9.3 Reduction Theory

Recall that a binary quadratic form is a polynomial of the form $f(x,y) = ax^2+bxy+cy^2$. Our motivating problem is to decide which numbers are represented by f; i.e., for which integers n do there exist integers x, y such that $ax^2 + bxy + cy^2 = n$? If $g \in \mathrm{SL}_2(\mathbb{Z})$ then $f(x,y)$ and $f|_g(x,y) = f\left(g\begin{bmatrix} x \\ y \end{bmatrix}\right)$ represent exactly the same set of integers. Also, $\mathrm{disc}(f) = \mathrm{disc}(f|_g)$, where $\mathrm{disc}(f) = b^2 - 4ac$, and f is called *positive definite* if $\mathrm{disc}(f) < 0$ and $a > 0$.

This section is about reduction theory, which allows us to decide whether or not two positive definite binary quadratic forms are equivalent under the action of $\mathrm{SL}_2(\mathbb{Z})$.

9.3.1 Reduced Forms

Definition 9.3.1 (Reduced). A positive definite quadratic form (a, b, c) is *reduced* if $|b| \leq a \leq c$ and if, in addition, when one of the two inequalities is an equality (i.e., either $|b| = a$ or $a = c$), then $b \geq 0$.

There is a geometric interpretation of the notion of being reduced. Let $D = \mathrm{disc}(a,b,c) = b^2 - 4ac$ and set $\tau = \frac{-b+\sqrt{D}}{2a}$, so τ is the root of $ax^2 + bx + c$ with positive imaginary part. The right action of $\mathrm{SL}_2(\mathbb{Z})$ on positive definite binary quadratic forms corresponds to the left action of $\mathrm{SL}_2(\mathbb{Z})$ by linear fractional transformations on the complex upper half plane $\mathfrak{h} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. The standard "fundamental domain" for the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathfrak{h}$ is

$$\mathcal{F} = \left\{\tau \in \mathfrak{h} : \mathrm{Re}(\tau) \in \left[-\frac{1}{2}, \frac{1}{2}\right), |\tau| > 1 \text{ or } |\tau| = 1 \text{ and } \mathrm{Re}(\tau) \leq 0\right\}.$$

Then (a, b, c) is reduced if and only if the corresponding complex number τ lies in $\mathcal{F}$. For example, if (a, b, c) is reduced then $\mathrm{Re}(\tau) = -b/2a \in [-1/2, 1/2)$ since $|b| \leq a$ and if $|b| = a$ then $b \geq 0$. Also

$$|\tau| = \sqrt{\frac{b^2 + 4ac - b^2}{4a^2}} = \sqrt{\frac{c}{a}} \geq 1$$

and if $|\tau| = 1$ then $b \geq 0$ so $\mathrm{Re}(\tau) \leq 0$.

The following theorem highlights the importance of reduced forms.

Theorem 9.3.2. *There is exactly one reduced form in each equivalence class of positive definite binary quadratic forms.*

Proof. We have to prove two things. First, that every class contains at least one reduced form, and second that this reduced form is the only one in the class.

We first prove that there is a reduced form in every class. Let $\mathcal{C}$ be an equivalence class of positive definite quadratic forms of discriminant D. Let (a,b,c) be an element of $\mathcal{C}$ such that a is minimal (amongst elements of $\mathcal{C}$). Note that for any such form we have $c \geq a$, since (a,b,c) is equivalent to $(c,-b,a)$ (use the matrix $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$). Applying the element $\left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ to (a,b,c) for a suitably chosen integer k (precisely, $k = \lfloor (a-b)/2a \rfloor$) results in a form (a',b',c') with $a' = a$ and $b' \in (-a', a']$. Since $a' = a$ is minimal, we have just as above that $a' \leq c'$, hence (a',b',c') is "just about" reduced. The only possible remaining problem would occur if $a' = c'$ and $b' < 0$. In that case, changing (a',b',c') to $(c'',b'',a'') = (c',-b',a')$ results in an equivalent form with $b'' > 0$, so that (c'',b'',a'') is reduced.

Next suppose (a,b,c) is a reduced form. We will now establish that (a,b,c) is the only reduced form in its equivalence class. First, we check that a is minimal amongst all forms equivalent to (a,b,c). Indeed, every other a' has the form $a' = ap^2 + bpr + cr^2$ with p, r coprime integers (see this by hitting (a,b,c) by $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right)$). The identities

$$ap^2 + bpr + cr^2 = ap^2\left(1 + \frac{b}{a}\frac{r}{p}\right) + cr^2 = ap^2 + cr^2\left(1 + \frac{b}{c}\frac{p}{r}\right)$$

then imply our claim since $|b| \leq a \leq c$ (use the first identity if $r/p < 1$ and the second otherwise). Thus any other reduced form (a',b',c') equivalent to (a,b,c) has $a' = a$. But the same identity implies that the only forms equivalent to (a,b,c) with $a' = a$ are obtained by applying a transformation of the form $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ (corresponding to $p = 1$, $r = 0$). Thus $b' = b + 2ak$ for some k. Since $a = a'$ we have $b, b' \in (-a, a]$, so $k = 0$. Finally

$$c' = \frac{(b')^2 - D}{4a'} = \frac{b^2 - D}{4a} = c,$$

so $(a',b',c') = (a,b,c)$. $\square$

9.3.2 Finding an Equivalent Reduced Form

Here is how to find the reduced form equivalent to a given positive definite form (a,b,c). This algorithm is useful for solving problems 8 and 9 on the homework assignment. Consider the following two operations, which can be used to diminish one of a and $|b|$, without altering the other:

1. If $c < a$, replace (a,b,c) by the equivalent form $(c,-b,a)$.
2. If $|b| > a$, replace (a,b,c) by the equivalent form (a,b',c') where $b' = b + 2ka$ and k is chosen so that $b' \in (-a, a]$ (more precisely, $k = \lfloor \frac{a-b}{2a} \rfloor$), and c' is found from the fact that $(b')^2 - 4ac' = D = \mathrm{disc}(a,b,c)$, so $c' = \frac{(b')^2 - D}{4a}$.

Starting with (a, b, c), if you iterate the appropriate operation, eventually you will find the reduced form that is equivalent to (a, b, c).

Example 9.3.3. Let $f = 458x^2 + 214xy + 25y^2$.

Equivalent form	What I did	Matrix
$(458, 214, 25)$		
$(25, -214, 458)$	(1)	$\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$
$(25, -14, 2)$	(2) with $k = 4$	$\left(\begin{smallmatrix} 1 & 4 \\ 0 & 1 \end{smallmatrix}\right)$
$(2, 14, 25)$	(1)	$\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$
$(2, 2, 1)$	(2) with $k = -3$	$\left(\begin{smallmatrix} 1 & -3 \\ 0 & 1 \end{smallmatrix}\right)$
$(1, -2, 2)$	(1)	$\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$
$(1, 0, 1)$	(2) with $k = 1$	$\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$

Let

$$\begin{aligned} g &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & -3 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 3 & 4 \\ -13 & -17 \end{pmatrix}. \end{aligned}$$

Then

$$f|_g = x^2 + y^2!$$

9.4 Class Numbers

Proposition 9.4.1. *Let $D < 0$ be a discriminant. There are only finitely many equivalence classes of positive definite binary quadratic forms of discriminant D.*

Proof. Since there is exactly one reduced binary quadratic form in each equivalence class, it suffices to show that there are only finitely many reduced forms of discriminant D. Recall that if a form (a, b, c) is reduced, then $|b| \leq a \leq c$. If (a, b, c) has discriminant D then $b^2 - 4ac = D$. Since $b^2 \leq a^2 \leq ac$, we have $D = b^2 - 4ac \leq -3ac$, so

$$3ac \leq -D.$$

There are only finitely many positive integers a, c that satisfy this inequality. $\square$

Definition 9.4.2. A binary quadratic form (a, b, c) is called *primitive* if $\gcd(a, b, c) = 1$.

Definition 9.4.3. The *class number* h_D of discriminant $D < 0$ is the number of equivalence classes of primitive positive definite binary quadratic forms of discriminant D.

Table 9.1 lists the class numbers h_D for $-D \leq 599$. Notice that there are just a few 1s at the beginning and then no more.

Theorem 9.4.4 (Heegner, Stark-Baker, Goldfeld-Gross-Zagier). *Suppose D is a negative discriminant that is either square free or* 4 *times a square-free number. Then*

- $h_D = 1$ *only for* $D = -3, -4, -7, -8, -11, -19, -43, -67, -163$.
- $h_D = 2$ *only for* $D = -15, -20, -24, -35, -40, -51, -52, -88, -91, -115, -123, -148, -187, -232, -235, -267, -403, -427$.
- $h_D = 3$ *only for* $D = -23, -31, -59, -83, -107, -139, -211, -283, -307, -331, -379, -499, -547, -643, -883, -907$.
- $h_D = 4$ *only for* $D = -39, -55, -56, -68, \ldots, -1555$.

To quote Henri Cohen: "The first two statements concerning class numbers 1 and 2 are very difficult theorems proved in 1952 by Heegner and in 1968–1970 by Stark and Baker. The general problem of determing all imaginary quadratic fields with a given class number has been solved in principle by Goldfeld-Gross-Zagier, but to my knowledge the explicit computations have been carried to the end only for class numbers 3 and 4 (in addition to the already known class numbers 1 and 2).

TABLE 9.1. Class Numbers

$-D$	h_D	$-D$	h_D	$-D$	h_D	$-D$	h_D	$-D$	h_D
3	**1**	123	2	243	3	363	4	483	4
7	**1**	127	5	247	6	367	9	487	7
11	**1**	131	5	251	7	371	8	491	9
15	2	135	6	255	12	375	10	495	16
19	**1**	139	3	259	4	379	3	499	3
23	3	143	10	263	13	383	17	503	21
27	**1**	147	2	267	2	387	4	507	4
31	3	151	7	271	11	391	14	511	14
35	2	155	4	275	4	395	8	515	6
39	4	159	10	279	12	399	16	519	18
43	**1**	163	**1**	283	3	403	2	523	5
47	5	167	11	287	14	407	16	527	18
51	2	171	4	291	4	411	6	531	6
55	4	175	6	295	8	415	10	535	14
59	3	179	5	299	8	419	9	539	8
63	4	183	8	303	10	423	10	543	12
67	**1**	187	2	307	3	427	2	547	3
71	7	191	13	311	19	431	21	551	26
75	2	195	4	315	4	435	4	555	4
79	5	199	9	319	10	439	15	559	16
83	3	203	4	323	4	443	5	563	9
87	6	207	6	327	12	447	14	567	12
91	2	211	3	331	3	451	6	571	5
95	8	215	14	335	18	455	20	575	18
99	2	219	4	339	6	459	6	579	8
103	5	223	7	343	7	463	7	583	8
107	3	227	5	347	5	467	7	587	7
111	8	231	12	351	12	471	16	591	22
115	2	235	2	355	4	475	4	595	4
119	10	239	15	359	19	479	25	599	25