary $\text{E}\Upsilon\text{PHKA! num} = \Delta + \Delta + \Delta$ after proving this theorem. Consequently it is often called the **Eureka Theorem**

The Three Square-Theorem - Consequences II

Theorem (Lagrange's Four-Square Theorem)

Every positive integer n can be expressed as a sum of four squares.

Proof.

If n is a sum of three squares, append 0^2.

Otherwise $n = 4^k(8m + 7)$. Then

$$n = 4^k(8m + 7) = 4^k(8m + 6) + (2^k)^2.$$

Then write $4^k(8m + 6) = x^2 + y^2 + z^2$ for $x, y, z \in \mathbb{Z}$.

Setting $w = 2^k$ gives $n = x^2 + y^2 + z^2 + w^2$. □

Note: This theorem can be proved much more directly!

Looking Ahead - Fermat and Waring

Theorem (Fermat's Polygonal Number Theorem)

Every positive integer can be written as a sum of n n-gonal numbers.

We have seen that the theorem holds for $n = 3$ and 4.

Waring's Problem

Waring's problem concerns expressing integers as sums of higher powers.

- Every positive integer can be written as the **sum of nine cubes**.
- Every positive integer can be written as the sum of **nineteen fourth powers!**.

Thank you for listening! :)

Contact: p.rodgers@warwick.ac.uk or via Facebook.