# 9

# Binary Quadratic Forms and Ideal Class Groups

In this chapter, we will study binary quadratic forms.

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 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 for proofs.

**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 $n_2$ 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

$$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1 x_2 + y_1 y_2)^2 + (x_1 y_2 - x_2 y_1)^2,$$

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 $n \in \mathbb{N}$, 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. $\square$

*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 $b^2 + c^2 = p$. $\square$

### 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. $\square$

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 $\lambda : R \to \mathbb{Z}_{\geq 0} = \mathbb{N} \cup \{0\}$ 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

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

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

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

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

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

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 $N(x)$ minimal. If $y \in I$ then $y = qx + r$ with $N(r) < N(x)$. Since $r = qx - y \in I$, it follows that $N(r) = 0$, so $r = 0$ and $y \in (x)$. Thus $I = (x)$. □

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.