

8430 HANDOUT 3: ELEMENTARY THEORY OF QUADRATIC FORMS

PETE L. CLARK

1. BASIC DEFINITIONS

An **integral binary quadratic form** is just a polynomial $f = ax^2 + bxy + cy^2$ with $a, b, c \in \mathbb{Z}$. We define the **discriminant** of such a form to be $\Delta(f) = b^2 - 4ac$.

A quadratic form is **nondegenerate** if $\Delta(f) \neq 0$. Generally we restrict attention to nondegenerate forms.

We say a quadratic form $q(x, y)$ **represents** an integer N if there exist integers x and y with $q(x, y) = N$. We say that q **primitively represents**¹ N if there exist relatively prime integers x and y such that $q(x, y) = N$.

Let $f = ax^2 + bxy + cy^2$ be a quadratic form and suppose that $d = \gcd(a, b, c) > 1$. Then f can only represent integers which are multiples of d – in particular it can represent at most one prime, and no primes at all if d is not prime. Moreover f represents dN iff the integral form $\frac{1}{d}f$ represents N , so there is no loss of generality in considering only the case $\gcd(a, b, c) = 1$. Such forms are said to be **primitive**.

Exercise 3.1.1: Show that any quadratic form of squarefree discriminant is primitive.

For any quadratic form f , $\Delta(f) = b^2 - 4ac \equiv b^2 \pmod{4}$, i.e., $\Delta(f)$ is 0 or 1 mod 4. Conversely, if $D \equiv 0 \pmod{4}$, then

$$q_D = x^2 - \frac{D}{4}y^2$$

is a form of discriminant D , and if $D \equiv 1 \pmod{4}$ then

$$q_D = x^2 + xy + \frac{1-D}{4}y^2$$

is a form of discriminant D . We have seen these forms before, of course; (1) is the norm form of the quadratic order $\mathbb{Z}[\sqrt{D}]$ and (2) is the norm form of the quadratic order $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$. Let us call the form q_D the **principal** form of discriminant D . It has the following nice property:

Proposition 1. *For any integer $D \equiv 0, 1 \pmod{4}$, the set of nonzero integers represented by the principal form q_D is a submonoid of the multiplicative monoid*

¹Cox's terminology is "properly represents." In the first draft of these notes and in my first lecture on the subject I used this terminology, but because "primitive representation" makes much more intuitive sense, I slipped into that terminology without noticing.

of all nonzero integers. More plainly, q_D represents 1, and if q_D represents N_1 and N_2 then it represents N_1N_2 .

Exercise 3.1.2: Prove Proposition 1.

2. MATRIX REPRESENTATIONS

To the binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ we may associate the 2×2 symmetric matrix

$$M_f = \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix},$$

the point being

$$f(x, y) = \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}.$$

Notice that $M_f \in M_2(\mathbb{Q})$, i.e., it has rational coefficients, and it lies in $M_2(\mathbb{Z})$ iff b is even.

A quadratic form such that $M_f \in M_2(\mathbb{Z})$ – a form $ax^2 + 2bxy + cy^2$ – is called **classically integral** or **integer-matrix**. When we wish to emphasize the slight additional generality of our definition, we refer to a form $ax^2 + bxy + cy^2$ (with b possibly odd) as **integer valued**. The following exercise justifies this terminology.

Exercise 3.2.1: Let $a, b, c \in \mathbb{C}$, and $f(x, y) = ax^2 + bxy + cy^2$. Show TFAE:

- (i) $\forall x, y \in \mathbb{Z}, f(x, y) \in \mathbb{Z}$.
- (ii) $a, b, c \in \mathbb{Z}$.

Remark: Comparison with the polynomial $\frac{x^2+x}{2}$ – which maps integers to integers despite not having integral coefficients – shows that the previous exercise was not as foregone a conclusion as one might have thought.

There is a centuries old debate as to whether integer-valued or integer-matrix is the “correct” notion of integrality for a quadratic form. Notably Gauss was a staunch advocate of the “integer-matrix” perspective, despite the fact that this restriction complicates the theory of Gauss composition. Note that a binary form $f(x, y) = ax^2 + bxy + cy^2$ has odd discriminant $D = b^2 - 4ac$ iff b is odd, so our expansion from quadratic orders of the form $\mathcal{O}_n = \mathbb{Z}[\sqrt{-n}]$ to all imaginary quadratic orders forces us to consider non-classical integral forms.

Does it really matter? In some sense the answer is no: if q is integer-valued, then $2q$ has an integer-matrix, so at worst we’re fussing about that factor of 2. Cassels makes the point (even in the title of) his book *Rational Quadratic Forms* that the integrality of the coefficients of the form in any sense is not critical. What is important is whether one regards two forms as equivalent if they differ by a matrix in $GL_2(\mathbb{Q})$ or in $GL_2(\mathbb{Z})$. The meaning of this will become clear momentarily.

However, it can certainly be true that a given assertion about integral matrix forms may not be true for integer valued forms. For instance, the Conway-Schneeberger Fifteen Theorem (proved in the 1990’s) asserts that for any positive definite integer-matrix quadratic form in four variables, if $f(x_1, x_2, x_3, x_4)$ represents the positive

integers 1 through 15, it represents all positive integers. The theorem does not hold for integer valued quadratic forms. Something similar does: a positive definite integer valued form in four variables which represents the first 290 positive integers represents all positive integers. But this latter theorem is much harder to prove: it was proved in 2007 by Bhargava and Hanke and required, among many other things, quite extensive computer calculation.

3. MATRIX ACTION ON QUADRATIC FORMS

3.1. Some notation for matrix rings and matrix groups.

Let R be a ring and $n \in \mathbb{Z}^+$. Then the $n \times n$ matrices with R -coefficients form a ring under entrywise addition and matrix multiplication, denoted $M_n(R)$. When $n = 1$ this is of course just R , so is commutative if R is.² For $n \geq 2$, then unless R is the zero ring, $M_n(R)$ is non-commutative. As with any ring, there is a group of invertible elements – here x is invertible means there exists y such that $xy = yx = 1$, and the two-sidedness of the inverse cannot be ignored – which is denoted $GL_n(R)$, the **general linear group** of order n over R . Recall from linear algebra the **adjoint equation**:

$$\forall A \in M_n(R), A \cdot \text{adj}(A) = \det(A)I_n.$$

This shows that A is invertible iff $\det(A)$ is invertible in R . In particular, when $R = \mathbb{Z}$, this shows that an element of $M_n(\mathbb{Z})$ is invertible (i.e., the inverse exists and has integral entries!) iff $\det(A) \in \mathbb{Z}^\times = \pm 1$.

The determinant map gives a homomorphism from the invertible matrices to the invertible scalars, whose kernel is, clearly the set of all matrices of determinant 1, denoted $SL_n(R)$ (**special linear group**). In other words, we have a short exact sequence of groups

$$1 \rightarrow SL_n(R) \rightarrow GL_n(R) \xrightarrow{\det} R^\times \rightarrow 1.$$

Exercise 3.3.1: a) Show that the **center** of the group $GL_n(R)$ is the subgroup of invertible $n \times n$ scalar matrices, i.e., αI_n for $\alpha \in R^\times$; this group is isomorphic to R^\times . In particular, the center of $GL_n(\mathbb{Z})$ is ± 1 .

b) Show that the center of the group $SL_n(R)$ is the subgroup of scalars αI_n such that $\alpha^n = 1$, i.e., the group $\mu_n(R)$ of n th roots of unity in R . In particular, the center of $SL_n(\mathbb{Z})$ is ± 1 when n is even and the trivial group when n is odd.

c) By definition $PGL_n(R)$ is the quotient of $GL_n(R)$ by its center, the **projective general linear group**. Likewise $PSL_n(R)$ is the quotient of $SL_n(R)$ by its center, the **projective special linear group**. Show there is an exact sequence

$$1 \rightarrow PSL_n(R) \rightarrow PGL_n(R) \rightarrow \mathbb{R}^\times / R^{\times n}.$$

d) Deduce from part c) that $PSL_n(\mathbb{Z}) = PGL_n(\mathbb{Z})$ when n is odd, and $[PGL_n(\mathbb{Z}) : PSL_n(\mathbb{Z})] = 2$ when n is even. In this case find an explicit representative for the nontrivial coset of $PSL_n(\mathbb{Z})$ in $PGL_n(\mathbb{Z})$.

e) FYI: For $n \geq 2$ and F any field, the groups $PSL_n(F)$ are all simple except for $PSL_2(\mathbb{F}_2)$ and $PSL_2(\mathbb{F}_3)$. The group $PSL_2(\mathbb{Z})$ is far from being simple: for any $N \geq$

²For simplicity, let us assume that R is commutative, although matrix rings over finite-dimensional noncommutative algebras are also very important in number theory.

2 the natural map $\mathrm{PSL}_2(\mathbb{Z}) \rightarrow \mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$ is a surjective group homomorphism, whose kernel is a nontrivial normal subgroup, denoted $\Gamma(N)$.

3.2. Action of $M_2(\mathbb{Z})$ on binary quadratic forms.

If $f(x, y) = ax^2 + bxy + cy^2$ is an integral binary quadratic form and $A = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in M_2(\mathbb{Z})$, we define

$$(A \cdot f)(x, y) = f(px + qy, rx + sy).$$

I claim that $A \cdot (B \cdot f) = AB \cdot f$. Of course this can be checked by brute force, but – as we saw in class – it is faster and more enlightening to think about the action in terms of the matrix representation M_f of f :

$$(A \cdot f)(x, y) = (A \begin{bmatrix} x \\ y \end{bmatrix})^t M_f \left(A \begin{bmatrix} x \\ y \end{bmatrix} \right) = [x \ y] A^t M_f A \begin{bmatrix} x \\ y \end{bmatrix},$$

i.e., the quadratic form $A \cdot f$ has defining matrix $A^t M_f A$. From this verification of the above claim is immediate. It is also clear that

$$\mathrm{disc}(M \bullet f) = -4 \det(A^t M_f A) = -4 \det(A)^2 \det(M_f) = \det(A)^2 \mathrm{disc}(f).$$

In particular, restricting to the group of units $\mathrm{GL}_2(\mathbb{Z})$, we get an **action** of $\mathrm{GL}_2(\mathbb{Z})$ on the set of all binary integral quadratic forms. Since $A \in \mathrm{GL}_2(\mathbb{Z})$ implies $\det(A)^2 = (\pm 1)^2 = 1$, we conclude that $\mathrm{disc}(M \bullet f) = \mathrm{disc}(f)$, i.e., the discriminant is an **invariant** of the GL_2 -orbit of f .

Exercise 3.3.2: Show that the action of $\mathrm{GL}_2(\mathbb{Z})$ (resp. $\mathrm{SL}_2(\mathbb{Z})$) on binary quadratic forms factors through to an effective action of $\mathrm{PGL}_2(\mathbb{Z})$ (resp. $\mathrm{PSL}_2(\mathbb{Z})$). In other words, if $A \in \mathrm{GL}_2(\mathbb{Z})$ is such that $A \bullet f = f$ for all binary quadratic forms, then $A = \pm I_2$.

Exercise 3.3.3: Suppose that f and f' are two quadratic forms in the same $\mathrm{GL}_2(\mathbb{Z})$ -orbit: i.e., $f' = A \cdot f$ for some $A \in \mathrm{GL}_2(\mathbb{Z})$. Show that f and f' represent exactly the same integers, counted with multiplicity: that is, for any $N \in \mathbb{Z}$,

$$\#\{(x, y) \in \mathbb{Z}^2 \mid f(x, y) = N\} = \#\{(x, y) \in \mathbb{Z}^2 \mid f'(x, y) = N\}.$$

We will call two quadratic forms in the same $\mathrm{GL}_2(\mathbb{Z})$ -orbit **widely equivalent**, and two quadratic forms in the same $\mathrm{SL}_2(\mathbb{Z})$ -orbit **properly equivalent**. If for quadratic forms f and f' there exists a matrix $A \in \mathrm{GL}_2(\mathbb{Z}) \setminus \mathrm{SL}_2(\mathbb{Z})$ (i.e., $\det(A) = -1$) such that $(A \bullet f) = f'$ then f and f' are said to be **improperly equivalent**. Warning: two improperly equivalent forms may or may not also be properly equivalent! Actually whether they are or not is a very important issue, but we will have to come back to it later.

Exercise 3.3.3 shows that so long as we are interested in representations of integers, we should regard widely equivalent (and hence *a fortiori* properly equivalent) quadratic forms as “the same.” Exactly why we will be more interested in proper equivalence than wide equivalence will become clear only later. (In other branches of the theory of quadratic forms, especially the study of quadratic forms over fields, such as \mathbb{Q} , one does generally use wide equivalence rather than proper equivalence.)

Automorphism group of a quadratic form: For a binary quadratic form f , let

$$O(f) = \{A \in \mathrm{GL}_2(\mathbb{Z}) \mid M \bullet f = f\}$$

and

$$SO(f) = \{A \in \mathrm{SL}_2(\mathbb{Z}) \mid M \bullet f = f\}.$$

We call $O(f)$ either the **wide automorphism group** of f or the **orthogonal group** of f ; and $SO(f)$ the **proper automorphism group** or the **special orthogonal group** of f .

Exercise 3.3.4: Evidently $SO(f) \subset O(f)$. Show that we either have equality or $[O(f) : SO(f)] = 2$.

Let $v = (x, y)^t$ be an arbitrary element of \mathbb{Z}^2 . Then by definition

$$(A \cdot f)(x, y) = v^t A^t M_f A v,$$

so that

$$\begin{aligned} A \bullet f = f &\iff \forall v \in \mathbb{Z}^2, v^t M_f v = v^t A^t M_f A v \\ &\iff M_f = A^t M_f A. \end{aligned}$$

Therefore

$$O(f) = \{A \in \mathrm{GL}_2(\mathbb{Z}) \mid A^t M_f A = M_f\}$$

with a similar description of $SO(f)$. It should now make at least some sense why we use the name “orthogonal group”; e.g. if $f(x, y) = x^2 + y^2$, so $M_f = I_2$, then $O(f)$ is precisely the set of 2×2 matrices such that $A^t A = I_2$: this is the usual group $O_n(\mathbb{R})$ of real orthogonal matrices intersected with the set of all matrices with integer entries.

Example: Let us compute the wide and proper automorphism groups of the form $f = x^2 - y^2$. As usual, write $e_1 = (1, 0)$, $e_2 = (0, 1)$. If $A \in O(f)$, then

$$f(Ae_1) = (A \bullet f)(e_1) = f(e_1) = 1,$$

and

$$f(Ae_2) = (A \bullet f)(e_2) = f(e_2) = -1.$$

Therefore Ae_1 is some vector (x, y) such that $1 = (x+y)(x-y)$, and one immediately checks that the only such vectors are $(\pm 1, 0)$. Similarly Ae_2 is some vector (x, y) such that $-1 = (x+y)(x-y)$, and the only such vectors are $(0, \pm 1)$. Since the matrix A is clearly determined by its action on e_1, e_2 , the only possible automorphisms are given by the four diagonal matrices with entries in ± 1 . Conversely, all four such matrices do give automorphisms of f , so that $O(f) = V_4 := \{\pm I_2, \pm \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\}$ is isomorphic to the Klein group $Z_2 \times Z_2$. Here $SO(f) = \{\pm I_2\}$; by Exercise X.X we know that we will always have $SO(f) \supseteq \{\pm I_2\}$.

Exercise 3.3.5: Let $D < 0$ be an imaginary quadratic discriminant and let q_D be the principal form of discriminant D , i.e., $x^2 - \frac{D}{4}y^2$ if $D \equiv 0 \pmod{4}$ and $x^2 + xy + \frac{1-D}{4}y^2$ if $D \equiv 1 \pmod{4}$. Let $w(D) = \#(\mathcal{O}(D))^\times$, the cardinality of the

unit group of the quadratic order of discriminant D . Show that $SO(f) \cong Z_{w(D)}$ (cyclic group of order $w(D)$) and $O(f) \cong D_{w(D)}$ (dihedral group of order $2w(D)$).

Exercise 3.3.6: Can you find a binary quadratic form f with $O(f) = \{\pm 1\}$?

Exercise 3.3.7: Let $D > 1$ be squarefree. Show that the automorphism group of $x^2 - Dy^2$ is infinite. (Hint: the key word is Pell's equation.)

Exercise 3.3.8: Let us say that the binary quadratic forms f and f' are **homothetic** if there exists $r \in \mathbb{Q}^\times$ such that $rf = f'$. Show that if f and f' are homothetic, then $O(f) = O(f')$ and $SO(f) = SO(f')$. (Suggestion: if you write it out in terms of defining matrices this is almost trivial.)

Exercise 3.3.9: Suppose that the quadratic forms f and f' are $\text{GL}_2(\mathbb{Z})$ -equivalent. Do we have $O(f) = O(f')$? If not, then what?

3.3. Extending quadratic forms to other rings.

All of the terminology we have set up so far holds in much greater generality. Let R be a domain whose quotient field *does not* have characteristic 2. An n -variable quadratic form over R is just a homogeneous quadratic polynomial

$$f(x_1, \dots, x_n) = \sum_{1 \leq i < j \leq n} a_{ij} x_i x_j, \quad a_{ij} \in R.$$

Putting $v = (x_1, \dots, x_n) \in R^n$, one finds exactly as above that

$$f(x_1, \dots, x_n) = v M_f v^t,$$

for a unique matrix M_f whose (i, i) entry is $a_{i,i}$ and whose (i, j) entry for $i \neq j$ is $\frac{a_{i,j}}{2}$. (Thus in general the matrix entries lie not in the domain R but in its quotient field, which is why we need to assume that $2 \neq 0$ in the quotient field.) We then have natural actions of $\text{GL}_n(R)$ (hence also $\text{SL}_n(R)$) on the set of " n -ary" quadratic forms with R -coefficients, can speak of quadratic forms being widely or properly equivalent, and can define automorphism groups $O(f)$ and $SO(f)$.

In fact, because there is a unique ring homomorphism from the integers \mathbb{Z} to our domain R , every n -ary quadratic form $q(x_1, \dots, x_n)$ can be viewed as an n -ary quadratic form with R -coefficients just by applying this homomorphism. In particular, it is (quite trivially, but still very usefully) true that for $N \in \mathbb{Z}$, an equation $q(x_1, \dots, x_n) = N$ has an integral solution iff it has a solution with $x_1, \dots, x_n \in \mathbb{Z}$ iff the same equation has a solution with R -coefficients for every ring R . On the one hand, as we have seen, this is a good way to rule out solutions: obviously $x^2 + y^2 = -1$ has no integral solution, because it has no \mathbb{R} -solution. Only slightly less obviously $x^2 + y^2 = (3k + 4)$ has no \mathbb{Z} -solution since it has no $\mathbb{Z}/4\mathbb{Z}$ -solution.

In general, if we can understand the behavior of the quadratic form viewed as a form over R , it may well help us understand the quadratic form over \mathbb{Z} , and there are choices of R for which quadratic forms over R are much easier to understand than integral quadratic forms.

For our present purposes the key example is $R = \mathbb{R}$, the real numbers.

Exercise 3.3.10: Let $f(x_1, \dots, x_n)$ be a nondegenerate quadratic form with \mathbb{R} -coefficients.

a) Show that f is $\text{GL}_n(\mathbb{R})$ -equivalent to a form f' whose associated matrix M' has $M'_{i,j} = \pm\delta_{i,j}$ i.e., is zero off the diagonal and has ± 1 entries on the diagonal. (Hint: the Spectral Theorem of linear algebra asserts that f is $O(n)$ -equivalent to a diagonal matrix, and the rest is easy.)

b) Consider the following conditions:

(PD1) $\forall (x_1, \dots, x_n) \in \mathbb{R}^n, f(x_1, \dots, x_n) \geq 0$, with equality iff $(x_1, \dots, x_n) = 0$.

(PD2) f is $\text{GL}_n(\mathbb{R})$ equivalent to the identity matrix I_n .

(ND1) $\forall (x_1, \dots, x_n) \in \mathbb{R}^n, f(x_1, \dots, x_n) \leq 0$, with equality iff $(x_1, \dots, x_n) = 0$.

(ND2) f is $\text{GL}_n(\mathbb{R})$ equivalent to $-I_n$.

(ID1) f takes on both positive and negative values.

(ID2) The symmetric matrix M_f has both positive and negative eigenvalues.

Show that (PD1) \iff (PD2), (ND1) \iff (ND2), (ID1) \iff (ID2), and that for any nondegenerate f exactly one of (PD1), (ND1) and (ID1) occurs. f is accordingly called **positive definite**, **negative definite** or **indefinite**, respectively.

Given a nondegenerate integral form $f(x_1, \dots, x_n)$, by viewing it as a form with \mathbb{R} -coefficients we may classify it as positive definite, negative definite or indefinite.

The key example of course is that the principal form q_D of discriminant D is positive definite if $D < 0$ and indefinite if $D > 0$. For binary forms, the complete classification is as follows:

Exercise 3.3.11: a) Let $f(x, y) = ax^2 + bxy + cy^2$ be an integral quadratic form of negative discriminant D . Show that f is positive definite iff $a > 0$ and negative definite iff $a < 0$. (Comment: Cox observes this by establishing the identity $4af(x, y) = (2ax + by)^2 - Dy^2$. There must be many other ways...)

b) Deduce the same result with a replaced by c .

Exercise 3.3.12: Let $f(x_1, \dots, x_n)$ be a nondegenerate quadratic form with real coefficients.

a) If f is either positive or negative definite, show that $O(f)$ is conjugate to $O(n)$, the usual orthogonal group $\{A \in M_n(\mathbb{R}) \mid A^t A = I_n\}$ (and similarly $SO(f) = SO(n)$). (Hint: a negative definite quadratic form is homothetic to a positive definite quadratic form.) In particular, $O(f)$ is a compact **compact** subgroup of $GL_n(\mathbb{R})$.

b) If f is indefinite, show that $O(f)$ is a **noncompact** subgroup of $GL_n(\mathbb{R})$.

c)* Show that the integral automorphism group $O(f)(\mathbb{Z})$ of a definite integral quadratic form $f(x_1, \dots, x_n)$ is finite. (Hint: by part a) it suffices to show that the integral automorphism group $O(f)(\mathbb{Z})$ is discrete in the real automorphism group $O(f)(\mathbb{R})$.) Does the converse hold?

Comment: By Exercise 3.3.10, an indefinite quadratic form is $\text{GL}_n(\mathbb{R})$ -equivalent to a diagonal matrix with M' with $m_{11} = m_{22} = \dots = m_{rr} = +1$, $m_{r+1, r+1} = \dots = m_{r+s, r+s} = -1$ for some number $0 < r < n$ and $r + s = n$. It is not obvious

that the number r of positive eigenvalues is invariant under $\mathrm{GL}_n(\mathbb{R})$ -equivalence, but it is true: this is Sylvester's Law of Nullity. (Equivalently, the number $r - s$ of positive eigenvalues minus negative eigenvalues is invariant; this quantity is called the **signature** of the real quadratic form and plays a prominent role in algebraic topology.) The automorphism group of a real quadratic form in $r + s = n$ variables with r positive and s negative eigenvalues is denoted $O(r, s)$ (and, as with most Lie groups, is ubiquitous in mathematics and modern physics).

In the systematic study of integral quadratic forms one also makes heavy use of $R = \mathbb{Q}_p$ (the field of p -adic numbers) and $R = \mathbb{Z}_p$ (the ring of p -adic integers). When discussing genus theory we will come close enough to these considerations to wave at \mathbb{Q}_p and \mathbb{Z}_p , but unfortunately not to really grapple with the local-global theory for integral quadratic forms (except possibly at the end of the course).

4. A CONVERSE TO THE FUNDAMENTAL CONGRUENCE

Well, of course we are interested in the quadratic form q_D , at least for $D \equiv 0 \pmod{4}$ – this is the problem we introduced at the very beginning. The question is why should we be interested in other primitive forms of the same discriminant? The answer is as follows.

Theorem 2. *Let $D \equiv 0, 1 \pmod{4}$ be a positive integer, and let m be an odd integer relatively prime to D . TFAE:*

- (i) D is a square modulo m .
- (ii) There is a primitive form of discriminant D which properly represents m .

Proof: (i) \implies (ii): let b be such that $D \equiv b^2 \pmod{m}$. Since m is odd, by replacing b by $b + m$ if necessary, we may assume that $D \equiv b \pmod{2}$, and then $D \equiv b^2 \pmod{4m}$, i.e., $D = b^2 - 4mc$ for some c , so that $mx^2 + bxy + cy^2$ primitively represents m – take $(x, y) = (1, 0)$ – and has discriminant D . This form is primitive, since $(m, D) = 1$ implies that no prime divides both b and m .

(ii) \implies (i): if there exists a primitive form $f(x, y) = ax^2 + bxy + c^2$ of discriminant D and relatively prime (p, q) such that $f(p, q) = m$, then there are integers r and s such that $ps - qr = 1$ and then $f(px + ry, qx + sy) =$

$$f(p, q)x^2 + (2apr + bps + brq + 2cqs)xy + f(r, s)y^2 = mx^2 + b'xy + c'y^2$$

has discriminant $D = (b')^2 - 4mc'$ and thus D is a square mod m .

Corollary 3. *(Fundamental Converse)*

For $n \in \mathbb{Z}^+$ and p an odd prime not dividing n , TFAE:

- (i) $-n$ is a square mod p (fundamental congruence):
- (ii) p is represented by some primitive form of discriminant $-4n$.

Proof: Apply the theorem with $D = -4n$ and note that $-n$ is a square mod p iff $-4n$ is a square mod p .

Exercise 3.4.1: Show that a quadratic form primitively represents a positive integer m iff there exist $b, c \in \mathbb{Z}$ such that f is properly equivalent to $mx^2 + bxy + cy^2$. (Hint: the nontrivial direction has already been done for you.)

Remark: I suppose this result – which is very nice; we will use it later – is the

reason why Cox says “proper representation” instead of “primitive representation.” (But it doesn’t seem like a good enough reason...)

5. THE REDUCTION THEOREM

So far the reader will notice that we have not really used the fact that $x^2 + ny^2$ is positive definite other than to reduce the question of whether a particular integer N is of the form $x^2 + ny^2$ to a finite computation. The following key definition – which is subtle enough to require some time to appreciate – for the first time takes advantage of the positive definiteness in an essential way.

Definition: A primitive positive definite form $ax^2 + bxy + cy^2$ is **reduced** if:

(R1) $|b| \leq a \leq c$.

(R2) If either $|b| = a$ or $a = c$ in (R1), then $b \geq 0$.

Theorem 4. (*Reduction Theorem*)

a) A primitive positive definite form is properly equivalent to a unique reduced form.

b) There is a simple algorithm which, given f , finds a reduced form equivalent to f .

c) If $ax^2 + bxy + cy^2$ is a reduced form of discriminant D , then $|b| \leq a \leq \sqrt{\frac{-D}{3}}$.

Since for fixed a, b, D there exists at most one integer c such that $b^2 - 4ac = D$, the number of proper equivalence classes of positive definite forms of discriminant D is at most $\frac{2}{3}|D|$.

It is not necessary to know the details of the reduction process in order to successfully apply the Reduction Theorem. So let us postpone the proof until we gain an appreciation for its significance.

We shall write $C(D)$ for the set of classes of properly equivalent positive definite forms of discriminant D . The Reduction Theorem tells us that $C(D)$ is finite, has size at most $\frac{2}{3}|D|$, and is effectively computable. Let’s try it out:

Example 0: The theorem asserts that there is a unique reduced form if $\frac{2}{3}|D| < 2$, i.e., if $|D| < 3$. Unfortunately there are no such discriminants. This shows that our bound on the size of $\frac{2}{3}|D|$ is certainly not sharp; it is just an easy bound that one can use for computations with D of a moderate size.

Example 1: $D = -4$. If $4ac - b^2 = 4$ then $b = 0$, $a = c = 1$, so the unique reduced form is $q_{-4} = x^2 + y^2$. Applying this together with the Fundamental Converse, we get a shiny new proof of the two squares theorem: an odd prime p is of the form $x^2 + y^2$ iff $\left(\frac{-1}{p}\right) = 1$. It also shows that $\mathbb{Z}[\sqrt{-1}]$ is a PID.

Example 2: $D = -3$. If $4ac - b^2 = 3$, then $0 \leq |b| \leq a \leq 1$, and we compute $(a, b, c) = (1, \pm 1, 1)$. By definition of reduced, we need $b = 1$, so the unique reduced form of discriminant -3 is $q_{-3}(x, y) = x^2 + xy + y^2$. So every odd prime with $\left(\frac{-3}{p}\right) = 1$ – i.e., $p \equiv 1 \pmod{3}$ – is a norm from the ring $\mathcal{O}(-3)$, i.e., the ring of integers of $\mathbb{Q}(\sqrt{-3})$. Tracking this back through our earlier work, we see that $\mathcal{O}(-3)$ is a Dedekind domain in which each prime ideal except possibly those lying over 2 is principal, and by Claborn’s Theorem this implies that $\mathcal{O}(-3)$ is a PID.

Example 3: $D = -12$. If $4ac - b^2 = 12$, then $0 \leq |b| \leq a \leq \sqrt{\frac{12}{3}} = 2$, and we compute $(a, b, c) = (2, 2, 2)$ or $(1, 0, 3)$. However the form $2x^2 + 2xy + 2y^2$ is not primitive. Therefore $x^2 + 3y^2$ is the only primitive reduced form of discriminant 12. Using the fundamental converse this shows that any odd prime with $(\frac{-12}{p}) = 1$ – i.e., any $p \equiv 1 \pmod{3}$ – is of the form $x^2 + 3y^2$.

Example 4: $D = -7$. If $4ac - b^2 = 7$, then $0 \leq |b| \leq a \leq \sqrt{\frac{7}{3}} < 2$, so $(a, b, c) = (1, \pm 1, 2)$, the unique reduced primitive quadratic form of discriminant -7 is q_{-7} , and $\mathcal{O}(-7)$ is a PID.

Example 5: $D = -28$. If $4ac - b^2 = 28$, $0 \leq |b| \leq a \leq \sqrt{\frac{28}{3}} < 4$, so $(a, b, c) = (1, 0, 7)$ or $(2, 2, 8)$, and the unique reduced primitive form of discriminant -28 is $q_{28}(x, y) = x^2 + 7y^2$. The fundamental converse then recovers our result on primes of the form $x^2 + 7y^2$.

Example 6: $D = -20$. If $4ac - b^2 = 20$, $0 \leq |b| \leq a \leq \sqrt{\frac{20}{3}} < 3$, so $(a, b, c) = (1, 0, 5)$ or $(2, 2, 3)$. Thus there is, aside from $x^2 + 5y^2$, another primitive reduced form of discriminant -20 , namely $2x^2 + 2xy + 3y^2$. In truth we knew this had to happen, because otherwise 3 would be of the form $x^2 + 5y^2$ and it isn't.

But now things get more interesting. Recall that on top of the fundamental congruence $(\frac{-5}{p}) = 1$, by going mod 4 we saw that $p = x^2 + 5y^2$ implies $p \equiv 1 \pmod{4}$, and our guess was that these two necessary conditions are sufficient: namely, we wish to show that $p = x^2 + 5y^2$ iff $p \equiv 1, 9 \pmod{20}$. But we know that if $(\frac{-5}{p}) = 1$ then at least one of our two reduced primitive forms represents p . So if we can show that a prime p satisfying $(\frac{-5}{p}) = 1$ and $p \equiv 3 \pmod{4}$ is **not** represented by $q' = 2x^2 + 2xy + 3y^2$, it will automatically be represented by $x^2 + 5y^2$! So suppose $p = 2x^2 + 2xy + 3y^2$ and reduce modulo 4:

$$p \equiv 2(x^2 + xy) - y^2 \pmod{4}.$$

The only way to get 1 (mod 4) would be if $x^2 + xy = x(x + y)$ and y are both odd, but that implies x is odd and then $x + y$ is even, contradiction. Therefore q' does not represent any prime which is 1 (mod 4), and we have shown:

Theorem 5. *A prime p is of the form $x^2 + 5y^2$ iff $p = 5$ or $p \equiv 1, 9 \pmod{20}$.*

This result represents a step forward in our understanding of primes of the form $x^2 + ny^2$: it is the first case in which we were able to answer the question when the density of the set was less than $\frac{1}{2}$.

Shall we continue?

Example 7: $D = -24$. If $4ac - b^2 = 24$, $0 \leq |b| \leq a \leq \sqrt{\frac{24}{3}} < 3$. The reduced primitive forms of discriminant -24 are q_{-24} and $q'(x, y) = 2x^2 + 3y^2$. A necessary condition for a prime $p > 3$ to be of the form $x^2 + 6y^2$ is $(\frac{-6}{p}) = 1$, which happens if $(p \equiv \pm 1 \pmod{8})$ and $p \equiv 1 \pmod{3}$ or $(p \equiv 3, 5 \pmod{8})$ and $p \equiv 2 \pmod{3}$. But by going mod 3 we get $p \equiv x^2 + 6y^2 \equiv x^2 \pmod{3}$, so in

fact we need $p \equiv 1 \pmod{3}$ and $p \equiv \pm 1 \pmod{8}$. But reducing $q' \pmod{3}$ we get $p \equiv 2x^2 + 3y^2 \equiv -x^2 \pmod{3}$. Therefore if $p \equiv 1 \pmod{3}$ and $p \equiv \pm 1 \pmod{8}$ then p must be represented by $x^2 + 6y^2$. Therefore we have shown:

Theorem 6. *A prime p is of the form $x^2 + 6y^2$ iff $p \equiv 1, 7 \pmod{24}$.*

Exercise 3.5.1: a) For each $D \equiv 0, 1 \pmod{4}$ $-200 < D < 0$, compute the complete list of reduced primitive forms of discriminant D . (Suggestion: write a three line computer program to do this for you.)

b) In particular, observe that in the above range, there exists a unique reduced quadratic form of discriminant D iff

$$D = -3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163.$$

c) Observe that the smallest discriminant for which the class number is odd and greater than 1 is $D = -44$.

Exercise 3.5.2: Find all primes of the form $x^2 + ny^2$ for the following values of n : 8, 9, 10, 12, 13, 15, 16, 18, 22, 25, 28, 37, 58. Show that in all cases it depends only on the class of p modulo $4n$.

Exercise 3.5.3: a) Show that each of the three reduced primitive forms of discriminant -44 represents exactly the same congruence classes modulo 44.

b)* Show that, in fact, the three quadratic forms represent the same congruence classes modulo N for any positive integer N . (This will probably require familiarity with Hensel's Lemma.)

Exercise 3.5.4: Let N_1, N_2 be positive integers.

a) Suppose that N_1 and N_2 are both represented by the form $x^2 + 6y^2$. Show that N_1N_2 is represented by $x^2 + 6y^2$.

b) Suppose N_1 and N_2 are both represented by $2x^2 + 3y^2$. Show that N_1N_2 is represented by $x^2 + 6y^2$.

c) Suppose N_1 is represented by $x^2 + 6y^2$ and N_2 is represented by $2x^2 + 3y^2$. Show that N_1N_2 is represented by $2x^2 + 3y^2$.

6. PROOF OF THE REDUCTION THEOREM

First observe that part b) follows easily from part a) and the definition of a reduced form: if $ax^2 + bxy + cy^2$ is reduced of discriminant $D < 0$, then $b^2 \leq a^2 \leq c^2$, so

$$-D = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2$$

and $a \leq \sqrt{\frac{-D}{3}}$.

Now let us prove that each primitive positive definite form f is properly equivalent to a unique reduced form.

Step 1: We claim that f is properly equivalent to a form f' with $|b(f')| \leq a(f') \leq c(f')$. Among all forms properly equivalent to f , choose an $f' = ax^2 + bxy + cy^2$ such that $|b|$ is minimal. If $a < |b|$, then

$$g(x, y) := f(x + my, y) = ax^2 + (2am + b)xy + c'y^2$$

is properly equivalent to f , and since $a < |b|$, we may choose m such that $|2am+b| < |b|$, contradiction. Thus $a \geq |b|$. By symmetry – or if you like, using $f(x, mx+y)$ – we must have $c \geq |b|$. If $a > c$, we may exchange the outer coefficients by the proper equivalence

$$f(x, y) \mapsto \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot f(x, y) = f(-y, x).$$

We get a properly equivalent form, say f_1 , with $|b| \leq a \leq c$.

Step 2: The form $f_1(x, y) = ax^2 + bxy + cy^2$ is already properly reduced unless $b < 0$ and ($a = c$ or $b = -a$). In that case, $f_2(x, y) = ax^2 - bxy + cy^2$ is reduced, so it will suffice to show that f_2 is properly equivalent to f_1 . If $a = c$, then $(x, y) \mapsto (-y, x)$ carries f_1 to f_2 ; if $b = -a$, then $(x, y) \mapsto (x+y, y)$ carries f_1 to f_2 .

Step 3: We need to show that the reduced form properly equivalent to f is unique. First observe that if $f(x, y) = ax^2 + bxy + cy^2$ with $|b| \leq a \leq c$, then

$$f(x, y) \geq (a - |b| + c) \min(x^2, y^2).$$

Thus $xy \neq 0$ implies $f(x, y) \geq a - |b| + c \geq c$, so that the smallest nonzero value of f is a .

Case 1: $b = a = c$. Then primitivity implies $a = b = c = 1$ and $f(x, y) = q_{-3}(x, y) = x^2 + xy + y^2$. This form represents 1 in 6 different ways, corresponding to the 6 norm one elements of $\mathbb{Z}[\frac{1+\sqrt{3}}{2}]$, and it is easy to check that no other primitive reduced form does so. Or note that we have already computed that q_3 is the unique reduced form of discriminant 3!

Case 2: $|b| < a = c$. Then $xy \neq 0$ implies $f(x, y) \geq a - |b| + c > c = a$. So f represents a precisely four times, by $(\pm 1, 0)$ and by $(0, \pm 1)$. Any equivalent reduced form would be of the form $f'(x, y) = ax^2 + b'xy + c'y^2$. Suppose $c' > a$. Then $f'(0, \pm 1) > a$ and for any $x, y \neq 0$, $f'(x, y) \geq a - |b'| + c' > a$, so that f' only represents a twice, a contradiction since equivalent definite forms represent the same integers exactly the same number of times. Therefore $c' = a$, and since f' is reduced we must have $f'(x, y) = ax^2 + b'xy + cy^2$ with $b' \geq 0$; since $(b')^2 - 4ac = b^2 - 4ac$ and $b, b' \geq 0$, we have $b = b'$ and $f = f'$.

Case 3: $a < c$. Then the second smallest nonzero number properly represented by f is c , so that the outer coefficients of a reduced form are characterized as being the smallest two numbers primitively represented by the form and are therefore unique. Fixing a, c and $D = b^2 - 4ac$, it follows that in this case the only other reduced form which could possibly be equivalent to $ax^2 + bxy + cy^2$ is $ax^2 - bxy + cy^2$.

Case 3(a): If $|b| = a$, then by definition of reduced we have $b \geq 0$ and there is nothing to show.

Case 3(b): Otherwise we have $|b| < a < c$, and this is easily seen to imply that the only vectors (x, y) such that $f(x, y) = a$ are $(\pm 1, 0)$ and the only vectors (x, y) such that $f(x, y) = c$ are $(0, \pm 1)$. In this case we claim that $ax^2 + bxy + cy^2$ and $ax^2 - bxy + cy^2$ may be equivalent, but they are not *properly equivalent*. Indeed,

suppose there exist integers p, q, r, s with $ps - qr = 1$ such that

$$g(x, y) = f(px + qy, rx + sy).$$

Then $a = g(1, 0) = f(p, q)$ and $c = g(0, 1) = f(r, s)$ are proper representations. Therefore $(p, q) = \pm(1, 0)$ and $(r, s) = \pm(0, 1)$, so that $q = r = 0$ and either $p = s = 1$ or $p = s = -1$. Either way $g(x, y) = f(x, y)$. This completes the proof of the Reduction Theorem.

7. AMBIGUOUS CLASSES

Note that any primitive form $f = ax^2 + bxy + cy^2 \in \mathcal{C}(D)$ is widely equivalent to the form $f' = ax^2 - bxy + cy^2$, since $\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \bullet f = f'$. One says that f , as well as its equivalence class in $\mathcal{C}(D)$, is **ambiguous** if it is also properly equivalent to f' . For instance, the principal class $[q_D]$ is always ambiguous.

Exercise 3.6.1: For $q = (a, b, c) = ax^2 + bxy + cy^2$ a primitive quadratic form of discriminant $D < 0$, define $\iota(q) := (a, -b, c) = ax^2 - bxy + cy^2$.

a) Show that $q \mapsto \iota(q)$ gives an involution on the set of primitive forms of discriminant D .

b) Show that if q is properly equivalent to q' , then $\iota(q)$ is properly equivalent to $\iota(q')$. (Hint: Represent ι as a matrix $\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ and show that ι normalizes $\text{SL}_2(\mathbb{Z})$.) Deduce that ι descends to an involution on the finite set $\mathcal{C}(D)$ of proper equivalence classes of primitive forms of discriminant D .

c) Let $\mathcal{C}_\iota(D) = (\mathcal{C}(D))/\iota$ be the quotient under the action of ι : i.e., we identify $[a, b, c]$ with $[a, -b, c]$. Show that this quotient is precisely the set of wide equivalence classes of primitive forms of discriminant D .

d) Represent a class $[q] \in \mathcal{C}(D)$ by its unique reduced form $q = (a, b, c)$. Show that $[q] = \iota[q]$ iff $q = (a, b, a)$ or $(a, 0, c)$.

Exercise 3.6.2: Let $n = p_1^{a_1} \cdots p_r^{a_r}$, and let $D = -4n$. Exhibit 2^{r-1} distinct reduced primitive forms of discriminant D , and therefore conclude $\#\mathcal{C}(-4n) \geq 2^{r-1}$.

The full story is given by the following result:

Theorem 7. *Let D be a negative quadratic discriminant, and let r be the number of odd primes dividing D . Define a number μ as follows: if $D \equiv 1 \pmod{4}$, then $\mu = r$; otherwise $D = -4n$ and*

$$\mu = \left\{ \begin{array}{ll} r, & n \equiv 3 \pmod{4}. \\ r+1, & n \equiv 1, 2 \pmod{4}. \\ r+1, & n \equiv 4 \pmod{8}. \\ r+2, & n \equiv 0 \pmod{8}. \end{array} \right\}.$$

The number $h_2(D)$ of ambiguous classes of discriminant D is $2^{\mu-1}$.

Project 2: Prove Theorem 7. Note that this appears as Proposition 3.11 on p.52 of Cox's book, and he gives some but not all of the proof. (As with several other results in this course, the proof is not particularly difficult, but still requires a fair amount of time and energy.)

Comment: Soon enough we will see that $\mathcal{C}(D)$ has the natural structure of a commutative group, and with respect to this structure $\iota([q]) = [q]^{-1}$. This shows first that the wide equivalence classes of quadratic forms have the structure of a finite commutative group modulo inversion, hence *not* a natural group structure (this explains why we work with proper equivalence), and second that the elements of order 2 are given by part d).

8. LANDAU'S THEOREM

Theorem 8. (*Landau, 1903*) *For a positive integer n , TFAE:*

- (i) *The only primitive reduced form of discriminant $-4n$ is $x^2 + ny^2$.*
- (ii) *$n = 1, 2, 3, 4$ or 7 .*

Proof: It suffices (and is necessary!) to exhibit, for each positive integer n different from 1, 2, 3, 4, 7, a nonprincipal primitive reduced form (nprf) of discriminant $-4n$. We resort to a case by case analysis.

Case 1: If $n = 8$, then $3x^2 + 2xy + 3y^2$ is a nprf of discriminant -32 . If $n = 31$, $5x^2 \pm 4xy + 7y^2$ is nprf of discriminant -124 .

Case 2: Suppose n is not a prime power. Then we may factor $n = ac$ with $1 < a < c$ and $\gcd(a, c) = 1$. Then the form $ax^2 + cy^2$ is reduced of discriminant $-4n$. (We saw this already when $n = 6$.)

Case 3: Suppose $n = p^r$ for an odd prime p , $n + 1 \neq 2^s$. Then we may write $n + 1 = ac$ with $1 < a < c$ and $\gcd(a, c) = 1$ and $ax^2 + 2xy + cy^2$ is a nprf of discriminant $-4n$.

Case 4: $n = p^r$ for an odd prime p , $n + 1 = 2^s$. The cases $s = 1, 2, 3$ correspond to $n = 1, 3, 7$ so are excluded from consideration. If $s = 4$, then $n = 15$ is covered by Case 2. If $s = 5$, $n = 31$ is covered by Case 1. Otherwise $s \geq 6$. Then $8x^2 + 6xy + (2^{s-3} + 1)y^2$ is a nprf of discriminant $36 - 4(8)(2^{s-3} + 1) = -4 \cdot 2^s + 4 = -4(2^s - 1) = -4n$.

Case 5: Otherwise $n = 2^r$. The cases $s = 1, 2$ correspond to $n = 2, 4$ so are excluded. The case $r = 3$, then $n = 8$ is covered by Case 1. Otherwise $r \geq 4$. Then $4x^2 + 4xy + (2^{r-2} + 1)y^2$ is nonprincipal, primitive and reduced of discriminant $-2^{r+2} = -4n$.