MATH 115, SUMMER 2012
LECTURE 20

JAMES MCIVOR

If you read this before class: don't be alarmed by the 6 pages - there's no way I'll get through all of this material today!

last time:

- defined quadratic forms, discriminant of a binary QF, and indefiniteness/semidefiniteness, etc.
- used discriminant to tell whether $f(x,y) = 0$ has a nontrivial solution
- used discriminant to tell whether a form is indefinite ($d > 0$), semidefinite (but not definite) ($d = 0$), or definite ($d < 0$)
- recall also the "key formula" involving the discriminant, which we obtained by completing the square:

$$4af(x,y) = (2ax + by)^2 - dy^2$$

1. Discriminant and Representability

- let $f(x,y)$ be a binary QF. Recall that we say f **represents** the integer n if there are integers x, y such that $f(x,y) = n$. In other words, if n is an output of f. The representation is **proper** if x and y are coprime.
- our main question is: which integers can be represented by a given form?
- the following results don't exactly answer this question, but they say which integers can be represented by any form at all.

Theorem 1. *Let n and d be two integers with n nonzero. Then n can be properly represented by a binary QF of discriminant d if and only if $x^2 \equiv d \mod 4|n|$ has a solution.*

Proof. - First we assume that n is an integer properly represented by some form $f(x,y) = ax^2 + bxy + cy^2$ whose discriminant is $d = b^2 - 4ac$.

- that means there are integers s, t such that $f(s,t) = n$, and moreover, s and t are coprime (since the representation is proper).
- We wish to show that the congruence $x^2 \equiv d \mod 4|n|$ has a solution (note we need the absolute value because n could be negative, but mod only makes sense for positive values).
- So we just have to find an x that works.
- MAIN IDEA for this direction: break the modulus $4|n|$ into two pieces, construct a solution for each smaller modulus, and then put them together using CRT
- First, as always, factor the modulus $4|n|$ into prime powers:

$$4|n| = p_1^{a_1} \cdots p_r^{a_r}$$

- some of the p_i may divide s. Some may divide t. But no p_i can divide both since $(s,t) = 1$.

- rewrite it as

$$4|n| = p_1^{a_1} \cdots p_k^{a_k} \cdot q_1^{b_1} \cdots q_m^{b_m}$$

where the p_i divide s and the q_i do not divide s

- then set $m_1 = \prod p_i^{a_i}$, $m_2 = \prod q_i^{b_i}$.

- we have $m_1 m_2 = 4|n|$, $(m_1, m_2) = 1$, and $(m_2, s) = 1$ by the definitions of m_1, m_2

- we also have $(m_1, t) = 1$, for if some p_i divides t, then since it divides s also we have $p_i|(s,t) = 1$, contradiction.

- now apply "key formula", replacing $f(s,t)$ by n

$$4an = (2as + bt)^2 - dt^2$$

- reduce mod m_1:

$$dt^2 \equiv (2as + bt)^2 \mod m_1$$

- since $(m_1, t) = 1$, t has a multiplicative inverse mod m_1, and we get

$$d \equiv (t^{-1}(2as + bt))^2 \mod m_1$$

- so we have a solution to $x^2 \equiv d \mod m_1$.

- could also complete the square for y and obtain a different "key formula", namely

$$4cf(x,y) = (2cy + bx)^2 - dx^2$$

- if we plug in s, t, and reduce this mod m_2, we find a solution to $x^2 \equiv d \mod m_2$

- by CRT (since $(m_1, m_2) = 1$, we get a solution to $x^2 \equiv d \mod m_1 m_2 = 4|n|$.

- end of one direction

- other way: assume there is a solution to $x^2 \equiv d \mod 4|n|$.

- we need to construct a form $f(x,y)$ with discriminant d which has n as one of its outputs.

- let our solution to the congruence be $x = \alpha$

- then $\alpha^2 - d = 4|n|k$ for some k.

- if n positive, can drop the absolute value. if n negative can replace k by $-k$ and then drop the absolute value. either way, get rid of the absolute value, giving

$$\alpha^2 - d = 4nk \text{ or equivalently, } d = \alpha^2 - 4nk$$

- this looks suspiciously like the formula for discriminant, so we set

$$f(x,y) = nx^2 + \alpha xy + ky^2$$

- this is a form, with discriminant d, but does it represent n? and properly?

- yes, since $f(1,0) = n$ and the gcd of 1 and 0 is 1.

□

The next result is just the special case when n is a prime p.

Corollary 1. *Let d be an integer that is congruent to 0 or 1 mod 4, and p be an odd prime. There is a form of discriminant d that properly represents p if and only if $p|d$ or $\left(\frac{d}{p}\right) = 1$.*

- note: the conditions $p|d$ or $\left(\frac{d}{p}\right) = 1$ are the same as saying that d is a square mod p.

Proof. - Since $d \equiv 1$ or 0, we know d is a square mod 4.

- there is a form properly representing p iff d is a square mod $4p$ (by Thm)

- since p is odd, $(4, p) = 1$, so d is a square mod $4p$ iff it's a square mod 4 and p separately iff it's a square mod p (since d is already assumed to be a square mod 4)

- d is a square mod p iff $\left(\frac{d}{p}\right) = 1$ or 0.

- string these "iff"s together and we're done

□

2. Equivalent Forms

Before we can address the main question above at all, we observe that some forms represent the same integers:

Example 2.1. Let $f(x, y) = x^2 + xy + y^2$, and $g(x, y) = (x-1)^2 + (x-1)(y-1) + (y-1)^2$. These forms have the same outputs, since they differ by a change of variables $x \mapsto x - 1$, $y \mapsto y - 1$. Consider for example the representation of 19 by f:

$$f(3, 2) = 3^2 + 3 \cdot 2 + 2^2 = 19.$$

We can see right away that g represents 19 also:

$$g(4, 3) = f(3, 2) = 19$$

So if we're interested in representability, we should consider these forms the same. To understand this better, think again of a QF f as a function from the integer lattice $\mathbb{Z}^2$ to integers $\mathbb{Z}$

What happens if we first apply a transformation T from $\mathbb{Z}^2$ to itself, and then apply our quadratic form f?

$$\mathbb{Z}^2 \xrightarrow{T} \mathbb{Z}^2 \xrightarrow{f} \mathbb{Z}$$

Since $\mathbb{Z}^2$ is a subset of $\mathbb{R}^2$, and (linear) maps from $\mathbb{R}^2$ to itself are matrices, we should ask: which matrices take $\mathbb{Z}^2$ to $\mathbb{Z}^2$?

The answer is easy:

Proposition 1. *If A is a 2×2 matrix, such that whenever a vector $\boldsymbol{x}$ has integer entries, $A\boldsymbol{x}$ also has integer entries, then all the entries of A must be integers.*

Proof. The columns of A are just $A\mathbf{e}_1$ and $A\mathbf{e}_2$, where $\mathbf{e}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\mathbf{e}_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. By our assumption, these columns have integer entries.

□

In the example above, f and g differed by a change of variables (in integers). A change of variables needs to be invertible. So now we ask: which integer matrices are invertible?

Proposition 2. *If A is an invertible 2×2 matrix with integer entries, then its determinant is ± 1.*

Proof. - Since A is invertible, there is another matrix B such that $AB = I$, the 2×2 identity matrix.

- Note that B also sends lattice points to lattice points, using the previous prop.

- By linear algebra, we know the determinants of A and B are nonzero, and that $\det AB = \det A \det B$

- Since $AB = I$, we have $1 = \det AB = \det A \det B$, so both $\det A$ and $\det B$ are units in $\mathbb{Z}$

- the only units in $\mathbb{Z}$ are ± 1.

□

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 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 $N = A^T M A$.

Proposition 3. *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 next thm:

Theorem 2. *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 $d = -4 \det A$.

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

- 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.

□

3. 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: for each equivalence class, there's only one which has the property of being reduced, defined below.

- The definition is bizarre, but turns out to be useful:

- for the rest of this material, we need to avoid forms whose discriminant is a perfect square - these are called **degenerate**, and if the discriminant is not a perfect square, the form is **nondegenerate**

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

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

- To see why reduced forms are interesting, we 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 is incredibly powerful.

- it is a stronger version of theorems 3.18 and 3.19 in your book, but with the additional hypothesis that f be positive definite.

Theorem 3 (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."

Proof. It's long - do it later.

□

Thursday Problem Session Ideas

1. Explain action of modular group on upper half plane
2. explain generators S and T of modular group