Additive Number Theory Seminar, MATH 3952
Columbia University
Spring 2024
Jinoo Kim

Talk 1

Quadratic Forms, Sums of Three Squares

1 Introduction to Quadratic Forms

In Section 2 we will be working towards a classification of binary quadratic forms. In order to do this we will need to define quadratic forms and understand some of their basic properties.

Consider the ring of $n \times n$ matrices, $M_n(\mathbb{Z})$ and the group of $n \times n$ matrices of determinant 1, $SL_n(\mathbb{Z})$, both of which we saw in Talk 0. We will say that two matrices A and B in $M_n(\mathbb{Z})$ are *equivalent* ($A \sim B$) if $B = A \cdot U = U^T AU$ for some $U \in SL_n(\mathbb{Z})$.

It is easy to see that this relation is symmetric, transitive, and reflexive. Thus, this is an equivalence relation. The equivalence relation preserves determinants since

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

so $A \sim B \implies \det(A) = \det(B)$. It also preserves symmetry of a matrix. One can also think of this as a group action of the special linear group on the set of $n \times n$ matrices.

The important takeaway from this construction is that both the equivalence classes constructed by the equivalence relation and the orbits constructed by the group action partition the set of symmetric matrices in $M_n(\mathbb{Z})$ into equivalence classes based on their determinant. So if you take any equivalence class and any two matrices A, B in that equivalence class, they will have the same determinant.

Definition 1. *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 $F_A(x_1, ..., x_n) = x^T Ax$.

We say that two forms are equivalent if their associated matrices are equivalent and so $A \sim B \iff F_A \sim F_B$. This is again an equivalence relation between two forms.

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 $N, x_1, ..., x_n \in \mathbb{Z}$. If $F_A \sim F_B$, then $A \sim B$ and $\exists U \in SL_n(\mathbb{Z})$ such that $A = B \cdot U = U^T BU$. Recall the column vector x defined above.

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

So any two quadratic forms in the same equivalence class represent the same integers.

Definition 2. *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.*

Definition 3. *A **Binary** quadratic form is over two variables (x_1, x_2) and a **Ternary** quadratic form is over three.*

2 Binary Quadratic Forms

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 each other.

Definition 4. *The **discriminant** of the quadratic form F_A is the determinant of the matrix A.*

As a general sketch of the proof, we will first be defining a set of necessary and sufficient conditions on the matrix A in order for F_A to be positive-definite (**Lemma 1**). We will then show that every equivalence class of positive-definite binary quadratic forms of a fixed discriminant contains at least one form whose associated matrix A satisfies another set of conditions (**Lemma 2**). Finally we will show that for some arbitrary form of discriminant 1, since it is equivalent to a form of discriminant whose associated matrix satisfies the conditions outlined in **Lemma 2**, it must be equivalent to the form $x_1^2 + x_2^2$. That is **Theorem 1**.

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 discrimnant d satisfies*

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

• **Pf.** If F_A is positive-definite, when we evaluate $F_A(1, 0) = a_{1,1}$, it must be ≥ 1.

Further, we can evaluate $F_A(-a_{1,2}, a_{1,1}) = a_{1,1}(a_{1,1}a_{2,2} - a_{1,2}^2) = a_{1,1}d \geq 1$. Thus, $d \geq 1$ since it must be an integer and if it was 0 or negative, then $F_A(-a_{1,2}, a_{1,1})$ would be 0 or negative.

Doing the other direction, if $a_{1,1} \geq 1$ and $d \geq 1$, then

$$a_{1,1}F_A(x_1, x_2) = (a_{1,1}x_1 + a_{1,2}x_2)^2 + dx_2^2 \geq 0$$

and $F_A(x_1, x_2) = 0$ if and only if $(x_1, x_2) = (0, 0)$. Thus, if $a_{1,1} \geq 1$ and $d \geq 1$, F_A is positive definite. □

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

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

• **Pf.** Let's use the same F_A and matrix A as in Lemma 1.

Let $b_{1,1}$ be the smallest positive integer represented by F_A. Then there exists r_1, r_2 such that $F_A(r_1, r_2) = b_{1,1}$. If a positive integer h divides both r_1 and r_2 then $b_{1,1} \leq F_A(r_1/h, r_2/h) = \frac{F_A(r_1,r_2)}{h^2} = \frac{b_{1,1}}{h^2} \leq b_{1,1}$. Thus, $h = 1$ (because $b_{1,1}$ is minimal) and (r_1, r_2) are coprime. We can then use Bezout's identity to write

$$1 = r_1 s_2 - r_2 s_1 = r_1(s_2 + r_2 t) - r_2(s_1 + r_1 t)$$

for all integers t and for some integers s_1, s_2. This allows us to construct the following matrix:

$$U = \begin{pmatrix} r_1 & s_1 + r_1 t \\ r_2 & s_2 + r_2 t \end{pmatrix} \in SL_2(\mathbb{Z})$$

Let $B = U^T A U$ so that

$$B = \begin{pmatrix} F_A(r_1, r_2) & b'_{1,2} + F_A(r_1, r_2)t \\ b'_{1,2} + F_A(r_1, r_2)t & F_A(s_1 + r_1 t, s_2 + r_2 t) \end{pmatrix} = \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{1,2} & b_{2,2} \end{pmatrix}$$

We can define

$$b'_{1,2} = b_{1,1} r_1 s_1 + b_{1,2}(r_1 s_2 + r_2 s_1) + b_{2,2} r_2 s_2$$
$$b_{1,2} = b'_{1,2} + b_{1,1} t$$
$$b_{2,2} = F_A(s_1 + r_1 t, s_2 + r_2 t) \geq b_{1,1}$$

This last fact follows from the fact that $b_1, 1$ is the smallest positive number represented by F_A. Now, we can try and formulate the inequality that we are trying to prove.

We know that $|b_{1,2}| = |b'_{1,2} + b_{1,1} t|$. There must exist t such that $|b'_{1,2} + b_{1,1} t| \leq \frac{b_{1,1}}{2}$ because $b_{1,1}$ is positive and thus the t variable can be adjusted as needed in order to ensure $b'_{1,2} + b_{1,1} t$ is in $(-\frac{b_{1,1}}{2}, \frac{b_{1,1}}{2})$. So we have $|b_{1,2}| \leq \frac{b_{1,1}}{2}$. We further have that $2|b_{1,2}| \leq b_{1,1}$ (so this completes one half of the inequality we need to prove) and we already know that $b_{1,1} \leq b_{2,2}$.

We already declared $B = U^T A U$ so $A \sim B$ and thus F_A is equivalent to F_B as defined in the lemma and it is true for F_B that $2|b_{1,2}| \leq b_{1,1} \leq b_{2,2}$.

Let $d = \det(B)$ or the discriminant of F_B. It is then true that

$$b_{1,1}^2 \leq b_{1,1} b_{2,2} = d + b_{1,2}^2 \leq d + \frac{b_{1,1}^2}{4}$$

because $b_{1,1} \leq b_{2,2}$ and $2|b_{1,2}| \leq b_{1,1} \implies 4|b_{1,2}|^2 \leq b_{1,1}^2 \implies b_{1,2}^2 \leq \frac{b_{1,1}^2}{4}$.

This then implies that $\frac{3a_{1,1}^2}{4} \leq d \implies a_{1,1} \leq \frac{2}{\sqrt{3}}\sqrt{d}$ $\square$

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

• **Pf.** Let F be a 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

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

Since $a_{1,1} \geq 1$, we must have $a_{1,1} = 1$. This implies that $a_{1,2} = 0$. Since the discriminant is 1, it follows that $a_{2,2} = a_{1,1}a_{2,2} - a_{1,2}^2 = 1$.

Thus, the form F is equivalent to $x_1^2 + x_2^2$ and we are done. □

3 Ternary Quadratic Forms

We will now give an analogous classification of ternary quadratic forms. Having already gone through the full proof of the classification of Binary Quadratic Forms, I will omit most of the details of this classification (these can be found in Nathanson §1.4).

A similar pattern is followed as for binary quadratic forms, however. First, a set of necessary and sufficient conditions for a form to be considered positive definite is defined. Second, we use this to show that within each equivalence class of positive-definite ternary forms for a certain discriminant, there is at least one form whose associated matrix satisfies certain conditions. Finally, we show **Thm. 2**.

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

4 Sums of Three Squares

We require three 'ingredients' to classify integers that can be written as the sum of three squares. We will, of course, use **Thm. 2**, as well as Gauss's law of quadratic reciprocity (**Thm. 3**), and Dirichlet's theorem on primes in arithmetic progressions (**Thm. 4**).

Definition 5. *If a is a* ***Quadratic Residue*** *modulo m, it means that there exist integers x and y such that $x^2 - a = ym$.*

Theorem 3 (Gauss)**.** *Let p and q be distinct odd prime numbers, and define the Legendre symbol as:*

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

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

Theorem 4 (Dirichlet)**.** *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 mod q.*

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.*

• **Pf.** By definition $\exists x, y \in \mathbb{Z}$ s.t. $x^2 + d' = y(d'n - 1) = ym$. We know that $m = d'n - 1 \geq 2d' - 1 \geq 1$ since $n \geq 2$ and $d' \geq 1$.

We can also see that $d' = ym - x^2$. We can now construct a symmetric matrix A which corresponds to a ternary form F_A which represents n and has discriminant 1. From **Theorem 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).

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

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. □

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

• **Pf.** Since $4n$ and $n - 1$ are coprime, we can use **Theorem 4** 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 $n \equiv 2 \pmod 4$,

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

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, $p \equiv -1 \pmod{q_i}$.

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

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

$\prod_{q_i|d'} (\frac{-1}{q_i})^{k_i} = \prod_{q_i|d', q_i \equiv 3 (mod 4)} (-1)^{k_i}$ results from the fact that primes congruent to 3 mod 4 are never residues and thus the Legendre Symbol in that case is always -1.

$\prod_{q_i|d', q_i \equiv 3 (mod 4)} (-1)^{k_i} = 1$ is true because of the following.

$d' = 1$ mod 4 by definition. Note that $(-1)^{k_i} = 3^{k_i} = q_i^{k_i} \pmod 4$ when $q_i = 3$ mod 4. Now, consider the alternate case where $q_i = 1$ mod 4. Then $q_i^{k_i} = 1^{k_i} = 1$ mod 4. So $d' = q_i^{k_i}$ 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. □

Lemma 5. *If n is a positive integer such that $n \equiv 1, 3, 5$ (mod 8) then n can be represented as the sum of three squares*

The proof of this is structurally quite similar to **Lemma 4**. We use **Theorem 4** to obtain an algebraic expression of some prime. We then use **Lemma 3** to reduce the problem to showing that $-d'$ is a quadratic residue. Showing this is slightly more complicated but still only involves the Legendre symbol/quadratic reciprocity and properties of factorization. The full proof can be found in Nathanson §1.5 but I will not mention it here for time's sake.

Theorem 5 (Legendre)**.** *A positive integer N can be represented as the sum of three squares if and only if N is not of the form $N = 4^a(8k + 7)$.*

• **Pf.** 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 $N = x^2 + y^2 + z^2$ (mod 8). We can again manually check that N can only be $0, 1, 2, 3, 4, 5$, or 6 modulo 8.

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 $8k + 7 \equiv 7$ (mod 8). So if $N = 8k + 7$, i.e. $a = 0$, then it cannot be the sum of three squares.

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.

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: $N_i = 4^{a-i}(8k + 7) = (\frac{x_1}{2^i})^2 + (\frac{x_2}{2^i})^2 + (\frac{x_3}{2^i})^2$

We continually divide until either at least one of the three terms is odd and/or we cannot divide by 4 any further. If we cannot divide by 4 any further, our expression looks as follows: $N_a = 4^{a-a}(8k + 7) = (\frac{x_1}{2^a})^2 + (\frac{x_2}{2^a})^2 + (\frac{x_3}{2^a})^2$. This is a contradiction, however, since we know that $(8k + 7)$ cannot be represented as the sum of three squares. If one of the terms is odd, then 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 again 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. Thus it is not possible for a sum of three squares to be written in the form $4^a(8k + 7)$.

To prove the other direction ($\impliedby$), we notice that every positive integer can be written in the form $4^a m$, where m is either 2 (mod 4) or $1, 3, 5, 7$ (mod 8) and 4^a is the highest possible power of 4. 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 ($\implies$) 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).

From **Lemma 5** and **Lemma 6**, we know that if $m = 1, 2, 3, 5, 6 \bmod 8$, then it can be represented as the sum of three squares. Since m cannot be divisible by 4, it is not possible for m to be 0 or 4 mod 8. So that means 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. $\square$