MATH 115, SUMMER 2012
LECTURE 21

JAMES MCIVOR

last time:

- given n and d, there is a form if disc d representing n iff $x^2 \equiv d \mod 4|n|$ has a solution.

- study QFs by studying matrices: a form $f(x,y) = ax^2 + bxy + cy^2$ can be written as

$$f(x,y) = \mathbf{x}^T \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \mathbf{x}$$

- began to talk about integer matrices. invertible iff determinant is ± 1.

1. Equivalent Forms

We will be mostly interested in integer matrices with determinant one. These get a special name.

Definition 1. The group of 2×2 integer matrices with determinant one is called the **modular group**[1], written Γ.

- Here a **group** just means a set in which you can multiply, which has an identity element (the identity matrix), and all elements have inverses.

- we can use the modular group to define precisely when two QFs are " the same"

- notation: let us write an ordered pair of integers (x,y) as the vector $\mathbf{x}$, and write $f(x,y)$ as $f(\mathbf{x})$.

- if we multiply the vector $\mathbf{x}$ by a matrix A in Γ, we get a new pair of integers, which we'll just write simply as $A\mathbf{x}$. Then it makes sense to write $f(A\mathbf{x})$, too.

Definition 2. Let f and q be two binary quadratic forms. We say f and g are **equivalent**, written $f \sim g$, if there is a matrix $A \in \Gamma$ such that for all $\mathbf{x} = (x,y)$, we have $g(\mathbf{x}) = f(A\mathbf{x})$

- relate this to matrix notation: can write a QF $f(x,y)$ as

$$f(x,y) = \mathbf{x}^T M \mathbf{x}$$

for some matrix M (which we can take to be symmetric, as we saw last time)

Similarly

$$g(x,y) = \mathbf{x}^T N \mathbf{x}$$

- so in terms of the matrices M and N associated to f and g, we can say $f \sim g$ if

$$f(A\mathbf{x}) = (A\mathbf{x})^T M A\mathbf{x} = \mathbf{x}^T A^T M A\mathbf{x} = g(\mathbf{x}) = \mathbf{x}^T N \mathbf{x}$$

i.e., if $N = A^T M A$.

[1] It's also sometimes called $SL_2(\mathbb{Z})$.

Proposition 1. *Equivalence of forms is an equivalence relation on the set of all binary QFs.*

Proof. Sort of boring. Maybe skip. Problem session? □

- as mentioned above, equivalent forms represent the same integers. But they also *properly* represent the same integers, which is the nontrivial part of the next thm:

Theorem 1. *If $f \sim g$, and n is an integer, then*

(1) *f represents n if and only if g represents n.*
(2) *f properly represents n if and only if g properly represents n.*
(3) *f and g have the same discriminant.*

Proof. (1) is because, f and g differ by a one-to-one and onto function on the inputs, and this doesn't affect the set of outputs.

(3) follows from the formula last time: if $f(x,y) = \mathbf{x}^T A\mathbf{x}$, then $d = -4\det A$.

- the only really interesting part of the theorem is (2). To prove this, we show that changing variables by an element of the modular group does not affect the gcd of the two coordinates.

- i.e., if $M \in \Gamma$, and $\mathbf{x}_1 = (x_1, y_1)$ and $M\mathbf{x} = (x_2, y_2)$, then $\gcd(x_1, y_1) = \gcd(x_2, y_2)$.

- for this, let $g_1 = \gcd(x_1, y_1)$, and write $\mathbf{x} = (x_1, y_1)$, $M\mathbf{x} = (x_2, y_2)$. Since $g_1 | x_1, y_1$, $(x_1/g_1, y_1/g_1)$ is a lattice point, and so M sends it to a lattice point.

- by linear algebra (matrix multiplication is a linear transformation), we have

$$M \begin{pmatrix} x_1/g_1 \\ y_1/g_1 \end{pmatrix} = \frac{1}{g_1} M\mathbf{x}$$

- this means that g_1 divides both x_2 and y_2, so it divides their gcd.

- we also can write $M^{-1}(x_2, y_2) = \mathbf{x}$ and do the same argument, so the gcd of x_2 and y_2 divides g_1.

- thus the two pairs have gcds which divide one another, so the gcds must be the same.

□

2. Reduced Forms

- since $\sim$ is an equivalence relation, it partitions the set of all QFs into equivalence classes. It would be convenient if there was one special member of each equivalence class, that we could work with.

- there is, if we restrict our attention to only certain forms.

- for the rest of this material, we need to avoid forms whose discriminant is a perfect square - these are called **degenerate**[2], and if the discriminant is not a perfect square, the form is **nondegenerate**. Every positive definite form is nondegenerate (negative numbers are not perfect squares).

- things become nicer still if we consider only positive definite forms: for each equivalence class, there's only one which has the property of being reduced, defined below. DRAW JANKY VENN DIAGRAM.

- The definition is bizarre, but turns out to be useful (in the problem session we'll see a cool geometric interpretation of this condition):

[2]Remember our exercise from the problem session a few days ago - the discriminant is a perfect square iff the quadratic form factors into two linear terms

Definition 3. Let $f(x,y) = ax^2 + bxy + cy^2$ be a positive definite QF. We say f is **reduced** if

(1) $-|a| < b \leq |a| < |c|$, or
(2) $0 \leq b \leq |a|$ and $|a| = |c|$

Example 2.1. We will be increasingly interested in forms of the type

$$f_D = x^2 + Dy^2,$$

where D is some integer.

- for which D is this positive definite?
- for which D is this form reduced?

- As mentioned above, to make sure we have exactly one reduced form in each equivalence class, we must restrict our attention to primitive positive definite forms.
- **Primitive** means the gcd of the coefficients a, b, c of f is 1.
- Then we have the following result, which, as we will see tomorrow, is incredibly powerful.
- it combines theorems 3.18 and 3.19 and 3.25 in your book.

Theorem 2 (The Reduction Theorem)**.** *Let $f(x,y) = ax^2+bxy+cy^2$ be a primitive positive definite QF (integral and binary as usual). Then*

(1) *f is equivalent to a unique reduced form.*
(2) $|b| \leq a \leq \sqrt{-d/3}$
(3) *The number of equivalence classes of positive definite forms of discriminant d is less than or equal to $-2d/3$.*

- note that for a positive definite form, $d < 0$, hence the negative signs on all the d's
- recall that the equivalence relation $\sim$ doesn't affect the discriminant, so it makes sense to speak of "equivalence classes of forms of discriminant d."
- part 1 without the uniqueness claim is Thm 3.18 in the book. part 2 is Thm 3.19, and part 3 is a stronger version of the final claim in that Thm.

Definition 4. The number of equivalence classes of pos def forms of discriminant d is called the **class number** of d, written $H_p(d)$. We use the subscript p, which is different from the book, to indicate we are considering only positive definite forms.

- Thus the third part of the theorem says that $H_p(d) \leq -2d/3$.
- We will not give a complete proof of the theorem, but work out an example to convince ourselves that it's reasonable.
- first we have the following useful fact:

Proposition 2. *The modular group is generated by the matrices*

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

which means that any matrix in the modular group can be written as a product of S and T and their inverses.[3]

[3]If you know some group theory, we can say a little more: Γ has the presentation: $\langle S, T \mid S^2 = (ST)^3 = 1 \rangle$.

- note that $T^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$

- let's do an example to see that given any positive definite form, we can use the matrices S and T to find an equivalent reduced form:

- first fix some terminology, let's call replacing a matrix A by S^TAS, **conjugating** A by S, and similarly for T.

- for us, the matrices A will have the form $A = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$.

- to get a feel for how these matrices act, we first compute the action of conjugation by S, T, and T^{-1}:

$$S^TAS = \begin{pmatrix} c & -b/2 \\ -b/2 & a \end{pmatrix},$$
$$T^TAT = \begin{pmatrix} a & a+b/2 \\ a+b/2 & a+c+b \end{pmatrix},$$
$$(T^{-1})^TAT^{-1} = \begin{pmatrix} a & b/2-a \\ b/2-a & a+c-b \end{pmatrix}$$

Example 2.2. Let $f(x,y) = 5x^2 + 20xy + 21y^2$. Find a reduced form equivalent to f.

Solution: First note in passing that the discriminant of f is $20^2 - 4 \cdot 5 \cdot 21 = -20 < 0$, so f is positive definite.

- first write f in matrix form: $f(x,y) = \mathbf{x}^TA\mathbf{x}$, where

$$A = \begin{pmatrix} 5 & 10 \\ 10 & 21 \end{pmatrix}$$

- It's not reduced: b is 20, which is bigger than $a = 5$

- idea: conjugating A by S or T in the appropriate order will eventually produce a reduced form:

- **ALGORITHM:**

(1) If $c < a$, conjugate by S.
(2) If $|b| > a$, conjugate by T^k, where k is the greatest integer less than or equal to $\frac{a-b}{2a}$, i.e., $k = \lfloor \frac{a-b}{2a} \rfloor$.

- Note: the first step reduces the value of a, while the second reduces the value of $|b|$, so this gives you a hint that the process should terminate after a finite number of steps.

- CAUTION: remember that when we write the matrix for a QF, the upper right / bottom left entry is $b/2$, not b, so be sure to double it before checking which step to apply next.

Let's apply the algorithm to A above. Here $20 = |b| > a = 5$, so we do step 2. $k = \lfloor \frac{-15}{10} \rfloor = -2$, so we conjugate by T^{-2}, giving

$$\begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix}$$

Here $1 = c < a = 5$, so we apply step 1, conjugating by S, which gives

$$\begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}$$

This is reduced - indeed, it is our old friend $f_5(x,y) = x^2 + 5y^2$!

- so maybe this convinces you that we can always reduce a pos def form to a reduced one.

- then we also have to check that there is only one reduced form in each equivalence class - this is Theorem 3.25 in your book. The proof is rather long, and we may skip it entirely, or sketch it tomorrow.