BASIC NUMBER THEORY: LECTURE 2

WENHAN DAI

1. Quadratic forms

Definition 1. A *quadratic form* on $\mathbb{Z}$ is a function in two variables $f(x,y) = ax^2+bxy+cy^2 \in \mathbb{Z}[x,y]$ with $a,b,c \in \mathbb{Z}$.

(1) $f(x,y)$ is called *primitive* if $(a,b,c) := \gcd(a,b,c) = 1$.

(2) Two quadratic forms $f(x,y)$ and $g(x,y)$ are *equivalent*, denoted by $f(x,y) \sim g(x,y)$, if

$$\exists \begin{pmatrix} p & r \\ q & s \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}), \quad g(x,y) = f\left((x,y)\begin{pmatrix} p & r \\ q & s \end{pmatrix}\right) = f(px+qy, rx+sy).$$

Moreover, they are *properly equivalent* if the matrix lies in $\mathrm{SL}_2(\mathbb{Z})$.

(3) An integer $m \in \mathbb{Z}$ is *represented by f* if there exist $x, y \in \mathbb{Z}$ such that $f(x,y) = m$. It is *properly represented by f* if moreover $(x,y) := \gcd(x,y) = 1$.

Remark 2. (1) It can be proved that (proper) equivalence is actually an equivalence relation.

(2) Suppose $f \sim g$. Then they represent the same set of integers in $\mathbb{Z}$. Moreover, if this is a proper equivalence, then they properly represent the same set.

Lemma 3. *A quadratic form f properly represents some integer m if and only if $f \sim mx^2 + Bxy + Cy^2$ for some $B, C \in \mathbb{Z}$.*

Proof. The necessity is obvious as one may take $x = 1$ and $y = 0$. Conversely, suppose $f(p,q) = m$ with some p, q satisfying $(p,q) = 1$. Choose $r, s \in \mathbb{Z}$ with p, q given such that the matrix $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Then

$$f\left((x,y)\begin{pmatrix} p & q \\ r & s \end{pmatrix}\right) = f(px+ry, qx+sy) = f(p,q)x^2 + \underbrace{f(r,s)}_{=B}y^2 + Cxy$$

for some $C \in \mathbb{Z}$ that is computable. □

Definition 4. The *discriminant* of a quadratic form $f(x,y) = ax^2+bxy+cy^2$ is

$$D(f) = b^2 - 4ac \equiv 0, 1 \bmod 4.$$

Exercise 5. Check that if $g(x,y) = f\left((x,y)\begin{pmatrix} p & r \\ q & s \end{pmatrix}\right)$, then $D(g) = D(f)(ps-qr)^2$. From this, we see whenever f is properly equivalent to g, then $D(f) = D(g)$. Namely, the discriminant is a invariant under the proper equivalence.

Date: September 25, 2020.

The definition of discriminant together with Exercise 5 gives arise of a natural map

$$\{\text{proper equivalence classes of quadratic forms over } \mathbb{Z}\} \longrightarrow \{D \in \mathbb{Z} : D \equiv 0, 1 \bmod 4\}.$$

It is natural to ask for a formal converse of this map, even if it is not well-defined.

Lemma 6. *Let $D \equiv 0, 1 \bmod 4$ and m be an odd integer with $(m, D) = 1$. Then the following are equivalent.*

- *m is properly represented by some f with $D(f) = D$, and*
- *$\left(\frac{D}{m}\right) = 1$, i.e. D is a quadratic residue of m.*

Proof. Supposing the first condition, by Lemma 3 we have $f \sim mx^2 + Bxy + Cy^2$ for some $B, C \in \mathbb{Z}$. Taking the discriminant, we have $D = D(f) = B^2 - 4mC \equiv B^2 \bmod m$. Hence D is a quadratic residue modulo m. Conversely, say $D \equiv B^2 \bmod m$ with m odd, then (replacing $B' = B + 2m$ if necessary) $D \equiv B'^2 \bmod 4m$ for some B'. Thus, there exists $C \in \mathbb{Z}$ such that $D = B'^2 - 4mC$ with $f \sim mx^2 + Bxy + Cy^2$. □

Corollary 7. *Let p be an odd prime with $p \nmid n$. Then p is represented by a primitive form f with discriminant $D(f) = -4n$ if and only if*

$$\left(\frac{-n}{p}\right) = 1.$$

Proof. First we observe that

$$\left(\frac{-4n}{p}\right) = \left(\frac{2}{p}\right)^2 \left(\frac{-n}{p}\right) = \left(\frac{-n}{p}\right).$$

So we are in the case of Lemma 6. Hence the equivalence goes to say p is represented by some f such that $D(f) = D = -4n$. Again, using Lemma 3, can choose $f = px^2 + B'xy + Cy^2$ with $B', C \in \mathbb{Z}$. Moreover, as p is odd and $p \nmid n$, we see $(p, B', C) = 1$ and the primitivity follows. □

Definition 8. (1) A primitive quadratic form $f(x, y)$ is *positive definite* if for all $(x, y) \in \mathbb{Z}$, $f(x, y) > 0$.
(2) A primitive positive definite form (ppdf) $ax^2+bxy+cy^2$ is called *reduced* if $|b| \leqslant a \leqslant c$ and $b \geqslant 0$ if either $|b| = a$ or $a = c$.

Note from the definition that if f is a reduced ppdf, then $D(f) < 0$ and $D(f) \equiv 0, 1 \bmod 4$. On the other hand, it turns out that the inverse of our desired map

$$\{D \in \mathbb{Z} : D \equiv 0, 1 \bmod 4\} \longrightarrow \{\text{proper equivalence classes of quadratic forms over } \mathbb{Z}\}$$

is formally one-to-many. The main issue is that it is almost impossible to restrict the formal converse into a one-to-one map even if some conditions (like representing some integer m in Lemma 6) inserted. We are thus forced to rather consider

$$\{D \in \mathbb{Z} : D \equiv 0, 1 \bmod 4\} \longrightarrow \left\{\begin{matrix}\text{families of proper equivalence classes of primitive} \\ \text{positive definite forms with discriminant } D\end{matrix}\right\}.$$

Moreover, using the reduced primitive positive definite forms, the representatives of each proper equivalence class can be chosen uniquely. See the following theorem.

Theorem 9. *Each primitive positive definite form is properly equivalent to a unique reduced form.*

Proof. We only sketch the idea of the proof in the most typical cases.

(1) **Existence.**
Suppose $f = ax^2 + bxy + cy^2$ is a ppdf, and then $a, c > 0$. Consider via the proper equivalence relation that

$$g(x,y) = f\left((x,y)\begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix}\right) = f(x+my,y) = ax^2 + (2am+b)xy + c'y^2$$

for some computable $c' \in \mathbb{Z}$. One can take each of the following two operations:
 (i) Choose some m such that $|2am+b| \leqslant a$ and replace b with $2am+b$. Hence we have $ax^2 + bxy + cy^2$ with $|b| \leqslant a$.
 (ii) If $a > c$, use the change of variables

$$(x,y) \mapsto (y,-x) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \rightsquigarrow \quad ax^2 + bxy + cy^2 \mapsto cx^2 - bxy + ay^2.$$

By swapping a and c, we get $a \leqslant c$.

After taking finitely many operators (i) and (ii), we get $ax^2 + bxy + cy^2$ with $|b| \leqslant a \leqslant c$ using $\mathrm{SL}_2(\mathbb{Z})$-actions, i.e., via the proper equivalence. It remains to deal with the second condition in Definition 8(2). If $ax^2 + bxy + cy^2$ is still non-reduced, then either $b < 0$, $-b = a$ or $b < 0$, $a = c$. For the former case, choose $m = 1$ in (i); for the latter case, use the transform $(x,y) \mapsto (-y,x)$. Then the existence follows.

(2) **Uniqueness.**
Suppose $|b| < a < c$. If $xy \neq 0$ then $f(x,y) \geqslant a + c - |b|$ and $\min\{x^2,y^2\} > \max\{a,c\}$, with $f(x,0) = ax^2$ and $f(0,y) = cy^2$. Thus, a is the smallest nonzero value of f and c is the next smallest nonzero value which is properly represented by f (which is still valid if $|b| \leqslant a < c$). They are reached via

$$f(x,y) = a \iff (x,y) = (\pm 1, 0), \quad f(x,y) = c \iff (x,y) = (0, \pm 1).$$

Now suppose $f \sim g = a'x^2 + b'xy + c'y^2$ is reduced. Then a' is the smallest nonzero value of g, so $a' = a$. If $a' = c'$ then $g(\pm 1, 0) = g(0, \pm 1) = c' = a$. However, f has only two ways to properly represent an integer, which leads to a contradiction. So $a' < c'$, and $g(0, \pm 1) = c'$ is the next smallest nonzero value that is properly represented by g. We infer that $c = c'$, and $g(x,y) = c'$ with $(x,y) = 1$ if and only if $(x,y) = (0, \pm 1)$.

Again, we then suppose $g(x,y) = f\left((x,y)\begin{pmatrix} p & r \\ q & s \end{pmatrix}\right)$. Plugging conditions on a and c into this, we see

$$(\pm 1, 0) = (\pm 1, 0)\begin{pmatrix} p & r \\ q & s \end{pmatrix}, \ (0, \pm 1)\begin{pmatrix} p & r \\ q & s \end{pmatrix} = (0, \pm 1) \implies \begin{pmatrix} p & r \\ q & s \end{pmatrix} = \pm I_2.$$

This almost completes the proof, and the argument in remaining cases is left as an exercise. $\square$

2. Class number

Definition 10. For an integer $D < 0$ such that $D \equiv 0, 1 \bmod 4$, define the *class number* $h(D)$ to be the number of properly equivalent classes of primitive positive definite forms of discriminant D (or equivalently, by Theorem 9, the number of different reduced forms with discriminant D).

Theorem 11. *For all $D \in \{D \in \mathbb{Z}_{<0} : D \equiv 0, 1 \bmod 4\}$, $h(D)$ is finite.*

Proof. By definition, we regard $h(D)$ as the number of different reduced forms with discriminant D. For each reduced ppdf $f = ax^2 + bxy + cy^2$ with $D = D(f) = b^2 - 4ac$, the condition $|b| \leqslant a \leqslant c$ implies $D \leqslant -3a^2 \leqslant 0$. Hence for a fixed D, there are only finitely many possibilities of a, and hence finitely many choices of b. The value of c is totally determined whenever a, b, D are given. $\square$

The following table lists out some numerical results for the cases where $D(x^2 + ny^2) = -4n$.

D	$h(D)$	Reduced forms
-4	1	$x^2 + y^2$
-8	1	$x^2 + 2y^2$
-12	1	$x^2 + 3y^2$
-20	2	$x^2 + 5y^2,\ 2x^2 + 2xy + 3y^2$
-28	1	$x^2 + 7y^2$
-56	4	$x^2 + 14y^2,\ 2x^2 + 7y^2,\ 3x^2 \pm 2xy + 5y^2$
-108	3	$x^2 + 27y^2,\ 4x^2 \pm 2xy + 7y^2$
-256	4	$x^2 + 64y^2,\ 4x^2 + 4xy + 17y^2,\ 5x^2 \pm 2xy + 13y^2$

Theorem 12. *Suppose $n \in \mathbb{Z}_{>0}$. Then $h(-4n) = 1$ if and only if $n \in \{1, 2, 3, 4, 7\}$.*

Remark 13. More generally, given $D \in \mathbb{Z}_{<0}$ that $D \equiv 0, 1 \bmod 4$, then $h(D) = 1$ if and only if

$$D \in \{-4, -8, -12, -16, -28\} \cup \{-3, -7, -11, -19, -27, -43, -67, -143\}.$$

For a given negative integer D, we will associate an order of discriminant D in $K = \mathbb{Q}(\sqrt{D})$. In particular, $\mathcal{O}_K$ is the maximal order.

School of Mathematical Sciences, Peking University, 100871, Beijing, China
Email address: daiwenhan@pku.edu.cn