Chapter 5
What numbers are the edges of a right triangle?

In this chapter we study numbers that appear as the side lengths of primitive right triangles. We use rings of Gaussian integers to prove our main theorems. We give a quick review of the basic properties of the ring of Gaussian integers. We then prove that the ring of Gaussian integers is a Euclidean domain, leading to the analogue of the Fundamental Theorem of Arithmetic in this context. We also determine the irreducible elements and units of $\mathbb{Z}[i]$. For a more thorough exposition of the theory of Gaussian integers we refer the reader to the classical text by Sierpinski [46] or Conrad [69]. In this chapter we also determine what numbers are a sum of two squares (Theorem 5.2) and determine the numbers which appear as the hypotenuse of a primitive right triangle (Theorem 5.1). In the Notes we state a famous theorem of Dirichlet (Theorem 5.11) and say a couple of words about algebraic number theory.

5.1 The theorem

If n is an odd number, then it is the side length of some right triangle. In fact, we can always write $n = xy$ with x, y coprime and odd. Then the following set

$$\tau(x, y) = \left\{ \frac{x^2 - y^2}{2}, n = xy, \frac{x^2 + y^2}{2} \right\}$$

is the set of side lengths of a primitive right triangle.

If n is an even number, then we can write $n = 2xy$ with x, y coprime. If one of x or y is even, i.e., if n is divisible by 4, then again the set $\{x^2 - y^2, 2xy, x^2 + y^2\}$ is the set of side lengths of a primitive right triangle. If on the other hand $2||n$, then n cannot be the side length of a primitive right triangle.

R. Takloo-Bighash, *A Pythagorean Introduction to Number Theory*,
Undergraduate Texts in Mathematics, https://doi.org/10.1007/978-3-030-02604-2_5

It turns out that the question of whether a natural number can occur as the length of the hypotenuse of a primitive right triangle is more subtle. Recall the list of the first few Pythagorean triples at the beginning of §3.1. The hypotenuse lengths that occur in the list are 5, 13, 17, 25, 29, 29, 37, 41, 53. The prime numbers occurring in the prime factorization of these numbers are 5, 13, 17, 29, 37, 41, 53, and a quick check reveals that all of these prime numbers are of the form $4k + 1$. In this chapter we prove the following theorem:

Theorem 5.1. *A number n is the length of the hypotenuse of some primitive right triangle if and only if all of its prime factors are of the form $4k + 1$.*

Recall the formula for the hypotenuse of a primitive right triangle, $x^2 + y^2$ if x, y are coprime of different parity, or $(x^2 + y^2)/2$ if x, y are coprime and both odd. Clearly something is going on with sums of two squares! And in fact the first step to prove the theorem is understanding what numbers can be written as a sum of two squares. We start by examining the sequence of natural numbers. Clearly, $1 = 1^2 + 0^2$, 2 = $1^2 + 1^2$, 3 is not a sum of two squares, $4 = 2^2 + 0^2$, $5 = 2^2 + 1^2$, 6 is not, 7 is not, $8 = 2^2 + 2^2$, $9 = 3^2 + 0$, $10 = 3^2 + 1^2$, 11 is not, 12 is not, $13 = 3^2 + 2^2$, 14 is not, 15 is not, $16 = 4^2 + 0^2$, $17 = 4^2 + 1^2$, $18 = 3^2 + 3^2$, $20 = 4^2 + 2^2$, 21 is not, 22 is not, 23 is not, 24 is not, $25 = 5^2 + 0^2$, $26 = 5^2 + 1^2$, 27 is not, 28 is not, $29 = 5^2 + 2^2$, 30 is not, 31 is not, $32 = 4^2 + 4^2$, etc. While it is not immediately clear that one should do this next thing, but we look at the prime factorization of the integers that are *not* sums of two squares: 3, $6 = 2 \cdot 3$, 7, 11, $12 = 2^2 \cdot 3$, $14 = 2 \cdot 7$, $15 = 3 \cdot 5$, $21 = 3 \cdot 7$, $22 = 2 \cdot 11$, 23, $24 = 2^3 \cdot 3$, $27 = 3^3$, $28 = 2^2 \cdot 7$, $30 = 2 \cdot 3 \cdot 5$, 31. The common feature of all of these numbers is that they all have at least one prime factor of the form $4k + 3$ which appears with an odd exponent. In fact, we will prove the following theorem:

Theorem 5.2. *A number n is the sum of two squares if and only if every one of its prime factors of the form $4k + 3$ has even exponent in its prime factorization.*

We refer to Theorem 5.2 as the *Two Squares Theorem*. As we noted it is clear that 3 is not the sum of two squares. If on the other hand some number which is a multiple of 3 is a sum of two squares $a^2 + b^2$, then this means $3 \mid a^2 + b^2$. Now, $0^2 \equiv 0$, $1^2 \equiv 0$, $2^2 \equiv 1 \bmod 3$. Consequently, in order for $a^2 + b^2 \equiv 0 \bmod 3$, we need to have $a \equiv 0$, $b \equiv 0 \bmod 3$, i.e., both a, b are divisible by 3. This implies that $a^2 + b^2$ is actually divisible by 3^2. Note that 3 is a prime of the form $4k + 3$. The sort of situation we just described does not happen for primes of the form $4k + 1$ such as 5 as for example $5 = 1^2 + 2^2$, and neither 1 nor 2 is divisible by 5.

The proof we present for these theorems is best expressed in terms of the arithmetic of complex integers which we present in the next section. The idea is that if we have a complex number $z = x + iy$, with $x, y \in \mathbb{R}$, then $|z|^2 = x^2 + y^2$, and these are the sorts of expressions that we wish to study. Since in our theorem we need to look at those cases where $x, y \in \mathbb{Z}$, we are led to study complex numbers $z = x + iy$ with $x, y \in \mathbb{Z}$.

5.2 Gaussian integers

A *Gaussian integer* is a complex number $x + iy$ with $x, y \in \mathbb{Z}$. We define the *ring of Gaussian integers* to be

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\},$$

where here and elsewhere $i^2 = -1$. Equipped with the standard addition and multiplication of complex numbers, $\mathbb{Z}[i]$ is a commutative ring with identity. For $z \in \mathbb{Z}[i]$, we define $\bar{z}$ to be the complex conjugate of z, i.e.,

$$\overline{a + bi} = a - bi,$$

and we define the *norm* of z, $N(z)$, to be

$$N(z) = z \cdot \bar{z}.$$

A computation shows that

$$N(a + ib) = a^2 + b^2.$$

We let $|z| = N(z)^{1/2}$.

Lemma 5.3. *For all $z, w \in \mathbb{Z}[i]$,*

$$N(zw) = N(z)N(w).$$

Proof. It is easy to check that $\overline{z \cdot w} = \bar{z} \cdot \bar{w}$. Then we have

$$N(zw) = zw \cdot \overline{zw} = zw \cdot \bar{z} \cdot \bar{w} = (z\bar{z}) \cdot (w\bar{w}) = N(z)N(w).$$

□

An element $u \in \mathbb{Z}[i]$ is called a *unit*, if there is a $v \in \mathbb{Z}[i]$ such that $uv = 1$. Taking norms gives $N(u) \cdot N(v) = 1$. Since the norm is always nonnegative, this identity implies $N(u) = 1$. It is easy to check that these are indeed units. It is also easy to check if $u \in \mathbb{Z}[i]$ satisfies $N(u) = 1$, then u is a unit, because then $u \cdot \bar{u} = N(u) = 1$. An easy examination shows that u can only be one of the following elements: $+1$, -1, i, and $-i$. Gaussian integers x, y are called *associates* if $x = uy$ for a unit u.

Divisibility and unique factorization

There is a division algorithm in $\mathbb{Z}[i]$:

Theorem 5.4. *If $a, b \in \mathbb{Z}[i]$ with $b \neq 0$, then there are $q, r \in \mathbb{Z}[i]$ such that*

$$a = bq + r$$

with $N(r) < N(b)$. Consequently, $\mathbb{Z}[i]$ is a Euclidean domain.

Proof. We wish to write

$$\frac{a}{b} = q + \frac{r}{b}$$

with $q \in \mathbb{Z}[i]$ and $N(r/b) < 1$. Write a/b as $a\bar{b}/N(b)$, and set $a\bar{b} = u + iv$. By the last statement in Theorem 2.8 we can write

$$u = q_1 N(b) + r_1,$$

$$v = q_2 N(b) + r_2,$$

with $|r_1|, |r_2| \leq N(b)/2$. Consequently,

$$\frac{a}{b} = \frac{a\bar{b}}{N(b)} = \frac{u + iv}{N(b)} = q_1 + iq_2 + \frac{r_1 + ir_2}{N(b)}.$$

If we set $q = q_1 + iq_2$, we get

$$a = qb + \frac{r_1 + ir_2}{\bar{b}}.$$

Since a and qb are in $\mathbb{Z}[i]$, we see that

$$r := \frac{r_1 + ir_2}{\bar{b}} \in \mathbb{Z}[i].$$

We just need to show that

$$N(r) < N(b).$$

We have

$$N(r) = N(\frac{r_1 + ir_2}{\bar{b}}) = \frac{r_1^2 + r_2^2}{N(\bar{b})}$$

$$\leq \frac{N(b)^2/4 + N(b)^2/4}{N(b)} = \frac{N(b)}{2} < N(b).$$

□

Here is an alternative, geometric way to *see* the above theorem. Let's fix the non-zero Gaussian integer b as in the theorem, and examine the set of all Gaussian integers of the form qb with $q \in \mathbb{Z}[i]$. Write $q = q_1 + q_2 i$ with $q_1, q_2 \in \mathbb{Z}$, to obtain

$$qb = (q_1 + q_2 i)b = q_1 \cdot b + q_2 \cdot ib.$$

The Gaussian integer ib is obtained from b via a counterclockwise 90-degree rotation around the origin as in Figure 5.1.

This means that $0, b, ib$, and $ib + b$ are the four vertices of a square. Furthermore, since every Gaussian integer of the form qb is an integral linear combination of b and ib, the set of all such points qb is going to be a square grid in the plane as in the diagram. Now, every Gaussian integer a falls in one of these squares. The distance between a to the closest vertex of the square in which it lives is at most the side

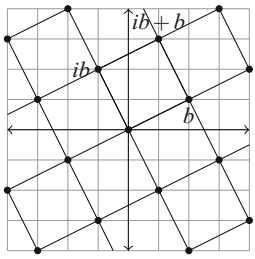

Fig. 5.1 The geometric proof of Theorem 5.4

length of the square, $|b|$, i.e., $|a - qb| < |b|$ for some Gaussian integer q. Squaring this inequality gives $N(a - bq) < N(b)$, as claimed.

Since $\mathbb{Z}[i]$ is a Euclidean domain, it is a *principal ideal domain* (PID), and therefore a *unique factorization domain*; see [25, Ch. 3, §7]. The latter means that every element of $\mathbb{Z}[i]$ is a product of *irreducible elements* in an essentially unique way. Recall that we call an element ϖ of $\mathbb{Z}[i]$ an *irreducible element* if any identity of the form $\varpi = xy$ with $x, y \in \mathbb{Z}[i]$ implies either x or y is a unit. Since $\mathbb{Z}[i]$ is a UFD, every irreducible element is prime. Recall that an element p of a domain R is called *prime* if the principal ideal (p) is prime.

5.3 The proof of Theorem 5.2

The proof of Theorem 5.2 uses three ingredients:

Lemma 5.5 (Ingredient 1). *If m and n are expressible as sums of squares, then so is mn.*

Proof. The easiest way to see this is by using complex numbers. If $m = a^2 + b^2$, then $m = N(a + ib)$, the norm of the complex number $a + ib$. Similarly, if $n = c^2 + d^2$, then $n = N(c + id)$. Next, by Lemma 5.3,

$$mn = N(a + ib)N(c + id) = N((a + ib)(c + id))$$

$$= N((ac - bd) + i(ad + bc)) = (ac - bd)^2 + (ad + bc)^2.$$

□

Lemma 5.6 (Ingredient 2). *If p is a prime of the form $4k + 3$, and if for integers a, b, $p \mid a^2 + b^2$, then $p \mid a$ and $p \mid b$.*

Proof. If $p \nmid a$, then $a^2 + b^2 \equiv 0 \bmod p$ implies

$$(ba^{-1})^2 \equiv -1 \mod p.$$

This means the equation $x^2 \equiv -1 \mod p$ has a solution u modulo p. By Theorem 2.51 there is a $g \mod p$ such that $o_p(g) = p-1$. We write $u \equiv g^i \mod p$ for some $0 < i < p-1$. On the other hand, since $g^{(p-1)/2} \not\equiv +1 \mod p$, and $(g^{(p-1)/2})^2 \equiv +1 \mod p$, we conclude that

$$g^{(p-1)/2} \equiv -1 \mod p.$$

Consequently,

$$g^{2i} \equiv g^{(p-1)/2} \mod p.$$

Lemma 2.47 implies

$$2i \equiv \frac{p-1}{2} \mod (p-1).$$

But since $2i$ and $p-1$ are even, and $(p-1)/2$ is odd, this is a contradiction. □

We will see in Lemma 6.7 that the equation $x^2 \equiv -1 \mod p$ has a solution modulo p if and only if p is not of the form $4k+3$.

The next ingredient is a substantial theorem due to Fermat. Here we will give an algebraic proof for the theorem. We will also present a geometric proof in Chapter 10 and another proof using the theory of quadratic forms in §12.2.

Theorem 5.7 (Ingredient 3). *An odd prime number is expressible as a sum of two squares if and only if it is of the form* $4k+1$.

Proof. First suppose $p = x^2 + y^2$. Look at everything modulo 4. Then $x^2 \equiv 0, 1 \mod 4$, and as a result $x^2 + y^2 \equiv 0, 1, 2 \mod 4$. This means $p \equiv 0, 1, 2 \mod 4$. Obviously if $p \equiv 0 \mod 4$, it cannot be a prime number. If $p \equiv 2 \mod 4$, then $p = 2$, and not odd. Consequently, $p \equiv 1 \mod 4$ is the only possibility, proving the necessity of the condition.

Now we show if p is of the form $4k+1$, then p is expressible as a sum of two squares. The proof of this statement requires several steps:

Step 1. There exists a such that $a^2 \equiv -1 \mod p$.

By Wilson's Theorem, Equation (2.8), $(p-1)! \equiv -1 \mod p$. Next,

$$x \cdot (p-x) \equiv -x^2 \mod p.$$

Hence

$$-1 \equiv (p-1)! \equiv (-1)^{(p-1)/2} \left((\frac{p-1}{2})! \right)^2 \equiv \left((\frac{p-1}{2})! \right)^2 \mod p$$

as for $p \equiv 1 \mod 4$, $(p-1)/2$ is even. Consequently, $a = ((p-1)/2)!$ satisfies $a^2 \equiv -1 \mod p$. Note that this means $a^2 + 1 \equiv 0 \mod p$. It is also clear that if b is another integer such that $b^2 \equiv -1 \mod p$, then $a \equiv \pm b \mod p$.

Step 2. Now, with the choice of a as in Step 1, for every integer x we have $x^2(a^2+1) \equiv 0 \bmod p$, or $x^2 + (ax)^2 \equiv 0 \bmod p$. This means $p \mid x^2 + (ax)^2$. So if y is an integer such that $y \equiv \pm ax \bmod p$, we have $p \mid x^2 + y^2$. Conversely, suppose we have integers u, v such that $p \mid u^2 + v^2$, but p is not a factor of either u or v. Then $v^2 \equiv -u^2 \bmod p$, and consequently, $(vu^{-1})^2 \equiv -1 \bmod p$, so that $vu^{-1} \equiv \pm a \bmod p$, and $v \equiv \pm au \bmod p$.

Step 3. Assume there are integers x, y such that $p = x^2 + y^2$. By Step 2, $y \equiv \pm ax \bmod p$. Furthermore, since $x^2 < p$ and $y^2 < p$, we have $x \leq [\sqrt{p}]$ and $y \leq [\sqrt{p}]$. Conversely, suppose we have non-zero integers x, y such that $x, y \leq [\sqrt{p}]$ and $y \equiv \pm ax \bmod p$. Then by Step 2, $p \mid x^2 + y^2 \leq [\sqrt{p}]^2 + [\sqrt{p}]^2 < \sqrt{p}^2 + \sqrt{p}^2 = p + p = 2p$. (Here we have used the fact that since p is not a square, $\sqrt{p}$ is not an integer, and as such, $[\sqrt{p}] < \sqrt{p}$.) Hence, $x^2 + y^2$ is a positive integer smaller than $2p$ and divisible by p. This means $x^2 + y^2 = p$.

Step 4. So we are reduced to proving the following statement which is known as Thue's Lemma: Suppose a satisfies $a \not\equiv 0 \bmod p$. Then there are integers $x, y \in \{1, \ldots, [\sqrt{p}]\}$ such that $y \equiv \pm ax \bmod p$. We prove this fact using the Pigeon-Hole Principle, Theorem A.7. Look at the following set:

$$A = \{ax - y \mid 0 \leq x, y \leq [\sqrt{p}]\}.$$

The number of choices for the pairs (x, y) is $(1 + [\sqrt{p}])^2 > p$. By Theorem A.7, there are distinct pairs (x, y) and (x', y') such that $ax - y \equiv ax' - y' \bmod p$, or $y - y' \equiv a(x - x') \bmod p$. Note that $-[\sqrt{p}] \leq y - y', x - x' \leq [\sqrt{p}]$. By multiplying with appropriate signs we may assume that $y - y' \geq 0$ and $x - x' \geq 0$. The price to pay is an ambiguity of sign which we write as $y - y' \equiv \pm a(x - x') \bmod p$. Since the pairs (x, y) and (x', y') are distinct, at least one of the quantities $y - y'$ or $x - x'$ is non-zero, but whichever is non-zero, it will also be non-zero modulo p, and the relation $y - y' \equiv \pm a(x - x') \bmod p$ implies that the other one is non-zero modulo p as well, and consequently, non-zero. So if we let $X = x - x'$ and $Y = y - y'$, we see that X, Y are non-zero, $0 \leq X, Y \leq [\sqrt{p}]$ and $Y \equiv \pm aX \bmod p$. This finishes the proof of Thue's Lemma, and hence the proof of the theorem. □

Corollary 5.8. *The equation $x^2 \equiv -1 \bmod p$ has a solution modulo p if and only if p is not of the form $4k + 3$.*

Now we can prove Theorem 5.2:

Proof of Theorem 5.2. It is clear that a number whose square-free part is a sum of two squares is a sum of two squares. By Ingredient 3, every prime of the form $4k + 1$ is a sum of two squares, and also $2 = 1^2 + 1^2$. By Ingredient 1, any product of such is a sum of two squares. This proves one direction of the theorem.

For the other direction, suppose n is a sum of two squares $a^2 + b^2$, and $p^\alpha \| n$. We just need to show that if p is of the form $4k+3$, then α is even. Write $n = p^\alpha m$ with m coprime to p. By ingredient 2, $p \mid a$ and $p \mid b$, hence we can write $a = pc$ and $b = pd$. Then

$$p^\alpha m = (pc)^2 + (pd)^2 = p^2(c^2 + d^2),$$

so

$$p^{\alpha-2} m = c^2 + d^2.$$

If α is odd, by repeating this process we reach

$$pm = r^2 + s^2$$

for natural numbers r, s. Ingredient 2 again implies $p \mid r$, $p \mid s$, and consequently $p^2 \mid pm$. This last statement means $p \mid m$. This is a contradiction. □

5.4 Irreducible elements in $\mathbb{Z}[i]$

We now determine the collection of irreducible elements in $\mathbb{Z}[i]$. To start, we note that if $N(\varpi)$ is a prime number in $\mathbb{Z}$, then ϖ is irreducible. For example, since $N(1+i) = 2$, $1+i$ is irreducible. More interestingly, if p is a rational prime such that $p \equiv 1 \bmod 4$, then by Theorem 5.7, $p = a^2 + b^2$ with $a, b \in \mathbb{Z}$. This implies $N(a+ib) = p$. Consequently, $a+ib$ is irreducible in $\mathbb{Z}[i]$. We now examine primes of the form $4k+3$. Suppose p is one such prime and that we can write

$$p = z \cdot w$$

for $z, w \in \mathbb{Z}[i]$. Then by taking norms we get

$$p^2 = N(z)N(w). \tag{5.1}$$

This implies $p \mid N(z)N(w)$. Hence, p must divide either $N(z)$ or $N(w)$. Suppose $z = \alpha + i\beta$ and $p \mid N(z) = \alpha^2 + \beta^2$. By Lemma 5.6, $p \mid \alpha$ and $p \mid \beta$. Consequently, $p^2 \mid \alpha^2 + \beta^2$. Equation (5.1) then implies $N(z) = p^2$ and $N(w) = 1$. This means w is a unit. This discussion provides support for the following theorem:

Theorem 5.9. *The elements $1 \pm i$, $a+ib$ with a^2+b^2 a prime congruent to 1 modulo 4, and primes of the form $4k+3$, and their associates are all the irreducible elements in $\mathbb{Z}[i]$.*

Proof. If ϖ is an irreducible element in $\mathbb{Z}[i]$, $\varpi \mid \varpi\overline{\varpi} = N(\varpi) \in \mathbb{Z}$. Write the prime factorization of $N(\varpi)$ as $p_1 p_2 \dots p_k$, with p_j's not necessarily distinct. Now back in $\mathbb{Z}[i]$, $\varpi \mid p_1 p_2 \dots p_k$. Since ϖ is irreducible, and $\mathbb{Z}[i]$ is a Euclidean domain, it has to be prime, so there is at least one j such that $\varpi \mid p_j$. This means ϖ must occur as a factor of some rational prime p. If $p \equiv 1 \bmod 4$ or $p = 2$, then $p = a^2 + b^2$ for integers a, b, and as we observed in the paragraph preceding the

statement of the theorem, $a+ib$ and $a-ib$ are irreducible elements in $\mathbb{Z}[i]$. Since $\varpi \mid p = (a+ib)(a-ib)$, we conclude that either $\varpi \mid a+ib$ or $\varpi \mid a-ib$. If $\varpi \mid a+ib$, since both of these are irreducible, they have to be associates, and similarly for $a-ib$. On the other hand, if $p \equiv 3 \bmod 4$ we proceed as follows. Write $\varpi = m+in$. Since $\varpi \mid p$, then $N(\varpi) \mid N(p) = p^2$. This means $m^2+n^2 \mid p^2$, from which it follows that $m^2+n^2 = 1$, or $m^2+n^2 = p$, or $m^2+n^2 = p^2$. The case $m^2+n^2 = 1$ is not possible as that would imply that ϖ is a unit. If $m^2+n^2 = p$, then Lemma 5.6 shows that $p \mid m$, $p \mid n$, from which it follows $p^2 \mid m^2+n^2$, a contradiction. So the only possibility is $m^2+n^2 = p^2$. Again Lemma 5.6 shows that $m = pm_1$ and $n = pn_1$ for $m_1, n_1 \in \mathbb{Z}$. Hence $p^2 = m^2+n^2 = (pm_1)^2+(pn_1)^2 = p^2(m_1^2+n_1^2)$. As a result $m_1^2+n_1^2 = 1$, implying that m_1+in_1 is a unit in $\mathbb{Z}[i]$. Consequently, $\varpi = m+in = pm_1+ipn_1 = p(m_1+in_1)$, showing that ϖ is an associate of p. □

If p is a prime number of the form $4k+1$, there is a unique representation of the form $p = a^2+b^2$ with $a > b > 0$. We set

$$\varpi_p = a+ib.$$

We call the irreducibles $1+i$, ϖ_p and $\overline{\varpi}_p$ for primes of the form $4k+1$, and primes q of the form $4k+3$, *standard*. Every other irreducible is an associate of a standard irreducible.

The following theorem follows from general properties of unique factorization domains [25, Ch. 3, §7]:

Theorem 5.10. *Every Gaussian integer can be written as*

$$um(1+i)^a \prod_{p \equiv 1 \bmod 4} \varpi_p^{e_p} \overline{\varpi}_p^{f_p}$$

in an essentially unique fashion, i.e., unique up to a permutation of the factors. Here u is one of the four units in $\mathbb{Z}[i]$; m a rational integer which is a product of primes of the form $4k+3$; and all but finitely many of the nonnegative integers e_p, f_p are zero, meaning the product is finite.

For example, the number 2 considered as an element of $\mathbb{Z}[i]$ has the prime factorization $-i(1+i)^2$, and

$$12 = -3 \cdot (1+i)^4, \quad 60 = -3 \cdot (1+i)^4 \cdot (2+i) \cdot (2-i).$$

5.5 Proof of Theorem 5.1

Now we can prove the main theorem of this chapter, Theorem 5.1. By Theorem 3.4 the hypotenuse of a primitive right triangle is an odd number which is the sum of

two squares that are coprime to each other. Using Ingredient 2 above we see that no prime factor of such a number can be of the form $4k + 3$. Next we show that every number all of whose prime factors are of the form $4k + 1$ is the hypotenuse of some primitive right triangle.

We proceed in two steps:

Step 1. Suppose $(m, n) = 1$, and assume $m = a^2 + b^2$ and $n = c^2 + d^2$ with $(a, b) = 1$ and $(c, d) = 1$. Then $mn = (ac - bd)^2 + (ad + bc)^2$ with $(ac - bd, ad + bc) = 1$.

We have

$$mn = (ac - bd)^2 + (ad + bc)^2.$$

We claim that $\gcd(ac - bd, ad + bc) = 1$. Suppose for a prime p, $p \mid ac - bd$ and $p \mid ad + bc$. Then

$$p \mid c(ac - bd) + d(ad + bc) = a(c^2 + d^2) = an,$$

and

$$p \mid -d(ac - bd) + c(ad + bc) = b(c^2 + d^2) = bn.$$

Similarly, $p \mid cm$ and $p \mid dm$. Since $\gcd(m, n) = 1$, p cannot divide both m and n, so suppose p does not divide m. Then since $p \mid cm$, $p \mid c$ and similarly $p \mid d$. This contradicts the assumption that $\gcd(c, d) = 1$. The case $p \nmid n$ is similar.

Step 2. Let p be a prime of the form $4k + 1$. Then if $t \in \mathbb{N}$, p^t is the sum of two squares that are coprime to each other.

Note that this is not obvious. It is of course clear that if we write $p = u^2 + v^2$, then $(u, v) = 1$, because if $(u, v) = \delta$, then $\delta^2 \mid p$ which is impossible, unless $\delta = 1$. Next, assuming $p = u^2 + v^2$, we get $p^3 = (pu)^2 + (pv)^2$, so for $t > 1$, there are certainly expressions $p^t = a^2 + b^2$ such that a, b are *not* coprime. The content of this step is that it is possible to find an expression $p^t = a^2 + b^2$ such that a, b *are* coprime, but not that every such expression has the property that $(a, b) = 1$.

Write $p = u^2 + v^2 = N(u + iv)$. Then

$$p^t = N(u + iv)^t = N((u + iv)^t) = N(u_t + iv_t) = u_t^2 + v_t^2,$$

where u_t and v_t are defined to be the real and imaginary parts of $(u+iv)^t$, respectively. We claim $\gcd(u_t, v_t) = 1$. Suppose not, and let q be a prime factor of $\gcd(u_t, v_t)$. Then $q \mid u_t^2 + v_t^2 = p^t$. This implies that $q = p$, meaning every prime factor of $\gcd(u_t, v_t)$ is equal to p, i.e., $\gcd(u_t, v_t) = p^r$ for some r. We wish to show $r = 0$. We do this by induction on t. We already know the statement to be true for $t = 1$. Suppose for some t,

$$\gcd(u_{t-1}, v_{t-1}) = 1.$$

Then we have

$$u_t + iv_t = (u+iv)^t = (u+iv)(u+iv)^{t-1} = (u+iv)(u_{t-1} + iv_{t-1})$$
$$= (uu_{t-1} - vv_{t-1}) + i(uv_{t-1} + vu_{t-1}).$$

As in the first step we conclude $p^r \mid u_{t-1}(u^2+v^2) = pu_{t-1}$ and $p^r \mid pv_{t-1}$, but since by assumption $\gcd(u_{t-1}, v_{t-1}) = 1$, we conclude that $r \leq 1$. If $r = 0$, we are done. So assume $r = 1$. This means $p \mid u_t$, which, if we use $u_t = uu_{t-1} - vv_{t-1}$, gives

$$uu_{t-1} \equiv vv_{t-1} \mod p. \tag{5.2}$$

Now we write u_{t-1} and v_{t-1} in terms of u, v, u_{t-2}, v_{t-2}:

$$u_{t-1} = uu_{t-2} - vv_{t-2}, \quad v_{t-1} = vu_{t-2} + uv_{t-2}.$$

Using these identities Equation (5.2) reads

$$u(uu_{t-2} - vv_{t-2}) \equiv v(vu_{t-2} + uv_{t-2}) \mod p.$$

Rearranging terms gives

$$(u^2 - v^2)u_{t-2} \equiv 2uvv_{t-2} \mod p.$$

Since $u^2 + v^2 = p$, $-v^2 \equiv u^2 \bmod p$, and we obtain

$$2u^2u_{t-2} \equiv 2uvv_{t-2} \mod p.$$

Canceling out $2u$ gives

$$uu_{t-2} \equiv vv_{t-2} \mod p.$$

As a result, $p \mid uu_{t-2} - vv_{t-2} = u_{t-1}$. Since $v_{t-1}^2 = p^{t-1} - u_{t-1}^2$, and $t \geq 2$, we conclude $p \mid v_{t-1}^2$, and consequently, $p \mid v_{t-1}$. As a result, $p \mid u_{t-1}$, $p \mid v_{t-1}$, and this contradicts $\gcd(u_{t-1}, v_{t-1}) = 1$. □

Exercises

5.1 Write the following numbers as a product of irreducibles of $\mathbb{Z}[i]$:

a. 56;
b. $4 + 6i$;
c. $3 + 5i$;
d. $9 + i$;
e. $7 + 24i$.

5.2 Compute $\gcd(6 - 17i, 18 + i)$.
5.3 Solve the equation $x + y + z = xyz = 1$ in Gaussian integers.

5.4 Determine all irreducible elements with norm less than 100.
5.5 Devise a test to decide whether $x + iy$ is the square of a Gaussian integer.
5.6 Determine all Gaussian integers which are the sum of two squares of Gaussian integers.
5.7 Show that a Gaussian integer $x + iy$ is a sum of the squares of three Gaussian integers if and only if y is even.
5.8 What can you say about right triangles with integral sides such that the legs differ by 1? What if the difference is a fixed number d?
5.9 What can you say about right triangles with integral sides such that the sum of the legs is a fixed number s?
5.10 What can you say about a right triangle with integral sides such that the perimeter and the hypotenuse are squares?
5.11 Write 45305 as a sum of two squares.
5.12 For a natural number n, show that if the equation $n = x^2 + y^2, x, y > 0, 2 \mid x$, has more than one solution, then n is not prime.
5.13 Find a formula for the number of primitive right triangles with a leg equal to a number n in terms of the divisors of n.
5.14 Prove the following result of Gauss [16, page 172]: Every hypotenuse composed of k distinct primes belongs to

$$\left[\frac{k}{1}\right] + 2\left[\frac{k}{2}\right] + 2^2\left[\frac{k}{3}\right] + \cdots + 2^{k-1}\left[\frac{k}{k}\right]$$

different right triangles. Of these triangles, 2^{k-1} are primitive.
5.15 (✠) Determine if 31897485916040 is a sum of two squares. If it is, determine in how many ways.

Notes

Primes of special forms

The problem of deciding which polynomials produce prime numbers goes back centuries. Euler made the famously wrong claim that the polynomial $f(x) = x^2 - x + 41$ has the property that $f(n)$ is a prime number for every integer n. The values $f(0), f(1), f(2), f(3), \ldots, f(40)$ are all prime, though $f(41)$ is clearly not. We will see in Exercise 6.2 that there are no non-constant polynomials $f(x)$ such that $f(n)$ is a prime number for every integral value of n. Despite this rather disappointing statement, one could still ask whether there are polynomials that produce infinitely many primes. The answer is a definite yes. For example, every odd prime is either congruent to 1 modulo 4 or congruent to 3 modulo 4. This means that at least one of the polynomials $4x + 1$ or $4x + 3$ produces infinitely many primes. We will see in Chapter 6 that in fact both of these polynomials capture infinitely many primes.

For a general polynomial of degree 1, one can effectively decide whether the polynomial produces infinitely many primes. Suppose $f(x) = ax + b$ with $a, b \in \mathbb{Z}$. If $\gcd(a, b) = d > 1$, then the polynomial has no chance of producing infinitely many primes. It turns out that this is the only obstruction. The following is a celebrated theorem of Dirichlet [2, Theorem 7.3]:

Theorem 5.11. *If a, b are integers with $b > 0$, and $\gcd(a, b) = 1$, then the arithmetic progression*

$$a, a + b, a + 2b, a + 3b, a + 4b, \ldots$$

contains infinitely many prime numbers.

Unfortunately, we do not know an algebraic/elementary proof of this fact. The standard proofs of Dirichlet's Theorem use complex analysis and, though not terribly hard, are beyond the scope of this small volume. We give several examples of this theorem in Chapter 6. We also present the proof of an important special case in Exercise 6.22.

For polynomials of degree larger than 1 the situation is considerably more complicated. For example, in 1912, Landau conjectured that the polynomial $f(x) = x^2 + 1$ produces infinitely many primes. At the time of this writing it is still not known if Landau's Conjecture is true. The best result in this direction is due to Henryk Iwaniec who in 1978 proved that there are infinitely many integers n such that $n^2 + 1$ is the product of at most two prime numbers.

If we consider quadratic polynomials in more than one variable, then the situation is better understood. Theorem 5.7 gives a linear necessary and sufficient condition for the representability of a prime by a quadratic expression—namely, that an odd prime p is representable by the quadratic form $x^2 + y^2$ if and only if p is of the form $4k + 1$, implying that there are infinitely many primes of the form $x^2 + y^2$. There are other results of similar nature for representability of prime numbers by polynomials of the form $x^2 + ny^2$ dating back to, at least, Fermat and Euler. For example, a prime is of the form $x^2 + 2y^2$ for integers x, y if and only if $p \equiv 1, 3 \bmod 8$. See Cox [14] for an in-depth study of primes that are representable by quadratic forms in two variables.

Algebraic number theory

We understand the phrase *algebraic number theory* in two different, but related, ways. The first one is *algebraic number/theory*, as in number theory done using algebraic methods, and the second one is *algebraic/number theory* as in the theory of algebraic numbers. In terms of the first interpretation, Chinese Remainder Theorem 2.24 is really a statement about ideals in a general ring; Euler's Theorem 2.31 is a special case of Lagrange's theorem in finite group theory; Lemma 2.49 is a consequence of the statement that every finite subgroup of a field is cyclic. What we did in this

chapter with Gaussian integers is part of the second interpretation, and as we saw in this chapter we used our results on Gaussian integers to prove a statement about ordinary integers. Another example is our results from Appendix B which we will use in our proof of the Law of Quadratic Reciprocity in Chapter 7.

An important result in this chapter is Theorem 5.10 which establishes unique factorization in Gaussian integers. Unfortunately, this uniqueness of factorization fails in general number rings. A famous example is the ring $\mathbb{Z}[\sqrt{-5}] = \{x + y\sqrt{-5} \mid x, y \in \mathbb{Z}\}$. We have $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$, and it is not hard to see that $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ are all irreducible elements. It was Richard Dedekind who discovered that the fix for the failure of unique factorization in this and other number rings was to utilize *ideals*. Let us briefly explain Dedekind's ideas in a slightly more modern language than was available to him. We will use the notion of an *algebraic integer* defined in Appendix B. We define a *number field* to be a field K obtained by adjoining a finite number of algebraic integers to $\mathbb{Q}$. Define *the ring of integers* $\mathcal{O}_K$ of K to be set of all algebraic integers contained in K. Theorem B.4 shows that $\mathcal{O}_K$ is a ring. Dedekind showed that every ideal of $\mathcal{O}_K$ is a product of prime ideals of $\mathcal{O}_K$ in an essentially unique fashion. Since every ideal of $\mathbb{Z}$ and $\mathbb{Z}[i]$ is principal, Dedekind's result implies the unique factorization theorems of these rings.

Algebraic number theory was brought to new heights in the hands of David Hilbert and Emil Artin who early in 20th century found spectacular generalizations of the Law of Quadratic Reciprocity, known as *Reciprocity Laws*. These laws were further generalized by Shimura and Taniyama, who also discovered new connections to the theory of elliptic curves and modular forms. The most general reciprocity laws were conjectured by Robert Langlands in the 60s and 70s. Even though these conjectures remain largely open, they have inspired much progress in the last few decades.

For an elementary introduction to algebraic number theory, see [50]. Samuel [43] is a timeless classic. Murty and Esmonde's book [37] is a much recommended problem-solving-based approach to algebraic number theory. More advanced readers already familiar with basic algebraic number theory, abstract algebra, and measure theory are encouraged to read Weil's *Basic Number Theory* [56]. This book is far from basic, but in the words of Norbert Schappacher, if you learn number theory from this book, you will never forget it. Mazur [86] is an excellent expository article explaining the connections between modular forms and Diophantine equations. The book [17] is an account of the history of class field theory. Gelbart [75] is a not-so-elementary introduction to the Langlands program.