Binary quadratic forms

November 15, 2012

1 First Part of Homework set due Tuesday Nov 27

1. Show that given any pair of relatively prime integers (a, b) there is a matrix

$$A := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with $A \in \mathrm{SL}_2(\mathbf{Z})$.

2. Prove that the discriminant of a binary quadratic form is invariant under orientation-equivalence.

3. Find a negative discriminant such that there is more than one reduced binary quadratic form of that discriminant.

4. (Not to be handed in or graded, but think about this:)

   (a) How might you show that your reduced binary quadratic forms (of the previous exercise) are *not* orientation-equivalent?

   (b) Do the exercise below.

2 S and T

Consider these "basic" elements of $\mathrm{SL}_2(\mathbf{Z})$:

$$T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and

$$S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

.

Note that

$$T^n := \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix}$$

for any $n \in \mathbf{Z}$, and that $S^4 = 1$. **Note this fact (we haven't proven it though):** These operators S and T generate the group $\mathrm{SL}_2(\mathbf{Z})$.

3 Recall binary quadratic forms

Definition 1 *A* **binary quadratic form** *over a commutative ring R is a homogeneous form*

$$F(x, y) = ax^2 + bxy + cy^2 \in R[x, y],$$

of degree two in two variables with coefficients in R.

We will be considering–this hour—binary quadratic forms for $R = \mathbf{Z}$, i.e., over the integers, and—for short—we'll omit saying that they are over $\mathbf{Z}$ and just call them "binary quadratic forms." We denote an F as above with coefficients a, b, c as above, by the symbol (a, b, c) (for short).

Definition 2 *Two binary quadratic forms (a, b, c) and (a', b', c') will be called* **orientation-equivalent** *if there is a matrix*

$$A := \begin{pmatrix} u & v \\ w & t \end{pmatrix}$$

in $\mathrm{SL}_2(\mathbf{Z})$ such that if we make the linear change of variables:

$$\begin{pmatrix} u & v \\ w & t \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x' \\ y' \end{pmatrix}$$

and define the binary quadratic form $G(x, y) := F(x', y')$ we have that $G(x, y) = a'x^2 + b'xy + c'y^2$.

4 Formulas:

$a' = au^2 + buw + cw^2$

...

Exercise: Work out the formulas for b', c'.

We denote orientation-equivalence by a "tilde" as in:

$$(a, b, c) \ \sim \ (a', b', c').$$

5 Invariant(s)

The discriminant; the set of properly represented integers.

Definition 3 $\Delta(a,b,c) := b^2 - 4ac$.

Definition 4 $\mathcal{N}(a,b,c) \subset \mathbf{Z}$ *is the set of integers of the form* $au^2 + buv + cv^2$ *for* u, v *relatively prime integers with* $(u,v) = 1$. *An integer in* $\mathcal{N}(a,b,c)$ *will be referred to as an integer that is* **properly represented by** (a,b,c).

Compute Δ for the fundamental quadratic forms.

Completing the square:

Making the transformation (now over $\mathbf{Q}$ rather than over $\mathbf{Z}$)

$$x \mapsto x - \frac{b}{2a}y; \qquad y \mapsto y$$

we have the quadratic form (over $\mathbf{Q}$):

$$ax^2 + \frac{-\Delta}{4a}y^2$$

which is *definite* if $\Delta < 0$ and *indefinite* if $\Delta > 0$. A *definite form* is **positive** or **negative** definite according to the sign of "a."

Theorem 1 *If* $(a,b,c) \sim (a',b',c')$ *then*

$$\Delta(a,b,c) = \Delta(a',b',c')$$

and

$$\mathcal{N}(a,b,c) = \mathcal{N}(a',b',c').$$

Theorem 2 *If* $a' \in \mathcal{N}(a,b,c)$ *then there are integers* b', c' *such that* $(a,b,c) \sim (a',b',c')$. *Equivalently, any integer represented by a quadratic form* (a,b,c) *can be taken as the first coefficient of a form equivalent to* (a,b,c).

Relate the signs of elements in $\mathcal{N}(a,b,c)$ to the question of whether or not the binary quadratic form is positive definite, negative definite, or indefinite.

6 Congruence conditions

Theorem 3 *If $n \in \mathcal{N}(a,b,c)$ then Δ is a quadratic residue modulo $4|n|$. Conversely, if an integer Δ is a quadratic residue modulo $4|n|$ then there is a binary quadratic form (a,b,c) with $\Delta(a,b,c) = \Delta$, with respect to which n is properly representable.*

Moral: If Δ is such that there is *only one* equivalence class of binary quadratic forms with discriminant Δ, the above gives a complete solution to the problem of representing numbers by that quadratic form.

7 Examples:

1. $\Delta = -4$. $x^2 + y^2$ is the only *positive* definite form (up to equivalence); so $n > 0$ is properly represented by it if and only if -1 is a square mod n. We know this... but let's go through the proof.
2. $\Delta = -7$. $x^2 + xy + 2y^2$ is the only positive definite form (up to equivalence); supposing that $n > 0$ is odd, we see that it is properly represented by $x^2 + xy + 2y^2$ if and only if -7 is a square mod $4n$. This happens if and only if n has no prime factor congruent to $3, 5$, or 6 mod 7 and is not divisible by 49.
3. $\Delta = 8$ (an indefinite form). $x^2 - 2y^2$ is the unique quadratic form of that discriminant: n must have no prime factor congruent to ± 1 mod 8 and must not be divisible by 4.

8 Positive definite forms

We now restrict to these.

Definition 5 *A* **reduced positive definite form** *is a form (a,b,c) such that*

$$-a < b \leq a \leq c$$

and such that if $a = c$ then $b \geq 0$.

Theorem 4 *Any positive definite form is equivalent to a reduced positive definite form*

Theorem 5 * *There is a unique reduced positive definite form in every equivalence class of positive definite forms*