Math 4527 (Number Theory 2)

Lecture #35 of 37 $\sim$ April 15, 2021

Binary Quadratic Forms, Part 1

- Binary Quadratic Forms
- Representations of Integers
- Equivalence of Forms

This material represents §9.2.3 from the course notes.

Binary Quadratic Forms, I

We will now discuss representations of integers by binary quadratic forms, which are expressions of the form $ax^2 + bxy + cy^2$ for fixed integers a, b, c.

- We have already classified the integers that are represented by the forms $x^2 + y^2$, $x^2 + 2y^2$, $x^2 + xy + y^2$, and $x^2 + 3y^2$ using unique factorization in the quadratic integer rings $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$, and $\mathcal{O}_{\sqrt{-3}}$.
- Our goal is now to broaden our focus and analyze integers represented by other quadratic forms.

Binary Quadratic Forms, II

First, some terminology:

Definition

The discriminant of the binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ is $\Delta = b^2 - 4ac$. We also classify the behavior of f based on its values:

- *If f takes both positive and negative values on $\mathbb{R}$, f is indefinite.*
- *If f takes only nonnegative values, f is positive semidefinite.*
- *If in addition $f = 0$ only when $(x, y) = (0, 0)$, f is positive definite.*
- *Finally, f is negative semidefinite (respectively, negative definite) if $-f$ is positive semidefinite (respectively, positive definite).*

Binary Quadratic Forms, III

Most of these behaviors are determined by the discriminant.

- If $D > 0$ then f has two real roots (they are rational iff Δ is a perfect square), while if $\Delta = 0$ then f has a repeated (rational) root, and if $D < 0$ then f has no real roots. Thus:
- f is indefinite precisely when $\Delta > 0$.
- f is definite precisely when $\Delta < 0$: it is positive definite for $a > 0$ and negative definite for $a < 0$.
- f is semidefinite but not definite when $\Delta = 0$: it is positive semidefinite when $a + c > 0$ and negative semidefinite when $a + c < 0$.

Binary Quadratic Forms, IV

Examples:

1. The forms $x^2 - y^2$ ($\Delta = 4$), xy ($\Delta = 1$), and $x^2 - 5xy + y^2$ ($\Delta = 21$) are all indefinite.
2. The forms $x^2 + y^2$ ($\Delta = -4$), $x^2 + 2xy + 3y^2$ ($\Delta = -8$), x^2 ($\Delta = 0$), and $x^2 + 2xy + y^2$ ($\Delta = 0$) are all positive semidefinite. The first two are positive definite while the last two are not.
3. The forms $-x^2 + 2xy - 2y^2$ ($\Delta = -4$) and $-4x^2 - 6xy - 9y^2$ ($\Delta = 0$) are both negative semidefinite. The first is negative definite while the second is not.

Binary Quadratic Forms, V

We will observe that the discriminant Δ of any quadratic form is always congruent to 0 or 1 modulo 4, so it is always the discriminant of a quadratic integer ring up to a square factor.

- Conversely, if Δ is 0 or 1 modulo 4 and is squarefree up to a factor of 4, then the norm $N(x + y\omega)$ where ω is the generator of the quadratic integer ring $\mathcal{O}_{\sqrt{D}}$ ($\sqrt{D}$ or $\frac{1+\sqrt{D}}{2}$) gives a quadratic form of discriminant Δ. In this case, Δ is simply the discriminant of the ring $\mathcal{O}_{\sqrt{D}}$ itself.

You'll doubtless be shocked when I tell you later about a bunch of other deep connections between the quadratic integer rings and the binary quadratic forms we are discussing.

Binary Quadratic Forms, VI

Now we can discuss representations of integers by quadratic forms:

Definition

If f is a binary quadratic form and $n \in \mathbb{Z}$, we say f represents n if there exist integers x and y such that $f(x, y) = n$, and we say f properly represents n if these x, y are also relatively prime.

Examples:

1. $f = x^2 + y^2$ represents 2, 9, and 13, but it does not properly represent 9 because there is no solution to $x^2 + y^2 = 9$ with x, y relatively prime.
2. $f = x^2 + xy + y^2$ represents 3, 4, and 7, but it does not properly represent 4 because there is no solution to $x^2 + xy + y^2 = 4$ with x, y relatively prime.

Binary Quadratic Forms, VII

Ultimately, we would like to be able to classify the integers represented (or properly represented) by a given quadratic form.

- This turns out to be an incredibly difficult problem, and we will not be able to fully address the question in this class, since one really needs the full power of class field theory to make major headway[1].
- Nonetheless, we will still be able to say quite a few substantial things, particularly when we restrict our attention to representations of primes.

[1] I will mention that there is an entire *book* on ostensibly the easiest case of this question, titled "Primes of the form $x^2 + ny^2$"

Binary Quadratic Forms, VIII

We will generally adopt the approach of fixing the discriminant and considering all forms of that discriminant.

Proposition (Representations by Forms of Discriminant Δ)

Suppose Δ is a nonzero integer congruent to 0 or 1 modulo 4.

1. *If n is a nonzero integer, then there exists a binary quadratic form of discriminant Δ that properly represents n if and only if D is a quadratic residue modulo $4n$.*
2. *If p is an odd prime, then there exists a binary quadratic form of discriminant Δ that represents p if and only if Δ is a quadratic residue modulo p.*

Binary Quadratic Forms, IX

1. If n is a nonzero integer, then there exists a binary quadratic form of discriminant Δ that properly represents n if and only if D is a quadratic residue modulo $4n$.

Proof:

- First suppose that Δ is a quadratic residue modulo $4n$, say with $\Delta \equiv b^2 \pmod{4n}$, so that $b^2 - \Delta = 4nc$ for some integer c.
- Then the quadratic form $f(x, y) = nx^2 + bxy + cy^2$ has discriminant $b^2 - 4nc = \Delta$ and it properly represents n since $f(1, 0) = n$.

Binary Quadratic Forms, X

1. If n is a nonzero integer, then there exists a binary quadratic form of discriminant Δ that properly represents n if and only if D is a quadratic residue modulo $4n$.

Proof (converse):

- Conversely, suppose $ax^2 + bxy + cy^2 = n$ with x, y relatively prime and with $b^2 - 4ac = \Delta$. Multiplying by $4a$ and completing the square gives
$4an = 4a^2x^2 + 4abxy + 4acy^2 = (2ax + by)^2 + (b^2 - 4ac)y^2$
so that $(b^2 - 4ac)y^2 \equiv (2ax + by)^2 \pmod{4n}$.
- Therefore, $b^2 - 4ac$ is a quadratic residue modulo $4n/\gcd(y, 4n)$. By a symmetric argument, we see $b^2 - 4ac$ is also a quadratic residue modulo $4n/\gcd(x, 4n)$, and since x, y are relatively prime, this means $b^2 - 4ac$ is a quadratic residue modulo $4n$, as required.

Binary Quadratic Forms, XI

2. If p is an odd prime, then there exists a binary quadratic form of discriminant Δ that represents p if and only if Δ is a quadratic residue modulo p.

Proof:

- Since p is squarefree, any representation of p must automatically be proper.
- Then by (1), we see that p is represented by a form of discriminant Δ if and only if Δ is a quadratic residue modulo $4p$.
- However, since p is odd and Δ is 0 or 1 modulo 4 (hence is a square modulo 4), by the Chinese remainder theorem this is equivalent to saying that Δ is a quadratic residue modulo p.

Binary Quadratic Forms, XII

The results above give an easy way to decide whether there is *some* quadratic form of discriminant Δ that represents a given prime p.

- It therefore stands to reason that if we can understand the structure of the quadratic forms of a given discriminant Δ, then we might be able to determine whether p is represented by a *particular* quadratic form of discriminant Δ.
- As we will show, there actually is quite a lot of structure to the quadratic forms of a particular discriminant.

Binary Quadratic Forms, XII

To begin, we can see that there are simple changes of variable we can perform that do not affect representability.

- For example, the binary quadratic forms $f(x, y) = x^2 + y^2$ and $g(x, y) = f(x - y, y) = x^2 - 2xy + 2y^2$ represent the same integers, since $(x, y) \in \mathbb{Z}^2$ if and only if $(x - y, y) \in \mathbb{Z}^2$.
- The forms $h(x, y) = x^2 + 2y^2$ and $i(x, y) = h(2x + 3y, x + 2y) = 6x^2 + 20xy + 17y^2$ also represent the same integers, since $(x, y) \in \mathbb{Z}^2$ if and only if $(2x + 3y, x + 2y) \in \mathbb{Z}^2$.

On the other hand, not every linear change of variables preserves representability.

- For (counter)example, $f(x, y) = x^2 + y^2$ and $g(x, y) = f(2x, y) = 4x^2 + y^2$ do not represent the same integers (e.g., f represents 2 while g does not).

Binary Quadratic Forms, XIII

The point of these examples is to illustrate that, if we look at values of the quadratic form, we may identify any two quadratic forms that are obtained via a linear change of variables from one another, as long as the change of variables is invertible over $\mathbb{Z}$.

The correct way to keep track of all this is via matrices:

Definition

If $f(x,y) = ax^2 + bxy + cy^2$ is a binary quadratic form, its associated matrix is the symmetric matrix $M_f = \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$.

The connection is that the quadratic form $f(x,y)$ is equal to $\mathbf{x}^T M_f \mathbf{x}$ where $\mathbf{x} = \begin{bmatrix} x \\ y \end{bmatrix}$ is the column vector of the two variables.

Note also that $\det(M_f) = ac - b^2/4 = -\Delta/4$.

Binary Quadratic Forms, XIV

It is then easy to write down how a binary quadratic form f transforms under a change of coordinates $\mathbf{x} \mapsto A\mathbf{x}$.

- Explicitly, we have $f(A\mathbf{x}) = (A\mathbf{x})^T M_f (A\mathbf{x}) = \mathbf{x}^T [A^T M_f A]\mathbf{x}$, and so the associated matrix of the new form is $A^T M_f A$.
- For the purposes of representations of integers, we want only to consider changes of variables $\mathbf{x} \mapsto A\mathbf{x}$ that are a bijection from $\mathbb{Z}^2$ to itself, since this ensures that the possible input vectors $\mathbf{x}$ are the same for both forms. It is easy to see that this is equivalent to saying that A is an invertible matrix with integer entries whose inverse also has integer entries.
- These conditions imply that $\det(A^{-1}) = 1/\det(A) \in \mathbb{Z}$, so A must have determinant ± 1.

Binary Quadratic Forms, XV

Conversely, saying that A is an integer matrix with determinant ± 1 is actually sufficient.

- Explicitly, we can invoke the adjugate inverse formula $A^{-1} = \frac{1}{\det(A)}\mathrm{adj}(A)$, which for 2×2 matrices reads as $\begin{bmatrix} e & f \\ g & h \end{bmatrix}^{-1} = \frac{1}{eh - fg}\begin{bmatrix} h & -f \\ -g & e \end{bmatrix}$, to see that if $\det(A) = \pm 1$, then A^{-1} also has integer entries.
- Thus, the condition of having integer entries and determinant ± 1 is both necessary and sufficient for $\mathbf{x} \mapsto A\mathbf{x}$ to be a bijection from $\mathbb{Z}^2$ to itself.

Binary Quadratic Forms, XVI

For various reasons (primarily, that the resulting theory is much nicer), we will restrict our attention to changes of coordinates with determinant $+1$ only, which yields the matrix group $SL_2(\mathbb{Z}) = \{M \in GL_2(\mathbb{Z}) : \det(M) = 1\}$.

- From our discussion above, for any $A \in SL_2(\mathbb{Z})$, we see that the integers represented by the forms $f(\mathbf{x})$ and $f(A\mathbf{x})$ will be the same, as will the integers properly represented by these two forms.
- Another way to phrase all of this is that we have a group action of $SL_2(\mathbb{Z})$ on the set of binary quadratic forms of discriminant Δ. This action is not faithful, because its kernel is $\{\pm I\}$, so for this reason we often instead act by the group $PSL_2\mathbb{Z} = SL_2\mathbb{Z}/\{\pm I\}$. (This group is called the modular group and has a natural action on the upper half-plane via fractional linear transformations.)

Binary Quadratic Forms, XVII

Now we can talk about equivalence under this group action:

Definition

We define the relation $\sim$ on binary quadratic forms by writing $f \sim g$ if there exists a matrix $A \in SL_2(\mathbb{Z})$ such that $g(\mathbf{x}) = f(A\mathbf{x})$, which is to say that g is obtained from f by an invertible linear change of variables with integer coefficients. Equivalently, $f \sim g$ if there exists $A \in SL_2(\mathbb{Z})$ such that $M_g = A^T M_f A$.

It is not hard to see that $\sim$ is an equivalence relation:

1. To see $f \sim f$, simply take $A = 1$.
2. If $f \sim g$ then $M_g = A^T M_f A$ and so $(A^{-1})^T M_g (A^{-1}) = M_f$ so that $g \sim f$.
3. If $f \sim g$ and $g \sim h$ let $M_g = A^T M_f A$ and $M_h = B^T M_g B$: then $M_h = (AB)^T M_f (AB)$ so $f \sim h$.

Binary Quadratic Forms, XVIII

Examples:

1. The quadratic forms $f(x,y) = x^2 + y^2$ and $g(x,y) = f(x-y,y) = x^2 - 2xy + 2y^2$ have $f \sim g$, since we can take the matrix $A = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \in SL_2(\mathbb{Z})$. For the matrix calculation, we have $M_f = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $M_g = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix}$ and indeed we have $M_g = A^T M_f A$.
2. The quadratic forms $f(x,y) = x^2 + 2xy - y^2$ and $g(x,y) = 7x^2 + 22xy + 17y^2$ have $f \sim g$, since we can take the matrix $A = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix} \in SL_2(\mathbb{Z})$; one may check that $g(x,y) = f(2x+3y, x+2y)$.

Also, if $f \sim g$ then $\det(M_g) = \det(A^T)\det(M_f)\det(A) = \det(M_f)$, so forms in the same equivalence class have the same discriminant.

Binary Quadratic Forms, XIX

Since we are interested in representability of integers by quadratic forms, and representability is the same for different forms in the same equivalence class under $\sim$, our next task is to identify nice representatives for the equivalence classes under $\sim$.

Definition

If $f(x,y) = ax^2 + bxy + cy^2$ is a binary quadratic form whose discriminant Δ is not a square, we say f is reduced when $-|a| < b \leq |a| \leq |c|$, and if $b = |a|$ we also insist that $|a| < |c|$, while if $|a| = |c|$ then we also insist that $b \geq 0$.

Examples:

- The forms $x^2 + y^2$, $x^2 - y^2$, $-3x^2 + 3xy + 4y^2$, and $2x^2 + xy + 3y^2$ are all reduced.
- The forms $x^2 + 2xy$, $xy - 2y^2$, and $2x^2 + 2xy + y^2$ are not reduced.

Binary Quadratic Forms, XX

Using reduced forms we can show that there are finitely many equivalence classes:

Theorem (Reduced Forms)

Let Δ be a nonsquare integer congruent to 0 or 1 modulo 4 and suppose $f(x,y) = ax^2 + bxy + cy^2$ is a reduced form of discriminant Δ. Then the following hold:

1. *If $D < 0$ then a, c must have the same sign and $|a| \leq \sqrt{-\Delta/3}$. If $\Delta > 0$ then a, c have opposite signs and $|a| < \sqrt{\Delta}/2$. In either case, there are finitely many reduced forms of discriminant Δ.*
2. *Every equivalence class of quadratic forms of discriminant Δ contains at least one reduced form.*
3. *There are finitely many equivalence classes of binary quadratic forms of discriminant Δ.*

Binary Quadratic Forms, XXI

1. If $D < 0$ then a, c must have the same sign and $|a| \leq \sqrt{-\Delta/3}$. If $\Delta > 0$ then a, c have opposite signs and $|a| < \sqrt{\Delta}/2$. In either case, there are finitely many reduced forms of discriminant Δ.

Proof:

- If a, c have the same sign, $\Delta = b^2 - 4ac = b^2 - 4|a||c| \leq 0$, while if a, c are opposite, $\Delta = b^2 - 4ac = b^2 + 4|ac| \geq 0$.
- If $\Delta < 0$ then because $|a| \leq |c|$ we see that $\Delta = b^2 - 4|a||c| \leq a^2 - 4a^2 = -3a^2$ so $|a| \leq \sqrt{-\Delta/3}$. If $\Delta > 0$ then again because $|a| \leq |c|$ we see that $\Delta = b^2 + 4|ac| \geq 4a^2$ and so $|a| \leq \sqrt{\Delta}/2$.
- In either case there are finitely many values of a. For each of these values of a, there are only finitely many possible b since $|b| \leq |a|$, and then $c = (b^2 - \Delta)/(4a)$ is determined. Thus, there are only finitely many reduced forms of discriminant Δ.

Binary Quadratic Forms, XXII

2. Every equivalence class of quadratic forms of discriminant Δ contains at least one reduced form.

Motivation:

- The group $SL_2(\mathbb{Z})$ is generated[2] by the matrices $S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.
- The idea is then to show that if we have a non-reduced form, we must be able to apply either S or a power of T to obtain a "smaller" form, and so iterating this procedure must eventually yield a reduced form.

[2] Sketch proof: note that $T^{-q}M$ will subtract q times the second row from the first row, and SM will swap the rows and negate the first one: these (up to the scaling by -1) are precisely the operations in the Euclidean algorithm. Applying it will turn the first column into $[1\,0]^T$, and then the second column must be $[m\,1]^T$ since it is in $SL_2(\mathbb{Z})$. And this matrix is just T^m.

Binary Quadratic Forms, XXIII

2. Every equivalence class of quadratic forms of discriminant Δ contains at least one reduced form.

Proof:

- Suppose $f(x, y) = ax^2 + bxy + cy^2$ has discriminant Δ and has associated matrix M_f.
- Then $S^T M_f S = \begin{bmatrix} c & -b/2 \\ -b/2 & a \end{bmatrix}$ corresponds to the form $cx^2 - bxy + ay^2$, which swaps the x^2- and y^2-coefficients while leaving the absolute value of the xy-coefficient unchanged.
- Also, $(T^m)^T M_f T^m = \begin{bmatrix} a & a + mb/2 \\ a + mb/2 & m^2 a + mb + c \end{bmatrix}$ corresponds to the form $ax^2 + (b + 2am)xy + (am^2 + bm + c)y^2$, which leaves the x^2-coefficient unchanged and shifts the xy-coefficient by $2am$.

Binary Quadratic Forms, XXIV

2. Every equivalence class of quadratic forms of discriminant Δ contains at least one reduced form.

Proof (continued):

- Starting with $f = ax^2 + bxy + cy^2$, loop this algorithm:

(a) If b is not in the interval $(-|a|, |a|]$, let m be the unique integer such that $b + 2am \in (-|a|, |a|]$ and apply T^m to the quadratic form. This yields an equivalent form whose xy-coefficient is $b + 2am \in (-|a|, |a|]$ and whose x^2-coefficient is the same. Then go to step (b).

(b) If b is in the interval $(-|a|, |a|]$, test if $|a| = |c|$. If so and if $b \geq 0$, the form is reduced; otherwise if $b < 0$ then applying S will yield a reduced form. Otherwise, test whether $|a| < |c|$. If so, the form is reduced, and if not, apply S to the quadratic form. This yields an equivalent form whose x^2-coefficient is smaller in absolute value, and return to step (a).

Binary Quadratic Forms, XXV

2. Every equivalence class of quadratic forms of discriminant Δ contains at least one reduced form.

Proof (wrapup):

- After applying the steps once, the form is either reduced or has its x^2-coefficient strictly smaller in absolute value, so iterating the procedure must eventually yield a reduced form.
- Since each application of S or T yields an equivalent form, we conclude that every equivalence class contains at least one reduced form.

---

3. There are finitely many equivalence classes of binary quadratic forms of discriminant Δ.

Proof:

- Each equivalence class contains at least one reduced form by (2), and there are finitely many reduced forms by (1).

Binary Quadratic Forms, XXVI

The algorithm in (2) works to find equivalent reduced forms:

Example: Find a reduced form equivalent to
$f(x, y) = 17x^2 + 99xy - 46y^2$.

Binary Quadratic Forms, XXVI

The algorithm in (2) works to find equivalent reduced forms:

Example: Find a reduced form equivalent to $f(x, y) = 17x^2 + 99xy - 46y^2$.

- First, since $b \notin (-17, 17]$ we find m with $b + 34m \in (-17, 17]$, which gives $m = -3$.
- Applying T^3 yields the equivalent form $g(x, y) = f(x - 3y, y) = 17x^2 - 3xy - 190y^2$.
- Now because $|a| < |c|$, the resulting form $\boxed{17x^2 - 3xy - 190y^2}$ is reduced.

Binary Quadratic Forms, XXVII

Example: Find a reduced form equivalent to $f(x, y) = 119x^2 - 145xy + 17y^2$.

Binary Quadratic Forms, XXVII

Example: Find a reduced form equivalent to $f(x,y) = 119x^2 - 145xy + 17y^2$.

- First, since $b \notin (-119, 119]$ we find m with $b + 238m \in (-119, 119]$, which gives $m = 1$.
- Applying T yields the equivalent form $g(x,y) = f(x+y, y) = 119x^2 + 93xy - 9y^2$.
- Now because $|a| > |c|$ the form is not reduced so we apply S to get the form $h(x,y) = f(-y, x) = -9x^2 - 93xy + 119y^2$.
- Then since $b \notin (-9, 9]$ we find m with $b + 18m \in (-9, 9]$, which gives $m = 5$.
- Applying T^5 yields the equivalent form $i(x,y) = f(x+5y, y) = -9x^2 - 3xy + 359y^2$. Since $|a| < |c|$, this form $\boxed{-9x^2 - 3xy + 359y^2}$ is reduced.

Binary Quadratic Forms, XXVIII

Example: Find a reduced form equivalent to $f(x, y) = 81x^2 - 65xy + 13y^2$.

Binary Quadratic Forms, XXVIII

Example: Find a reduced form equivalent to $f(x, y) = 81x^2 - 65xy + 13y^2$.

- Applying the algorithm yields the following equivalent forms:
- Apply S, yielding $13x^2 + 65xy + 81y^2$.
- Apply T^{-2}, yielding $13x^2 + 13xy + 3y^2$.
- Apply S, yielding $3y^2 - 13xy + 13y^2$.
- Apply T^2, yielding $3y^2 - xy - y^2$.
- Apply S, yielding $-x^2 + xy + 3y^2$, which is reduced.

Binary Quadratic Forms, XXIX

For small values of Δ we can also use the partial description of reduced forms in (2) from the theorem to make a full list of reduced forms.

- By deciding which of these are equivalent to one another, we can then determine the precise number of equivalence classes of forms.

Binary Quadratic Forms, XXX: The Sensual Form

Example: Find all reduced forms of discriminant $\Delta = -4$ and show that there is only one equivalence class of positive-definite forms.

Binary Quadratic Forms, XXX: The Sensual Form

Example: Find all reduced forms of discriminant $\Delta = -4$ and show that there is only one equivalence class of positive-definite forms.

- From the analysis in (2) we see that any reduced form $ax^2 + bxy + cy^2$ of discriminant $\Delta = -4$ must have $|a| \leq \sqrt{4/3}$, so since $a \neq 0$ this means $a = \pm 1$. Then since $|b| \leq |a|$ we have $b = 0, \pm 1$.
- Also, since $c = (b^2 - \Delta)/(4a)$ must be an integer, b must be even. Thus the only possible forms have $a = \pm 1$ and $b = 0$, which yields the two forms $x^2 + y^2$ and its negative $-x^2 - y^2$.
- Therefore, since only $x^2 + y^2$ is positive-definite, it represents the only equivalence class of positive-definite forms.

Binary Quadratic Forms, XXXI

Example: Find all reduced forms of discriminant $\Delta = 13$ and determine the number of equivalence classes.

Binary Quadratic Forms, XXXI

Example: Find all reduced forms of discriminant $\Delta = 13$ and determine the number of equivalence classes.

- From the analysis in (2) we see that any reduced form $ax^2 + bxy + cy^2$ of discriminant $\Delta = 5$ must have $|a| \leq \sqrt{13}/2 < 2$, so since $a \neq 0$ this means $a = \pm 1$. Then since $b \in (-|a|, a)$ we must have $b = 0$ or $b = 1$.
- However, since $c = (b^2 - \Delta)/(4a)$ must be an integer, b must be odd, and so $b = 1$. We then get two possible forms for $a = -1$ and $a = 1$ respectively: $f(x, y) = -x^2 + xy + 3y^2$ and $g(x, y) = x^2 + xy - 3y^2$.
- Although both of these forms are reduced, they are in fact equivalent: if we take the matrix $A = \begin{bmatrix} 2 & -3 \\ 1 & -1 \end{bmatrix}$ then it is straightforward to check that $A^T M_f A = M_g$, and so $f \sim g$.
- Therefore, there is only one equivalence class with $\Delta = 13$.

Binary Quadratic Forms, XXXII

If we can classify all of the binary quadratic forms of a given discriminant, we can often identify exactly which primes may be represented by a given form.

- As we proved earlier, a prime p is (properly) represented by a form of discriminant Δ if and only if Δ is a square modulo p.
- If the equivalence classes of the forms of discriminant Δ are represented by $f_1, f_2, \ldots, f_k$, then (at least) one of the f_i represents p if and only if Δ is a square modulo p.
- In the particular case where there is only one equivalence class, we get a complete characterization of the prime values taken by (any) quadratic form of that discriminant.

Binary Quadratic Forms, XXXIII

Some examples:

- For $\Delta = -4$, p is represented by the unique equivalence class representative $f(x, y) = x^2 + y^2$ if and only if -4 is a square modulo p, which is in turn equivalent to saying that -1 is a square modulo p, which (as we have already noted numerous times) is equivalent to saying that $p \equiv 1 \pmod 4$.
- For $\Delta = 13$, we see that p is represented by the unique equivalence class representative $f(x, y) = x^2 + xy - 3y^2$ if and only if 13 is a square modulo p, which (by quadratic reciprocity) is equivalent to saying that p is a quadratic residue modulo 13, which is to say, when $p = 13$ or when $p \equiv 1, 3, 4, 9, 10, 12 \pmod{13}$.

Summary

We introduced binary quadratic forms, discussed representability and equivalence of forms, and established that there are only finitely many equivalence classes of forms of a given discriminant.

We discussed how to enumerate all reduced forms of a given discriminant.

Next lecture: Composition of forms and the class group.