Lecture 22: Binary Quadratic Forms II
Basic Notions

William Stein

Math 124 HARVARD UNIVERSITY **Fall 2001**

1 Introduction

A *binary quadratic form* is a homogeneous polynomial

$$ax^2 + bxy + cy^2 \in \mathbb{Z}[x, y].$$

(There is a theory of quadratic forms in n-variables, but we will not study it in this course.) Chapter VI of Davenport's book is clear and well written. Read it.

The Classic Problem: Given a binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$, what is the set of integers $\{f(x, y) : x, y \in \mathbb{Z}\}$?

That is, for which integers n are there integers x and y such that

$$ax^2 + bxy + cy^2 = n?$$

We gave a clean answer to this question in the last lecture in the case when $f(x, y) = x^2 + y^2$. The set of sums of two squares is the set of integers n such that any prime divisor p of n of the form $4m + 3$ exactly divides n to an even power (along with 0). In your homework (Problem 5), you will give a simple answer to the question of which numbers are of the form $x^2 + 2y^2$. Is there a simple answer in general?

2 Equivalence

Definition 2.1. The modular group $\mathrm{SL}_2(\mathbb{Z})$ is the group of all 2×2 integer matrices with determinant $+1$.

If $g = \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $f(x, y) = ax^2 + bxy + cy^2$ is a quadratic form, let

$$f|_g(x, y) = f(px + qy, rx + sy) = f\left(\begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{bmatrix} x \\ y \end{bmatrix}\right),$$

where for simplicity we will sometimes write $f\left(\begin{bmatrix} x \\ y \end{bmatrix}\right)$ for $f(x, y)$.

Proposition 2.2. *The above formula defines a right action of the group* $\mathrm{SL}_2(\mathbb{Z})$ *on the set of binary quadratic forms, in the sense that*

$$f|_{gh} = (f|_g)|_h.$$

Proof.

$$f|_{gh}(x,y) = f\left(gh\begin{bmatrix}x\\y\end{bmatrix}\right) = f|_g\left(h\left(\begin{bmatrix}x\\y\end{bmatrix}\right)\right) = (f|_g)|_h(x,y).$$

□

Proposition 2.3. *Let* $g \in \mathrm{SL}_2(\mathbb{Z})$ *and let* $f(x,y)$ *be a binary quadratic form. The set of integers represented by* $f(x,y)$ *is exactly the same as the set of integers represented by* $f|_g(x,y)$.

Proof. If $f(x_0,y_0) = n$ then since $g^{-1} \in \mathrm{SL}_2(\mathbb{Z})$, we have $g^{-1}\begin{bmatrix}x_0\\y_0\end{bmatrix} \in \mathbb{Z}^2$, so

$$f|_g\left(g^{-1}\begin{bmatrix}x_0\\y_0\end{bmatrix}\right) = f(x_0,y_0) = n.$$

Thus every integer represented by f is also represented by $f|_g$. Conversely, if $f|_g(x_0,y_0) = n$, then $f\left(g\begin{bmatrix}x_0\\y_0\end{bmatrix}\right) = n$, so f represents n. □

Define an equivalence relation $\sim$ on the set of all binary quadratic forms by declaring that f is equivalent to f' if there exists $g \in \mathrm{SL}_2(\mathbb{Z})$ such that $f|_g = f'$.

For simplicity, we will sometimes denote the quadratic form $ax^2+bxy+cy^2$ by (a,b,c). Then, for example, since $g = \left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, we see that $(a,b,c) \sim (c,-b,a)$, since if $f(x,y) = ax^2+bxy+cy^2$, then $f(-y,x) = ay^2-bxy+cx^2$.

Example 2.4. Consider the binary quadratic form

$$f(x,y) = 458x^2 + 214xy + 25y^2.$$

Solving the representation problem for f might, at first glance, look hopeless. We find $f(x,y)$ for a few values of x and y:

$$\begin{aligned} f(-1,-1) &= 17\cdot 41\\ f(-1,0) &= 2\cdot 229\\ f(0,-1) &= 5^2\\ f(1,1) &= 269\\ f(-1,2) &= 2\cdot 5\cdot 13\\ f(-1,3) &= 41 \end{aligned}$$

Each number is a sum of two squares! Letting $g = \left(\begin{smallmatrix}4 & -3\\ -17 & 13\end{smallmatrix}\right)$, we have

$$f|_g = 458(4x-3y)^2 + 214(4x-3y)(-17x+13y) + 25(-17x+13y)^2 = \cdots = x^2+y^2!!$$

By Proposition 2.3, f represents an integer n if and only if n is a sum of two squares.

3 Discriminants

Definition 3.1. The *discriminant* of $f(x,y) = ax^2 + bxy + cy^2$ is $b^2 - 4ac$.

Example 3.2. $\mathrm{disc}(x^2 + y^2) = -4$ and

$$\mathrm{disc}(458, 214, 25) = 214^2 - 4 \cdot 25 \cdot 458 = -4.$$

That the discriminants are the same is a good hint that $(1,0,1)$ and $(458,214,25)$ are closely related. Inspecting discriminants is more effective than simply computing $f(x,y)$ for many values of x and y and staring at the result.

Proposition 3.3. *If $f \sim f'$, then* $\mathrm{disc}(f) = \mathrm{disc}(f')$.

Proof. By tedious but elementary algebra (see page 133 of Davenport's book), one sees that if $g \in \mathrm{SL}_2(\mathbb{Z})$, then

$$\mathrm{disc}(f|_g) = \mathrm{disc}(f) \cdot (\det(g))^2 = \mathrm{disc}(f).$$

Since $f' = f|_g$ for some $g \in \mathrm{SL}_2(\mathbb{Z})$, the proposition follows. □

WARNING: The converse of the proposition is false! Forms with the same discriminant need not be equivalent. For example, the forms $(1,0,6)$ and $(2,0,3)$ have discriminant -24, but are not equivalent. To see this, observe that $(1,0,6)$ represents 1, but $2x^2 + 3y^2$ does not represent 1.

Proposition 3.4. *The set of all discriminants of forms is exactly the set of integers d such that $d \equiv 0$ or $1 \pmod 4$.*

Proof. First note that $b^2 - 4ac$ is a square modulo 4, so it must equal 0 or 1 modulo 4. Next suppose d is an integer such that $d \equiv 0$ or $1 \pmod 4$. If we set

$$c = \begin{cases} -d/4, & \text{if } d \equiv 0 \pmod 4 \\ -(d-1)/4 & \text{if } d \equiv 1 \pmod 4, \end{cases}$$

then $\mathrm{disc}(1,0,c) = d$ in the first case and $\mathrm{disc}(1,1,c) = d$ in the second. □

Definition 3.5. The form $(1,0,-d/4)$ or $(1,1,-(d-1)/4)$ of discriminant d that appears in the proof of the previous proposition is called the *principal form* of discriminant d.

d	principal form	
-4	(1,0,1)	$x^2 + y^2$
5	(1,1,-1)	$x^2 + xy - y^2$
-7	(1,1,2)	$x^2 + xy + 2y^2$
8	(1,0,-2)	$x^2 - 2y^2$
-23	(1,1,6)	$x^2 + xy + 6y^2$
389	(1,1,-97)	$x^2 + xy - 97y^2$

4 Definite and Indefinite Forms

Definition 4.1. A quadratic form with negative discriminant is called *definite*. A form with positive discriminant is called *indefinite*.

Let (a, b, c) be a quadratic form. Multiply by $4a$ and complete the square:

$$\begin{aligned} 4a(ax^2 + bxy + cy^2) &= 4a^2x^2 + 4abxy + 4acy^2 \\ &= (2ax + by)^2 + (4ac - b^2)y^2 \end{aligned}$$

If $\mathrm{disc}(a, b, c) < 0$ then $4ac - b^2 = -\mathrm{disc}(a, b, c) > 0$, so $ax^2 + bxy + cy^2$ takes only positive or only negative values, depending on the sign of a. In this sense, (a, b, c) is very definite about its choice of sign. If $\mathrm{disc}(a, b, c) > 0$, then $(2ax+by)^2+(4ac-b^2)y^2$ takes both positive and negative values, so (a, b, c) does also.

We will consider only definite forms in the next two lectures.

5 Real Life

The following text is from the documentation for binary quadratic forms in the MAGMA computer algebra system. A quick scan of the buzzwords emphasized (by me) below conveys an idea of where binary quadratic forms appear in mathematics.

> A binary quadratic form is an integral form $ax^2 + bxy + cy^2$ which is represented in MAGMA by a tuple (a, b, c). Binary quadratic forms play an central role in the *ideal theory of quadratic fields*, the classical theory of *complex multiplication*, and the theory of *modular forms*. Algorithms for binary quadratic forms provide efficient means of computing in the *ideal class group of orders* in a *quadratic field*. By using the explicit relation of definite quadratic forms with lattices with nontrivial endomorphism ring in the complex plane, one can apply *modular and elliptic functions* to forms, and exploit the analytic theory of complex multiplication.
>
> The structures of quadratic forms of a given discriminant D correspond to ordered bases of ideals in an order in a *quadratic number field*, defined up to scaling by the rationals. A form is primitive if the coefficients a, b, and c are coprime. For negative discriminants the primitive reduced forms in this structure are in bijection with the *class group of projective or invertible ideals*. For positive discriminants, the reduced orbits of forms are used for this purpose. Magma holds efficient algorithms for composition, enumeration of reduced forms, *class group computations*, and *discrete logarithms*. A significant novel feature is the treatment of nonfundamental discriminants, corresponding to nonmaximal orders, and the collections of homomorphisms between different class groups coming from the inclusions of these orders.
>
> The functionality for binary quadratic forms is rounded out with various functions for applying modular and elliptic functions to forms, and for *class polynomials* associated to *class groups* of definite forms.