Binary Quadratic Forms

By: Fahad Hossaini

Basics

A linear Diophantine equation is of the form:

$ax + by = c$ where $a, b, c \in \mathbb{Z}$ are given. The variables are $x, y \in \mathbb{Z}$.

The classification of these equations is fully determined by basic number theory and the Euclidean Algorithm.

In some sense, the 'way' to the solution pops out as a very natural consequence of a known theorem.

What does Binary Quadratic Form mean?

Binary: Two variables.

Quadratic: Degree two.

Form: Homogeneous polynomial.

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

Once again, we might want to classify these forms. When do we have a solution?

The Problem

These equations are harder to work because of that ‘quadratic’ part.

But we still have a nice classification.

Gauss was the first one who really investigated this stuff, and came up with some remarkable results which we’ll show!

Representations and Discriminants

Representing n

We say that a binary quadratic form (primatively) represents n if there exists some coprime pair x, y so that $ax^2 + bxy + cy^2 = n$.

Now, the discriminant of a binary quadratic form: $D(f(x,y)) = b^2 - 4ac$.

Why do we care about the discriminant? It turns out to be very important, and as the talk proceeds, we'll see where it shows up.

We say that a binary quadratic form (primatively) represents n if there exists some coprime pair x, y so that $ax^2 + bxy + cy^2 = n$.

Now, the discriminant of a binary quadratic form: $D(f(x, y)) = b^2 - 4ac$.

Why do we care about the discriminant? It turns out to be very important, and as the talk proceeds, we'll see where it shows up.

The key theorem: If n is represented by some form $f(x, y)$, then d is a square mod $4n$, or, $d^2 \in \mathbb{Z}_{4n}$.

Let's set $f_1(x, y) = x^2 + xy + y^2$ and $f_2(x, y) = x^2 + 3xy + 2y^2$.

Then, $D(f_1) = -3$ and $D(f_2) = 1$.

Note that 1 is always a square regardless of what n is. So, $n = 12$ possibly has a solution, and we don't break any laws of math.

Indeed, $f_2(2, 1) = 4 + 6 + 2 = 12$

Let's set $f_1(x, y) = x^2 + xy + y^2$ and $f_2(x, y) = x^2 + 3xy + 2y^2$.

Then, $D(f_1) = -3$ and $D(f_2) = 1$.

Note that 1 is always a square regardless of what n is. So, $n = 12$ possibly has a solution, and we don't break any laws of math.

Indeed, $f_2(2, 1) = 4 + 6 + 2 = 12$

What about -3?

Indeed, when $n = 3$, $-3 \equiv 9 \bmod 12$, so, n could possibly be represented by $f_1(x, y)$. Indeed, $f_1(1, 1) = 3$.

When $n = 4$, $-3 \equiv 13 \bmod 16$. By trial and error, 13 is not a square mod 16, so by contrapositive, n cannot be represented by this form. But what about other forms?

As always, we ask the question: is the converse true? Place your bets.

Indeed, when $n = 3$, $-3 \equiv 9 \bmod 12$, so, n could possibly be represented by $f_1(x, y)$. Indeed, $f_1(1, 1) = 3$.

When $n = 4$, $-3 \equiv 13 \bmod 16$. By trial and error, 13 is not a square mod 16, so by contrapositive, n cannot be represented by this form. But what about other forms?

As always, we ask the question: is the converse true? Place your bets.

Not exactly! The proper converse is: If d is a square mod $4n$, then n is represented by some form with discriminant d.

Equivalence

Motivating Equivalence

The first thing we want to do is form some sort of ‘equivalence’ between different quadratic forms.

Change of Variables

There are a few ways to transform a form to maintain the discriminant:

1. Replace x with $-x$
2. Replace x with $x + By$
3. Swap x and y

Let's work through an example: Replace x with $x + y$:

Worked Example

So, we have: $f(x, y) = ax^2 + bxy + cy^2$.

After the change of variables, we get:

$$\begin{aligned} f(x+y, y) &= a(x+y)^2 + b(x+y)y + cy^2 \\ &= ax^2 + (2a+b)xy + (a+b+c)y^2 \end{aligned}$$

So, we have: $f(x,y) = ax^2 + bxy + cy^2$.

After the change of variables, we get:

$$\begin{aligned} f(x+y,y) &= a(x+y)^2 + b(x+y)y + cy^2 \\ &= ax^2 + (2a+b)xy + (a+b+c)y^2 \end{aligned}$$

The main thing: The discriminant stays unchanged!

In some way, the discriminant is an 'invariant.'

Also, the greatest common divisor of the coefficients of f stays the same.

Discriminant as an Invariant

So, what are all the transformations that preserve the discriminant?

Discriminant as an Invariant

So, what are all the transformations that preserve the discriminant?

Let $x \to Ax + By$ and $y \to Cx + Dy$. Maybe that helps...

Discriminant as an Invariant

So, what are all the transformations that preserve the discriminant?

Let $x \to Ax + By$ and $y \to Cx + Dy$. Maybe that helps...

One more hint: $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$

Discriminant as an Invariant

So, what are all the transformations that preserve the discriminant?

Let $x \to Ax + By$ and $y \to Cx + Dy$. Maybe that helps...

One more hint: $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$

We need this matrix to have determinant 1. So, in particular, the group $SL_2(\mathbb{Z})$ 'acts' on the set of Binary Quadratic Forms in such a way that we preserve the numbers representable by forms (the values of x and y might be different though).

This is the Gauss Composition Law.

Inequivalent Forms

Not all forms are equivalent! Let's take a specific example, $D = -12$.

Let $f_1(x, y) = 2x^2 + 2xy + 2y^2$ and $f_2(x, y) = x^2 + 3y^2$.

The first form is always even, but the second one isn't! So, despite having the same discriminant, they fall into different equivalence classes.

Inequivalent Forms

Not all forms are equivalent! Let's take a specific example, $D = -12$.

Let $f_1(x, y) = 2x^2 + 2xy + 2y^2$ and $f_2(x, y) = x^2 + 3y^2$.

The first form is always even, but the second one isn't! So, despite having the same discriminant, they fall into different equivalence classes.

One more for the road!

Let $D = -15$, $f_3(x, y) = 2x^2 + xy = 2y^2 . f_4(x, y) = x^2 + xy + 4y^2$.

We can represent 1 with the latter form, but not the former.

Minimality

Finding a Good Representative

We want to find a good representative for a given discriminant.

We'll do so by the following: Minimize a and b

For example, we can minimize $2x^2 + 10xy + 13y^2$ to $x^2 + y^2$ (trust me on this one)

Finding a Good Representative

We want to find a good representative for a given discriminant.

We'll do so by the following: Minimize a and b

For example, we can minimize $2x^2 + 10xy + 13y^2$ to $x^2 + y^2$ (trust me on this one)

We say a form is reduced if: $|b| \leq |a| \leq |c|$. Indeed, if $|a| \leq |c|$, then applying the transformation $x \to x + ny$ for a suitable n shows that $-|a| \leq |b| \leq |a|$

Simplifying Assumptions

At this point, we should mention: Negative discriminants are *much* nicer to work with. So, that's where the focus of the talk will rest!

Finiteness

We'll show that there are only finitely many reduced forms for a given negative discriminant (assuming $a > 0$ and $c > 0$).

Finiteness

We'll show that there are only finitely many reduced forms for a given negative discriminant (assuming $a > 0$ and $c > 0$).

Proof: Let $b^2 - 4ac = d < 0$ and the form be reduced, so that $|b| \leq |a| \leq |c|$.

We have the following:

$3a^2 = 4a^2 - a^2 \leq 4ac - b^2 = -d$, so, $a \leq \sqrt{-\frac{d}{3}}$

So, there are finitely many values for a and therefore, b as well.

Finally, $c = \frac{-d+b^2}{a}$ so c is determined by a, b, d. ∎

Specific Discriminants

Note that we care when the discriminant is negative.

Note that: $d = b^2 - 4ac \equiv b^2 \bmod 4$.

Thus, $d \equiv 0, 1 \bmod 4$.

So, let's take on a few examples!

We'll always start the same: $3a^2 \leq |d| \Rightarrow a = \pm 1$.

We always take $a > 0$ and $c > 0$. So, $b = 1$ and thus $c = 1$.

The possibilites are: $x^2 + xy + y^2$ and $x^2 - xy + y^2$.

But these are equivalent by swapping x and $-y$.

Since we only have one equivalence class of forms, we know that n is representable by every form with discriminant $d = -3$ if and only if -3 is a square mod $4n$.

-3 is a square mod $4n$ if and only if -3 is a square mod n (as $4n \equiv n \bmod 3$).

What primes are representable by this class of forms?

-3 is a square mod $4n$ if and only if -3 is a square mod n (as $4n \equiv n \bmod 3$).

What primes are representable by this class of forms?

-3 is a square mod p if and only if $p \equiv 0, 1 \bmod 3$ (result from quadratic reciprocity).

So, $p = 19$ is representable. Indeed, $19 = 3^2 + 3 \cdot 2 + 2^2$.

-3 is a square mod $4n$ if and only if -3 is a square mod n (as $4n \equiv n \bmod 3$).

What primes are representable by this class of forms?

-3 is a square mod p if and only if $p \equiv 0, 1 \bmod 3$ (result from quadratic reciprocity).

So, $p = 19$ is representable. Indeed, $19 = 3^2 + 3 \cdot 2 + 2^2$.

A smart change of variables and case analysis shows that the form $x^2 + 3y^2$ represents the same set of numbers. This form is reduced and has discriminant -12. So:

A prime is of the form $x^2 + 3y^2$ if and only if $p \equiv 0, 1 \bmod 3$.

Ok, we'll use a cool trick for this one!

We know $3a^2 < |d| \Rightarrow a = \pm 1$.

But b has to be even for $d \equiv 0 \bmod 4$. so in fact, $b = 0$.

Thus, the only reduced form is: $x^2 + y^2$

-4 is a square mod $4n$ if and only if -4 is a square mod n, because -4 is a square mod 4.

Finally, given a prime p, -4 is a square mod p if and only if $p \equiv 1, 2 \bmod 4$.

This is an alternative proof of Fermat's Sum of Two Squares theorem!

Indeed, $113 = 64 + 49$.

$3a^2 < |12| \Rightarrow a = \pm 1, \pm 2$. Also, remember, b must be even!

1. $a = 1, b = 0$, we get: $x^2 + 3y^2$
2. $a = 2, b = -2, 0, 2$, we get: $2x^2 \pm 2xy + 2y^2$. Both are equivalent.

In case 2, when $b = 0, 4ac = -12$ and $c \notin \mathbb{Z}$.

$3a^2 < |12| \Rightarrow a = \pm 1, \pm 2$. Also, remember, b must be even!

1. $a = 1, b = 0$, we get: $x^2 + 3y^2$
2. $a = 2, b = -2, 0, 2$, we get: $2x^2 \pm 2xy + 2y^2$. Both are equivalent.

In case 2, when $b = 0$, $4ac = -12$ and $c \notin \mathbb{Z}$.

In this case, we have two different equivalent forms. So, if -12 is a square mod $4n$, we need to do more case analysis!

Indeed, if n is odd, it can't be represented by any form equivalent to the second case.

$3a^2 \leq |-163| \Rightarrow 0 \leq a \leq 7$. Note that b must be odd.

Note that: $ac = \frac{163+b^2}{4}$, so when $b = 1, 3, 5, 7$, we get that $ac = 41, 43, 47, 53$. Since all are prime, we must have that $a = 1$ since $|a| \leq |c|$.

Finally, $b = \pm 1$, but we end up with an equivalent form: $x^2 + xy + 41y^2$.

d = −163

$3a^2 \leq |-163| \Rightarrow 0 \leq a \leq 7$. Note that b must be odd.

Note that: $ac = \frac{163+b^2}{4}$, so when $b = 1, 3, 5, 7$, we get that $ac = 41, 43, 47, 53$. Since all are prime, we must have that $a = 1$ since $|a| \leq |c|$.

Finally, $b = \pm 1$, but we end up with an equivalent form: $x^2 + xy + 41y^2$.

This is the smallest discriminant with a unique equivalence class of forms.

Heegner Numbers

The list of discriminants with unique forms: $\{-3, -4, -7, -8, -11, -19, -43, -67, -163\}$

These are called Heegner numbers. Here are two fun facts:

1. $x^2 + x + 41$ is prime for $0 \leq x < 40$ (generates $41, 43, 47, 53$)
2. $e^{\pi\sqrt{163}} = 262537412640768743.99999999999925...$

Finally, we'll look at a positive discriminant and try to see where differences occur.

We can't use the trick that $3a^2 \leq d$, but we use a more naive estimate, $4a^2 \leq d$.

In this case, $a = \pm 1$ and $b = \pm 1$.

Finally, we'll look at a positive discriminant and try to see where differences occur.

We can't use the trick that $3a^2 \leq d$, but we use a more naive estimate, $4a^2 \leq d$.

In this case, $a = \pm 1$ and $b = \pm 1$.

We get four forms: $x^2 + xy - y^2, x^2 - xy - y^2, -x^2 + xy + y^2, -x^2 - xy + y^2$.

It's harder to tell if all of these are equivalent or not, right!

Finally, we'll look at a positive discriminant and try to see where differences occur.

We can't use the trick that $3a^2 \leq d$, but we use a more naive estimate, $4a^2 \leq d$.

In this case, $a = \pm 1$ and $b = \pm 1$.

We get four forms: $x^2 + xy - y^2, x^2 - xy - y^2, -x^2 + xy + y^2, -x^2 - xy + y^2$.

It's harder to tell if all of these are equivalent or not, right!

Indeed, they are all equivalent!

Examples

We'll use the form: $x^2 + xy - y^2$

We need 5 to be a square mod $4n$. Indeed, if n is prime, we only need 5 to be a square mod n.

This is the same as saying $p \equiv 1, 4 \bmod 5$ or $p = 5$.

Examples

We'll use the form: $x^2 + xy - y^2$

We need 5 to be a square mod $4n$. Indeed, if n is prime, we only need 5 to be a square mod n.

This is the same as saying $p \equiv 1, 4 \bmod 5$ or $p = 5$.

So, $29 = 5^2 + 5 \cdot 1 - 1$

And $131 = 11^2 + 11 \cdot 1 - 1$

When $d = -8$, we get the form $2x^2 - y^2$.

Turns out representations need not be unique for positive discriminants!

When $d = -8$, we get the form $2x^2 - y^2$.

Turns out representations need not be unique for positive discriminants!

Indeed, $7 = 2 \cdot 4 - 1 = 2 \cdot 16 - 25 = 2 \cdot 64 - 121$.

But for negative discriminants, we can get uniqueness! Indeed, the sum of two squares is a unique identity!

When $d = -8$, we get the form $2x^2 - y^2$.

Turns out representations need not be unique for positive discriminants!

Indeed, $7 = 2 \cdot 4 - 1 = 2 \cdot 16 - 25 = 2 \cdot 64 - 121$.

But for negative discriminants, we can get uniqueness! Indeed, the sum of two squares is a unique identity!

We still don't know if there are infinitely many discriminants with only one equivalence class.

But we think it should be infinite!

We’re Done!

Acknowledgements

This talk’s content is mainly pulled from Richard E. Borcherd’s Number Theory playlist (He won the Fields medal! Cool guy).