Quadratic Forms, Sums of Three Squares

Jinoo Kim

Columbia University
Department of Mathematics

Instructor:
Avi Zeff

Additive Number Theory Seminar
Jan 31, 2024

Introduction

1. Introduction to Quadratic Forms
2. Classification of Binary Quadratic Forms
3. Classification of Ternary Quadratic Forms
4. Sums of Three Squares

Ex An example of an equivalence relation is $A \sim B \iff a - b \equiv 0 \pmod 2$.

Say that two matrices $A, B \in M_n(\mathbb{Z})$ are **equivalent**

$$A \sim B \iff B = A \cdot U = U^T A U$$

for some $U \in SL_n(\mathbb{Z})$.

This equivalence relation preserves determinants, so $A \sim B \implies$ det(A) =det(B)

$$\implies \det(A \cdot U) = \det(U^T A U) = \det(U^T)\det(A)\det(U) = \det(A)$$

The **equivalence classes** constructed by the equivalence relation partition the set of symmetric matrices in $M_n(\mathbb{Z})$ into equivalence classes based on their determinant.

Ex Let $U = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}$ and $A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$.

$$B = U^T A U = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 13 & 31 \\ 31 & 74 \end{pmatrix}$$

Introduction to Quadratic Forms III

Def Each $n \times n$ symmetric matrix A (where the entry in the ith row and jth column is $a_{i,j}$) has an associated **Quadratic Form** F_A:

$$F_A(x_1, ..., x_n) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{i,j} x_i x_j.$$

We can think of the x_i's as entries in a column vector, x. This allows us to write the quadratic form as $F_A(x_1, ..., x_n) = x^T A x$.

We say that two forms are **equivalent** if their associated matrices are equivalent and so

$$A \sim B \iff F_A \sim F_B.$$

Introduction to Quadratic Forms IV

Ex The identity matrix I_2 has an associated Quadratic Form $x_1^2 + x_2^2$.

$$\begin{aligned} F_A(x_1, x_2) &= \begin{pmatrix} x_1 & x_2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \\ &= \begin{pmatrix} x_1 & x_2 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \\ &= x_1^2 + x_2^2 \end{aligned}$$

Introduction to Quadratic Forms V

We say that F_A **represents** N if $\exists x_1, ..., x_n$ such that $F_A(x_1, ..., x_n) = x^T Ax = N$, where $N, x_1, ..., x_n \in \mathbb{Z}$.

Ex The quadratic form $x_1^2 + x_2^2$ represents $13 = 2^2 + 3^2$ but not 7.

Any two quadratic forms in the same equivalence class represent the same integers.

$$\implies F_A(x) = x^T Ax = x^T U^T BUx = (Ux)^T B(Ux) = F_B(Ux)$$

Introduction to Quadratic Forms VI

Def The quadratic form F_A is called **Positive-Definite** if $F_A(x_1, ..., x_n) \geq 1$ for all $(x_1, ..., x_n) \neq (0, ..., 0)$. Every form equivalent to a positive-definite quadratic form is positive-definite.

Def A **Binary** quadratic form is over two variables (x_1, x_2) and a **Ternary** quadratic form is over three.

Binary Quadratic Forms I

Def The **discriminant** of the quadratic form F_A is the determinant of the matrix A.

In this section we will be classifying binary quadratic forms, in particular, by proving that every positive-definite binary quadratic form of discriminant 1 is equivalent to the form $x_1^2 + x_2^2$.

This is mainly useful in helping us understand ternary quadratic forms, which we will ultimately use in our proof about the sums of three squares.

Binary Quadratic Forms II

Lemma 1

Let
$$A = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{1,2} & a_{2,2} \end{pmatrix}$$
be a 2×2 symmetric matrix and let
$$F_A(x_1, x_2) = a_{1,1}x_1^2 + 2a_{1,2}x_1x_2 + a_{2,2}x_2^2$$
be the quadratic form. F_A **is positive definite if and only if** $a_{1,1} \geq 1$ and the discriminant d satisfies
$$d = \det(A) = a_{1,1}a_{2,2} - a_{1,2}^2 \geq 1.$$

To prove an if and only if, we prove the forward and converse direction. First, we assume F_A is positive-definite then show that the conditions are satisfied. Second, we assume the conditions are satisfied and show that F_A is positive-definite.

Binary Quadratic Forms III

Lemma 1

Let

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{1,2} & a_{2,2} \end{pmatrix}$$

be a 2×2 symmetric matrix and let

$$F_A(x_1, x_2) = a_{1,1}x_1^2 + 2a_{1,2}x_1x_2 + a_{2,2}x_2^2$$

be the quadratic form. F_A **is positive definite if and only if** $a_{1,1} \geq 1$ and the discriminant d satisfies

$$d = \det(A) = a_{1,1}a_{2,2} - a_{1,2}^2 \geq 1.$$

- F_A is positive definite $\implies F_A(1,0) = a_{1,1} \geq 1$
- F_A is positive definite $\implies F_A(-a_{1,2}, a_{1,1}) = a_{1,1}(a_{1,1}a_{2,2} - a_{1,2}^2)$ $= a_{1,1}d \geq 1.$
  d must be an integer and it can not be 0 or negative, otherwise $a_{1,1}d$ would be 0 or negative. Thus, $d \geq 1$.

Binary Quadratic Forms IV

Lemma 1

Let
$$A = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{1,2} & a_{2,2} \end{pmatrix}$$
be a 2×2 symmetric matrix and let
$$F_A(x_1, x_2) = a_{1,1}x_1^2 + 2a_{1,2}x_1x_2 + a_{2,2}x_2^2$$
be the quadratic form. F_A **is positive definite if and only if** $a_{1,1} \geq 1$ and the discriminant d satisfies
$$d = \det(A) = a_{1,1}a_{2,2} - a_{1,2}^2 \geq 1.$$

If $a_{1,1} \geq 1$ and $d \geq 1$, then
$$a_{1,1}F_A(x_1, x_2) = (a_{1,1}x_1 + a_{1,2}x_2)^2 + dx_2^2 \geq 0$$
Thus, if $a_{1,1} \geq 1$ and $d \geq 1$, F_A is positive definite. $(F_A = 0?)$ □

Binary Quadratic Forms V

The conditions we outlined in **Lemma 1** then help us prove **Lemma 2**:

Lemma 2

Every equivalence class of positive definite binary quadratic forms of discriminant d **contains at least one form**

$$F_B(x_1, x_2) = b_{1,1}x_1^2 + 2b_{1,2}x_1x_2 + b_{2,2}x_2^2$$

for which

$$2|b_{1,2}| \leq b_{1,1} \leq \frac{2}{\sqrt{3}}\sqrt{d}$$

This proof is quite technical and so for time's sake I will simply outline it here. The details of the proof can be found in Nathanson $\S1.3$ (Lemma 1.2) or in my lecture notes.

Binary Quadratic Forms VI

Lemma 2

Every equivalence class of positive definite binary quadratic forms of discriminant d **contains at least one form**

$$F_B(x_1, x_2) = b_{1,1}x_1^2 + 2b_{1,2}x_1x_2 + b_{2,2}x_2^2$$

for which

$$2|b_{1,2}| \leq b_{1,1} \leq \frac{2}{\sqrt{3}}\sqrt{d}$$

- I take arbitrary matrix A and construct a subsequent matrix $U \in SL_2(\mathbb{Z})$.
- When I conjugate A by U, I get a matrix $B = U^T AU$ which is positive-definite.
- I am then able to prove the inequality in the lemma, using a combination of clever algebraic manipulation and the properties outlined in **Lemma 1**

Binary Quadratic Forms VII

Thm Every positive-definite binary quadratic form of discriminant 1 is equivalent to the form $x_1^2 + x_2^2$.

Let F be some arbitrary positive-definite binary quadratic form of discriminant 1. By **Lemma 2**, the form F is equivalent to a form $a_{1,1}x_1^2 + 2a_{1,2}x_1x_2 + a_{2,2}x_2^2$ for which

$$2|a_{1,2}| \leq a_{1,1} \leq \frac{2}{\sqrt{3}}\sqrt{d}$$

- Since $a_{1,1} \geq 1$, $d = 1$, and $a_{1,1} \leq \frac{2}{\sqrt{3}}\sqrt{d}$, we must have $a_{1,1} = 1$
- If $a_{1,1} = 1$ and $2|a_{1,2}| \leq a_{1,1}$, we have that $a_{1,2} = 0$
- Since $d = 1$, it follows that $a_{2,2} = a_{1,1}a_{2,2} - a_{1,2}^2 = 1$.

Plugging $a_{2,2} = 1, a_{1,2} = 0, a_{1,1} = 1$ into our quadratic form, we get that the form F is equivalent to $x_1^2 + x_2^2$ and we are done. □

Ternary Quadratic Forms

Details of the classification of Ternary Quadratic Forms can be found in Nathanson $\S1.4$. However, the general proof structure is similar and we end up proving a similar result.

Thm Every positive-definite ternary quadratic form of discriminant 1 is equivalent to the form $x_1^2 + x_2^2 + x_3^2$.

Sums of Three Squares I

In this section we will ultimately look to classify integers that can be written as the sum of three squares:

Thm A positive integer N can be represented as the sum of three squares if and only if N is not of the form $N = 4^a(8k+7)$

We require three preliminary 'ingredients' to prove this. We will, of course, use the theorem we just stated:

Thm Every positive-definite ternary quadratic form of discriminant 1 is equivalent to the form $x_1^2 + x_2^2 + x_3^2$.

as well as Gauss's law of quadratic reciprocity, and Dirichlet's theorem on primes in arithmetic progressions. (see next slide)

Sums of Three Squares II

Def If a is a **Quadratic Residue** modulo m, it means that there is some n such that $n^2 \equiv a \pmod{m}$.

Ex 4 is a quadratic residue modulo 8 because $6^2 \equiv 4 \pmod{8}$. As is 2^2.

Sums of Three Squares III

Law of Quadratic Reciprocity

Let p and q be distinct odd prime numbers, and define the Legendre symbol as:

$$\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if } n^2 \equiv q \bmod p \text{ for some integer } n \\ -1 & \text{otherwise} \end{cases}$$

Using the Legendre symbol, the quadratic reciprocity law can be stated concisely: $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$

$(\frac{p}{q}) = (\frac{q}{p})$ if p or $q \equiv 1$ (mod 4)
$(\frac{-1}{p}) = 1$ if and only if $p \equiv 1$ (mod 4)

Further, the Legendre Symbol is multiplicative: $\left(\frac{a}{b}\right)\left(\frac{c}{d}\right) = \left(\frac{ac}{bd}\right)$

Sums of Three Squares IV

Dirichlet's Theorem on Primes in Arithmetic Progressions

For fixed $a, q \in \mathbb{N}$, a, q coprime, there are infinitely many primes of the form $a + qn$, i.e. there are infinitely many primes congruent to $a \bmod q$.

Ex There are infinitely many primes congruent to $1 \pmod 4$ but finitely many primes congruent to $2 \pmod 4$.

Sums of Three Squares V

Lemma 3

Let $n \geq 2$. If there exists a positive integer d' such that $-d'$ is a quadratic residue modulo $d'n - 1$, then n can be represented as the sum of three squares.

Recall that $-d'$ is a quadratic residue modulo $d'n - 1$ if there is some n such that $x^2 = -d' \pmod{d'n - 1}$.

Let $m = d'n - 1$.

- By definition, $\exists x \in \mathbb{Z}$ such that $x^2 \equiv -d' \pmod{m}$. So for some y, we can also say $x^2 = my - d' \implies d' = my - x^2$.
- We assumed in the lemma that $n \geq 2$ and $d' \geq 1$. Thus, $m = d'n - 1 \geq 2d' - 1 \geq 1$.

Sums of Three Squares VI

We can now construct a symmetric matrix A which corresponds to a ternary form F_A which represents n and has discriminant 1. Given this matrix and using the previously stated theorem,

Thm Every positive-definite ternary quadratic form of discriminant 1 is equivalent to the form $x_1^2 + x_2^2 + x_3^2$.

we know that this means n can be written as the sum of three squares. (See Lemma 1.3 in Nathanson for proof that A is also positive-definite).

Sums of Three Squares VII

Lemma 3

Let $n \geq 2$. If there exists a positive integer d' such that $-d'$ is a quadratic residue modulo $d'n - 1$, then n can be represented as the sum of three squares.

$$A = \begin{pmatrix} y & x & 1 \\ x & m & 0 \\ 1 & 0 & n \end{pmatrix}$$

Recall from earlier in the proof that $d' = my - x^2$.

- $\det(A) = (my - x^2)n - m = d'n - m$
- We defined $m = d'n - 1$ and so $\det(A) = 1$.

This matrix has determinant 1 and thus F_A has discriminant 1. If we let x be (0, 0, 1) then $F_A(0, 0, 1) = n$. We are thus done. $\square$

Sums of Three Squares VIII

Lemma 4

If n is a positive integer and $n \equiv 2 \pmod 4$, then n can be represented as the sum of three squares.

Since $4n$ and $n-1$ are coprime, we can use **Dirichlet's Theorem** to say that there are infinitely many primes congruent to $n-1$ mod $4n$.

Choose $j \geq 1$ such that $p = 4nj + n - 1 = (4j+1)n - 1$ is prime. Let $d' = 4j + 1$ and since $n \equiv 2 \pmod 4$,

$$p = d'n - 1 \equiv 1 \pmod 4$$

Sums of Three Squares IX

By **Lemma 3**, we just need to show that $-d'$ is a quadratic residue mod p in order to show that n can be represented as the sum of three squares. If we say that q_i are the distinct primes dividing d', then we have

$$p = d'n - 1 \equiv -1 \pmod{q_i}.$$

This is because p is by definition one less than $d'n$ which is a multiple of any q_i. Thus, $p \equiv -1 \pmod{q_i}$.

Sums of Three Squares X

We can write the prime factorization of d' as a series of $q_i^{k_i}$ where q_i is the underlying prime and k_i is the exponent:

$$d' = \prod_{q_i | d'} q_i^{k_i}$$

By quadratic reciprocity, we have that $(\frac{-1}{p}) = 1$ since $p \equiv 1 \pmod{4}$.

$$(\frac{-d'}{p}) = (\frac{-1}{p})(\frac{d'}{p}) \quad (1)$$

$$= (\frac{d'}{p}) \quad (2)$$

(1) follows because of multiplicativity

Sums of Three Squares XI

$$(\frac{d'}{p}) = \prod_{q_i|d'} (\frac{q_i}{p})^{k_i} \quad (3)$$

$$= \prod_{q_i|d'} (\frac{p}{q_i})^{k_i} \quad (4)$$

$$= \prod_{q_i|d'} (\frac{-1}{q_i})^{k_i} \quad (5)$$

- (3) follows from multiplicativity (each $q_i^{k_i}$ multiplied together equals d').
- (3) to (4) follows since p is 1 (mod 4) $\implies (\frac{q_i}{p}) = (\frac{p}{q_i})$.
- (4) to (5) follows since $p \equiv -1$ (mod q_i) so if p is a quadratic residue so is -1 and vice versa

Sums of Three Squares XII

$$\prod_{q_i|d'}(\frac{-1}{q_i})^{k_i} = \prod_{q_i|d',q_i\equiv 3(mod 4)}(-1)^{k_i} \tag{6}$$

Primes congruent to 3 mod 4 are never residues and thus the Legendre Symbol in that case is always -1.

Sums of Three Squares XIII

$$\prod_{q_i | d', q_i \equiv 3 (mod 4)} (-1)^{k_i} = 1 \qquad (7)$$

$d' = 1$ mod 4 by definition. Further, each of the q_i are 1 or 3 mod 4.

- When $q_i = 3$ (mod 4), $(-1)^{k_i} = 3^{k_i} = q_i^{k_i}$ (mod 4)
- When $q_i = 1$ (mod 4), $q_i^{k_i} = 1^{k_i} = 1$ (mod 4)
- So $d' = q_i^{k_i} \cdot 1 = q_i^{k_i}$ which is equivalent to $(-1)^{k_i}$ for each of the $q_i = 3$ mod 4.

Given this, the product $(-1)^{k_i}$ for each of the $q_i = 3$ mod 4 is congruent to d' which is 1 mod 4. Since $(-1)^{k_i}$ must be 1 or -1 and congruent to 1 mod 4, we see that it must be equal to 1. So $(\frac{-d'}{p}) = 1$ and we are done. □

Sums of Three Squares XIV

Lemma 5

If n is a positive integer such that $n \equiv 1, 3, 5 \pmod{8}$ then n can be represented as the sum of three squares

The proof of this is structurally quite similar to **Lemma 4**. The full proof can be found in Nathanson §1.5 but I will not mention it here for time's sake.

Sums of Three Squares XV

Thm A positive integer N can be represented as the sum of three squares if and only if N is not of the form $N = 4^a(8k+7)$

We first prove ($\implies$), that a sum of three squares can not have the form $N = 4^a(8k+7)$.

We can confirm by hand that only $0, 1, 4$ are quadratic residues modulo 8. ($0^2 = 0, 1^2 = 1, 2^2 = 4$ etc.). Now, consider $N = x^2 + y^2 + z^2 \pmod 8$. We can again manually check that N can only be $0, 1, 2, 3, 4, 5,$ or 6 modulo 8.

Sums of Three Squares XVI

Thm A positive integer N can be represented as the sum of three squares if and only if N is not of the form $N = 4^a(8k+7)$

Let us assume for the sake of contradiction that there does exist a sum of three squares that has form $4^a(8k+7)$. So we assume that we can write N as such: $N = 4^a(8k+7) = x_1^2 + x_2^2 + x_3^2$.

Note that $8k+7 \equiv 7 \pmod{8}$. So if $N = 8k+7$, i.e. $a = 0$, then it cannot be the sum of three squares.

Sums of Three Squares XVII

Thm A positive integer N can be represented as the sum of three squares if and only if N is not of the form $N = 4^a(8k + 7)$

Now, let's consider what happens when we multiply $8k + 7$ by powers of 4. If N could be written as a sum of three squares $x_1^2 + x_2^2 + x_3^2$ and is divisible by 4, then x_1, x_2, x_3 must all be even. This can again be manually verified since we know only $0, 1, 4$ are quadratic residues modulo 8. If any of x_1^2, x_2^2, x_3^2 are not even, i.e. congruent to 1 modulo 8, then it is impossible for their sum to be divisible by 4.

Sums of Three Squares XVIII

Thm A positive integer N can be represented as the sum of three squares if and only if N is not of the form $N = 4^a(8k+7)$

Since x_1, x_2, x_3 are all even we can divide by 4:
$N_1 = 4^{a-1}(8k+7) = (\frac{x_1}{2})^2 + (\frac{x_2}{2})^2 + (\frac{x_3}{2})^2$. We can repeat this process, continually obtaining N_i's as follows:
$N_i = 4^{a-i}(8k+7) = (\frac{x_1}{2^i})^2 + (\frac{x_2}{2^i})^2 + (\frac{x_3}{2^i})^2$

Sums of Three Squares XIX

Thm A positive integer N can be represented as the sum of three squares if and only if N is not of the form $N = 4^a(8k+7)$

We continually divide until we have one of two cases (1) one of the three terms is odd or (2) we cannot divide by 4 any further.

In the case of (1): we have $N_j = 4^{a-j}(8k+7) = (\frac{x_1}{2^j})^2 + (\frac{x_2}{2^j})^2 + (\frac{x_3}{2^j})^2$, where $j < a$ and at least one of $\frac{x_1}{2^j}, \frac{x_2}{2^j}, \frac{x_3}{2^j}$ are odd. This yields a contradiction since if the left side is divisible by 4 then all of $\frac{x_1}{2^j}, \frac{x_2}{2^j}, \frac{x_3}{2^j}$ must be even.

Sums of Three Squares XX

Thm A positive integer N can be represented as the sum of three squares if and only if N is not of the form $N = 4^a(8k+7)$

In the case of (2), i.e. we cannot divide by 4 any further, our expression looks as follows: $N_a = 4^{a-a}(8k+7) = 8k+7 = (\frac{x_1}{2^a})^2 + (\frac{x_2}{2^a})^2 + (\frac{x_3}{2^a})^2$. This again is a contradiction, however, since we know that $(8k+7)$ cannot be represented as the sum of three squares. Thus it is not possible for a sum of three squares to be written in the form $4^a(8k+7)$.

Sums of Three Squares XXI

Thm A positive integer N can be represented as the sum of three squares if and only if N is not of the form $N = 4^a(8k + 7)$

Let's now prove the other direction ($\Longleftarrow$), that is, if N is not of the above form, it can be represented as the sum of three squares.

Sums of Three Squares XXII

Thm A positive integer N can be represented as the sum of three squares if and only if N is not of the form $N = 4^a(8k+7)$

Notice that every positive integer can be written in the form $4^a m$, where m is either $2 \pmod 4$ or $1, 3, 5, 7 \pmod 8$ and 4^a is the highest possible power of 4.

Sums of Three Squares XXIII

Thm A positive integer N can be represented as the sum of three squares if and only if N is not of the form $N = 4^a(8k+7)$

If m is even, then it is not divisible by 4 so it is 2 mod 4 and if m is odd then it is necessarily 1,3,5, or 7 mod 8. We know from proving the ($\Longrightarrow$) direction, that if m can be written as a sum of three squares then so can $4^a m$ (we just multiply x_1, x_2, x_3 each by 2^a).

Sums of Three Squares XXIV

Thm A positive integer N can be represented as the sum of three squares if and only if N is not of the form $N = 4^a(8k+7)$

From **Lemma 5** and **Lemma 6**, we know that if $m = 1, 2, 3, 5, 6$ mod 8, then it can be represented as the sum of three squares.

So for any m that is not equivalent to 7 mod 8, it can be represented as the sum of three squares. Thus, if N is not of the form $4^a(8k+7)$, N can be represented as the sum of three squares and we are done. $\square$