9

Binary Quadratic Forms and Ideal Class Groups

In this chapter, we will study binary quadratic forms.[1] 1

A simple example of a binary quadratic form is

$$f(x, y) = x^2 + y^2.$$

For which integers n do there exist integer x and y such that $x^2 + y^2 = n$? We will answer this question in Section 9.1.

9.1 Sums of Two Squares

Theorem 9.1.1. *A number n is a sum of two squares if and only if all prime factors of n of the form $4m + 3$ have even exponent in the prime factorization of n.*

In this section we give two very different proofs of Theorem 9.1.1. The first is very arithmetic and builds on results about continued fractions from Chapter 7. The second more algebraic proof uses quadratic reciprocity from Chapter 6 to understand splitting of ideals in the ring $\mathbb{Z}[i]$ of Gaussian integers.

Before tackling the proofs, we consider a few examples. Notice that $5 = 1^2 + 2^2$ is a sum of two squares, but 7 is not a sum of two squares, because the congruence $x^2 + y^2 \equiv 7 \pmod{8}$ has no solution. Since 2001 is divisible

[1] Put a complete chapter outline here, with philosophy.

by 3 (because 2 + 1), but not by 9 (since 2 + 1 is not), Theorem 9.1.1 implies that 2001 is not a sum of two squares. The theorem implies that $2 \cdot 3^4 \cdot 5 \cdot 7^2 \cdot 13$ is a sum of two squares, but that $21 = 3 \cdot 7$ is not a sum of two squares even though $21 \equiv 1 \pmod 4$.

Remark 9.1.2. More generally, every natural number is a sum of four integer squares. A natural number is a sum of three squares if and only if it is not a power of 4 times a number that is congruent to 7 modulo 8. For example, 7 is not a sum of three squares, as one can easily see by considering $x^2 + y^2 + z^2 \equiv 7 \pmod 8$. See[2] for proofs. 2

Definition 9.1.3 (Primitive). A representation $n = x^2 + y^2$ is *primitive* if x and y are coprime.

Lemma 9.1.4. *If n is divisible by a prime p of the form $4m+3$, then n has no primitive representations.*

Proof. Suppose $p = 4m + 3$ divides n. If n has a primitive representation, $n = x^2 + y^2$, then

$$p \mid x^2 + y^2 \quad \text{and} \quad \gcd(x, y) = 1,$$

so $p \nmid x$ and $p \nmid y$. Since $\mathbb{Z}/p$ is a field we divide by y^2 in the equation $x^2 + y^2 \equiv 0 \pmod p$ to see that $(x/y)^2 \equiv -1 \pmod p$. Thus the quadratic residue symbol $\left(\frac{-1}{p}\right)$ equals $+1$. However, by Proposition 6.2.1,

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = (-1)^{(4m+3-1)/2} = (-1)^{2m+1} = -1,$$

a contradiction. Thus no prime of the form $4m + 3$ divides n. $\square$

Proof of Theorem 9.1.1 ($\Longrightarrow$). Suppose that p is of the form $4m + 3$, that $p^r \parallel n$ (exactly divides) with r odd, and that $n = x^2 + y^2$. Letting $d = \gcd(x, y)$, we have

$$x = dx', \quad y = dy', \quad n = d^2 n'$$

with $\gcd(x', y') = 1$ and

$$(x')^2 + (y')^2 = n'.$$

Because r is odd, $p \mid n'$, so Lemma 9.1.4 implies that $\gcd(x', y') > 1$, a contradiction. $\square$

To prepare for our two proofs of the ($\Longleftarrow$) direction of Theorem 9.1.1, we reduce the problem to the case when n is prime. Write $n = n_1^2 n_2$ where

[2] Choose a nice reference. Hardy-Wright?

n_2 has no prime factors of the form $4m+3$. It suffices to show that n_2 is a sum of two squares. Also note that

$$(x_1^2+y_1^2)(x_2^2+y_2^2) = (x_1x_2 - y_1y_2)^2 + (x_1y_2 + x_2y_1)^2,$$

so a product of two numbers that are sums of two squares is also a sum of two squares. (This algebraic identity is the assertion that the norm $N : \mathbb{Q}(i)^\times \to \mathbb{Q}^\times$ sending $x+iy$ to $(x+iy)(x-iy) = x^2+y^2$ is a group homomorphism.) Also, $2 = 1^2 + 1^2$ is a sum of two squares.

It thus suffices to show that if $p = 4m+1$, then p is a sum of two squares.

9.1.1 Arithmetic Proof of Theorem 9.1.1

Lemma 9.1.5. *If $x \in \mathbb{R}$ and $n \in \mathrm{N}$, then there is a fraction $\dfrac{a}{b}$ in lowest terms such that $0 < b \leq n$ and*

$$\left| x - \frac{a}{b} \right| \leq \frac{1}{b(n+1)}.$$

Proof. Consider the continued fraction expansion $[a_0, a_1, \ldots]$ of x. By Corollary 7.2.10, for each m

$$\left| x - \frac{p_m}{q_m} \right| < \frac{1}{q_m \cdot q_{m+1}}.$$

Since $q_{m+1} \geq q_m + 1$ and $q_0 = 1$, either there exists an m such that $q_m \leq n < q_{m+1}$, or the continued fraction expansion of x is finite and n is larger than the denominator of the rational number x, in which case we take $\frac{a}{b} = x$ and are done. In the first case,

$$\left| x - \frac{p_m}{q_m} \right| < \frac{1}{q_m \cdot q_{m+1}} \leq \frac{1}{q_m \cdot (n+1)},$$

so $\dfrac{a}{b} = \dfrac{p_m}{q_m}$ satisfies the conclusion of the lemma. □

Proof of Theorem 9.1.1 ($\Longleftarrow$). Suppose $p = 4m+1$ is a prime. Since

$$(-1)^{(p-1)/2} = (-1)^{(4m+1-1)/2} = +1,$$

Proposition 6.2.1 implies that -1 is a square modulo p; i.e., there exists $r \in \mathbb{Z}$ such that $r^2 \equiv -1 \pmod{p}$. Lemma 9.1.5, with $n = \lfloor \sqrt{p} \rfloor$ and $x = -\frac{r}{p}$, implies that there are integers a, b such that $0 < b < \sqrt{p}$ and

$$\left| -\frac{r}{p} - \frac{a}{b} \right| \leq \frac{1}{b(n+1)} < \frac{1}{b\sqrt{p}}.$$

Let $c = rb + pa$; then

$$|c| < \frac{pb}{b\sqrt{p}} = \frac{p}{\sqrt{p}} = \sqrt{p}$$

and

$$0 < b^2 + c^2 < 2p.$$

But $c \equiv rb \pmod{p}$, so

$$b^2 + c^2 \equiv b^2 + r^2b^2 \equiv b^2(1 + r^2) \equiv 0 \pmod{p}.$$

Thus $b^2 + c^2 = p$. □

9.1.2 Algebraic Proof of Theorem 9.1.1

Let p be a prime that is congruent to 1 modulo 4. In this section we show that p is a sum of two squares by factoring the ideal generated by p in the Gaussian integers as a product of principal ideals.

The Gaussian integers are

$$R = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \subset \mathbb{C},$$

where $i^2 = -1$. The *ideal* generated by $x_1, \ldots, x_n \in R$ is the set (in fact, R-module)

$$(x_1, \ldots, x_n) = Rx_1 + \cdots + Rx_n \subset R$$

of R-linear combinations of the x_i.

Lemma 9.1.6. *There is an integer r such that*

$$(p) = (i - r, p)(i + r, p),$$

where the equality is an equality of ideals in R.

Proof. Because $p \equiv 1 \pmod{4}$, we have $(-1)^{(p-1)/2} = 1$, so by Proposition 6.2.1, there is an $r \in \mathbb{Z}$ such that $r^2 \equiv -1 \pmod{p}$. The ideal product $(i - r, p)(i + r, p)$ is, by definition, the ideal generated by all products of elements in $(i - r, p)$ with elements in $(i + r, p)$. In particular, it contains p^2, $1 + r^2 = -(i - r)(i + r)$, and $-2pr = p(i - r) - p(i + r)$. Since p is odd and divides $1 + r^2$, the greatest common divisor of p^2, $1 + r^2$, and $-2pr$ is p, so $(p) \subset (i - r, p)(i + r, p)$. Since $(i - r)(i + r) = -1 - r^2$ is a multiple of p we see that every element of $(i - r, p)(i + r, p)$ is a multiple of p, which completes the proof. □

The lemma is not quite enough to conclude that p is of the form $a^2 + b^2$. For that, we show that $(i - r, p)$ is generated by a single element, i.e., it is *principal.* The following proposition asserts that every ideal of R is principal by observing that an analogue of the division algorithm holds in R.

Proposition 9.1.7. *The ring R is a principal ideal domain (because it is a Euclidean domain).*

Proof. First we show that R is a Euclidean domain, i.e., there is a function $\lambda : R \to \mathbb{Z}_{\geq 0} = \mathrm{N} \cup \{0\}$ such that for all $x, y \in R$ with $x \neq 0$, there exist $q, r \in R$ such that $y = xq + r$ with $\lambda(r) < \lambda(x)$. To see this, let

$$\lambda(a + bi) = \mathbb{N}(a + bi) = a^2 + b^2$$

be the norm. Then if $x = a + bi \neq 0$ and $y = c + di$, we have

$$\frac{y}{x} = \frac{c + di}{a + bi} = \frac{ac + bd}{\mathbb{N}(x)} + \frac{ad - bc}{\mathbb{N}(x)} i.$$

Let e and f be the integers that are closest to the real and imaginary parts of y/x, respectively. Let $q = e + if$ and $r = y - xq$. Then

$$\mathbb{N}(r) = \mathbb{N}(y/x - q)\mathbb{N}(x) \leq \frac{1}{2} \cdot \mathbb{N}(x).$$

It is now easy to deduce that R is a principal ideal domain. Suppose $I \subset R$ is any nonzero ideal. Let x be an element of I with $\mathbb{N}(x)$ minimal. If $y \in I$ then $y = qx + r$ with $\mathbb{N}(r) < \mathbb{N}(x)$. Since $r = qx - y \in I$, it follows that $\mathbb{N}(r) = 0$, so $r = 0$ and $y \in (x)$. Thus $I = (x)$. $\square$

Recall that

$$(p) = (i - r, p)(i + r, p).$$

By Proposition 9.1.7 the ideals on the right side are principal, so there exists $a + bi \in R$ such that

$$(p) = (a + bi)(a - bi).$$

Since $(a + bi)(a - bi) = (a^2 + b^2)$, it follows that $p = (a^2 + b^2)u$ for some unit u. The units of R are $\pm 1, \pm i$, so since p and $a^2 + b^2$ are positive real numbers, the only possibility is that $u = 1$. Thus $p = a^2 + b^2$, which completes our algebraic proof of Theorem 9.1.1.

This proof is longer than the proof in Section 9.1.1, but every step involves learning about the structure of interesting basic number-theoretic objects. Moreover, the underlying idea of the proof is clearer and suggests generalizations to the problem of representation of primes by more general expressions.

9.2 Binary Quadratic Forms

9.2.1 Introduction

A *binary quadratic form* is a homogeneous polynomial

$$f = ax^2 + bxy + cy^2 \in \mathbb{Z}[x, y].$$

We say that n is *represented* by f if there are integers $x, y \in \mathbb{Z}$ such that $f(x, y) = n$. The representability problem will partially motivate our interest in quadratic forms.

Problem 9.2.1. Given a binary quadratic form f, give a good way to determine whether or not any given integer n is represented by f.

We gave a simple solution to this problem in Section 9.1 in the case when $f = x^2 + y^2$. The set of sums of two squares is the set of integers n such that any prime divisor p of n of the form $4m + 3$ exactly divides n to an even power (along with 0).

9.2.2 Equivalence

For simplicity below we will sometimes write $f\begin{pmatrix} x \\ y \end{pmatrix}$ for $f(x, y)$.

Definition 9.2.2. The modular group $\mathrm{SL}_2(\mathbb{Z})$ is the group of all 2×2 integer matrices with determinant $+1$.

If $\gamma = \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $f(x, y) = ax^2 + bxy + cy^2$ is a quadratic form, let

$$f|_\gamma(x, y) = f(px + qy, rx + sy) = f\left(\begin{pmatrix} p & q \\ r & s \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}\right).$$

Proposition 9.2.3. *The above formula defines a right action of the group* $\mathrm{SL}_2(\mathbb{Z})$ *on the set of binary quadratic forms, in the sense that*

$$f|_{\gamma\delta} = (f|_\gamma)|_\delta,$$

for any $\gamma, \delta \in \mathrm{SL}_2(\mathbb{Z})$.

Proof. Suppose $\gamma, \delta \in \mathrm{SL}_2(\mathbb{Z})$. Then

$$f|_{\gamma\delta}\begin{pmatrix} x \\ y \end{pmatrix} = f\left(\gamma\delta\begin{pmatrix} x \\ y \end{pmatrix}\right) = f|_\gamma\left(\delta\begin{pmatrix} x \\ y \end{pmatrix}\right) = (f|_\gamma)|_\delta\begin{pmatrix} x \\ y \end{pmatrix}.$$

□

Proposition 9.2.4. *Let* $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ *and let* f *be a binary quadratic form. The set of integers represented by* f *is exactly the same as the set of integers represented by* $f|_\gamma$. *(The converse is not true; see Example 9.3.4.)*

Proof. If $f(x_0, y_0) = n$ then since $\gamma^{-1} \in \mathrm{SL}_2(\mathbb{Z})$, we have $\gamma^{-1}\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \in \mathbb{Z}^2$, so

$$f|_\gamma\left(\gamma^{-1}\begin{pmatrix} x_0 \\ y_0 \end{pmatrix}\right) = f\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = n.$$

Thus every integer represented by f is also represented by $f|_\gamma$. Conversely, if $f|_\gamma\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = n$, then $f\left(\gamma\begin{pmatrix} x_0 \\ y_0 \end{pmatrix}\right) = n$, so f represents n. □

Define an equivalence relation $\sim$ on the set of all binary quadratic forms by $f \sim f'$ if there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $f|_\gamma = f'$.

For simplicity, we will sometimes denote the quadratic form $ax^2 + bxy + cy^2$ by (a, b, c). Then, for example, since $\gamma = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, we see that $(a, b, c) \sim (c, -b, a)$, since if $f(x, y) = ax^2 + bxy + cy^2$, then $f(-y, x) = ay^2 - bxy + cx^2$.

Example 9.2.5. Consider the binary quadratic form

$$f(x, y) = 458x^2 + 214xy + 25y^2.$$

Solving the representation problem for f might, at first glance, look hopeless. We find $f(x, y)$ for a few values of x and y:

$$\begin{aligned} f(-1,-1) &= 17 \cdot 41 \\ f(-1,0) &= 2 \cdot 229 \\ f(0,-1) &= 5^2 \\ f(1,1) &= 269 \\ f(-1,2) &= 2 \cdot 5 \cdot 13 \\ f(-1,3) &= 41 \end{aligned}$$

Each number is a sum of two squares! Letting $\gamma = \left(\begin{smallmatrix} 4 & -3 \\ -17 & 13 \end{smallmatrix}\right)$, we have

$$\begin{aligned} f|_\gamma &= 458(4x - 3y)^2 + 214(4x - 3y)(-17x + 13y) + 25(-17x + 13y)^2 \\ &= \cdots = x^2 + y^2!! \end{aligned}$$

Thus by Proposition 9.2.4, f represents an integer n if and only if n is a sum of two squares.

9.2.3 Discriminants

Definition 9.2.6. The *discriminant* of $f(x, y) = ax^2 + bxy + cy^2$ is $b^2 - 4ac$.

Example 9.2.7. Notice that $\mathrm{disc}(x^2 + y^2) = -4$ and

$$\mathrm{disc}(458, 214, 25) = 214^2 - 4 \cdot 25 \cdot 458 = -4.$$

That the discriminants are the same indicates that $(1, 0, 1)$ and $(458, 214, 25)$ are closely related.

Proposition 9.2.8. *If $f \sim f'$, then* $\mathrm{disc}(f) = \mathrm{disc}(f')$.

Proof. By elementary algebra, one sees that if $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, then

$$\mathrm{disc}(f|_\gamma) = \mathrm{disc}(f) \cdot \det(\gamma)^2 = \mathrm{disc}(f).$$

Since $f' = f|_\gamma$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, the proposition follows. □

The converse of the proposition is false. Forms with the same discriminant need not be equivalent. For example, the forms $(1,0,6)$ and $(2,0,3)$ have discriminant -24, but are not equivalent. To see this, observe that $(1,0,6)$ represents 1, but $2x^2 + 3y^2$ can not represent 1.

Proposition 9.2.9. *The set of all discriminants of forms is exactly the set of integers d such that $d \equiv 0$ or* $1 \pmod 4$.

Proof. First note that $b^2 - 4ac$ is a square modulo 4, so it must equal 0 or 1 modulo 4. Next suppose d is an integer such that $d \equiv 0$ or $1 \pmod 4$. If we set

$$c = \begin{cases} -d/4, & \text{if } d \equiv 0 \pmod 4 \\ -(d-1)/4 & \text{if } d \equiv 1 \pmod 4, \end{cases}$$

then $\mathrm{disc}(1,0,c) = d$ in the first case and $\mathrm{disc}(1,1,c) = d$ in the second. □

Definition 9.2.10. The form $(1, 0, -d/4)$ or $(1, 1, -(d-1)/4)$ of discriminant d that appears in the proof of the previous proposition is called the *principal form* of discriminant d.

d	principal form	
-4	(1,0,1)	$x^2 + y^2$
5	(1,1,-1)	$x^2 + xy - y^2$
-7	(1,1,2)	$x^2 + xy + 2y^2$
8	(1,0,-2)	$x^2 - 2y^2$
-23	(1,1,6)	$x^2 + xy + 6y^2$
389	(1,1,-97)	$x^2 + xy - 97y^2$

9.2.4 Definite and Indefinite Forms

Definition 9.2.11. A quadratic form with negative discriminant is called *definite*. A form with positive discriminant is called *indefinite*.

This definition is motivated by the fact that the nonzero integers represented by a definite form are all either positive or negative. To see this, let (a, b, c) be a quadratic form, multiply by $4a$ and complete the square:

$$\begin{aligned} 4a(ax^2 + bxy + cy^2) &= 4a^2x^2 + 4abxy + 4acy^2 \\ &= (2ax + by)^2 + (4ac - b^2)y^2 \end{aligned}$$

If $\mathrm{disc}(a,b,c) < 0$ then $4ac - b^2 = -\mathrm{disc}(a,b,c) > 0$, so the nonzero values taken on by $ax^2 + bxy + cy^2$ are only positive or only negative, depending on the sign of a. On the other hand, if $\mathrm{disc}(a,b,c) > 0$, then $(2ax+by)^2+(4ac-b^2)y^2$ takes both positive and negative values, so (a,b,c) does also.

9.2.5 Rings of Integers in Quadratic Fields

We have seen quadratic number fields several times before. We now make the theory more precise, in order to see how the arithmetic of quadratic number fields is closely linked to the theory of quadratic forms.

Let $D \neq 0, 1$ be a square-free integer. The quadratic field obtained by adjoining $\sqrt{D}$ to $\mathbb{Q}$ is

$$K = \mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\}.$$

Definition 9.2.12 (Integral). An element $x \in K$ is *integral over* $\mathbb{Z}$ if it is the root of a quadratic polynomial of the form $x^2 + ax + b$ with $a, b \in \mathbb{Z}$.

The integral elements of K form an important subring of K.

Definition 9.2.13 (Ring of Integers). The *ring of integers* in K is

$$\mathcal{O}_K = \{x \in K \mid x \text{ is integral over } \mathbb{Z}\}.$$

It's not at all clear from the definition just what $\mathcal{O}_K$ is, or even that it's a ring. Proposition 9.2.16 below will give a more explicit description of $\mathcal{O}_K$.

Lemma 9.2.14. *The map $K \to K$ given by*

$$a + b\sqrt{D} \mapsto \overline{a + b\sqrt{D}} = a - b\sqrt{D}$$

is an isomorphism of fields.

Proof. We have

$$\begin{aligned}
\overline{(a+b\sqrt{D})(c+d\sqrt{D})} &= \overline{(ac+bd)+(ad+bc)\sqrt{D}}\\
&= (ac+bd)-(ad+bc)\sqrt{D}\\
&= (a-b\sqrt{D})(c-d\sqrt{D})\\
&= \overline{a+b\sqrt{D}c+d\sqrt{D}}.
\end{aligned}$$

□

Lemma 9.2.15. *Let $\alpha \in K$. The determinant of left multiplication by α on the 2-dimensional $\mathbb{Q}$-vector space K is $\mathrm{N}(\alpha) = \alpha\overline{\alpha}$. The trace of left multiplication is $\mathrm{Tr}(\alpha) = \alpha + \overline{\alpha}$. The characteristic polynomial of left multiplication by α is $x^2 - \mathrm{Tr}(\alpha)x + \mathrm{N}(\alpha)$.*

Proof. A basis for K as a $\mathbb{Q}$-vector space is $1, \sqrt{D}$. The matrix of left multiplication by $\alpha = a + b\sqrt{D}$ on this basis is $\begin{pmatrix} a & Db \\ b & a \end{pmatrix}$. Since $T(\alpha) = 2a$ and $\mathbb{N}(\alpha) = a^2 - Db^2$, the lemma follows. $\square$

Proposition 9.2.16. *If* $D \equiv 1 \pmod 4$ *let* $\alpha = (1+\sqrt{D})/2$, *and otherwise let* $\alpha = \sqrt{D}$. *Then*

$$\mathcal{O}_K = \mathbb{Z}[\alpha] = \{a\alpha + b : a, b \in \mathbb{Z}\}.$$

Proof. First we prove that if $x = a + b\alpha \in \mathbb{Z}[\alpha]$, then $x \in \mathcal{O}_K$. By Lemma 9.2.15 it suffices to show that $\mathrm{Tr}(x)$ and $\mathrm{N}(x)$ lie in $\mathbb{Z}$. First we verify this for $x = \alpha$ by noting that $\mathrm{Tr}(\alpha) = 1$ and

$$\mathbb{N}(\alpha) = \begin{cases} (1-D)/4 & \text{if } D \equiv 1 \pmod 4 \\ D & \text{otherwise.} \end{cases}$$

More generally, if $x = a + b\alpha$ with $a, b \in \mathbb{Z}$, then

$$\mathrm{Tr}(x) = \mathrm{Tr}(a + b\alpha) = 2a + b\,\mathrm{Tr}(\alpha) = 2a + b \in \mathbb{Z},$$

and

$$\begin{aligned} \mathrm{N}(x) &= (a + b\alpha)(a + b\overline{\alpha}) \\ &= a^2 + ab(\alpha + \overline{\alpha}) + b^2\alpha\overline{\alpha} \\ &= a^2 + ab\,\mathrm{Tr}(\alpha) + b^2\,\mathrm{N}(\alpha) \in \mathbb{Z}. \end{aligned}$$

For the other inclusion, suppose $x = a + b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$ is integral over $\mathbb{Z}$. Then $\mathrm{Tr}(x) = 2a \in \mathbb{Z}$ and $\mathrm{N}(x) = a^2 - b^2 D \in \mathbb{Z}$. Thus $a = a'/2$ for some $a' \in \mathbb{Z}$ and $(a')^2/4 - b^2 D \in \mathbb{Z}$. Thus $(2b)^2 D \in \mathbb{Z}$, so since D is square free the denominator of b is either 1 or 2. The denominator of b is 2 if and only if the denominator of a is 2 since $a^2 - b^2 D \in \mathbb{Z}$. If the denominator of b is 1, then $a, b \in \mathbb{Z}$ and we are done, and if the denominator of b is 2, then $2b \in \mathbb{Z}$ and $(a')^2 \equiv (2b)^2 D \pmod 4$, so D is a perfect square modulo 4 and hence $D \equiv 1 \pmod 4$ (since D is square free) and $x \in \mathbb{Z}[\alpha]$. $\square$

Definition 9.2.17 (Field Discriminant). Let $K = \mathbb{Q}[\sqrt{D}]$ with D squarefee. The *discriminant* of K is D if $D \equiv 1 \pmod 4$ and $4D$ otherwise.

Let d be the discriminant of $\mathbb{Q}[\sqrt{D}]$. In Section 9.5 we will see that there is an bijection between certain equivalence classes of ideals in $\mathcal{O}_K$ and equivalence classes of binary quadratic forms of discriminant d. The set of equivalence classes of ideals in $\mathcal{O}_K$ will have the structure of finite abelian group induced by multiplication of ideals. Understanding whether or not numbers are represented by certain quadratic forms, is related to deciding whether or not certain ideals are principal in $\mathcal{O}_K$; this leads to class field theory, one of the major accomplishments of 20th century number theory.

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 $f|_g(x, y) = f\left(g\begin{pmatrix}x\\y\end{pmatrix}\right)$ 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 $(a',b',c') = (a,b,c)$. □

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

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

Example 9.3.4. If f_1 and f_2 are binary quadratic forms that represent exactly the same integers, is $f_1 \sim f_2$? The answer is no. For example, $f_1 = (2,1,3) = 2x^2 + xy + 3y^2$ and $f_2 = (2,-1,3) = 2x^2 - xy + 3y^2$ are inequivalent reduced positive definite binary quadratic forms that represent exactly the same integers. Note that $\mathrm{disc}(f_1) = \mathrm{disc}(f_2) = -23$.

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 $-D \leq 599$ with D odd. 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 fundamental discriminant. 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).

This is somewhat out of date, though I don't trust anything[3] from Math- 3
world... For what it's worth:

```
http://mathworld.wolfram.com/GausssClassNumberProblem.html

``Oesterl\'e (1985) solved the case h=3,
and Arno (1992) solved the case h=4.  Wagner (1996) solve[d]
the cases n=5, 6, 7.  Arno et al. (1993) solved the problem
for odd h satisfying 5 \leq h \leq 23.  In his thesis,
M. Watkins has solved the problem for all h \leq 16."
```

[3] Finish later.

TABLE 9.1. Class Numbers For D Odd

$-D$	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

9.5 Correspondence Between Binary Quadratic Forms and Ideals

[This section currently must contain typos, because I typed it in very quickly, and did NOT have a chance to proofread it at all.]

In this section we describe a bijection between equivalence classes of ideals and equivalence classes of binary quadratic forms. Since equivalence classes of ideals have a natural group structure, this bijection induces a group structure on equivalence classes of binary quadratic forms.

For the rest of this section, $K = \mathbb{Q}(\sqrt{d})$ is a quadratic field with discriminant d (see Definition 9.2.17). Thus $d \equiv 1 \pmod 4$ and d is square free, or $d \equiv 0 \pmod 4$ and $/4$ is square free and $\not\equiv 1 \pmod 4$. Let $\mathcal{O}_K$ denote the ring of all algebraic integers in K, as in Section 9.2.5.

9.5.1 Correctly Ordered Basis For Ideals

Proposition 9.5.1. *Suppose $I \subset \mathcal{O}_K$ is an ideal. Then there exists $\alpha, \beta \in \mathcal{O}_K$ such that*

$$I = \mathbb{Z}\alpha + \mathbb{Z}\beta = \{x\alpha + y\beta : x, y \in \mathbb{Z}\}.$$

Proof. As an abelian group, $\mathcal{O}_K$ is isomorphic to $\mathbb{Z}^2$. By the structure theorem for finitely generated abelian groups and the fact that subgroups of finitely generated abelian groups are finitely generated, I is isomorphic to $\mathbb{Z}^r$ for some positive integer r. Thus there is an inclusion $\mathbb{Z}^r \to \mathbb{Z}^2$. This extends to an injective vector space homomorphism $\mathbb{Q}^r \to \mathbb{Q}^2$, so $r \leq 2$. Since I is an ideal, I has finite index in $\mathcal{O}_K$, so $r \geq 2$. Thus I is generated as a $\mathbb{Z}$-module by two elements, α and β. $\square$

Henceforth we will let $[\alpha, \beta]$ denote $\mathbb{Z}\alpha + \mathbb{Z}\beta$. Thus Proposition 9.5.1 asserts that for every ideal I is of the form $[\alpha, \beta]$ for some $\alpha, \beta \in \mathcal{O}_K$. Note, however, that there are many choices of α, β so that $[\alpha, \beta]$ is not an ideal. For example, $[2, i]$ in $K = \mathbb{Q}(\sqrt{-1})$ is not equal to $\mathbb{Z}[i]$, but it contains the unit i, so if it were an ideal then it would have to equal $\mathbb{Z}[i]$.

It is natural to define a binary quadratic form associated to $I = [\alpha, \beta]$ as follows:

$$Q(x, y) = \mathbb{N}(\alpha x + \beta y) = (\alpha x + \beta y)(\alpha' x + \beta' y) = (\alpha\alpha')x^2 + (\alpha\beta' + \beta\alpha')xy + \beta\beta' y^2.$$

Surprisingly, this definition would lead to a disasterous breakdown of the theory! The quadratic form associated to I and the conjugate $I' = [\alpha', \beta']$ would be the same. We will later define a group structure on equivalence classes of ideals, and in this group the equivalence classes $[I]$ and $[I']$ are inverses. Since there should be a bijection between equivalence classes of binary quadratic forms and ideal classes, we would have to have that $[I][I] = [I][I'] = 1$, so the group of ideals would be a finite 2-torsion group, hence have order a power of 2, which is generally not the case. We must be much more careful in associated a binary quadratic form to an ideal.

Definition 9.5.2 (Correctly Ordered). A basis $[\alpha, \beta]$ for an ideal I is *correctly ordered* if

$$\frac{\alpha\beta' - \beta\alpha'}{\sqrt{d}} > 0.$$

Example 9.5.3. Let $d = -4$ and let I be the ideal generated by $(5, i-2)$. Note that $\mathcal{O}_K = \mathbb{Z}[i]$, so $\mathcal{O}_K/I \cong \mathbb{Z}/5$. We have $I = [5, i-2]$, since $[5, i-2] \subset I$ and $\det\left(\begin{smallmatrix} 5 & -2 \\ 0 & 1 \end{smallmatrix}\right) = 5$ (so that $\#(\mathcal{O}_K/[5, i-2]) = 5$). Notice that $[5, i-2]$ is not correctly ordered because

$$\frac{5(-i-2) - (i-2)5}{\sqrt{-4}} = -5 < 0.$$

The basis $[i-2, 5]$ is correctly ordered.

Proposition 9.5.4. *Any two correctly ordered bases of an ideal I are equivalent by an element in* $\mathrm{SL}_2(\mathbb{Z})$*, and conversely.*

Proof. Suppose $[\alpha, \beta] = [\gamma, \delta]$ are two correctly ordered basis for an ideal I. Because γ, δ are two different basis for the same free $\mathbb{Z}$-module, there are $a, b, c, d \in \mathbb{Z}$ such that

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = A \begin{pmatrix} \gamma \\ \delta \end{pmatrix},$$

and $\det(A) = \pm 1$ (this is just like a change of basis matrix in linear algebra; its determinant is a unit in the base ring). Since $a, b, c, d \in \mathbb{Z}$ and the conjugation automorphism fixes $\mathbb{Z}$, we have

$$\begin{pmatrix} \alpha & \alpha' \\ \beta & \beta' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \gamma & \gamma' \\ \delta & \delta' \end{pmatrix}.$$

Taking determinans, we have

$$\alpha\beta' - \beta\alpha' = \det(A)(\gamma\delta' - \delta\gamma'). \tag{9.1}$$

Since $[\alpha, \beta]$ and $[\gamma, \delta]$ are correctly oriented, we must have $\det(A) = +1$, so $A \in \mathrm{SL}_2(\mathbb{Z})$.

Conversely, if $A \in \mathrm{SL}_2(\mathbb{Z})$ and $[\gamma, \delta]$ is a correctly oriented basis then,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \gamma & \gamma' \\ \delta & \delta' \end{pmatrix} = \begin{pmatrix} alpha & \alpha' \\ \beta & \beta' \end{pmatrix}$$

and by (9.1) $[\alpha, \beta]$ is also correctly oriented. $\square$

9.5.2 Equivalence of Ideals

For the rest of this section, let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field with discriminant d.

Definition 9.5.5. Two ideals $I, J \subset \mathcal{O}_K$ are *equivalent*, written $I \sim J$, if there are $\alpha, \beta \in \mathcal{O}_K$ such that

$$\alpha I = \beta J \qquad \text{and} \qquad \mathbb{N}(\alpha\beta) > 0.$$

We will denote the set of equivalence classes of **nonzero** ideals in $\mathcal{O}_K$ by $\mathrm{Cl}(\mathcal{O}_K)$.

Proposition 9.5.6. *Multiplication of ideals gives* $\mathrm{Cl}(\mathcal{O}_K)$ *an abelian group structure in which the ideal class of* $\mathcal{O}_K = (1)$ *is the identity element.*

Proof. If I and J are ideals of $\mathcal{O}_K$ then their product $IJ = \{xy : x \in I, y \in J\}$ is again an ideal in $\mathcal{O}_K$. Multiplication of ideals is easily seen to be associative and commutative, since the usual multiplication of elements in $\mathcal{O}_K$ is associative and commutative. Next we check that multiplication of ideals induces a well-defined multiplication of ideal classes. If $I_0 \sim J_0$ and $I_1 \sim J_1$, then there exists $\alpha_0, \beta_0, \alpha_1, \beta_1 \in \mathcal{O}_K$ such that $\alpha_i I_i = \beta_i J_i$ for $i = 0, 1$. Multiplying these two equalities, we see that $\alpha_0 I_0 \alpha_1 I_1 = \beta_0 J_0 \beta_1 J_1$, so $\alpha_0\alpha_1 I_0 I_1 = \beta_0\beta_1 J_0 J_1$, hence $I_0 I_1 \sim J_0 J_1$. This proves that multiplication of ideals induces a well-defined associative commutative multiplication of ideal classes.

To finish the proof, we verify that every element of $\mathrm{Cl}(\mathcal{O}_K)$ has an inverse. Let $I = [\alpha, \beta]$ be an ideal in $\mathcal{O}_K$. Then the ideal I' generated by the conjugates of elements of I is $[\alpha', \beta']$. The product II' is the principal ideal generated by the positive integer $\#(\mathcal{O}_K/I)$. [4] Thus $II' \sim 1$, so I has an inverse. 4

□

Example 9.5.7. Let $K = \mathbb{Q}[\sqrt{-20}]$. Then $\mathrm{Cl}(\mathcal{O}_K)$ is cyclic of order 2. A nonidentity element of $\mathrm{Cl}(\mathcal{O}_K)$ is $I = [1 + \sqrt{-5}, 2]$.

9.5.3 Correspondence Between Ideals and Forms

Definition 9.5.8 (Norm). Let I be a nonzero ideal of $\mathcal{O}_K$. The *norm* $\mathbb{N}(I)$ is $\#(\mathcal{O}_K/I)$.

The norm of an ideal is a positive integer.

[4] This is true, but I don't know a simple proof of this right now, and I don't have time left to find one. Here's a nontrivial proof, since it requires knowing that ideals factor as products of prime ideals: factor I as a product of prime ideals and note that the statement is clearly true for each prime factor, hence true for their product.

Proposition 9.5.9. *Let I be an ideal in the ring of integers of $\mathbb{Q}(\sqrt{d})$ and let $[\alpha, \beta]$ be a properly ordered basis for I. Then the quadratic form*

$$Q(x,y) = \frac{N(\alpha x + \beta y)}{N(I)} = ax^2 + bxy + cy^2$$

has integral coefficients and is a primitive form of discriminant d (i.e., $\gcd(a,b,c) = 1$ and $b^2 - 4ac = d$.

Note that the numerator $N(\alpha x + \beta y)$ in the definition of Q depends on the order of α and β.

Example 9.5.10. Let $K = \mathbb{Q}[\sqrt{-20}]$ and $I = [1 + \sqrt{-5}, 2]$, as in Example 9.5.7. Then

$$\begin{aligned} N(\alpha x + \beta y) &= ((1+\sqrt{-5})x + 2y)((1-\sqrt{-5})x + 2y) \\ &= 6x^2 + 4xy + 4y^2. \end{aligned}$$

The norm of I is $|\det(\left(\begin{smallmatrix} 1 & 2 \\ 1 & 0 \end{smallmatrix}\right))| = 2$. Thus $Q(x,y) = 3x^2 + 2xy + 2y^2$. Notice as a check that $\mathrm{disc}(Q) = b^2 - 4ac = 2^2 - 4 \cdot 3 \cdot 2 = -20$.

Proof. Next time. □

Proposition 9.5.11. *Let $Q(x,y) = Ax^2 + Bxy + Cy^2$ be a quadratic form of discriminant d. Write $Q(x,y) = t(ax^2 + bxy + cy^2)$ with $\gcd(a,b,c) = 1$, and $t > 0$ if $d > 0$, or $a > 0$ if $d < 0$. Let*

$$I = [\alpha, \beta] = \begin{cases} [a, \frac{b-\sqrt{d}}{2}] & \text{if } a > 0, \\ [a\sqrt{d}, (\frac{b-\sqrt{d}}{2})\sqrt{d}] & \text{if } a < 0. \end{cases}.$$

Then I is an ideal of $\mathcal{O}_K$ and $[\alpha, \beta]$ is a correctly ordered basis for I.

Example 9.5.12. Let $d = -20$ and $Q(x,y) = 3x^2 + 2xy + 2y^2$. Then $I = [3, 1 - \sqrt{-5}]$. Notice that $I \neq [1 + \sqrt{-5}, 2]$, so the operations of the two propositions are not inverses. They are however, after passing to equivalence classes, as we will see.

Proof. Next time. □

Theorem 9.5.13. *Propositions 9.5.9–9.5.11 sets up a bijection between equivalence classes of quadratic forms of discriminant d and ideal classes in $\mathcal{O}_K$. (Note: When d is negative we only allow positive definition (instead of negative definite) forms.)*

Proof. Next time. □