Chapter 3

Quadratic Extensions of the Integers, $\mathbb{Z}[\sqrt{d}]$

If Chapter Two represented a zoom in to look at smaller, simpler rings than $\mathbb{Z}$, then this chapter will represent more of a zoom out as we situate $\mathbb{Z}$ inside some other rings, mostly the Gaussian integers $\mathbb{Z}[i]$, but also other rings of the form $\mathbb{Z}[\sqrt{d}]$ (for a square-free integer $d$). By seeing how these rings are similar to, and different from, the ring of integers $\mathbb{Z}$, we hope to learn more about both of these objects of study. For example, you have most likely seen and used the fundamental theorem of arithmetic so often that you probably don’t find its statement very interesting nor its proof very illuminating. But by repeating this argument (rather, making analogous arguments) in a less familiar setting, I hope that you will see the power of unique factorization; and by seeing how it can fail, we see what an important fact it is about the ring $\mathbb{Z}$.

31 Divisibility in $\mathbb{Z}[i]$

In $\mathbb{Z}$, to prove that we have unique factorization into primes, we needed the well-ordering principle and the fact that for integers $a$ and $b$ with $(a,b) = d$, we have

$$d = ax + by$$

for some integers $x$ and $y$.

This was proved via the Euclidean algorithm, using the amazing array to undo the continued fraction for $\frac{a}{b}$. Our norm function, $N$, (or its absolute value) will give us a way to use the well-ordering principle, since the norm of an element in $\mathbb{Z}[\sqrt{d}]$ is in some sense a measure of its size. What about the Euclidean algorithm? Will this work in $\mathbb{Z}[i]$? in $\mathbb{Z}[\sqrt{2}]$? in other rings $\mathbb{Z}[\sqrt{d}]$?
Let’s try to find the GCD of $-23 - i$ and $2 + 5i$. Notice that $N(-23 - i) = 530$ and $N(2 + 5i) = 29$. We calculate:

$$
-23 - i = (2 + 5i)(-2 + 4i) + (1 + i) \\
2 + 5i = (1 + i)(3 + 2i) + 1 \\
1 + i = 1(1 + i) + 0
$$

so it works—we think the GCD of $-23 - i$ and $2 + 5i$ is 1 and they are relatively prime. If $2 + 5i = (z_1)(z_2)$ then by taking norms we get $29 = N(z_1)N(z_2)$ so $N(z_1) = 1$ or $N(z_2) = 1$ so one of them is a unit. Thus $2 + 5i$ acts like a prime in $\mathbb{Z}[i]$, since any factorization must have one factor being a unit. What could $(-23 - i, 2 + 5i)$ be? It must divide $2 + 5i$ so it must be $2 + 5i$ or 1, right? But if it is $2 + 5i$, then $(2 + 5i)|(-23 - i)$ so

$$-23 - i = (2 + 5i)z$$

for some Gaussian integer $z$, and then by taking norms we get

$$530 = 29 \cdot N(z)$$

so $29|530$ and this is false! So we can use the norm function to prove that the two Gaussian integers are relatively prime, just as we found from the Euclidean algorithm. We need some preliminaries before we generalize this. Recall the definition of a prime in any ring $R$:

**Definition 22** In a ring $R$, an element $p$ that is not a unit is called prime if

$$p = a \cdot b \implies a \text{ or } b \text{ is a unit.}$$

**Proposition 22** If $N(z)$ is a prime in $\mathbb{Z}$, then $z$ is prime in $\mathbb{Z}[i]$.

**Proof.** Just as we did above, suppose $N(z)$ is prime and suppose $z$ factors in $\mathbb{Z}[i]$ as $z = a \cdot b$. Then we have $N(z) = N(a)N(b)$ so either $N(a)$ or $N(b)$ is a unit in $\mathbb{Z}$. But norms in $\mathbb{Z}[i]$ are non-negative, so we must have $N(a) = 1$ or $N(b) = 1$. Thus either $a$ or $b$ is a unit.

The converse of this theorem is false; for instance we will prove soon that 3 is a prime in $\mathbb{Z}[i]$, but it certainly not true that $N(3) = 9$ is a prime in $\mathbb{Z}$.

Following Exercise 7 in Section 7, we have

**Definition 23** For Gaussian integers $a$ and $b$, we write $a|b$ if there is a Gaussian integer $c$ such that $b = a \cdot c$.

We immediately get

$$a|b \implies b = a \cdot c \implies N(b) = N(a)N(c) \implies N(a)|N(b).$$
You should think about whether the converse is true: does \( N(a)|N(b) \implies a|b? \)

All the properties of divisibility still hold (compare Proposition 23 to Proposition 3 in Section 7), sometimes modified as follows:

**Proposition 23** For \( a, b, c, \) and \( d \) in \( \mathbb{Z}[i], \)

1. \( a|0, 1|a, \) and \( a|a \) for all \( a \in \mathbb{Z}[i] \)
2. \( a|1 \iff a \) is a unit \( \iff N(a) = 1 \iff a = \pm 1 \) or \( \pm i \)
3. \( a|b \) and \( b|c \implies a|c \)
4. \( a|b \) and \( b|a \iff a = (\text{unit})b \iff a = \pm b \) or \( a = \pm ib \)
5. \( a|b \) and \( c|d \implies ac|bd \)
6. \( a|b \) and \( b \neq 0 \implies N(a) \leq N(b) \)
7. \( a|b \) and \( a|c \implies a|(bx + cy) \) for any Gaussian integers \( x \) and \( y. \)

**Proof.** The proofs of 1, 3, 5, and 7 are exactly like their analogs in \( \mathbb{Z}, \) since all that was used there were closure, the distributive property, the definition of divisibility, etc.; facts that are true in any ring. The proofs of 2, 4, and 6 are left to the reader. \( \blacksquare \)

**Exercises**

1. (a) Show that 3, 7, and 107 are primes in \( \mathbb{Z}[i]. \)
   (b) Conjecture a rule for which prime integers are prime in \( \mathbb{Z}[i]. \)

2. Is \( 6 + 7i \) a prime in \( \mathbb{Z}[i]? \) You will need to either factor this Gaussian integer (to show the answer is no) or give an argument as to why it cannot be factored (to show the answer is yes).


4. Prove part 4 of Proposition 23.

5. Prove part 6 of Proposition 23.

6. Prove that, just like \( \mathbb{Z}, \mathbb{Z}[i] \) has no zero divisors.

7. Show that if \( (N(z), N(w)) = 1, \) then \( z \) and \( w \in \mathbb{Z}[i] \) are relatively prime.

8. Calculate \( (2 - i)(3 - 3i) + (9 + 2i)(i). \) Use this to show that \( 2 - i \) and \( 9 + 2i \) are relatively prime. Note that this shows the converse of Exercise 7 is false.
32 The Euclidean algorithm in \( \mathbb{Z}[i] \)

What is \((60, 34)\)? It’s 2, remember. Why? Because \(2 \mid 60\) and \(2 \mid 34\), so 2 is a common divisor; and if \(c \mid 60\) and \(c \mid 34\) so that \(c\) is also a common divisor, we must also have \(c \mid 2\). But the above also holds for \(-2\); we write \((60, 34) = 2\) only because we always want our GCDs to be positive. Without that condition, we could write, say, \((60, 34) = \pm 2 = (\text{unit})2\). Earlier, we had

\[
-23 - i = (2 + 5i)(-2 + 4i) + (1 + i)
\]

\[
2 + 5i = (1 + i)(3 + 2i) + 1
\]

\[
1 + i = 1(1 + i) + 0
\]

but the last two steps could have easily been

\[
\begin{align*}
2 + 5i &= (1 + i)(4 + i) + (-1) \\
1 + i &= -1(-1 - i) + 0 \quad \text{or}
\end{align*}
\]

\[
\begin{align*}
2 + 5i &= (1 + i)(3 + i) + i \\
1 + i &= i(1 - i) + 0 \quad \text{or}
\end{align*}
\]

So we could have ended with a GCD of any unit. How did I find the correct quotients, especially in the step

\[
-23 - i = (2 + 5i)(-2 + 4i) + (1 + i)\?
\]

Think about the modified division algorithm in Section 13, where we divide and choose the nearest integer as the quotient, rather than always rounding down as we did originally. We can do the same here: we divide and choose the nearest Gaussian integer! Let’s see:

\[
\begin{align*}
\frac{-23 - i}{2 + 5i} &= \frac{-23 - i}{2 + 5i} \cdot \frac{2 - 5i}{2 - 5i} = \frac{-51 + 113i}{2^2 + 5^2} = \frac{-51 + 113i}{29} \\
&= \approx -1.76 + 3.89i.
\end{align*}
\]

Now you can see why I chose \(-2 + 4i\) as the correct multiplier to use: it was the nearest Gaussian integer to the fraction above (which is in the field \(\mathbb{Q}[i]\)).

When we try this for the next step we get

\[
\begin{align*}
\frac{2 + 5i}{1 + i} &= \frac{2 + 5i}{1 + i} \cdot \frac{1 - i}{1 - i} = \frac{7 + 3i}{1^2 + 1^2} = \frac{7}{2} + \frac{3}{2}i = 3.5 + 1.5i,
\end{align*}
\]

and it isn’t clear what to choose, since the Gaussian integers \(4 + 2i\), \(4 + i\), \(3 + 2i\), and \(3 + i\) are all the same distance away. That’s why we have a choice as to what the GCD is. What we get, in general, is

\[
\frac{a + bi}{c + di} = \frac{a + bi}{c + di} \cdot \frac{c - di}{c - di} = \frac{(ac + bd) + (bc - ad)i}{c^2 + d^2} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2}i
\]

\[
\begin{align*}
&= (q_1 + q_2i) + (\epsilon_1 + \epsilon_2i)
\end{align*}
\]
where \( q_1 + q_2i \) is a Gaussian integer and \( \epsilon_1 + \epsilon_2i \) isn’t, but we have that \( \epsilon_1 \) and \( \epsilon_2 \) are fractions with \( |\epsilon_1| \leq \frac{1}{2} \) and \( |\epsilon_2| \leq \frac{1}{2} \). Then

\[
a + bi = (c + di)(q_1 + q_2i) + (c + di)(\epsilon_1 + \epsilon_2i)
\]

and the remainder, \((c + di)(\epsilon_1 + \epsilon_2i)\), must be a Gaussian integer since it is also \( a + bi - (c + di)(q_1 + q_2i) \). We also have

\[
N(\text{remainder}) = N((c + di)(\epsilon_1 + \epsilon_2i)) = N(c + di)N(\epsilon_1 + \epsilon_2i) = (c^2 + d^2)((\epsilon_1)^2 + (\epsilon_2)^2) \leq (c^2 + d^2)
\frac{1}{4} + \frac{1}{4}
= \frac{1}{2}N(c + di).
\]

We have just proved that we have a division algorithm, and hence a Euclidean algorithm, for \( \mathbb{Z}[i] \)—therefore, we should be able to prove that \( \mathbb{Z}[i] \) has unique factorization also!

**Proposition 24** If \( z \) and \( w \neq 0 \) are in \( \mathbb{Z}[i] \), then there are Gaussian integers \( q = q_1 + q_2i \) and \( r = r_1 + r_2i \) (not necessarily unique), with

\[
z = w \cdot q + r
\]

and \( 0 \leq N(r) \leq \frac{1}{2}N(w) \).

Let’s look at the situation geometrically, which will provide a different proof of this very important proposition. We will draw \( \mathbb{Z}[i] \) as a lattice in two dimensions, where the Gaussian integer \( a + bi \) is graphed as the point \( (a, b) \); thus we have identified the usual plane \( \mathbb{R}^2 \) as the complex plane \( \mathbb{C} \), and then we see that \( \mathbb{Z}[i] \) is a discrete subset of that plane. The word “discrete” is often contrasted with the word “continuous” in mathematics, but I would like instead to contrast discrete with dense. The rational numbers, \( \mathbb{Q} \), are said to be dense in \( \mathbb{R} \), by which we mean that in any small neighborhood (or open interval \( (c, d) \subseteq \mathbb{R} \)), there exists at least one element of \( \mathbb{Q} \) (and thus an infinite number of them). You may or may not have seen that idea in another class. Thus \( \mathbb{Q} \) may be thought of as appearing almost everywhere in \( \mathbb{R} \) (though if you know the difference between countable and uncountable you know that there is still a wide gap between \( \mathbb{Q} \) and \( \mathbb{R} \)). By contrast, when we think of \( \mathbb{Z} \) as a subset of the real line \( \mathbb{R} \), we see that for each \( z \in \mathbb{Z} \), there exists a neighborhood \( (z - h, z + h) \) such that no other element of \( \mathbb{Z} \) (besides \( z \) itself) lies within this interval. So in some sense \( \mathbb{Z} \) appears hardly anywhere in \( \mathbb{R} \). That is the intuitive sense of discrete.

Now when we thought about the usual (or the modified) division algorithm geometrically, we first thought about all the integer multiples of the integer \( b \). The integer we were trying to divide, \( a \), could be found between two of them, etc. So our first step now is to think about all the multiples of \( w \) by all other Gaussian integers. As before, multiplication by an integer simply increases the distance from the origin, perhaps with a flip if the integer multiplier is negative. But what does
multiplication by \(i\), or by \(-4i\), or by \(3-6i\), do? Well, multiplying \(a+bi\) by \(i\) gives \(-b+ai\), and a little experimentation should convince you that what happens is that

multiplication by \(i\) corresponds to rotation by 90° counterclockwise.

Some more experimentation with multiplication will show that all the multiples of \(w\) form a square sublattice of \(\mathbb{Z}[i]\); see Figure 7.

![Figure 7: Multiples of 3-5i in \(\mathbb{Z}[i]\)](image)

All multiples of \(w = c+di\) form a lattice, so in general \(z = a+bi\) will fall inside one of the squares making up this sublattice, and thus \(z\) will be between four multiples of \(w\), namely the four corners of the square in which \(z\) resides. Hence we can write \(z = a+bi\) as a multiple of \(c+di\) plus a remainder that will make up the difference between \(z\) and the closest (or most convenient) corner of this square. Hence we get

\[
N(\text{remainder}) = (\text{length of remainder})^2 \\
\leq \left(\frac{\sqrt{2}}{2} \text{length of side}\right)^2 \\
= \frac{1}{2} (\text{length of side})^2 \\
= \frac{1}{2} N(w).
\]

The picture for the division we did on page 130 looks like Figure 8.

This completes a second proof that the ring \(\mathbb{Z}[i]\) has a division algorithm. The fact that the norm decreases at each step (and is a positive integer) immediately implies that \(\mathbb{Z}[i]\) has a Euclidean algorithm, which will end in a finite number of steps, and thus the final non-zero remainder will be a common divisor, \(d\), of \(z\) and \(w\), and by reversing the algebra of the Euclidean algorithm (perhaps by using the
amazing array?)), we know that we can write \( d \) as a linear combination of \( z \) and \( w \): \( d = rz + sw \) for some Gaussian integers \( r \) and \( s \). Does that imply that \( d \) is a GCD? In fact, how do we make sense of or define the GCD in \( \mathbb{Z}[i] \)? Recall our old definition of the GCD in \( \mathbb{Z} \): \( d = (a, b) \) means

- \( d \geq 0 \), and \( d = 0 \) \( \iff \) \( a = b = 0 \)
- \( d|a \) and \( d|b \)
- if \( c|a \) and \( c|b \), then \( c|d \).

We can’t use the first condition since there is no easy way to order the Gaussian integers. What we will do is just to give up the idea of having a unique GCD. We need the following definition, which deals with the slipperiness of Gaussian integers.

**Definition 24** In a ring \( R \), \( a \) and \( b \) are said to be associates if \( a = bu \) where \( u \) is a unit in \( R \). We write \( a \sim b \).

Thus, in \( \mathbb{Z} \), \( a \sim b \) \( \iff \) \( a = \pm b \). In \( \mathbb{Z}[i] \), \( a \sim b \) \( \iff \) \( a = \pm b \) or \( a = \pm ib \). We also have

**Proposition 25** In any ring \( R \),

1. \( a \sim a \) for all \( a \in R \)
2. \( a \sim b \iff b \sim a \)
3. \( a \sim b \) and \( b \sim c \implies a \sim c \).
Thus being associates is an example of an equivalence relation.

Notice that \( a \sim 1 \iff a = 1 \cdot \text{(unit)} \iff a \text{ is a unit.} \) We will often write “\( a \sim 1 \)” instead of “\( a \text{ is a unit} \)” from now on.

Another way to characterize this equivalence relation is

**Proposition 26** In a ring with no zero-divisors, \( R, a \sim b \iff (a|b \text{ and } b|a). \)

**Definition 25** In \( \mathbb{Z}[i] \), the GCD of two numbers is defined (by the Euclidean algorithm as modified for \( \mathbb{Z}[i] \) above) only up to associates. For \( z, w \in \mathbb{Z}[i] \), we write \( (z, w) \sim d \) if \( d \) is a Gaussian integer such that

- \( d|z \text{ and } d|w \)
- \( \text{if } c|z \text{ and } c|w, \text{ then } c|d. \)

Thus we proved earlier that \( (-23 - i, 2 + 5i) \sim 1. \) As in \( \mathbb{Z} \), having only trivial common divisors means that two Gaussian integers will be called relatively prime.

**Definition 26** Elements \( z \) and \( w \) are relatively prime in \( \mathbb{Z}[i] \) if \( (z, w) \sim 1 \) (i.e., the only common divisors of \( z \) and \( w \) are the units).

**Exercises**

1. Prove part 1 of Proposition 25.
2. Prove part 2 of Proposition 25.
3. Prove part 3 of Proposition 25.
5. Note that \( 4 + 3i \not\sim 3 + 4i \), but \( 4 + 3i \sim 3 - 4i \). Is it always true that \( N(z) = N(w) \implies (z \sim w) \text{ or } (z \sim \overline{w})? \)
6. Use the Euclidean algorithm in \( \mathbb{Z}[i] \) to find \( d \sim (1 + 2i, 9 - 12i) \). Use the amazing array to solve \((1 + 2i)u + (9 - 12i)v = d \) for \( u \) and \( v \in \mathbb{Z}[i] \).
7. Use the Euclidean algorithm in \( \mathbb{Z}[i] \) to find \( d \sim (3 - 4i, 15 + 5i) \). Use the amazing array to solve \((3 - 4i)u + (15 + 5i)v = d \) for \( u \) and \( v \in \mathbb{Z}[i] \).
8. Let \( z, w, \) and \( d \) be Gaussian integers, with \( (z, w) \sim d \). Mimic the proof of Proposition 4 on page 34 and prove that there exist Gaussian integers \( u \) and \( v \) such that \( zu + wv = d \).
33. Unique factorization in $\mathbb{Z}[i]$

Theorem 17 (Unique Factorization in $\mathbb{Z}[i]$) Any Gaussian integer $z$ that is not zero and not a unit can be written as

$$z = up_1^{e_1}p_2^{e_2}p_3^{e_3} \ldots p_r^{e_r}$$

or

$$z \sim p_1^{e_1}p_2^{e_2}p_3^{e_3} \ldots p_r^{e_r} = \prod_{j=1}^r p_j^{e_j}$$

where $u$ is a unit and the $p_j$ are distinct primes in $\mathbb{Z}[i]$. This representation is unique in the sense that if

$$z = vq_1^{f_1}q_2^{f_2}q_3^{f_3} \ldots q_s^{f_s} \sim \prod_{k=1}^s q_k^{f_k}$$

with $v$ a unit and the $q_j$ primes in $\mathbb{Z}[i]$, then we have

- $r = s$
- For each $j$, there is a $k$ for which $p_j \sim q_k$ and $e_j = f_k$.

In fact we could reword the fundamental theorem of arithmetic exactly this way: any integer $n \in \mathbb{Z}$ can be written as

$$n \sim p_1^{e_1}p_2^{e_2}p_3^{e_3} \ldots p_r^{e_r}$$

where the $p_j$ are distinct integer primes (not necessarily positive), and this representation is unique in the sense that if

$$n = vq_1^{f_1}q_2^{f_2}q_3^{f_3} \ldots q_s^{f_s} \sim \prod_{j=1}^s q_k^{f_k}$$

with $v$ a unit in $\mathbb{Z}$ and the $q_j$’s primes in $\mathbb{Z}$, then we have

- $r = s$
- For each $j$, there is a $k$ such that $p_j \sim q_k$ and $e_j = f_k$.

We prove the theorem exactly the same way we proved the theorem in $\mathbb{Z}$: First we see that if $(a,b) \sim d$ then

$$d = ax + by \quad \text{for some } x, y \in \mathbb{Z}[i].$$

This comes from the Euclidean algorithm, exactly as before (recall that you can use the amazing array to find $x$ and $y$). Next we prove the (reworded) prime theorem and Euclid’s lemma:

Theorem 18 (Prime Theorem in $\mathbb{Z}[i]$) For $p$ a prime in $\mathbb{Z}[i]$ and Gaussian integers $a$ and $b$, $p | ab \implies p | a$ or $p | b$. 
Chapter 3. Quadratic Extensions of the Integers, \( \mathbb{Z}[\sqrt{d}] \)

**Theorem 19 (Euclid’s Lemma)** For Gaussian integers \( a, b, \) and \( c, \)
\[ c|ab \quad \text{and} \quad (a,c) \sim 1 \implies c|b. \]

Then we write down the same lemmas as before:

**Lemma 8** For \( p \) a prime in \( \mathbb{Z}[i] \) and Gaussian integers \( a_i, \) we have
\[ p | a_1 a_2 a_3 \cdots a_n \implies p | a_j \quad \text{for some} \quad j, 1 \leq j \leq n. \]

**Lemma 9** If \( p \) and all \( q_i \) are prime in \( \mathbb{Z}[i], \) then we have
\[ p | q_1 q_2 q_3 \cdots q_n \implies p \sim q_j \quad \text{for some} \quad j, 1 \leq j \leq n. \]

The proofs of Lemmas 8 and 9 are left to the reader.

**Lemma 10** Any \( z \) in \( \mathbb{Z}[i] \) that is not zero and not a unit has a factorization into primes: we can write
\[ z \sim p_1 p_2 p_3 \cdots p_r \]
where the \( p_i \) are primes in \( \mathbb{Z}[i]. \)

**Proof.** Let
\[ S = \{ z \in \mathbb{Z}[i] : z \neq 0, \ z \text{ is not a unit, and} \ z \text{ has no such factorization} \} \]
and assume \( S \) is non-empty. Then choose an element of smallest norm (the well-ordering principle insures there is such an element, but it may not be unique). Call this smallest element \( s. \) We know \( s \) is not prime, so we must have \( s = z \cdot w, \) where neither \( z \) nor \( w \) is a unit. Thus \( N(z) > 1 \) and \( N(w) > 1, \) so we have \( 1 < N(z), N(w) < N(s). \) Thus \( z \) and \( w \) have factorizations into primes, say \( z \sim p_1 p_2 p_3 \cdots p_s \) and \( w \sim q_1 q_2 q_3 \cdots q_t, \) so \( s = z \cdot w \sim p_1 p_2 p_3 \cdots p_s q_1 q_2 q_3 \cdots q_t \) does also. This contradiction shows us that \( S \) is indeed empty.

We thus have only to prove the uniqueness of the factorization. Let
\[ S = \{ z \in \mathbb{Z}[i] : z \neq 0, \ z \text{ is not a unit, and} \ z \text{ has more than one such factorization} \} \]
and assume \( S \) is non-empty. Then we may choose an element of \( S \) with the smallest norm (there may be choice involved in choosing it, but the smallest norm represented by elements of \( S \) exists, by the well-ordering principle), call it \( s, \) so we have at least two factorizations of \( s: \)
\[ s \sim p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_r^{e_r} \sim q_1^{f_1} q_2^{f_2} q_3^{f_3} \cdots q_s^{f_s} \]
and we have \( p_1 | q_1^{f_1} q_2^{f_2} q_3^{f_3} \cdots q_s^{f_s} \implies p_1 \sim q_k \) for some \( k, \) by Lemma 9. If \( \frac{s}{p_1} \sim 1, \) we have \( s \sim p_1 \sim q_k \) and the factorization must be unique. Otherwise, we have
that $\frac{s}{p_1}$ is a Gaussian integer that is not a unit, and $1 < N\left(\frac{s}{p_1}\right) < N(s)$, so $\frac{s}{p_1}$ has the unique factorization

$$\frac{s}{p_1} \sim p_1^{e_1-1}p_2^{e_2}p_3^{e_3} \cdots p_r^{e_r} \sim q_1^{f_1}q_2^{f_2}q_3^{f_3} \cdots q_r^{f_r},$$

so we must have $e_1 = f_k$, $r = s$, and for each $j$, there is a $k$ with $p_j \sim q_k$ and $e_j = f_k$. But then the two factorizations of $s$ are not different. This contradiction shows that $S$ is empty, and the theorem is proved.

**Exercises**

1. Let $d \sim (3 + 5i, 7 - 6i)$.
   
   (a) Find $d$.
   
   (b) Solve $(3 + 5i)(z + wi) + (7 - 6i)(x + yi) = d$.

2. Let $d \sim (3 + 4i, 4 + 3i)$.
   
   (a) Find $d$.
   
   (b) Solve $(3 + 4i)(z + wi) + (4 + 3i)(x + yi) = d$.

3. Let $d \sim (6 - 57i, 14 + 29i)$.
   
   (a) Find $d$.
   
   (b) Solve $(6 - 57i)(z + wi) + (14 + 29i)(x + yi) = d$.


5. Prove Lemma 9 on page 136.

6. (Compare this to Exercise 7 on page 67.) Given Gaussian integers $z$, $w$, and $v$, which have factorizations

$$z \sim p_1^{e_1}p_2^{e_2}p_3^{e_3} \cdots p_k^{e_k}, \quad w \sim q_1^{f_1}q_2^{f_2}q_3^{f_3} \cdots q_k^{f_k}, \quad v \sim r_1^{g_1}r_2^{g_2}r_3^{g_3} \cdots r_k^{g_k},$$

where all the $p$s, $q$s, and $r$s are prime Gaussian integers, how do you determine (using the factorizations above) if

(a) $z|w$?

(b) $(z, w) \sim 1$?

(c) $(z, w) \sim v$?

(d) $[z, w] \sim v$ (where $[a, b]$ is a least common multiple of $a$ and $b$, as defined by you in analogy with Exercise 6 in Section 8)?

(e) $z$ is a perfect square? (That is, $z = u^2$ for some Gaussian integer $u$.)

(f) $z$ is a perfect cube?

(g) $z$ is a perfect $m$th power? (That is, $z = u^m$ for some Gaussian integer $u$ and some positive integer $m$.)

(h) $z \cdot w = v$?

7. Prove Theorem 18 on page 135.

34 The structure of $\mathbb{Z}[\sqrt{2}]$

Recall that

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \in \mathbb{R} : a, b \in \mathbb{Z}\}$$

and we have the norm function $N(a + b\sqrt{2}) = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$. Unlike in $\mathbb{Z}[i]$, in $\mathbb{Z}[\sqrt{2}]$ the norm may be negative.

**Proposition 27** $u = a + b\sqrt{2}$ is a unit in $\mathbb{Z}[\sqrt{2}]$ if and only if $N(u) = a^2 - 2b^2 = \pm 1$.

**Proof.** If $u$ is a unit, then there is a $u^{-1}$ in $\mathbb{Z}[\sqrt{2}]$ such that $u \cdot u^{-1} = 1$. Then we get

$$N(u)N(u^{-1}) = N(u \cdot u^{-1}) = N(1) = N(1 + 0\sqrt{2}) = 1^2 - 2 \cdot 0^2 = 1$$

so $N(u)$ is a unit in $\mathbb{Z}$, hence $N(u) = \pm 1$.

If $N(a + b\sqrt{2}) = 1$, then $(a + b\sqrt{2})(a - b\sqrt{2}) = 1$ so $u = a + b\sqrt{2}$ is a unit, with inverse $a - b\sqrt{2}$. If $N(a + b\sqrt{2}) = -1$, then $(a + b\sqrt{2})(a - b\sqrt{2}) = -1$ so $u = a + b\sqrt{2}$ is a unit, with inverse $-(a - b\sqrt{2}) = -a + b\sqrt{2}$.

It is straightforward to show that $\sqrt{2} = [1, \frac{3}{2}]$. This gives the following amazing array, with an added row for the values of $P_n^2 - 2Q_n^2$:

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>2</th>
<th>2</th>
<th>2</th>
<th>2</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>3</td>
<td>7</td>
<td>17</td>
<td>41</td>
<td>99</td>
<td>239</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>5</td>
<td>12</td>
<td>29</td>
<td>70</td>
</tr>
</tbody>
</table>

$P_n^2 - 2Q_n^2$

<table>
<thead>
<tr>
<th></th>
<th>2</th>
<th>2</th>
<th>2</th>
<th>2</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>1</td>
</tr>
</tbody>
</table>

$P_n^2 - 2Q_n^2$

There seems to be a pattern to the $Q_n$: can you see it? The sum of the $n$th column is always $Q_{n+1}$: for $n \geq 1$, we have $P_n + Q_n = Q_{n+1}$. Also, with a little more effort we can find a pattern for the $P_n$: $P_n = Q_n + Q_{n-1}$ for $n \geq 1$. Can we prove these assertions? What are the rules for constructing the $P_n$ and $Q_n$? They are

$$n \geq 2 \implies P_n = 2P_{n-1} + P_{n-2} \quad \text{and} \quad Q_n = 2Q_{n-1} + Q_{n-2}$$

and we have verified (by eye) that these formulas hold for $1 \leq n \leq 8$. That is more than adequate for a base case to do induction: let’s assume the formulas are true for $n = 1, 2, 3, \ldots, k$ and let’s try to prove them for $n = k + 1$: we have

$$Q_{k+1} = 2Q_k + Q_{k-1}$$

$$= 2(P_{k-1} + Q_{k-1}) + (P_{k-2} + Q_{k-2})$$

$$= 2P_{k-1} + P_{k-2} + 2Q_{k-1} + Q_{k-2}$$

$$= P_k + Q_k$$
and the first formula is proved for all $n \geq 1$. As for the second formula, we assume $P_n = Q_n + Q_{n-1}$ for all $n = 1, 2, 3, \ldots, k$, and try to prove it for $n = k + 1$:

\[
P_{k+1} = 2P_k + P_{k-1} = 2(Q_k + Q_{k-1}) + (Q_{k-1} + Q_{k-2}) = (2Q_k + Q_{k-1}) + (2Q_{k-1} + Q_{k-2}) = Q_{k+1} + Q_k
\]

and the formula is proved for all $n \geq 1$.

Also,

\[
(1 + \sqrt{2})^2 = 3 + 2\sqrt{2}
\]
\[
(1 + \sqrt{2})^3 = 3 + 2\sqrt{2} + 3\sqrt{2} + 4 = 7 + 5\sqrt{2}
\]
\[
(1 + \sqrt{2})^4 = 9 + 8 + 12\sqrt{2} = 17 + 12\sqrt{2}
\]

We conjecture that $(1 + \sqrt{2})^{n+1} = P_n + Q_n\sqrt{2}$. We have just checked that the equation is true for $n = 0, 1, 2, 3$, so we may assume it is true for $0 \leq n \leq k$ and try to prove it for $n = k + 1$:

\[
(1 + \sqrt{2})^{k+2} = (1 + \sqrt{2})^{k+1}(1 + \sqrt{2}) = (P_k + Q_k\sqrt{2})(1 + \sqrt{2}) = (P_k + 2Q_k) + (P_k + Q_k)\sqrt{2} = (P_k + Q_k + Q_k) + Q_k + 1\sqrt{2} = (Q_{k+1} + Q_k) + Q_{k+1}\sqrt{2} = P_{k+1} + Q_{k+1}\sqrt{2}
\]

and the formula is proved for all $n \geq 0$. So these units are all powers of $1 + \sqrt{2}$, the fundamental unit of the ring $\mathbb{Z}[\sqrt{2}]$. Also, their inverses must be negative powers of $1 + \sqrt{2}$, and so are all the units $-(1 + \sqrt{2})^n = -P_n - Q_n\sqrt{2}$. We hope that these are all the units. Can we prove this? See Exercise 5.

**Proposition 28** For $u = a + b\sqrt{2}$ in $\mathbb{Z}[\sqrt{2}]$, we have

\[
N(u) = \pm 1 \iff u \text{ is a unit} \iff u = \pm(1 + \sqrt{2})^n \text{ for some integer } n.
\]

In other words, the group of units in $\mathbb{Z}[\sqrt{2}]$ is

\[
(\mathbb{Z}[\sqrt{2}])^\times = \{\pm(1 + \sqrt{2})^n, n \in \mathbb{Z}\}.
\]

This proposition generalizes as follows.

**Theorem 20** Let $d$ be a positive, square-free integer. Form the amazing array for $\sqrt{d}$, and let $P_s/Q_s$ be the first convergent for which $P_s^2 - dQ_s^2 = \pm 1$. Then the group of units in $\mathbb{Z}[\sqrt{d}]$ is

\[
(\mathbb{Z}[\sqrt{d}])^\times = \{\pm(P_s + Q_s\sqrt{d})^n, n \in \mathbb{Z}\}.
\]

Furthermore, if the continued fraction for $\sqrt{d}$ has period $t$, then the fundamental unit is $P_{t-1} + Q_{t-1}\sqrt{d}$, and $(P_{t-1} + Q_{t-1}\sqrt{d})^n = P_{tn-1} + Q_{tn-1}\sqrt{d}$ for all $n \in \mathbb{N}$. 
For a proof of almost all of this, see Project J. The proof of the rest is beyond the scope of this book.

Exercises

1. Show that every column of the amazing array for the continued fraction expansion of \( \sqrt{5} \) represents a unit in \( \mathbb{Z}[\sqrt{5}] \). Are these units all of the form \( \pm(a + b\sqrt{5})^n, n \in \mathbb{Z} \), for some fundamental unit \( a + b\sqrt{5} \)?

2. Find units in \( \mathbb{Z}[\sqrt{3}] \), recalling how we found them in \( \mathbb{Z}[\sqrt{2}] \), and noticing the differences. Are they all of the form \( \pm(a + b\sqrt{3})^n, n \in \mathbb{Z} \), for some fundamental unit \( a + b\sqrt{3} \)?

3. Find units in \( \mathbb{Z}[\sqrt{7}] \), recalling how we found them in \( \mathbb{Z}[\sqrt{2}] \), and noticing the differences. Are they all of the form \( \pm(a + b\sqrt{7})^n, n \in \mathbb{Z} \), for some fundamental unit \( a + b\sqrt{7} \)?

4. Find units in \( \mathbb{Z}[\sqrt{13}] \), recalling how we found them in \( \mathbb{Z}[\sqrt{2}] \), and noticing the differences. Are they all of the form \( \pm(a + b\sqrt{13})^n, n \in \mathbb{Z} \), for some fundamental unit \( a + b\sqrt{13} \)?

5. Prove that every unit in \( \mathbb{Z}[\sqrt{2}] \) is of the form \( \pm(1 + \sqrt{2})^n \) for some integer \( n \). (This completes the proof of Proposition 28.)

35 The Euclidean algorithm in \( \mathbb{Z}[\sqrt{d}] \)

Let’s try the Euclidean algorithm in \( \mathbb{Z}[\sqrt{d}] \):

\[
\begin{align*}
\frac{a + b\sqrt{d}}{c + e\sqrt{d}} &= \frac{a + b\sqrt{d}}{c + e\sqrt{d}} \cdot \frac{c - e\sqrt{d}}{c - e\sqrt{d}} \\
&= \frac{(ac - bde) + (bc - ae)\sqrt{d}}{c^2 - de^2} \\
&= \frac{ac - bde}{c^2 - de^2} + \frac{bc - ae}{c^2 - de^2}\sqrt{d} \\
&= (q_1 + q_2\sqrt{d}) + (\epsilon_1 + \epsilon_2\sqrt{d}),
\end{align*}
\]

where \( q_1 + q_2\sqrt{d} \) is in \( \mathbb{Z}[\sqrt{d}] \) and \( \epsilon_1 + \epsilon_2\sqrt{d} \in \mathbb{Q}[\sqrt{d}] \), and \( \epsilon_1 \) and \( \epsilon_2 \) are fractions with \( |\epsilon_1| \leq \frac{1}{2} \) and \( |\epsilon_2| \leq \frac{1}{2} \). Then

\[
a + b\sqrt{d} = (c + e\sqrt{d})(q_1 + q_2\sqrt{d}) + (c + e\sqrt{d})(\epsilon_1 + \epsilon_2\sqrt{d})
\]

and despite appearances the remainder, \( (c + e\sqrt{d})(\epsilon_1 + \epsilon_2\sqrt{d}) \), must be in the ring \( \mathbb{Z}[\sqrt{d}] \) since it is also \( a + b\sqrt{d} - (c + e\sqrt{d})(q_1 + q_2\sqrt{d}) \). We also have

\[
|N(\text{remainder})| = \left| N \left( (c + e\sqrt{d})(\epsilon_1 + \epsilon_2\sqrt{d}) \right) \right| = \left| N(c + e\sqrt{d})N(\epsilon_1 + \epsilon_2\sqrt{d}) \right| = |c^2 - de^2| \left| (\epsilon_1)^2 - d(\epsilon_2)^2 \right|.
\]
Now we have $0 \leq \epsilon_1 \leq \frac{1}{2}$ and $0 \leq \epsilon_2 \leq \frac{1}{2}$. If $d < 0$, we have $(\epsilon_1)^2 - d(\epsilon_2)^2 \geq 0$ and also

$$(\epsilon_1)^2 - d(\epsilon_2)^2 \leq \frac{1}{4}(1 - d)$$

so we can get a Euclidean algorithm as long as

$$\frac{1}{4}(1 - d) < 1 \iff 1 - d < 4 \iff -3 < d$$

so we have proved there is a Euclidean algorithm for the ring $\mathbb{Z}[\sqrt{2}]$, as well as for the ring $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$. On the other hand, if $d > 0$ then $(\epsilon_1)^2 - d(\epsilon_2)^2$ may be negative as well as positive, depending on $\epsilon_1$ and $\epsilon_2$. But we certainly have

$$-\frac{1}{4}d \leq -d(\epsilon_2)^2 \leq (\epsilon_1)^2 - d(\epsilon_2)^2 \leq \frac{1}{4} \leq \frac{1}{4}d$$

and thus

$$0 \leq |(\epsilon_1)^2 - d(\epsilon_2)^2| \leq \frac{1}{4}d.$$ 

Since we want this to be less than 1, we must have $d < 4$; thus there is a Euclidean algorithm for the rings $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[\sqrt{3}]$ also. The norm function, or rather its absolute value, will provide us a way of using the well-ordering principle to find smallest elements, and so you should be able to see that we have (the beginnings of) a proof of unique factorization in the ring $\mathbb{Z}[\sqrt{d}]$ for $d = -2, -1, 2,$ and $3$.

On the other hand, just because we can’t prove it doesn’t mean that we don’t have unique factorization in other rings as well. We need some counterexamples: in $\mathbb{Z}[\sqrt{-3}]$ we have

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$$

and in this ring $N(a + b\sqrt{-3}) = a^2 + 3b^2$. Thus $N(2) = 4$, $N(4) = 16$, and $N(1 \pm \sqrt{-3}) = 4$. But it is clear that $a^2 + 3b^2$ can never equal 2, so there are no elements with norm 2. If 2 or 1 $\pm \sqrt{-3}$ were to factor in $\mathbb{Z}[\sqrt{-3}]$, it would have to be into two elements of norm 2; since there are no such elements, these numbers must be primes! We have thus used the norm function to prove that 4 has two different factorizations into primes in $\mathbb{Z}[\sqrt{-3}]$, so the ring $\mathbb{Z}[\sqrt{-3}]$ does not have unique factorization. Similarly, in $\mathbb{Z}[\sqrt{-5}]$ we have

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

and in this ring $N(a + b\sqrt{-5}) = a^2 + 5b^2$. Thus $N(2) = 4$, $N(3) = 9$, and $N(1 \pm \sqrt{-5}) = 6$. But it is clear that $a^2 + 5b^2$ can never equal 2 or 3, so there are no elements of norm 2 or 3. Just as above, we conclude that the elements above must be primes. Thus 6 has two different factorizations into primes in $\mathbb{Z}[\sqrt{-5}]$, so the ring $\mathbb{Z}[\sqrt{-5}]$ does not have unique factorization. Similarly, in $\mathbb{Z}[\sqrt{10}]$ we have

$$6 = 2 \cdot 3 = (-2 + \sqrt{10})(2 + \sqrt{10})$$

and the norm function is $N(a + b\sqrt{10}) = a^2 - 10b^2$. Thus $N(2) = 4$ and $N(3) = 9$ as before, but now we have $N(\pm 2 + \sqrt{10}) = -6$. Suppose we could find integers such that $a^2 - 10b^2 = \pm 2$. Then in $\mathbb{Z}/5\mathbb{Z}$ this equation would be $a^2 \equiv \pm 2 \pmod{5}$, which has no solutions since the only squares in $\mathbb{Z}/5\mathbb{Z}$ are 0 and $\pm 1$. Thus there are no integers $a$ and $b$ that solve $a^2 - 10b^2 = \pm 2$. Similarly, there are no integers $a$ and $b$ that solve $a^2 - 10b^2 = \pm 3$. Thus there are no elements of $\mathbb{Z}[\sqrt{10}]$ with norm $\pm 2$ or.
\[ 3, \text{ so the elements above, with norms 4, 9, and } -6, \text{ must be primes in } \mathbb{Z}[\sqrt{-10}], \text{ so again 6 has two different factorizations into primes in the ring } \mathbb{Z}[\sqrt{-10}]. \text{ Thus once again we have given a counterexample to show that the ring } \mathbb{Z}[\sqrt{-10}] \text{ does not have unique factorization.}

We have not given here a complete characterization of which rings of the form \( \mathbb{Z}[\sqrt{d}] \) have unique factorization and which do not; it is beyond the scope of this book, and such questions are the subject of ongoing research. These questions have been the subject of some controversy in the past; most of the controversy has to do with which rings are eligible (\( \mathbb{Z}[\rho] \) vs. \( \mathbb{Z}[\phi] \)) and what exactly is meant by unique factorization vs. whether a Euclidean algorithm exists, etc. Feel free to research this topic further on your own (see [Marcus]).

To return to the case where \( d < 0 \), we have shown that there exists a Euclidean algorithm in \( \mathbb{Z}[i] \) and \( \mathbb{Z}[\sqrt{-2}] \). The geometric picture in \( \mathbb{Z}[i] \) was based on the square lattice \( \mathbb{Z}[i] \); the ring \( \mathbb{Z}[\sqrt{-2}] \) has a different geometry. If we draw \( \mathbb{Z}[\sqrt{-2}] \) as a subset of \( \mathbb{C} \), we will need to have the number \( a + b\sqrt{-2} = a + (b\sqrt{2})i \) correspond to the point \( (a, b\sqrt{2}) \), and thus we will get a rectangular lattice, stretched in the vertical direction, as shown in Figure 9.

![Figure 9: The geometry of \( \mathbb{Z}[\sqrt{-2}] \)](image)

Now if we multiply all the elements of \( \mathbb{Z}[\sqrt{-2}] \) by some non-zero \( w \in \mathbb{Z}[\sqrt{-2}] \), say \( w = 5 + 3\sqrt{-2} \), we will get a rectangular sublattice, as in Figure 10. And if we want to divide \( w \) into some \( z \), we can see that \( z \) lies inside one rectangle, and so we should once again choose the nearest corner, and that will give the correct \( q \) and \( r \) to use for the division algorithm. The largest possible remainder will occur if \( z \) happens to be in the very center on the rectangle, but a simple calculation shows that in that case the length of the remainder, \( q \), will be \( \frac{\sqrt{3}}{2} \) the length of the short side of the rectangle, which means that \( N(r) \leq \frac{3}{4}N(w) \); thus the geometry exactly confirms the algebra done earlier.

What happens in \( \mathbb{Z}[\sqrt{-3}] \)? Well, the rectangular lattice is now stretched a little more in the vertical direction, but essentially we have the same picture as in \( \mathbb{Z}[\sqrt{-2}] \). However, once we form the rectangular sublattice of multiples of \( w \), an interesting change occurs: the worst possible case, when \( z \) is in the center of a rectangle, makes the length of the remainder equal to the length of the shortest side of the rectangle, and so we have \( N(r) \leq N(w) \), which is not enough to ensure that the norm shrinks (in fact, it is possible to do a division algorithm calculation over and over and never
get anywhere, since the norms don’t shrink). Again, this agrees with the algebra we saw earlier, and so we are in difficulty with \( \mathbb{Z}[\sqrt{-3}] \). This difficulty will be dealt with in subsequent sections. None of this geometry applies to the cases \( \mathbb{Z}[\sqrt{2}] \) and \( \mathbb{Z}[\sqrt{3}] \), where a Euclidean algorithm also exists; we will see if we can look at these rings from another perspective.

**Exercises**

1. Find a GCD \( d \) for \( a = 104 - 79\sqrt{2} \) and \( b = 18 + 22\sqrt{2} \) in \( \mathbb{Z}[\sqrt{2}] \), and solve \( ax + by = d \) for \( x, y \in \mathbb{Z}[\sqrt{2}] \).

2. Find a GCD \( d \) for \( a = 104 - 79\sqrt{3} \) and \( b = 18 + 22\sqrt{3} \) in \( \mathbb{Z}[\sqrt{3}] \), and solve \( ax + by = d \) for \( x, y \in \mathbb{Z}[\sqrt{3}] \).

3. Find the GCD \( d \) for \( a = 16 + 25\sqrt{-3} \) and \( b = 25 - 3\sqrt{-3} \) in \( \mathbb{Z}[\sqrt{-3}] \), and solve \( ax + by = d \) for \( x, y \in \mathbb{Z}[\sqrt{-3}] \).

4. Is the following statement true or false?

\[
(26+15\sqrt{3})(10-3\sqrt{3}) = 125+72\sqrt{3} \implies 125 + 72\sqrt{3} \text{ is not a prime in } \mathbb{Z}[\sqrt{3}].
\]

Explain your reasoning why or why not.

5. Prove that for \( p \) a positive prime in \( \mathbb{Z} \), and \( d \) an integer,

\[\pm p = a^2 - db^2 \iff p \text{ is not prime in } \mathbb{Z}[\sqrt{d}].\]

6. Show directly that for \( p \) a prime integer,

\[p \text{ can be written as } p = a^2 - db^2 \implies d \text{ is a perfect square in } \mathbb{Z}/p\mathbb{Z}.\]

Hint: Are \( a \) and \( b \in \mathbb{Z}/p\mathbb{Z} \)? Are \( a \) and \( b \in (\mathbb{Z}/p\mathbb{Z})^\times \)?

7. Can you draw \( \mathbb{Z}[\sqrt{2}] \)? What are the difficulties? If you succeed in drawing a picture, what is the significance of the norm in your picture? Does it measure distance from zero? Also, what is the effect of multiplying by \( \sqrt{2} \) in your picture?
8. Calculate the continued fraction for \( \sqrt{7} \) and set up the amazing array, adding a final row where you calculate \( N(P_n + Q_n \sqrt{7}) = P_n^2 - 7Q_n^2 \). Are all the columns units, as proved in Exercise 1 on page 140 for \( \mathbb{Z}[\sqrt{2}] \)? Are all the units powers of some fundamental unit? For extra credit, you may try to prove that you have found all the units in \( \mathbb{Z}[\sqrt{7}] \).

9. Every element of \( \mathbb{Q} \) is a root of a polynomial in \( \mathbb{Z}[x] \); namely, \( \frac{a}{b} \) is a root of the polynomial \( bx - a \). The integers are special in that they are the only elements of \( \mathbb{Q} \) that are roots of monic polynomials, those whose leading coefficient is one. This is one way number theorists have used to distinguish the equivalent of the integers within certain fields (namely, finitely generated subfields of \( \mathbb{A} \), or (what is the same thing) finite field extensions of \( \mathbb{Q} \)). If \( K \) is the field in question, then \( \mathcal{O}_K \) is the ring of integers in that field. Thus \( \mathcal{O}_\mathbb{Q} = \mathbb{Z} \) itself. As another example, if we start with the field \( \mathbb{Q}[i] = \{a + bi \in \mathbb{C} : a \text{ and } b \in \mathbb{Q}\} \), each element of which is a root of a polynomial in \( \mathbb{Z}[x] \), then we could ask which elements of \( \mathbb{Q}[i] \) satisfy monic polynomials in \( \mathbb{Z}[x] \). That subset of \( \mathbb{Q}[i] \) (which is actually a subring of \( \mathbb{Q}[i] \)) is the ring of integers in \( \mathbb{Q}[i] \), designated \( \mathcal{O}_{\mathbb{Q}[i]} \).

(a) Show that every element of \( \mathbb{Q}[i] \) is a root of a quadratic polynomial in \( \mathbb{Z}[x] \).

(b) Determine \( \mathcal{O}_{\mathbb{Q}[i]} \), the ring of integers in \( \mathbb{Q}[i] \).

(c) Now let \( d \) be a fixed, square-free integer. Consider the field \( \mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \in \mathbb{C} : a \text{ and } b \in \mathbb{Q}\} \). Show that every element of \( \mathbb{Q}[\sqrt{d}] \) satisfies a quadratic polynomial in \( \mathbb{Z}[x] \).

(d) Show that the sets \( \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] := \left\{a + b \left(\frac{1+\sqrt{d}}{2}\right) : a \text{ and } b \in \mathbb{Z}\right\} \) and

\[
\left\{\frac{r}{2} + \frac{s}{2} \sqrt{d} : r \equiv s \pmod{2}\right\}
\]

are the same.

(e) Show that \( \mathcal{O}_{\mathbb{Q}[\sqrt{d}]} \), the ring of integers in \( \mathbb{Q}[\sqrt{d}] \), is

\[
\begin{cases} 
\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \pmod{4} \\
\mathbb{Z}[\sqrt{d}] & \text{else.}
\end{cases}
\]

(f) Show that if \( d \not\equiv 1 \pmod{4} \), then the set \( \left\{\frac{r}{2} + \frac{s}{2} \sqrt{d} : r \equiv s \pmod{2}\right\} \) is not a ring: in particular, show that it is not closed under multiplication, by considering \( \left(\frac{1+\sqrt{d}}{2}\right)^2 \).

36 Factoring in \( \mathbb{Z}[i] \)

We want to figure out how to factor Gaussian integers. We will get a partial converse to the earlier statement that for Gaussian integers \( z \) and \( w \),

\[ z|w \implies N(z)|N(w). \]

First, we need the
Definition 27  In $\mathbb{Z}[i]$, the conjugate of $z = a + bi$ is $\overline{z} = a - bi$.

Proposition 29  For any $z$ and $w$ in $\mathbb{Z}[i]$, we have

$$z + w = \overline{z} + \overline{w} \quad \text{and} \quad z \cdot w = \overline{z} \cdot \overline{w}.$$ 

Proof. Let $z = a + bi$ and $w = c + di$. Then

$$z + w = (a + c) + (b + d)i$$

and

$$\overline{z} + \overline{w} = (a - bi) + (c - di) = (a + c) - (b + d)i;$$

these Gaussian integers are clearly conjugates of each other. Similarly,

$$z \cdot w = (a + bi)(c + di) = (ac - bd) + (bc + ad)i$$

and

$$\overline{z} \cdot \overline{w} = (a - bi) \cdot (c - di) = (ac - bd) - (bc + ad)i;$$

again, these Gaussian integers are clearly conjugates of each other. 

Proposition 30  For $z$ and $w$ in $\mathbb{Z}[i]$, we have

$$z | w \iff \overline{z} | \overline{w}.$$ 

Proof. $z | w \implies w = z \cdot v$ for some Gaussian integer $v$. But then $\overline{w} = \overline{z} \cdot \overline{v} = \overline{z} \cdot \overline{v}$ so $\overline{z} | \overline{w}$. On the other hand, we have just proved that

$$\overline{z} | \overline{w} \implies \overline{z} | \overline{w}$$

and it is clear that $\overline{z} = z$ and $\overline{w} = w$. 

Proposition 31  If $a + bi \in \mathbb{Z}[i]$ and $2 | N(a + bi) = a^2 + b^2$, then

- $a^2 + b^2 = 2 \iff a + bi \sim 1 + i$
- $a^2 + b^2 > 2 \implies (1 + i)|(a + bi)$.

Proof. Clearly, $a^2 + b^2 = 2 \iff a = \pm 1$ and $b = \pm 1$. But $\pm 1 \pm i \sim 1 + i$, so we are done.

We have $(1 + i)(1 - i) = 2$ so $(1 + i)|2$. Then $2|(a^2 + b^2) \implies (1 + i)|(a^2 + b^2) = (a + bi)(a - bi)$ so we conclude that

$$(1 + i)|(a + bi) \quad \text{or} \quad (1 + i)|(a - bi).$$
This is because $N(1+i) = 2$, which is a prime in $\mathbb{Z}$, so we know that $1+i$ is a prime in $\mathbb{Z}[i]$, and we may apply the prime theorem in $\mathbb{Z}[i]$. If $1+i|a-bi$, then since $1+i|2$, we know that $1+i$ divides the linear combination $(a-bi) + 2(bi) = a+bi$. Thus we are done.

We might also notice that $2|a^2 + b^2 \iff a$ and $b$ are both even or they are both odd. Thus we have a very simple criterion for whether $1+i$ is a factor of $a+bi$: we know that

$$(1+i)|9817461027 + 31606813423i$$

but

$$(1+i)|14329485671497 - 109834172632i.$$  

This actually leads to a different proof: if $2|(a^2 + b^2)$, then it is clear that $a$ and $b$ are both even or they are both odd. Now

$$\frac{a+bi}{1+i} \cdot \frac{1-i}{1-i} = \frac{(a+b) + (b-a)i}{2} = \frac{a+b}{2} + \frac{b-a}{2}i$$

and this is a Gaussian integer since $a+b$ and $b-a$ are each even. Thus $(1+i)|(a+bi)$.

What about other Gaussian integers? What we used in this proof was the fact that $N(1+i) = 2$ is a prime in $\mathbb{Z}$, so $1+i$ was a prime in $\mathbb{Z}[i]$. Thus we could use the prime theorem in $\mathbb{Z}[i]$. Can we imitate this proof to get something like $5|(a^2 + b^2)$?

This seems promising, but an example may be instructive here: what about the Gaussian integer $4+7i$? It has norm $16+49 = 65$, so we have that $5|(a^2 + b^2)$. But

$$\frac{4+7i}{1+2i} = \frac{4+7i}{1+2i} \cdot \frac{1-2i}{1-2i} = \frac{18-i}{5}$$

and this is not a Gaussian integer, so $1+2i|4+7i$. What is happening here may be clearer if we notice that $4+7i = (2+i)(3+2i)$, so $1+2i|4+7i$, but $2+i|4+7i$. Also, notice that the only Gaussian integers with norm 5 are $\pm 2 \pm i$ and $\pm 1 \pm 2i$, and we have that

$$2+i \sim -1+2i \sim -2-i \sim 1-2i$$

while

$$1+2i \sim -2+i \sim -1-2i \sim 2-i$$

so these eight Gaussian integers split into two sets of four associates. The correct statement about this situation is

**Proposition 32** For a Gaussian integer $a+bi$, we have

$$5|(a^2 + b^2) \implies (1+2i)|(a+bi) \quad \text{or} \quad (2+i)|(a+bi).$$

**Proof.** Once again, we have two proofs: we have $5|(a+bi)(a-bi)$ and $(2+i)|5$ since $(2+i)(1+2i) = 5$. Thus $(2+i)|(a+bi)(a-bi)$ and, using the prime theorem in $\mathbb{Z}[i]$, we get

$$(2+i)|(a+bi) \quad \text{or} \quad (2+i)|(a-bi).$$
In the first case, we are done; in the second, we get $(2 - i)|(a + bi)$ by taking conjugates, and then we can multiply by the divisibility statement $i|1$ to get $(1 + 2i)|(a + bi)$, and we are done.

Alternate proof: $5|(a^2 + b^2) \implies a^2 + b^2 \equiv 0 \pmod{5}$. What are the perfect squares in $\mathbb{Z}/5\mathbb{Z}$? They are 0 and ±1. Thus

$$a^2 + b^2 \equiv 0 \pmod{5} \implies \begin{cases} a^2 \equiv b^2 \equiv 0 \pmod{5} \\ \text{or} \\ a^2 \equiv 1 \pmod{5} \text{ and } b^2 \equiv -1 \pmod{5} \\ \text{or} \\ a^2 \equiv -1 \pmod{5} \text{ and } b^2 \equiv 1 \pmod{5}. \end{cases}$$

Now, if $a^2 \equiv b^2 \equiv 0 \pmod{5}$, then $5|a$ and $5|b$, so $5|(a+bi)$ and $(2+i)|(a+bi)$ and $(1+2i)|(a+bi)$. So in this case we are done. On the other hand, $x^2 \equiv 1 \pmod{5} \iff x \equiv \pm 1 \pmod{5}$, and $x^2 \equiv -1 \pmod{5} \iff x \equiv \pm 2 \pmod{5}$.

Also, we have

$$\frac{a + bi}{2 + i} = \frac{a + bi}{2 + i} \cdot \frac{2 - i}{2 - i} = \frac{(2a + b) + (2b - a)i}{5}$$

and

$$\frac{a + bi}{1 + 2i} = \frac{a + bi}{1 + 2i} \cdot \frac{1 - 2i}{1 - 2i} = \frac{(a + 2b) + (b - 2a)i}{5}.$$ 

You may check for yourself that

$$\begin{cases} a \equiv 1 \pmod{5} \\ b \equiv -2 \pmod{5} \end{cases} \implies (2 + i)|(a + bi)$$

$$\begin{cases} a \equiv 1 \pmod{5} \\ b \equiv 2 \pmod{5} \end{cases} \implies (1 + 2i)|(a + bi)$$

$$\begin{cases} a \equiv -1 \pmod{5} \\ b \equiv -2 \pmod{5} \end{cases} \implies (1 + 2i)|(a + bi)$$

$$\begin{cases} a \equiv -1 \pmod{5} \\ b \equiv 2 \pmod{5} \end{cases} \implies (2 + i)|(a + bi).$$

The other four possibilities are checked similarly.

Can we generalize this to other Gaussian integers? We can try to prove the following

**Proposition 33** If $N(r + si) = p$, a prime in $\mathbb{Z}$, then $r + si$ is a prime in $\mathbb{Z}[i]$, and therefore

$$p|(a^2 + b^2) \implies (r + si)|(a + bi) \text{ or } (s + ri)|(a + bi).$$
Before we prove this proposition, let’s see how it can be useful. Suppose we wish to factor $18 + 25i$. We have $N(18 + 25i) = 18^2 + 25^2 = 324 + 625 = 949 = 13 \cdot 73$. We have $13 = 2^2 + 3^2$ and $73 = 8^2 + 3^2$. Thus if our proposition is true, we will know that $(2 + 3i)|(18 + 25i)$ or $(3 + 2i)|(18 + 25i)$; and further we will know the other factor also: it will be either $8 + 3i$ or $3 + 8i$, right? Let’s just try:

$$\frac{18 + 25i}{2 + 3i} = \frac{18 + 25i}{2 + 3i} \cdot \frac{2 - 3i}{2 - 3i} = \frac{111 - 4i}{13},$$

which is not a Gaussian integer. But, we also have

$$\frac{18 + 25i}{3 + 2i} = \frac{18 + 25i}{3 + 2i} \cdot \frac{3 - 2i}{3 - 2i} = \frac{104 + 39i}{13} = 8 + 3i$$

so we see that $18 + 25i = (3 + 2i)(8 + 3i)$. Let’s try another example: how does $34 + 13i$ factor? We have $N(34 + 13i) = 34^2 + 13^2 = 1156 + 169 = 1325 = 5 \cdot 265 = 5^2 \cdot 53$. The $5$ tells us that $2 + i$ or $1 + 2i$ is a factor; the $53$ tells us that $7 + 2i$ or $2 + 7i$ is a factor. Let’s try:

$$\frac{34 + 13i}{2 + i} = \frac{34 + 13i}{2 + i} \cdot \frac{2 - i}{2 - i} = \frac{81 - 8i}{5},$$

which doesn’t work, but

$$\frac{34 + 13i}{1 + 2i} = \frac{34 + 13i}{1 + 2i} \cdot \frac{1 - 2i}{1 - 2i} = \frac{60 - 55i}{5} = 12 - 11i.$$

Now we must factor $12 - 11i$, which has norm $12^2 + 11^2 = 144 + 121 = 265 = 5 \cdot 53$. Once again we have two options, $2 + i$ or $1 + 2i$:

$$\frac{12 - 11i}{2 + i} = \frac{12 - 11i}{2 + i} \cdot \frac{2 - i}{2 - i} = \frac{13 - 34i}{5},$$

which doesn’t work, but

$$\frac{12 - 11i}{1 + 2i} = \frac{12 - 11i}{1 + 2i} \cdot \frac{1 - 2i}{1 - 2i} = \frac{-10 - 35i}{5} = -2 - 7i.$$

So, we have

$$34 + 13i = (1 + 2i)(12 - 11i) = (1 + 2i)^2(-2 - 7i) = (-1)(1 + 2i)^2(2 + 7i).$$

Now we have the

Proof. We have $p = r^2 + s^2 = (r + si)(r - si)$, and $p|(a^2 + b^2) = (a + bi)(a - bi)$; thus $(r + si)p$ and $(r + si)|(a + bi)(a - bi)$, so we have

$$(r + si)|(a + bi) \quad \text{or} \quad (r + si)|(a - bi)$$

since we can apply the prime theorem in $\mathbb{Z}[i]$. Then if $(r + si)|(a + bi)$ we are done, and if $(r + si)|(a - bi)$ then $(r - si)|(a + bi)$ and we can multiply by $i|1$ to get $(s + ri)|(a + bi)$.

This will be a powerful weapon when we try to factor Gaussian integers.
Exercises

1. Factor $231 + 1792i$ into primes in $\mathbb{Z}[i]$.

2. Factor $4275 - 4121i$ into primes in $\mathbb{Z}[i]$.

3. Factor $1235 - 4121i$ into primes in $\mathbb{Z}[i]$.

4. Factor $28259 - 4240i$ into primes in $\mathbb{Z}[i]$.

5. How many Gaussian integers have norm $2 \cdot 5 \cdot 13$? Try to count them without doing a lot of calculations.

6. How many Gaussian integers have norm $2 \cdot 3^2 \cdot 5 \cdot 13$? Try to count them without doing a lot of calculations.

7. How many Gaussian integers have norm $2 \cdot 3^3 \cdot 5^3 \cdot 13^3$? Try to count them without doing a lot of calculations.

8. How many Gaussian integers have norm $3^2 \cdot 5^2 \cdot 7^2 \cdot 29^4$? Try to count them without doing a lot of calculations.

37 The primes in $\mathbb{Z}[i]$  

Now, which sort of primes in $\mathbb{Z}$ can be written as $p = r^2 + s^2$? We have gathered some evidence in the exercises:

<table>
<thead>
<tr>
<th>Can</th>
<th>Can't</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>13</td>
<td>7</td>
</tr>
<tr>
<td>17</td>
<td>11</td>
</tr>
<tr>
<td>29</td>
<td>19</td>
</tr>
<tr>
<td>37</td>
<td>23</td>
</tr>
<tr>
<td>41</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td>43</td>
</tr>
<tr>
<td></td>
<td>47</td>
</tr>
<tr>
<td></td>
<td>51</td>
</tr>
</tbody>
</table>

Any guesses about the prime 101? 103? 107? 109?

We get a

**Proposition 34** For $p$ a prime in $\mathbb{Z}$, we have

there are $a, b \in \mathbb{Z}$ with $p = a^2 + b^2 \iff p \equiv 1 \pmod{4}$ or $p = 2$.

**Proof.** You will prove $\implies$ in the exercises. We will prove $\iff$ later. □
We have seen that prime integers are the building blocks of \( \mathbb{Z} \), and prime Gaussian integers are building blocks of \( \mathbb{Z}[i] \). How can we find them? One way is directly: since \( a \mid b \implies |a| \leq |b| \) in \( \mathbb{Z} \), we can just try all numbers less than some integer \( n \)—if none is a proper factor, \( n \) must be a prime! An ancient Greek mathematician, Eratosthenes, had a good method for doing this: list all the positive integers up to some large number, say 1000. Then since 1 is the only integer less than 2, 2 must be a prime. Now cross out all multiples of 2, since they aren’t prime. Now what is the next integer not crossed out? 3, of course. So 3 must be prime, since it is not a multiple of anything smaller than it. Cross out all the multiples of 3, since they aren’t prime, and look for the next prime—5. Continue until you have finished your list. (Which happens once you have crossed out all multiples of 31—why?) This is called the Sieve of Eratosthenes: all the non-primes fall through the sieve, leaving the primes behind. There are other methods for checking specific numbers, but we will see them later. One way we’ve seen already (see Section 26, page 108): for \( n \neq 4 \), we have

\[
(n - 1)! \equiv \begin{cases} 
-1 \pmod{n} & \text{if } n \text{ is a prime} \\
0 \pmod{n} & \text{otherwise}.
\end{cases}
\]

However, this is not practical in the case of large numbers, since \((n - 1)!\) gets very large very quickly as \( n \) gets large.

We can use something similar to the Sieve of Eratosthenes to find the primes in \( \mathbb{Z}[i] \), but now the work we have done in \( \mathbb{Z} \) helps. First you list all the Gaussian integers, grouped by norm, up to some limit. Then you see that anything with prime norm must be a prime. Then you look at the Gaussian integers that remain and try to factor them, using the norm to eliminate all but a few candidates. Thus to factor the Gaussian integers with norm 65, we need only see if they can be divided by some Gaussian integer with norm 5. It turns out that this will always work, as we proved in Proposition 33, but even before we knew that proposition, we could see that we needed to perform at most two divisions to check all eight elements with norm 5 (since they come in two sets, of four associates each). Thus we have a (tedious) way of finding all the primes in \( \mathbb{Z}[i] \).

In fact, we can do more. Though we have not yet proved Proposition 34, we can use it to completely characterize all Gaussian integers and their factorizations into Gaussian integer primes.

**Theorem 21** Let \( z = a + bi \) be a Gaussian integer. Then \( N(z) \) has the factorization (into prime integers)

\[
N(z) = a^2 + b^2 = 2^t p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_s^{e_s} q_1^{2f_1} q_2^{2f_2} q_3^{2f_3} \cdots q_s^{2f_s},
\]

where \( t \in \mathbb{N} \), each \( p_j \equiv 1 \pmod{4} \) and each \( q_j \equiv 3 \pmod{4} \), \( r \) and \( s \) are in \( \mathbb{N} \), and each power \( e_j \) and \( f_j \) is a positive integer. Furthermore, \( z \) itself factors (uniquely, by Theorem 17) into Gaussian integers as follows

\[
z \sim (1 + i)^t \psi_1^{g_1} \psi_2^{g_2} \cdots \psi_r^{g_r} q_1^{f_1} q_2^{f_2} q_3^{f_3} \cdots q_s^{f_s}
\]

where \( p_j = a_j^2 + b_j^2 \) and \( \psi_j = a_j + b_j i \), \( \bar{\psi}_j = b_j - a_j i \), and for each \( j \), \( 0 \leq g_j \leq e_j \).
Specifically, every prime, \( \wp \), in \( \mathbb{Z}[i] \) takes one of three forms

- \( \wp \sim 1 + i \)
- \( \wp \sim a + bi \) where \( N(\wp) = a^2 + b^2 = p \equiv 1 \pmod{4} \) is a prime integer
- \( \wp \sim q_j \) where \( q_j \equiv 3 \pmod{4} \) is a prime integer.

We have phrased this as facts about the primes in the larger ring, \( \mathbb{Z}[i] \). We could instead phrase this as facts about what happens to the primes in \( \mathbb{Z} \) when we pass to the larger ring, \( \mathbb{Z}[i] \). Now we see that every prime integer, \( p \), falls into one of three categories:

- \( p \sim (a + bi)^2 \) (the prime \( p \) is said to be ramified in \( \mathbb{Z}[i] \), or to ramify in \( \mathbb{Z}[i] \))
- \( p \sim (a + bi)(c + di) \) with \( a + bi \not\sim c + di \) (the prime \( p \) is said to split in \( \mathbb{Z}[i] \))
- \( p \) is a prime element of the larger ring \( \mathbb{Z}[i] \) (the prime \( p \) is said to remain inert in \( \mathbb{Z}[i] \))

The only positive prime integer that ramifies in \( \mathbb{Z}[i] \) is 2. Positive prime integers that are 1 (mod 4) split in \( \mathbb{Z}[i] \), and positive prime integers that are 3 (mod 4) remain inert in \( \mathbb{Z}[i] \). (Alternatively, one may say that a prime in \( \mathbb{Z} \) of the form \( 4k + 1 \) is a split prime and a prime in \( \mathbb{Z} \) of the form \( 4k + 3 \) is an inert prime. This phrasing assumes that the larger ring (in this case, \( \mathbb{Z}[i] \)) is clear.)

These facts (about how elements of the larger rings factor into primes, and how prime integers factor in the larger ring) will be shown to have analogs in \( \mathbb{Z}[\sqrt{2}] \), \( \mathbb{Z}[\sqrt{-2}] \), \( \mathbb{Z}[\rho] \), \( \mathbb{Z}[\sqrt{-3}] \), \( \mathbb{Z}[\sqrt{5}] \), and \( \mathbb{Z}[\omega] \) (where \( \omega \) is the golden ratio). Each time, there will only be a finite number of ramified primes, which are distinguished from the split primes by the fact that they factor into powers of primes, not into products of distinct primes. As examples, \( 2 \sim (\sqrt{-2})^2 \) is the only ramified prime in \( \mathbb{Z}[\sqrt{-2}] \), and \( 3 \sim (1 + 2\rho)^2 \) is the only ramified prime in \( \mathbb{Z}[\rho] \).

**Exercises**

1. Prove the forward implication (\( \Rightarrow \)) in Proposition 34.

2. Prove Theorem 21. You may use Proposition 34, which will be proved in Section 39. You may well wish to write (and prove) a lemma along the lines of “If \( p \equiv 3 \pmod{4} \) is a prime and \( p|a^2 + b^2 \), then \( p|a \) and \( p|b \).”

3. Use Theorem 21 to characterize those integers that can be written in the form \( a^2 + b^2 \), and which cannot.

4. Following Exercise 3, and following up on Exercise 16 (page 79), characterize those integers \( n \) that can be written in the form \( n = a^2 - ab + b^2 \). We do not have a theorem that applies (yet). However, we have the following data:
<table>
<thead>
<tr>
<th>primes that can be written as $p = a^2 - ab + b^2$</th>
<th>primes that cannot be written as $p = a^2 - ab + b^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3, 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97, 103, 109, 127, 139, 151, 157, 163, 181, 193, 199, ...</td>
<td>2, 5, 11, 17, 23, 29, 41, 47, 53, 59, 71, 83, 89, 101, 107, 113, 131, 137, 149, 167, 173, 179, 191, 197, ...</td>
</tr>
<tr>
<td>composites that can be written as $n = a^2 - ab + b^2$</td>
<td>composites that cannot be written as $n = a^2 - ab + b^2$</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>4, 9, 12, 16, 21, 25, 27, 28, 36, 39, 48, 49, 52, 57, 63, 64, 75, 76, 81, 84, 91, 93, 100, ...</td>
<td>6, 8, 10, 14, 15, 18, 20, 22, 24, 26, 30, 32, 33, 34, 35, 38, 40, 42, 44, 45, 46, 50, 51, 54, 55, 56, 58, 60, 62, 65, 66, 68, 69, 70, 72, 74, ...</td>
</tr>
</tbody>
</table>