THE GAUSSIAN INTEGERS

KEITH CONRAD

Since the work of Gauss, number theorists have been interested in analogues of $\mathbf{Z}$ where concepts from arithmetic can also be developed. The example we will look at here is the Gaussian integers, introduced by Gauss in 1832 [1]:

$$\mathbf{Z}[i] = \{a + bi : a, b \in \mathbf{Z}\}.$$

Excluding the last two sections, the topics we will study are extensions of common properties of the integers. Here is what we will cover in each section:

(1) the norm on $\mathbf{Z}[i]$
(2) divisibility in $\mathbf{Z}[i]$
(3) the division theorem in $\mathbf{Z}[i]$
(4) the Euclidean algorithm $\mathbf{Z}[i]$
(5) Bezout's theorem in $\mathbf{Z}[i]$
(6) unique factorization in $\mathbf{Z}[i]$
(7) modular arithmetic in $\mathbf{Z}[i]$
(8) applications of $\mathbf{Z}[i]$ to the arithmetic of $\mathbf{Z}$
(9) primes in $\mathbf{Z}[i]$

1. The Norm

In $\mathbf{Z}$, size is measured by the absolute value. In $\mathbf{Z}[i]$, we use the norm.

Definition 1.1. For $\alpha = a + bi \in \mathbf{Z}[i]$, its *norm* is the product

$$\mathrm{N}(\alpha) = \alpha\overline{\alpha} = (a + bi)(a - bi) = a^2 + b^2.$$

For example, $\mathrm{N}(2 + 7i) = 2^2 + 7^2 = 53$. For $m \in \mathbf{Z}$, $\mathrm{N}(m) = m^2$. In particular, $\mathrm{N}(1) = 1$. Thinking about $a + bi$ as a complex number, its norm is the square of its usual absolute value:

$$|a + bi| = \sqrt{a^2 + b^2}, \quad \mathrm{N}(a + bi) = a^2 + b^2 = |a + bi|^2.$$

The reason we prefer to deal with norms on $\mathbf{Z}[i]$ instead of absolute values on $\mathbf{Z}[i]$ is that norms are integers (rather than square roots), and the divisibility properties of norms in $\mathbf{Z}$ will provide important information about divisibility properties in $\mathbf{Z}[i]$. This is based on the following algebraic property of the norm.

Theorem 1.2. *The norm is multiplicative: for α and β in $\mathbf{Z}[i]$, $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$.*

Proof. Write $\alpha = a + bi$ and $\beta = c + di$. Then $\alpha\beta = (ac - bd) + (ad + bc)i$. We now compute $\mathrm{N}(\alpha)\,\mathrm{N}(\beta)$ and $\mathrm{N}(\alpha\beta)$:

$$\mathrm{N}(\alpha)\,\mathrm{N}(\beta) = (a^2 + b^2)(c^2 + d^2) = (ac)^2 + (ad)^2 + (bc)^2 + (bd)^2$$

and

$$\begin{aligned} \mathrm{N}(\alpha\beta) &= (ac-bd)^2 + (ad+bc)^2 \\ &= (ac)^2 - 2abcd + (bd)^2 + (ad)^2 + 2abcd + (bc)^2 \\ &= (ac)^2 + (bd)^2 + (ad)^2 + (bc)^2. \end{aligned}$$

The two results agree, so $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$. □

Remark 1.3. The calculations above work when the integer coefficients are rational or even real. If for a complex number $z = x + yi$ with $x, y \in \mathbf{R}$ we define $\mathrm{N}(z) = x^2 + y^2$ then $\mathrm{N}(zw) = \mathrm{N}(z)\,\mathrm{N}(w)$ for all z and w in $\mathbf{C}$. This will be used in the proof of Theorem 3.1.

As a first application of Theorem 1.2, we determine the Gaussian integers with a multiplicative inverse in $\mathbf{Z}[i]$. The idea is to apply norms to reduce the question to invertibility in $\mathbf{Z}$.

Corollary 1.4. *The only Gaussian integers which are invertible in* $\mathbf{Z}[i]$ *are* ± 1 *and* $\pm i$.

Proof. It is easy to see ± 1 and $\pm i$ have inverses in $\mathbf{Z}[i]$: 1 and -1 are their own inverse and i and $-i$ are inverses of each other.

For the converse direction, suppose $\alpha \in \mathbf{Z}[i]$ is invertible, say $\alpha\beta = 1$ for some $\beta \in \mathbf{Z}[i]$. We want to show $\alpha \in \{\pm 1, \pm i\}$. Taking the norm of both sides of the equation $\alpha\beta = 1$, we find $\mathrm{N}(\alpha)\,\mathrm{N}(\beta) = 1$. This is an equation in $\mathbf{Z}$, so we know $\mathrm{N}(\alpha) = \pm 1$. Since the norm doesn't take negative values, $\mathrm{N}(\alpha) = 1$. Writing $\alpha = a + bi$, we have $a^2 + b^2 = 1$, and the integral solutions to this give us the four values $\alpha = \pm 1, \pm i$. □

Invertible elements are called *units*. The units of $\mathbf{Z}$ are ± 1. The units of $\mathbf{Z}[i]$ are ± 1 and $\pm i$. Knowing a Gaussian integer up to multiplication by a unit is analogous to knowing an integer up to its sign.

While there is no such thing as inequalities on Gaussian integers, we can talk about inequalities on their norms. In particular, induction on the norm (not on the Gaussian integer itself) is a technique to bear in mind if you want to prove something by induction in $\mathbf{Z}[i]$. We will use induction on the norm to prove unique factorization (Theorems 6.4 and 6.6).

The norm of every Gaussian integer is a non-negative integer, but it is not true that every non-negative integer is a norm. Indeed, the norms are the integers of the form $a^2 + b^2$, and not every positive integer is a sum of two squares. Examples include 3, 7, 11, 15, 19, and 21. No Gaussian integer has norm equal to these values.

2. Divisibility

Divisibility in $\mathbf{Z}[i]$ is defined in the natural way: we say β *divides* α (and write $\beta \mid \alpha$) if $\alpha = \beta\gamma$ for some $\gamma \in \mathbf{Z}[i]$. In this case, we call β a *divisor* or a *factor* of α.

Example 2.1. Since $14 - 3i = (4 + 5i)(1 - 2i)$, $4 + 5i$ divides $14 - 3i$.

Example 2.2. Does $(4 + 5i) \mid (14 + 3i)$? We can do the division by taking a ratio and rationalizing the denominator:

$$\frac{14+3i}{4+5i} = \frac{(14+3i)(4-5i)}{(4+5i)(4-5i)} = \frac{71-58i}{41} = \frac{71}{41} - \frac{58}{41}i.$$

This is not in $\mathbf{Z}[i]$: the real and imaginary parts are $71/41$ and $-58/41$, which are not integers. Therefore $4 + 5i$ does not divide $14 + 3i$ in $\mathbf{Z}[i]$.

Theorem 2.3. *A Gaussian integer $\alpha = a + bi$ is divisible by an ordinary integer c if and only if $c \mid a$ and $c \mid b$ in $\mathbf{Z}$.*

Proof. To say $c \mid (a + bi)$ in $\mathbf{Z}[i]$ is the same as $a + bi = c(m + ni)$ for some $m, n \in \mathbf{Z}$, and that is equivalent to $a = cm$ and $b = cn$, or $c \mid a$ and $c \mid b$. □

Taking $b = 0$ in Theorem 2.3 tells us divisibility between ordinary integers does not change when working in $\mathbf{Z}[i]$: for $a, c \in \mathbf{Z}$, $c \mid a$ in $\mathbf{Z}[i]$ if and only if $c \mid a$ in $\mathbf{Z}$. However, this does *not* mean other aspects in $\mathbf{Z}$ stay the same. For instance, we will see later that some primes in $\mathbf{Z}$ factor in $\mathbf{Z}[i]$.

The multiplicativity of the norm turns divisibility relations in $\mathbf{Z}[i]$ into divisibility relations in the more familiar setting of $\mathbf{Z}$, as follows.

Theorem 2.4. *For α, β in $\mathbf{Z}[i]$, if $\beta \mid \alpha$ in $\mathbf{Z}[i]$ then $\mathrm{N}(\beta) \mid \mathrm{N}(\alpha)$ in $\mathbf{Z}$.*

Proof. Write $\alpha = \beta\gamma$ for $\gamma \in \mathbf{Z}[i]$. Taking the norm of both sides, we have $\mathrm{N}(\alpha) = \mathrm{N}(\beta)\,\mathrm{N}(\gamma)$. This equation is in $\mathbf{Z}$, so it shows $\mathrm{N}(\beta) \mid \mathrm{N}(\alpha)$ in $\mathbf{Z}$. □

Corollary 2.5. *A Gaussian integer has even norm if and only if it is a multiple of $1 + i$.*

Proof. Since $\mathrm{N}(1 + i) = 2$, any multiple of $1 + i$ has even norm. Conversely, suppose $m + ni$ has even norm. Then $m^2 + n^2 \equiv 0 \bmod 2$. By taking cases, we see this means m and n are both even or both odd. In short, $m \equiv n \bmod 2$.

We want to write $m + ni = (1 + i)(u + vi)$ for some $u, v \in \mathbf{Z}$. This is the same as

$$m + ni = (u - v) + (u + v)i.$$

The solution here is $u = (n+m)/2$ and $v = (n-m)/2$. These are integers since $m \equiv n \bmod 2$. Thus $(1 + i) \mid (m + ni)$. □

Example 2.6. The norm of $1 + 3i$ is 10, and $1 + 3i = (1 + i)(2 + i)$.

Example 2.7. Since $1 - i$ has norm 2, it must be a multiple of $1 + i$. Indeed, $1 - i = (-i)(1 + i)$.

Theorem 2.4 is useful as a quick way of showing one Gaussian integer does *not* divide another: check the corresponding norm divisibility is not true in $\mathbf{Z}$. For example, if $(3+7i) \mid (10 + 3i)$ in $\mathbf{Z}[i]$, then (taking norms), $58 \mid 109$ in $\mathbf{Z}$, but that isn't true. Therefore $3 + 7i$ does not divide $10 + 3i$ in $\mathbf{Z}[i]$. Turning a divisibility problem in $\mathbf{Z}[i]$ into one in $\mathbf{Z}$ has an obvious appeal, since we are more comfortable with divisibility in $\mathbf{Z}$.

However, Theorem 2.4 only says norm-divisibility in $\mathbf{Z}$ follows from divisibility in $\mathbf{Z}[i]$. The converse is usually *false*. Consider $\alpha = 14 + 3i$ and $\beta = 4 + 5i$. While $\mathrm{N}(\beta) = 41$ and $\mathrm{N}(\alpha) = 205 = 41 \cdot 5$, so $\mathrm{N}(\beta) \mid \mathrm{N}(\alpha)$ in $\mathbf{Z}$, we saw in Example 2.2 that $4 + 5i$ does not divide $14 + 3i$.

The foolproof method of verifying divisibility in $\mathbf{Z}[i]$ is testing if the ratio is in $\mathbf{Z}[i]$ after rationalizing the denominator, as we did in Example 2.2. The norm-divisibility check in $\mathbf{Z}$ is a necessary condition for divisibility in $\mathbf{Z}[i]$ (when it fails, so does divisibility in $\mathbf{Z}[i]$), but it is not sufficient.

In $\mathbf{Z}$, if $|m| = |n|$ then $m = \pm n$, so m and n are unit multiples of each other. The corresponding statement in $\mathbf{Z}[i]$ is *false*: if $\mathrm{N}(\alpha) = \mathrm{N}(\beta)$ it is not generally true that α and β are unit multiples of each other. Consider $4 + 5i$ and $4 - 5i$. Both have norm 41, but the unit multiples of $4 + 5i$ are

$$4 + 5i, \quad -4 - 5i, \quad -5 + 4i, \quad 5 - 4i.$$

The number $4-5i$ is not on this list, so $4+5i$ and $4-5i$ are not unit multiples. We will see later (Example 4.5) that $4+5i$ and $4-5i$ are even relatively prime in $\mathbf{Z}[i]$. In short, taking the norm in $\mathbf{Z}[i]$ is a more drastic step than removing a sign on an integer.

3. The Division Theorem

One reason we will be able to transfer a lot of results from $\mathbf{Z}$ to $\mathbf{Z}[i]$ is the following analogue of division-with-remainder in $\mathbf{Z}$.

Theorem 3.1 (Division Theorem)**.** *For $\alpha, \beta \in \mathbf{Z}[i]$ with $\beta \neq 0$, there are $\gamma, \rho \in \mathbf{Z}[i]$ such that $\alpha = \beta\gamma + \rho$ and $\mathrm{N}(\rho) < \mathrm{N}(\beta)$. In fact, we can choose ρ so $\mathrm{N}(\rho) \leq (1/2)\,\mathrm{N}(\beta)$.*

The numbers γ and ρ are the quotient and remainder, and the remainder is bounded in size (according to its norm) by the size of the divisor β.

Before we prove Theorem 3.1 we note there is a subtlety in trying to calculate γ and ρ. This is best understood by working through an example.

Example 3.2. Let $\alpha = 27 - 23i$ and $\beta = 8 + i$. The norm of β is 65. We want to write $\alpha = \beta\gamma + \rho$ where $\mathrm{N}(\rho) < 65$. The idea is to consider the ratio α/β and rationalize the denominator:

$$\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{\beta\overline{\beta}} = \frac{(27-23i)(8-i)}{65} = \frac{193-211i}{65}. \tag{3.1}$$

Since $193/65 = 2.969\ldots$ and $-211/65 = -3.246\ldots$, we replace each fraction with its greatest integer and try $\gamma = 2 - 4i$. However,

$$\alpha - \beta(2-4i) = 7 + 7i,$$

and using $\rho = 7+7i$ is a bad idea: $\mathrm{N}(7+7i) = 98$ is larger than $\mathrm{N}(\beta) = 65$. The *usefulness* of a division theorem is the smaller remainder. Therefore our choice of γ and ρ is not desirable. This is the subtlety referred to before we started our example.

To correct our approach, we have to think more carefully about the way we replace $193/65 = 2.969\ldots$ and $-211/65 = -3.246\ldots$ with nearby integers. Notice that $193/65$ and $-211/65$ are each closer to the integer to their right rather than to their left. That is, $193/65$ is closer to 3 than to 2, and $-211/65$ is closer to -3 than to -4. Let's use the closest integer rather than the greatest integer: try $\gamma = 3 - 3i$. Then

$$\alpha - \beta(3-3i) = -2i,$$

and $-2i$ has norm less than $\mathrm{N}(\beta) = 65$. So we use $\gamma = 3 - 3i$ and $\rho = -2i$.

Choosing the nearest integer rather than the greatest integer could also be done in $\mathbf{Z}$. For instance, $34/9 = 3.77\ldots$ is closer to 4 than to 3. In terms of a division-with-remainder equation, this corresponds to preferring

$$34 = 9 \cdot 4 - 2$$

over

$$34 = 9 \cdot 3 + 7.$$

The remainder in the first equation is negative, but it is smaller in absolute value.

What we have found here is a modified division theorem in $\mathbf{Z}$. Usually, for integers a and b with $b \neq 0$, the division theorem in $\mathbf{Z}$ says: take bq to be the multiple of b which is nearest to a *from the left*: $bq \leq a < b(q+1)$. Then set $r = a - bq$, so $r \geq 0$ (since $bq \leq a$) and $r < |b|$ (since bq and $b(q+1)$ are $|b|$ integers apart and a will be closer to bq than $b(q+1)$

is). In the modified division theorem, take for bq the multiple of b which is closest to a, rather than just closest to a from the left. (Computationally, the q in the modified division theorem is the closest integer to a/b, which may lie to the right of a/b rather than to its left.) An integer is no more than $(1/2)|b|$ away from a multiple of b in either direction, so $|a - bq| \leq (1/2)|b|$. Write $r = a - bq$, so $a = bq + r$ with $|r| \leq (1/2)|b|$. In the usual division theorem, the remainder is nonnegative and bounded above by $|b|$. We have shrunken the upper bound at the cost of possibly making the remainder negative.

Sometimes a might land right in the middle between two multiples of b, in which case the quotient and remainder are not unique, *e.g.*, if $a = 27$ and $b = 6$ then a is right in the middle between $4b$ and $5b$:

$$27 = 6 \cdot 4 + 3, \quad 27 = 6 \cdot 5 - 3.$$

Thus we get two choices of r, either 3 or -3. The usual division theorem in $\mathbf{Z}$ has a unique quotient and remainder, but the modified version gives up on uniqueness. This might seem like a calamity, but it's exactly what we need to prove the division theorem in $\mathbf{Z}[i]$ (Theorem 3.1), which is what we turn to next. The proof is mostly a translation of the correct part of Example 3.2 into general algebraic terms. After the proof we will give further examples.

Proof. (of Theorem 3.1) We have $\alpha, \beta \in \mathbf{Z}[i]$ with $\beta \neq 0$ and we want to construct $\gamma, \rho \in \mathbf{Z}[i]$ such that $\alpha = \beta\gamma + \rho$ where $\mathrm{N}(\rho) \leq (1/2)\,\mathrm{N}(\beta)$.

Write

$$\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{\beta\overline{\beta}} = \frac{\alpha\overline{\beta}}{\mathrm{N}(\beta)} = \frac{m + ni}{\mathrm{N}(\beta)},$$

where we set $\alpha\overline{\beta} = m + ni$. Divide m and n by $\mathrm{N}(\beta)$ using the modified division theorem in $\mathbf{Z}$:

$$m = \mathrm{N}(\beta)q_1 + r_1, \quad n = \mathrm{N}(\beta)q_2 + r_2,$$

where q_1 and q_2 are in $\mathbf{Z}$ and $0 \leq |r_1|, |r_2| \leq (1/2)\,\mathrm{N}(\beta)$. Then

$$\begin{aligned} \frac{\alpha}{\beta} &= \frac{\mathrm{N}(\beta)q_1 + r_1 + (\mathrm{N}(\beta)q_2 + r_2)i}{\mathrm{N}(\beta)} \\ &= q_1 + q_2 i + \frac{r_1 + r_2 i}{\mathrm{N}(\beta)}. \end{aligned}$$

Set $\gamma = q_1 + q_2 i$ (this will be our desired quotient), so after a little algebra the above equation becomes

$$\alpha - \beta\gamma = \frac{r_1 + r_2 i}{\overline{\beta}}. \tag{3.2}$$

We will show $\mathrm{N}(\alpha - \beta\gamma) \leq (1/2)\,\mathrm{N}(\beta)$, so using $\rho = \alpha - \beta\gamma$ will settle the division theorem. Take norms of both sides of (3.2), where on the right side we use the norm on complex numbers and its multiplicativity (Remark 1.3). Letting $z = (r_1 + r_2 i)/\overline{\beta}$, so $z\overline{\beta} = r_1 + r_2 i$, $\mathrm{N}(z)\,\mathrm{N}(\overline{\beta}) = \mathrm{N}(r_1 + r_2 i) = r_1^2 + r_2^2$. Since $\mathrm{N}(\overline{\beta}) = \mathrm{N}(\beta)$,

$$\mathrm{N}(\alpha - \beta\gamma) = \frac{r_1^2 + r_2^2}{\mathrm{N}(\beta)}.$$

Feeding the estimates $0 \leq |r_1|, |r_2| \leq (1/2)\,\mathrm{N}(\beta)$ into the right side,

$$\mathrm{N}(\alpha - \beta\gamma) \leq \frac{(1/4)\,\mathrm{N}(\beta)^2 + (1/4)\,\mathrm{N}(\beta)^2}{\mathrm{N}(\beta)} = \frac{1}{2}\,\mathrm{N}(\beta).$$

□

Example 3.3. Let $\alpha = 11 + 10i$ and $\beta = 4 + i$. Then $\mathrm{N}(\beta) = 17$. We compute

$$\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{\mathrm{N}(\beta)} = \frac{54 + 29i}{17}.$$

Since $54/17 = 3.17\ldots$ and $29/17 = 1.70\ldots$, we use $\gamma = 3+2i$ (why?). Then $\alpha - \beta\gamma = 1 - i$, so we set $\rho = 1 - i$. Note $\mathrm{N}(\rho) = 2 \leq (1/2)\,\mathrm{N}(\beta)$.

Example 3.4. Let $\alpha = 41 + 24i$ and $\beta = 11 - 2i$. Then $\mathrm{N}(\beta) = 125$ and

$$\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{125} = \frac{403 + 346i}{125}$$

Since $403/125 = 3.224\ldots$ and $346/125 = 2.768\ldots$, we use $\gamma = 3 + 3i$ (why?) and find $\alpha - \beta\gamma = 2 - 3i$. Set $\rho = 2 - 3i$ and compare $\mathrm{N}(\rho)$ with $\mathrm{N}(\beta)$.

There is one interesting difference between the division theorem in $\mathbf{Z}[i]$ and the (usual) division theorem in $\mathbf{Z}$: the quotient and remainder are not unique in $\mathbf{Z}[i]$.

Example 3.5. Let $\alpha = 37 + 2i$ and $\beta = 11 + 2i$, so $\mathrm{N}(\beta) = 125$. If you carry out the algorithm for division in $\mathbf{Z}[i]$ as it was developed above, you will be led to

$$\alpha = \beta \cdot 3 + (4 - 4i).$$

However, it is also true that

$$\alpha = \beta(3 - i) + (2 + 7i).$$

The remainder in both cases has norm less than 125 (in fact, less than $125/2$).

Example 3.6. The reader may not be impressed by the previous example, since only the first outcome would actually come out of our division algorithm in $\mathbf{Z}[i]$. We now give an example where the division algorithm itself allows for two different outcomes. Let $\alpha = 1+8i$ and $\beta = 2 - 4i$. Then

$$\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{\mathrm{N}(\beta)} = \frac{-30 + 20i}{20} = -\frac{3}{2} + i.$$

Since $-3/2$ lies right in the middle between -2 and -1, we can use $\gamma = -1+i$ or $\gamma = -2+i$. Using the first choice, we obtain

$$\alpha = \beta(-1 + i) - 1 + 2i.$$

Using the second choice,

$$\alpha = \beta(-2 + i) + 1 - 2i.$$

That division in $\mathbf{Z}[i]$ lacks uniqueness in the quotient and remainder does not seriously limit the usefulness of division. Indeed, back in $\mathbf{Z}$, the uniqueness of the quotient and remainder for the usual division theorem is *irrelevant* for many important applications (such as Euclid's algorithm). All those applications will carry over to $\mathbf{Z}[i]$, with essentially the same proofs.

4. The Euclidean Algorithm

We begin by defining greatest common divisors in $\mathbf{Z}[i]$.

Definition 4.1. For non-zero α and β in $\mathbf{Z}[i]$, a *greatest common divisor* of α and β is a common divisor with maximal norm.

This is analogous to the usual definition of greatest common divisor in $\mathbf{Z}$, *except* the concept is not pinned down as a specific number. If δ is a greatest common divisor of α and β, so are (at least) its unit multiples $-\delta, i\delta$, and $-i\delta$. Perhaps there are other greatest common divisors; we just don't know yet. (We will find out in Corollary 4.7.) We can speak about *a* greatest common divisor, but not *the* greatest common divisor. A similar technicality would occur in $\mathbf{Z}$ if we defined the greatest common divisor as a common divisor with largest absolute value, rather than the largest positive common divisor. There is no analogue of positivity in $\mathbf{Z}[i]$ (at least not in this course), so we are stuck with the concept of greatest common divisor always ambiguous at least by a unit multiple.

Definition 4.2. When α and β only have unit factors in common, we call them *relatively prime*.

Theorem 4.3 (Euclid's algorithm)**.** *Let $\alpha, \beta \in \mathbf{Z}[i]$ be non-zero. Recursively apply the division theorem, starting with this pair, and make the divisor and remainder in one equation the new dividend and divisor in the next, provided the remainder is not zero:*

$$\begin{aligned} \alpha &= \beta\gamma_1 + \rho_1, \quad \mathrm{N}(\rho_1) < \mathrm{N}(\beta) \\ \beta &= \rho_1\gamma_2 + \rho_2, \quad \mathrm{N}(\rho_2) < \mathrm{N}(\rho_1) \\ \rho_1 &= \rho_2\gamma_3 + \rho_3, \quad \mathrm{N}(\rho_3) < \mathrm{N}(\rho_2) \\ &\vdots \end{aligned}$$

The last non-zero remainder is divisible by all common divisors of α and β, and is itself a common divisor, so it is a greatest common divisor of α and β.

Proof. The proof is identical to the usual proof that Euclid's algorithm works in $\mathbf{Z}$. We briefly summarize the argument. Reasoning from the first equation down shows every common divisor of α and β divides the last non-zero remainder. Conversely, reasoning from the final equation up shows the last non-zero remainder (which is in the second-to-last equation) is a common divisor of α and β. Therefore this last non-zero remainder is a common divisor which is divisible by all the others. Thus it must have maximal norm among the common divisors, so it is a greatest common divisor. □

Example 4.4. We compute a greatest common divisor of $\alpha = 32 + 9i$ and $\beta = 4 + 11i$. Details involved in carrying out the division theorem in each step of Euclid's algorithm are omitted. The reader could work them out as more practice with the division theorem. We find

$$\begin{aligned} 32 + 9i &= (4 + 11i)(2 - 2i) + 2 - 5i, \\ 4 + 11i &= (2 - 5i)(-2 + i) + 3 - i, \\ 2 - 5i &= (3 - i)(1 - i) - i, \\ 3 - i &= (-i)(1 + 3i) + 0. \end{aligned}$$

The last non-zero remainder is $-i$, so α and β only have unit factors in common. They are relatively prime. Notice that, unlike in $\mathbf{Z}^+$, when two Gaussian integers are relatively prime we do not necessarily obtain 1 as the last non-zero remainder. Rather, we just obtain *some* unit as the last non-zero remainder.

Example 4.5. We show $4+5i$ and $4-5i$, which are conjugates, are relatively prime in $\mathbf{Z}[i]$:

$$\begin{aligned} 4+5i &= (4-5i)i-(1-i) \\ 4-5i &= -(1-i)(-4)-i \\ -(1-i) &= -i(1+i)+0. \end{aligned}$$

The last non-zero remainder is a unit, so we are done.

Example 4.6. Here's an example where the greatest common divisor is not a unit. Let $\alpha = 11+3i$ and $\beta = 1+8i$. Then

$$\begin{aligned} 11+3i &= (1+8i)(1-i)+2-4i \\ 1+8i &= (2-4i)(-1+i)-1+2i \\ 2-4i &= (-1+2i)(-2)+0, \end{aligned}$$

so a greatest common divisor of α and β is $-1+2i$.

We could proceed in a different way in the second equation (which we already met in Example 3.6), and get a different last non-zero remainder:

$$\begin{aligned} 11+3i &= (1+8i)(1-i)+2-4i \\ 1+8i &= (2-4i)(-2+i)+1-2i \\ 2-4i &= (1-2i)(2)+0. \end{aligned}$$

Therefore $1-2i$ is also a greatest common divisor. Our two different answers are not inconsistent: a greatest common divisor is defined at best only up to a unit multiple anyway, and $-1+2i$ and $1-2i$ are unit multiples of each other: $-1+2i = (-1)(1-2i)$.

If δ is a greatest common divisor of α and β, then $\mathrm{N}(\delta)$ divides $\mathrm{N}(\alpha)$ and $\mathrm{N}(\beta)$, so $\mathrm{N}(\delta)$ divides $(\mathrm{N}(\alpha), \mathrm{N}(\beta))$. However, it can happen that $\mathrm{N}(\delta) < (\mathrm{N}(\alpha), \mathrm{N}(\beta))$. In Example 4.5, α and β are relatively prime and hence their greatest common divisor has norm 1, but $\mathrm{N}(\alpha) = \mathrm{N}(\beta) = 41$. In Example 4.6, $\mathrm{N}(\alpha) = 130$ and $\mathrm{N}(\beta) = 65$, which have greatest common divisor 65, while α and β have a greatest common divisor $-1+2i$, which has norm 5.

Suppose $(\mathrm{N}(\alpha), \mathrm{N}(\beta)) = 1$. Then any common divisor of α and β has norm dividing 1, so its norm must be 1, and thus the common divisor is a unit. We see that Gaussian integers with relatively prime norm have to be relatively prime themselves. (Again, the converse is false, as $4 \pm 5i$ shows.) For instance, returning to Example 4.4, we compute $\mathrm{N}(32+9i) = 1105 = 5 \cdot 13 \cdot 17$ and $\mathrm{N}(4+11i) = 137$ (a prime), which are relatively prime. Since the norms are relatively prime in $\mathbf{Z}$, $32+9i$ and $4+11i$ are relatively prime in $\mathbf{Z}[i]$. We could have avoided Euclid's algorithm in $\mathbf{Z}[i]$ in this case, by using it in $\mathbf{Z}$ (on the norms) first. But in general one needs Euclid's algorithm in $\mathbf{Z}[i]$ in order to compute greatest common divisors in $\mathbf{Z}[i]$.

The following corollary of Euclid's algorithm in $\mathbf{Z}[i]$ shows that a greatest common divisor in $\mathbf{Z}[i]$ is ambiguous only by a unit multiple. That is, the built-in unit ambiguity is the only one that actually occurs.

Corollary 4.7. *For non-zero α and β in $\mathbf{Z}[i]$, let δ be a greatest common divisor produced by Euclid's algorithm. Any greatest common divisor of α and β is a unit multiple of δ.*

Proof. Let δ' be a greatest common divisor of α and β. From the proof of Euclid's algorithm, $\delta' \mid \delta$ (because δ' is a common divisor). Write $\delta = \delta'\gamma$, so

$$\mathrm{N}(\delta) = \mathrm{N}(\delta')\,\mathrm{N}(\gamma) \geq \mathrm{N}(\delta').$$

Since δ' is a greatest common divisor, its norm is maximal among the norms of common divisors, so the inequality $\mathrm{N}(\delta) \geq \mathrm{N}(\delta')$ has to be an equality. That implies $\mathrm{N}(\gamma) = 1$, so $\gamma = \pm 1$ or $\pm i$. Thus δ and δ' are unit multiples of each other. □

5. Bezout's Theorem

In $\mathbf{Z}$, Bezout's theorem says for any non-zero a and b in $\mathbf{Z}$ that $(a, b) = ax + by$ for some x and y in $\mathbf{Z}$ found by back-substitution in Euclid's algorithm. The same idea works in $\mathbf{Z}[i]$ and gives us Bezout's theorem there.

Theorem 5.1 (Bezout's theorem)**.** *Let δ be any greatest common divisor of two non-zero Gaussian integers α and β. Then $\delta = \alpha x + \beta y$ for some $x, y \in \mathbf{Z}[i]$.*

Proof. Being able to write δ as a $\mathbf{Z}[i]$-combination of α and β is unaffected by replacing δ with a unit multiple. (For instance, if we can do this for $i\delta$, then we multiply through by $-i$ to do it for δ.) Thus, by Corollary 4.7, we only need to give a proof for δ a greatest common divisor coming from Euclid's algorithm. For such δ, back-substitution in Euclid's algorithm shows δ is a $\mathbf{Z}[i]$-combination of α and β. Further details here are identical to the integer case, and are left to the reader. □

Corollary 5.2. *The non-zero Gaussian integers α and β are relatively prime if and only if we can write*

$$1 = \alpha x + \beta y$$

for some $x, y \in \mathbf{Z}[i]$.

Proof. If α and β are relatively prime, then 1 is a greatest common divisor of α and β, so $1 = \alpha x + \beta y$ for some $x, y \in \mathbf{Z}[i]$ by Theorem 5.1. Conversely, if $1 = \alpha x + \beta y$ for some $x, y \in \mathbf{Z}[i]$, then any common divisor of α and β is a divisor of 1, and thus is a unit. That says α and β are relatively prime. □

Example 5.3. We saw in Example 4.4 that $\alpha = 32 + 9i$ and $\beta = 4 + 11i$ are relatively prime, since the last non-zero remainder in Euclid's algorithm is $-i$. We can reverse the calculations in Example 4.4 to express $-i$ as a $\mathbf{Z}[i]$-combination of α and β:

$$\begin{aligned} -i &= 2 - 5i - (3 - i)(1 - i) \\ &= 2 - 5i - (\beta - (2 - 5i)(-2 + i))(1 - i) \\ &= (2 - 5i)(1 + (-2 + i)(1 - i)) - \beta(1 - i) \\ &= (2 - 5i)(3i) - \beta(1 - i) \\ &= (\alpha - \beta(2 - 2i))(3i) - \beta(1 - i) \\ &= \alpha(3i) - \beta(7 + 5i). \end{aligned}$$

To write 1, rather than $-i$, as a combination of α and β, multiply by i:

$$1 = \alpha(-3) + \beta(5 - 7i). \tag{5.1}$$

Example 5.4. In Example 4.5, we checked that $4+5i$ and $4-5i$ are relatively prime. Using back-substitution in Example 4.5, we obtain

$$\begin{aligned} -i &= 4-5i-(-(1-i))(-4) \\ &= 4-5i-(4+5i-(4-5i)i)(-4) \\ &= (4+5i)(4)+(4-5i)(1-4i), \end{aligned}$$

and multiplying through by i gives

$$1 = (4+5i)(4i)+(4-5i)(4+i).$$

Example 5.5. In Example 4.6, we saw $-1+2i$ is a greatest common divisor of $\alpha = 11+3i$ and $\beta = 1+8i$. Reversing the steps of Euclid's algorithm,

$$\begin{aligned} -1+2i &= 1+8i-(2-4i)(-1+i) \\ &= 1+8i-(11+3i-(1+8i)(1-i))(-1+i) \\ &= (11+3i)(1-i)+(1+8i)(1+(1-i)(-1+i)) \\ &= (11+3i)(1-i)+(1+8i)(1+2i) \\ &= \alpha(1-i)+\beta(1+2i). \end{aligned}$$

Example 5.6. Let $\alpha = 10+91i$ and $\beta = 7+3i$. By Euclid's algorithm,

$$\begin{aligned} \alpha &= \beta(6+11i)+1-4i, \\ \beta &= (1-4i)(2i)+-1+i, \\ 1-4i &= (-1+i)(-3+i)-1, \\ -1+i &= -1(1-i)+0, \end{aligned}$$

so the last non-zero remainder is -1. That tells us α and β are relatively prime. Using back-substitution,

$$\begin{aligned} -1 &= 1-4i-(-1+i)(-3+i) \\ &= 1-4i-(\beta-(1-4i)(2i))(-3+i) \\ &= (1-4i)(1+(2i)(-3+i))-\beta(-3+i) \\ &= (1-4i)(-1-6i)+\beta(3-i) \\ &= (\alpha-\beta(6+11i))(-1-6i)+\beta(3-i) \\ &= \alpha(-1-6i)+\beta(-(6+11i)(-1-6i)+3-i) \\ &= \alpha(-1-6i)+\beta(-57+46i). \end{aligned}$$

We can negate to write 1 as a $\mathbf{Z}[i]$-combination of α and β:

$$1 = \alpha(1+6i)+\beta(57-46i). \tag{5.2}$$

While the previous example shows $10+91i$ and $7+3i$ do not have a common factor in $\mathbf{Z}[i]$, notice that their norms are

$$\mathrm{N}(10+91i) = 8381 = 17^2 \cdot 29, \quad \mathrm{N}(7+3i) = 58 = 2 \cdot 29,$$

so the norms of $10+91i$ and $7+3i$ have a common factor in $\mathbf{Z}$. We can understand how such phenomena (relatively prime Gaussian integers have non-relatively prime norms) happen by exhibiting the "prime factorizations" of $10+91i$ and $7+3i$ (without explaining how they are found, however):

$$10+91i = (1-4i)(4+i)(5+2i), \quad 7+3i = (1+i)(5-2i). \tag{5.3}$$

Now we see why such examples are possible: the factors $5 + 2i$ and $5 - 2i$ have the same norm (namely 29) but they are relatively prime to each other.

All the usual consequences of Bezout's theorem over $\mathbf{Z}$ have analogues over $\mathbf{Z}[i]$. Here are some of them.

Corollary 5.7. *Let $\alpha \mid \beta\gamma$ in $\mathbf{Z}[i]$ with α and β relatively prime. Then $\alpha \mid \gamma$.*

Proof. It's just like the integer proof, but we write up the details anyway. Set $\beta\gamma = \alpha\kappa$ for some κ in $\mathbf{Z}[i]$. Since α and β are relatively prime, we can solve the equation

$$1 = \alpha x + \beta y$$

for some $x, y \in \mathbf{Z}[i]$. Multiply both sides of the equation by γ:

$$\begin{aligned} \gamma &= \gamma\alpha x + \gamma\beta y \\ &= \alpha\gamma x + \alpha\kappa y \\ &= \alpha(\gamma x + \kappa y). \end{aligned}$$

Thus $\alpha \mid \gamma$. □

Corollary 5.8. *If $\alpha \mid \gamma$ and $\beta \mid \gamma$ in $\mathbf{Z}[i]$, with α and β relatively prime, then $\alpha\beta \mid \gamma$.*

Proof. Left to the reader. It's just like the integer case. □

Corollary 5.9. *For non-zero α, β, γ in $\mathbf{Z}[i]$, α and β are each relatively prime to γ if and only if $\alpha\beta$ is relatively prime to γ.*

Proof. Left to the reader. It's just like the integer case. □

We close out this section with an extension to $\mathbf{Z}[i]$ of several different characterizations of the greatest common divisor in $\mathbf{Z}$. The greatest common divisor of non-zero integers a and b can be described in several ways:

- the largest common divisor of a and b (definition)
- the positive common divisor which all other common divisors divide
- the smallest positive value of $ax + by$ $(x, y \in \mathbf{Z})$
- the positive value of $ax + by$ $(x, y \in \mathbf{Z})$ which divides all other values of $ax + by$ $(x, y \in \mathbf{Z})$

The corresponding characterizations of greatest common divisors of two non-zero Gaussian integers α and β are these:

- a common divisor of α and β with maximal norm (definition)
- a common divisor which all other common divisors divide
- a non-zero value of $\alpha x + \beta y$ $(x, y \in \mathbf{Z}[i])$ with smallest norm
- a non-zero value of $\alpha x + \beta y$ $(x, y \in \mathbf{Z}[i])$ which divides all other values of $\alpha x + \beta y$ $(x, y \in \mathbf{Z}[i])$

Verifying the equivalence of all four conditions is left to the interested reader. It is completely analogous to the arguments used in the integer case. Notice the switch from "the" to "a" when we pass from $\mathbf{Z}$ to $\mathbf{Z}[i]$: there are always four greatest common divisors, ambiguous up to multiplication by any of the four units.

6. Unique Factorization

We will define composite and prime Gaussian integers, and then prove unique factorization.

By Theorem 2.4, if $\beta \mid \alpha$, then $\mathrm{N}(\beta) \mid \mathrm{N}(\alpha)$, so $1 \leq \mathrm{N}(\beta) \leq \mathrm{N}(\alpha)$ when $\alpha \neq 0$. Which divisors of α have norm 1 or $\mathrm{N}(\alpha)$?

Lemma 6.1. *For $\alpha \neq 0$, any divisor of α whose norm is 1 or $\mathrm{N}(\alpha)$ is a unit or is a unit multiple of α.*

Proof. If $\beta \mid \alpha$ and $\mathrm{N}(\beta) = 1$, then β is ± 1 or $\pm i$. If $\beta \mid \alpha$ and $\mathrm{N}(\beta) = \mathrm{N}(\alpha)$, consider the complementary divisor γ, where $\alpha = \beta\gamma$. Taking norms of both sides and cancelling the common value $\mathrm{N}(\alpha)$, we see $\mathrm{N}(\gamma) = 1$, so γ is ± 1 or $\pm i$. Therefore β has to be $\pm\alpha$ or $\pm i\alpha$. □

Lemma 6.1 is *not* saying the only Gaussian integers whose norm is $\mathrm{N}(\alpha)$ are $\pm\alpha$ and $\pm i\alpha$. For instance, $1 + 8i$ and $4 + 7i$ both have norm 65 and neither is a unit multiple of the other. What Lemma 6.1 is saying is that the only Gaussian integers which *divide* α and have norm equal to $\mathrm{N}(\alpha)$ are $\pm\alpha$ and $\pm i\alpha$.

When $\mathrm{N}(\alpha) > 1$, there are always eight obvious factors of α: ± 1, $\pm i$, $\pm\alpha$, and $\pm i\alpha$. We call these the *trivial* factors of α. They are analogous to the four trivial factors ± 1 and $\pm n$ of any integer n with $|n| > 1$. Any other factor of α is called *non-trivial*. By Lemma 6.1, the non-trivial factors of α are the factors with norm strictly between 1 and $\mathrm{N}(\alpha)$.

Definition 6.2. Let α be a Gaussian integer with $\mathrm{N}(\alpha) > 1$. We call α *composite* if it has a non-trivial factor. If α only has trivial factors, we call α *prime*.

Writing $\alpha = \beta\gamma$, the condition $1 < \mathrm{N}(\beta) < \mathrm{N}(\alpha)$ is equivalent to: $\mathrm{N}(\beta) > 1$ and $\mathrm{N}(\gamma) > 1$. We refer to any such factorization of α, into a product of Gaussian integers with norm greater than 1, as a *non-trivial* factorization. Thus, a composite Gaussian integer is one which admits a non-trivial factorization.

For instance, a trivial factorization of $7+i$ is $i(1-7i)$. A non-trivial factorization of $7+i$ is $(1-2i)(1+3i)$. A non-trivial factorization of 5 is $(1+2i)(1-2i)$. How interesting: 5 is prime in $\mathbf{Z}$ but it is composite in $\mathbf{Z}[i]$. Even 2 is composite in $\mathbf{Z}[i]$: $2 = (1+i)(1-i)$. However, 3 is prime in $\mathbf{Z}[i]$, so some primes in $\mathbf{Z}$ stay prime in $\mathbf{Z}[i]$ while others do not.

To show 3 is prime in $\mathbf{Z}[i]$, we argue by contradiction. Assume it is composite and let a non-trivial factorization be $3 = \alpha\beta$. Taking the norm of both sides, $9 = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$. Since the factorization is non-trivial, $\mathrm{N}(\alpha) > 1$ and $\mathrm{N}(\beta) > 1$. Therefore $\mathrm{N}(\alpha) = 3$. Writing $\alpha = a + bi$, we get $a^2 + b^2 = 3$. There are no integers a and b satisfying that equation, so we have a contradiction. Thus, 3 has only trivial factorizations in $\mathbf{Z}[i]$, so 3 is prime in $\mathbf{Z}[i]$. (In Corollary 9.4, we will see any prime p in $\mathbf{Z}^+$ satisfying $p \equiv 3 \bmod 4$ is prime in $\mathbf{Z}[i]$.)

While we don't really need to construct primes explicitly in $\mathbf{Z}[i]$ in order to prove unique factorization in $\mathbf{Z}[i]$, it is good to have *some* method of generating Gaussian primes, if only to get a feel for what they look like by comparison with prime numbers. The following test for primality in $\mathbf{Z}[i]$, using the norm, provides a way to generate many Gaussian primes if we can recognize primes in $\mathbf{Z}$.

Theorem 6.3. *If the norm of a Gaussian integer is prime in $\mathbf{Z}$, then the Gaussian integer is prime in $\mathbf{Z}[i]$.*

For example, since $\mathrm{N}(4+5i) = 41$, $4+5i$ is prime in $\mathbf{Z}[i]$. Similarly, $4-5i$ is prime, as are $1 \pm i$, $1 \pm 2i$, $2 \pm 3i$, $1 \pm 4i$, and $15 \pm 22i$. Compute each of their norms and check the result is a prime number.

Proof. Let $\alpha \in \mathbf{Z}[i]$ have prime norm, say $p = \mathrm{N}(\alpha)$. We will show α only has trivial factors (that is, its factors have norm 1 or $\mathrm{N}(\alpha)$ only), so α is prime in $\mathbf{Z}[i]$.

Consider any factorization of α in $\mathbf{Z}[i]$, say $\alpha = \beta\gamma$. Taking norms, $p = \mathrm{N}(\beta)\,\mathrm{N}(\gamma)$. This is an equation in positive integers, and p is prime in $\mathbf{Z}^+$, so either $\mathrm{N}(\beta)$ or $\mathrm{N}(\gamma)$ is 1. Therefore β or γ is a unit, so α does not admit nontrivial factors. Thus α is prime. □

The converse of Theorem 6.3 is *false*: a Gaussian prime does not have to have prime norm. For instance, 3 has norm 9, but we saw 3 is prime in $\mathbf{Z}[i]$.

We have said enough about concrete Gaussian primes for now, and turn our attention to unique factorization. The existence of a prime factorization will be proved by a similar argument to the proof of prime factorization in $\mathbf{Z}$. First we will establish the existence of a prime factorization, then we treat its uniqueness.

Theorem 6.4. *Every $\alpha \in \mathbf{Z}[i]$ with $\mathrm{N}(\alpha) > 1$ is a product of primes in $\mathbf{Z}[i]$.*

Proof. We argue by induction on $\mathrm{N}(\alpha)$ (*not* by induction on α). Suppose that $\mathrm{N}(\alpha) = 2$. (In other words, $\alpha = 1 \pm i$ or $-1 \pm i$.) Then α is prime by Theorem 6.3.

Now assume $n \geq 3$ and every Gaussian integer with norm greater than 1 and less than n is a product of primes. We want to show every Gaussian integer with norm n is a product of primes. If there are no Gaussian integers with norm n (recall the end of Section 1), then there is nothing to prove. So we may assume there are Gaussian integers with norm n. Those which are prime are a product of primes (in $\mathbf{Z}[i]$). If we have a Gaussian integer α with norm n which is composite, write a non-trivial factorization of α as $\beta\gamma$, where $\mathrm{N}(\beta), \mathrm{N}(\gamma) < \mathrm{N}(\alpha) = n$. By the inductive hypothesis, β and γ are products of primes in $\mathbf{Z}[i]$. Therefore their product, which is α, is also a product of primes in $\mathbf{Z}[i]$. We are done. □

Having settled the existence of prime factorizations in $\mathbf{Z}[i]$, we aim for the uniqueness. We start with a lemma, which generalizes a familiar result about prime numbers in $\mathbf{Z}$.

Lemma 6.5. *Let π be prime in $\mathbf{Z}[i]$. For Gaussian integers $\alpha_1, \ldots, \alpha_r$, if $\pi \mid \alpha_1\alpha_2\cdots\alpha_r$ then π divides some α_j.*

Proof. We check the case $r = 2$. The proof for larger r is a straightforward induction.

Let $\pi \mid \alpha_1\alpha_2$. Suppose π does not divide α_1. This implies π and α_1 are relatively prime. Indeed, otherwise π and α_1 would have a non-unit greatest common divisor, which would have to be a unit multiple of π (since π only has trivial factors, as it is prime). This would imply π divides α_1, which is not the case.

Now that we know π and α_1 are relatively prime, $\pi \mid \alpha_2$ by Corollary 5.7. □

We're now ready to prove unique factorization in $\mathbf{Z}[i]$. However, it is not quite what you may expect. That is, the following is *false*: when

$$\pi_1\pi_2\cdots\pi_r = \pi_1'\pi_2'\cdots\pi_s'$$

where the π_i's and π_j's are all prime in $\mathbf{Z}[i]$, $r = s$ and $\pi_i = \pi_i'$ after a suitable relabelling. Well, the $r = s$ part is true. But there is no reason to expect we can match up the primes term-by-term. Consider

$$5 = (1+2i)(1-2i) = (2-i)(2+i).$$

The factors here are all prime in $\mathbf{Z}[i]$ (since their norms all equal the prime number 5), but the two primes in one factorization do not appear in the other. Does this violate the idea of unique factorization?

No. By allowing unit multiples, we can make a match between the two factorizations:

$$1 + 2i = (2 - i)i, \quad (1 - 2i) = (2 + i)(-i).$$

In fact, the same phenomenon can happen in $\mathbf{Z}$:

$$6 = 2 \cdot 3 = (-2) \cdot (-3).$$

This is not an example of non-unique factorization in $\mathbf{Z}$, since we can match the factors up to sign. Sign issues are avoided in $\mathbf{Z}$ by focusing attention on positive integers and positive primes only. As there is no positivity in $\mathbf{Z}[i]$ (at least in this course), we are forced to allow ambiguity up to unit multiples in our prime factorizations. This explains the role of units in unique factorization for $\mathbf{Z}[i]$.

Theorem 6.6 (Unique Factorization)**.** *Any $\alpha \in \mathbf{Z}[i]$ with $\mathrm{N}(\alpha) > 1$ has a unique factorization into primes in the following sense: If*

$$\alpha = \pi_1\pi_2 \cdots \pi_r = \pi_1'\pi_2' \cdots \pi_s',$$

where the π_i's and π_j''s are prime in $\mathbf{Z}[i]$, then $r = s$ and after a suitable renumbering each π_i is a unit multiple of π_i'.

Proof. Theorem 6.4 shows each $\alpha \in \mathbf{Z}[i]$ with $\mathrm{N}(\alpha) > 1$ has a prime factorization.

When α is prime, its prime factorization is obviously unique. Now we show uniqueness in general by induction on $\mathrm{N}(\alpha)$. The base case, $\mathrm{N}(\alpha) = 2$, has already been settled since such α's are prime.

Assume now that $n \geq 3$ and every Gaussian integer with norm greater than 1 and less than n has a unique prime factorization. We may assume there are Gaussian integers with norm n (otherwise there is nothing to check), and we only have to focus attention on composite α with norm n. Consider two prime factorizations of α as in the statement of the theorem. Since $\pi_1 \mid \alpha$, we can write

$$\pi_1 \mid \pi_1'\pi_2' \cdots \pi_s'.$$

By Lemma 6.5, $\pi_1 \mid \pi_j'$ for some j. Relabelling, we may suppose $j = 1$, *i.e.*, $\pi_1 \mid \pi_1'$. The only non-unit factors of π_1' are unit multiples of π_1', so $\pi_1 = u\pi_1'$ for some unit $u \in \{\pm 1, \pm i\}$. The two factorizations of α now look like this:

$$\alpha = u\pi_1'\pi_2 \cdots \pi_r = \pi_1'\pi_2' \cdots \pi_s',$$

We cancel π_1' on both sides and get

$$u\pi_2 \cdots \pi_r = \pi_2' \cdots \pi_s', \tag{6.1}$$

Call this common value β, so $\mathrm{N}(\beta) = \mathrm{N}(\alpha)/\mathrm{N}(\pi_1') < \mathrm{N}(\alpha)$.

Although u is a unit, the product $u\pi_2$ on the left side of (6.1) is itself a prime, so (6.1) gives two prime factorizations of β, with $r - 1$ primes on the left side and $s - 1$ primes on the right side. Since $\mathrm{N}(\beta) < n$, the inductive hypothesis tells us β has unique factorization, so $r - 1 = s - 1$ (thus $r = s$) and, after suitable relabelling, we have $u\pi_2$ and π_2' are unit multiples and π_i, π_i' are unit multiples for $i > 2$. Since $u\pi_2$ and π_2' are unit multiples, π_2 and π_2' are unit multiples, so we see every π_i is a unit multiple of π_i' and the proof is complete. □

Knowing there is a prime factorization in the abstract is different from being able to exhibit one in practice. For instance, what is the prime factorization of $3+4i$ or $2319+1694i$? You have no experience factoring in $\mathbf{Z}[i]$, but you have factored in $\mathbf{Z}$. Let's use the norm function to let your experience in $\mathbf{Z}$ be the first step in helping you factor in $\mathbf{Z}[i]$. Our goal is not to prove a theorem about practical factoring in $\mathbf{Z}[i]$, but to illustrate the method through some examples. Then you can try it out your own.

The key idea is this: any factorization in $\mathbf{Z}[i]$ implies a factorization in norms. Indeed,

$$\alpha = \beta\gamma \Longrightarrow \mathrm{N}(\alpha) = \mathrm{N}(\beta)\,\mathrm{N}(\gamma).$$

We will try to use the conclusion to tell us something about the hypothesis: use integer factorizations of the norm to suggest possible factors of the Gaussian integer.

For instance, take $\alpha = 3+4i$. Its norm is $25 = 5 \cdot 5$. If $3+4i$ factors, a non-trivial factor has to have norm 5. We know the Gaussian integers with norm 5: up to unit multiple they are $1+2i$ and $1-2i$. So we try the various possibilities:

$$(1+2i)(1+2i) = -3+4i, \quad (1+2i)(1-2i) = 5, \quad (1-2i)(1-2i) = -3-4i.$$

We recognize the last product as $-\alpha$, so

$$3+4i = -(1-2i)(1-2i) = -(1-2i)^2.$$

This is a prime factorization of $3+4i$.

What about $2319+1694i$? Its norm is 8247397, whose prime factorization in $\mathbf{Z}$ is

$$8247397 = 17 \cdot 29 \cdot 16729.$$

Let's look for the Gaussian integers with norm 17, 29, and 16729. and then try multiplying them together to get $2319+1694i$. Gaussian factors of 17, 29, and 16729 come from representations of each number as a sum of two squares:

$$17 = 1^2+4^2, \quad 29 = 2^2+5^2, \quad 16729 = 40^2+123^2.$$

(Admittedly, that last equation was not found by hand.) These give us prime factorizations in $\mathbf{Z}[i]$:

$$17 = (1+4i)(1-4i), \quad 29 = (2+5i)(2-5i), \quad 16729 = (40+123i)(40-123i)$$

(The Gaussian integers here are prime since their norms are prime in $\mathbf{Z}$.) Let's pick one factor from each product and multiply them together. Happily, the first choice gives us what we want:

$$(1+4i)(2+5i)(40+123i) = -2319-1694i.$$

Therefore the prime factorization of $2319+1694i$ is

$$2319+1694i = -(1+4i)(2+5i)(40+123i).$$

Except for the overall sign, each factor on the right is prime in $\mathbf{Z}[i]$ since its norm is prime in $\mathbf{Z}$.

As an application of these ideas, try to discover the prime factorizations in (5.3) on your own.

7. Modular arithmetic in $\mathbf{Z}[i]$

As in the integers, congruences are defined using divisibility.

Definition 7.1. For Gaussian integers α, β, and γ, we write $\alpha \equiv \beta \bmod \gamma$ when $\gamma \mid (\alpha - \beta)$.

Example 7.2. To check $1 + 12i \equiv 2 - i \bmod 3 + i$, we subtract and divide:

$$\frac{(1+12i)-(2-i)}{3+i} = \frac{-1+13i}{3+i} = 1 + 4i.$$

The ratio is in $\mathbf{Z}[i]$, so the congruence holds.

Congruences in $\mathbf{Z}[i]$ behave well under both addition and multiplication:

$$\alpha \equiv \alpha' \bmod \gamma, \quad \beta \equiv \beta' \bmod \gamma \Longrightarrow \alpha + \beta \equiv \alpha' + \beta' \bmod \gamma, \quad \alpha\beta \equiv \alpha'\beta' \bmod \gamma.$$

The details behind this are just like in $\mathbf{Z}$ and are left to the reader to check.

Since congruence modulo 0 means equality, we usually assume the modulus is non-zero.

A Gaussian integer can be reduced modulo α, if $\alpha \neq 0$, to get a congruent Gaussian integer with small norm by dividing by α and using the remainder.

Example 7.3. Let's compute $(3 + 2i)^2 \bmod 4 + i$. Since $(3 + 2i)^2 = 5 + 12i$ and $5 + 12i = (4 + i)(2 + 3i) - 2i$, we have $(3 + 2i)^2 \equiv -2i \bmod 4 + i$.

Example 7.4. To reduce $1 + 8i \bmod 2 - 4i$, we divide. This was already done in Example 3.6, where we found more than one possibility:

$$1 + 8i = (2 - 4i)(-1 + i) - 1 + 2i, \quad 1 + 8i = (2 - 4i)(-1 + i) + 1 - 2i.$$

Therefore $1 + 8i \equiv -1 + 2i \bmod 2 - 4i$ and $1 + 8i \equiv 1 - 2i \bmod 2 - 4i$. There is no reason to think $-1 + 2i$ or $1 - 2i$ is the more correct reduction. Both work.

There is a way to picture what modular arithmetic in $\mathbf{Z}[i]$ means, by plotting the multiples of a Gaussian integer in $\mathbf{Z}[i]$. For example, let's look at the $\mathbf{Z}[i]$-multiples of $1 + 2i$. Algebraically, a general $\mathbf{Z}[i]$-multiple of $1 + 2i$ is

$$(1 + 2i)(m + ni) = (1 + 2i)m + (1 + 2i)ni = m(1 + 2i) + n(-2 + i),$$

where m and n are in $\mathbf{Z}$. This is an integral combination of $1 + 2i$ and $-2 + i = (1 + 2i)i$. In Figure 1 we plot $1 + 2i$ and $-2 + i$ as the vectors $(1, 2)$ and $(-2, 1)$ in $\mathbf{R}^2$.

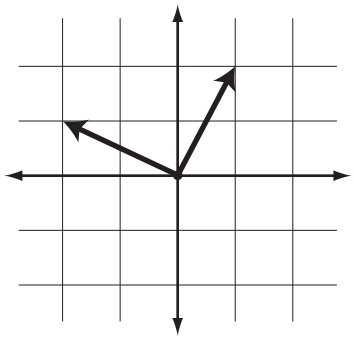

Figure 1. $1 + 2i$ and $-2 + i$

The $\mathbf{Z}[i]$-multiples of $1+2i$ are the integral combinations of the two vectors in Figure 1. Forming all these combinations produces the picture in Figure 2, where the plane is tiled by squares having the Gaussian multiples of $1+2i$ as the vertices. The significance of Figure 2 for modular arithmetic is that Gaussian integers are congruent modulo $1+2i$ precisely when they are located in the same relative positions within different squares of Figure 2. For example, $2+3i$ and $4-3i$ are in the same relative position within their squares, and their difference is a Gaussian multiple of $1+2i$:

$$\frac{(2+3i)-(4-3i)}{1+2i} = \frac{-2+6i}{1+2i} = \frac{(-2+6i)(1-2i)}{(1+2i)(1-2i)} = \frac{10+10i}{5} = 2+2i \in \mathbf{Z}[i].$$

Why are congruent Gaussian integers mod $1+2i$ in the same position within their respective squares? Because each square shares its sides with four other squares, and moving to these squares corresponds to adding $1+2i$, $-(1+2i)$, $-2+i$, or $-(-2+i)$. Moving from a position in any square to the same relative position in any other square is translation by a Gaussian multiple of $1+2i$.

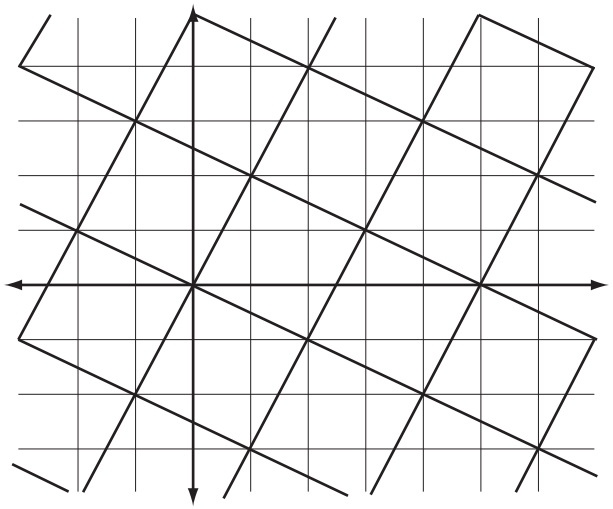

FIGURE 2. $\mathbf{Z}[i]$-multiples of $1+2i$

We can use Figure 2 to make a list of representatives for $\mathbf{Z}[i]/(1+2i)$: use the Gaussian integers inside a square and one of its vertices. (All the vertices are $\mathbf{Z}[i]$-multiples of $1+2i$, so we should use only one of them.) Choosing the square with edges $1+2i$ and $-2+i$, we get a list of 5 Gaussian integers:

$$0,\ i,\ 2i,\ -1+i,\ -1+2i.$$

Every Gaussian integer is congruent modulo $1+2i$ to exactly one of these. For instance, $2+3i \equiv -1+2i \bmod 1+2i$ since $2+3i$ and $-1+2i$ are in the same relative position in their respective squares. Using instead the square with edges $1+2i$ and $2-i$, we get the list

$$0,\ 1,\ 2,\ 1+i,\ 2+i,$$

and with this list we have $2 + 3i \equiv 1 + i \bmod 1 + 2i$. There is nothing special about using the vertex 0 in our lists: we could use any of the other vertices of the square in place of 0 for our list of representatives modulo $1 + 2i$. In fact, there is nothing special about using points inside or on a single square. We just need to use a set of points which fills out each relative position within all these squares. For instance, the numbers

$$0,\ 1,\ 2,\ 3,\ 4$$

could be used, and with this list we have $2 + 3i \equiv 3 \bmod 1 + 2i$.

Let's look at the picture for modulus $2 + 2i$. In Figure 3 we plot the $\mathbf{Z}[i]$-multiples of $2 + 2i$ as vertices of squares. Since

$$(2 + 2i)(m + ni) = (2 + 2i)m + (2 + 2i)ni = m(2 + 2i) + n(-2 + 2i),$$

the $\mathbf{Z}[i]$-multiples of $2 + 2i$ are the integral combinations of $2 + 2i$ and $-2 + 2i$, which form two edges of the shaded square in Figure 3.

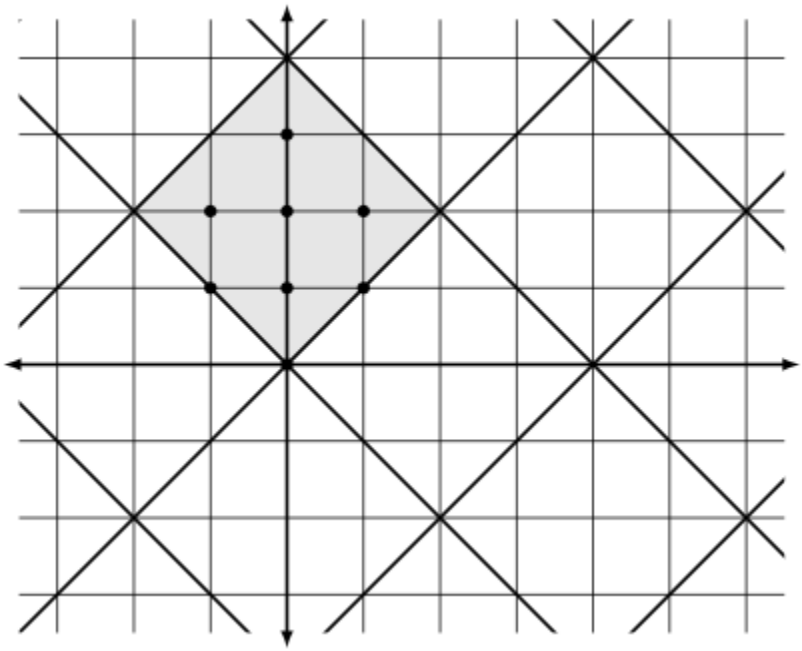

FIGURE 3. $\mathbf{Z}[i]$-multiples of $2 + 2i$

What is a set of representatives for $\mathbf{Z}[i]/(2 + 2i)$? Translating from one square to the same relative position in another square is the same as adding a Gaussian multiple of $2+2i$, so every Gaussian integer is congruent modulo $2 + 2i$ to a Gaussian integer inside or on one of the squares. Points in the same relative position on opposite edges of a square are congruent since adding $2 + 2i$ or $-2 + 2i$ takes us from one edge to another. We didn't have to worry about this issue for modulus $1 + 2i$ because there were no Gaussian integers on the edges of squares in Figure 2 except for vertices. Taking the edge identifications into account, a set of representatives for $\mathbf{Z}[i]/(2+2i)$ is all the Gaussian integers inside a square and on two adjacent edges of the square, with only one vertex counted. Using the square with edges $2 + 2i$ and $-2 + 2i$, we get the 8 representatives

$$0,\ i,\ 2i,\ 3i,\ 1 + i,\ 1 + 2i,\ -1 + i,\ -1 + 2i.$$

For example, $6+i \equiv 3i \bmod 2+2i$ since $6+i$ and $3i$ are in the same relative position within their squares in Figure 3.

Unlike in Figure 2, where ordinary integers can be used as representatives, we can't represent $\mathbf{Z}[i]/(2+2i)$ only using ordinary integers, because $\mathbf{Z}$ only represents 4 of the 8 congruence classes mod $2+2i$.

Figure 4 is a picture of $\mathbf{Z}[i]/(3)$. The squares have vertices that are $\mathbf{Z}[i]$-multiples of 3, which all look like $3(m+ni) = m\cdot 3 + n\cdot 3i$ where m and n are in $\mathbf{Z}$. A set of representatives for $\mathbf{Z}[i]/(3)$ can be formed from the Gaussian integers inside and on the shaded square with edges 3 and $3i$. Using two adjacent edges (and just one of the vertices), we have 9 representatives

$$0,\ 1,\ 2,\ i,\ 1+i,\ 2+i,\ 2i,\ 1+2i,\ 2+2i.$$

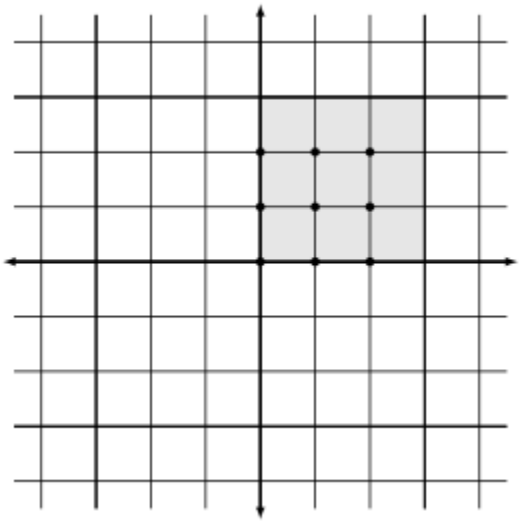

FIGURE 4. $\mathbf{Z}[i]$-multiples of 3

Finally, in Figure 5, we draw one square for modulus $3+i$. Its two edges with a vertex at 0 are the vectors $3+i = (3,1)$ and $(3+i)i = -1+3i = (-1,3)$. There are 10 representatives: 9 in the square and one vertex.

Algebraic properties of modular arithmetic in $\mathbf{Z}$ carry over to $\mathbf{Z}[i]$ practically word-for-word.

Theorem 7.5. *If π is prime in $\mathbf{Z}[i]$, then $\alpha\beta \equiv 0 \bmod \pi$ if and only if $\alpha \equiv 0 \bmod \pi$ or $\beta \equiv 0 \bmod \pi$.*

Proof. This is Lemma 6.5 with $r = 2$. □

Theorem 7.6. *For α and β in $\mathbf{Z}[i]$ with $\beta \neq 0$, $\alpha x \equiv 1 \bmod \beta$ is solvable if and only if α and β are relatively prime in $\mathbf{Z}[i]$. If α and β are relatively prime then any linear congruence $\alpha x \equiv \gamma \bmod \beta$ has a unique solution.*

Proof. To solve $\alpha x \equiv 1 \bmod \beta$ with $x \in \mathbf{Z}[i]$ amounts to solving $\alpha x + \beta y = 1$ with x and y in $\mathbf{Z}[i]$, which is equivalent to relative primality of α and β by Corollary 5.2.

Once we can invert $\alpha \bmod \beta$, we can solve $\alpha x \equiv \gamma \bmod \beta$ by multiplying both sides by the inverse of $\alpha \bmod \beta$. If there is going to be a solution this must be it, and it does work. □

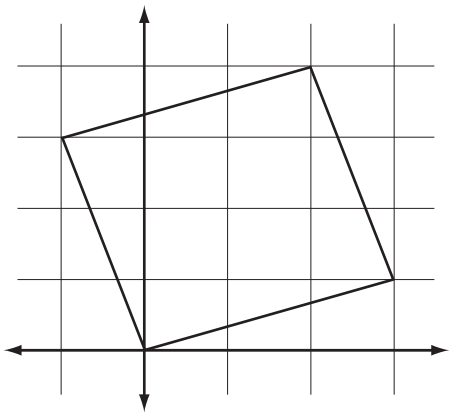

FIGURE 5. Representatives for $\mathbf{Z}[i]/(3+i)$

Example 7.7. Can we solve $(1+8i)x \equiv 1 \bmod 11+3i$? No, since $1+8i$ and $11+3i$ have a common factor of $-1+2i$ by Example 4.6.

Example 7.8. Can we solve $(7+3i)x \equiv 1 \bmod 10+91i$? According to Example 5.6, $7+3i$ and $10+91i$ are relatively prime (although their norms are not), so there is a solution. Moreover, by using Euclid's algorithm and back-substitution we found in (5.2) that

$$(7+3i)(57-46i) + (10+91i)(1+6i) = 1,$$

so a solution is $x = 57-46i$. (The norm of $57-46i$ is less than the norm of the modulus $10+91i$, so there is no great incentive to reduce our solution further $\bmod 10+91i$.)

Corollary 7.9. *Let π be a Gaussian prime. Every $\alpha \not\equiv 0 \bmod \pi$ has a multiplicative inverse modulo π and any polynomial congruence*

$$c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 \equiv 0 \bmod \pi,$$

where $c_i \in \mathbf{Z}[i]$ and $c_n \not\equiv 0 \bmod \pi$, has at most n solutions modulo π.

Proof. Since π is prime, any $\alpha \not\equiv 0 \bmod \pi$ is relatively prime to π and therefore $\alpha \bmod \pi$ has a multiplicative inverse by Theorem 7.6. Thus $\mathbf{Z}[i]/(\pi)$ is a field, so this corollary is a special case of the fact that polynomials have no more roots in a field than their degree. □

When we allow Gaussian integers into our congruences, does it change the meaning of congruences among ordinary integers? That is, if a, b, and c are in $\mathbf{Z}$, does the meaning of $a \equiv b \bmod c$ change when we think in $\mathbf{Z}[i]$? That is, could integers which are incongruent modulo c in $\mathbf{Z}$ become congruent modulo c in $\mathbf{Z}[i]$? No.

Theorem 7.10. *For a, b, and c in $\mathbf{Z}$, $a \equiv b \bmod c$ in $\mathbf{Z}$ if and only if $a \equiv b \bmod c$ in $\mathbf{Z}[i]$.*

Proof. In terms of divisibility, this is saying

$$c \mid (a-b) \text{ in } \mathbf{Z} \iff c \mid (a-b) \text{ in } \mathbf{Z}[i],$$

which is something we already checked in the paragraph after the proof of Theorem 2.3: divisibility between ordinary integers holds in $\mathbf{Z}$ if and only if it holds in $\mathbf{Z}[i]$. □

So far modular arithmetic in $\mathbf{Z}[i]$ behaves just like in $\mathbf{Z}$. But things now will get tricky, so pay attention!

One of the useful properties of modular arithmetic in $\mathbf{Z}$ is Fermat's little theorem. For a prime p in $\mathbf{Z}^+$, if $a \not\equiv 0 \bmod p$ then $a^{p-1} \equiv 1 \bmod p$. Naively translating this result into the Gaussian integers, using a Gaussian prime π, we get something like this: if $\alpha \not\equiv 0 \bmod \pi$ then $\alpha^{\pi-1} \equiv 1 \bmod \pi$. ???? If π is not a positive integer, then raising to the power $\pi - 1$ doesn't mean anything in a congruence. (Well, if you have had complex analysis you may know a way to do this, but then you would also know the result is almost certainly not going to be in $\mathbf{Z}[i]$, so it's the wrong idea for us.) Moreover, even when π is a positive integer that is prime in $\mathbf{Z}[i]$ the congruence $\alpha^{\pi-1} \equiv 1 \bmod \pi$ is usually *wrong*.

Example 7.11. Let $\pi = 3$, which is prime in $\mathbf{Z}[i]$. Take $\alpha = i$. Then $\alpha^{\pi-1} = i^2 = -1$, but $-1 \not\equiv 1 \bmod 3$, so $\alpha^{\pi-1} \not\equiv 1 \bmod \pi$.

Despite this setback, there *is* a good Gaussian integer version of Fermat's little theorem. The way to find it is to go back to the *proof* of Fermat's little theorem and remind ourselves how a^{p-1} actually showed up in the proof. It came from comparing two different sets of representatives for the non-zero integers modulo p: $1, 2, \ldots, p-1$ and $a, 2a, \ldots, (p-1)a$. The two products of all the numbers in both cases have to be congruent modulo p, and cancelling common terms on both sides of the congruence (essentially a factor of $(p-1)!$) leaves behind $1 \equiv a^{p-1} \bmod p$. So the source of a^{p-1} comes from the fact that there are $p-1$ non-zero numbers modulo p. It is the *size* of the set of non-zero numbers modulo p which gave us the exponent in Fermat's little theorem. There are p numbers in total modulo p, and we take away 1 because we don't count 0. With this insight, we get almost for free a $\mathbf{Z}[i]$-analogue.

Theorem 7.12. *Let π be a Gaussian prime and denote the number of Gaussian integers modulo π by $n(\pi)$. If $\alpha \not\equiv 0 \bmod \pi$, then $\alpha^{n(\pi)-1} \equiv 1 \bmod \pi$.*

Proof. There is no natural complete set of representatives for $\mathbf{Z}[i]/(\pi)$, but we can use any complete set of representatives at all. Denote it $\beta_1, \beta_2, \ldots, \beta_{n(\pi)}$, where we take $\beta_{n(\pi)} = 0$.

Since α is invertible modulo π, another complete set of representatives for $\mathbf{Z}[i]/(\pi)$ is $\alpha\beta_1, \alpha\beta_2, \ldots, \alpha\beta_{n(\pi)}$. The last term here is 0. Multiplying congruent numbers retains the congruence, so let's multiply each set of non-zero representatives together and compare:

$$\begin{aligned} \beta_1\beta_2\cdots\beta_{n(\pi)-1} &\equiv (\alpha\beta_1)(\alpha\beta_2)\cdots(\alpha\beta_{n(\pi)-1}) \bmod \pi \\ &\equiv \alpha^{n(\pi)-1}\beta_1\beta_2\cdots\beta_{n(\pi)-1} \bmod \pi. \end{aligned}$$

Since the β_i's here are non-zero modulo π (why?), we can cancel them on both sides and we are left with $1 \equiv \alpha^{n(\pi)-1} \bmod \pi$. □

As soon as we try to test this result in an example, we run into a problem. We defined $n(\pi)$ to be the size of $\mathbf{Z}[i]/(\pi)$ but we never gave a working formula for this size. For instance, what is $n(3)$? Or, to jazz things up, $n(3+4i)$?

Example 7.13. Let's show there are 9 elements in $\mathbf{Z}[i]/3$, so $n(3) = 9$. A Gaussian integer is divisible by 3 exactly when its real and imaginary parts are divisible by 3 (Theorem 2.3). Therefore

$$a + bi \equiv c + di \bmod 3 \iff a \equiv b \bmod 3 \text{ and } c \equiv d \bmod 3.$$

The real and imaginary parts have 3 possibilities modulo 3, so there is a total of $3 \cdot 3 = 9$ incongruent Gaussian integers modulo 3. We can even write down a nice set of representatives: $a + bi$ where $0 \leq a, b \leq 2$.

Since $n(3) = 9$, Theorem 7.12 says that if $\alpha \not\equiv 0 \bmod 3$ then $\alpha^8 \equiv 1 \bmod 3$. This works at $\alpha = i$ (unlike what we saw in Example 7.11). Using $\alpha = 1 + i$ shows the exponent 8 is optimal: $(1+i)^k \not\equiv 1 \bmod 3$ for $1 \leq k < 8$.

To make Theorem 7.12 really meaningful, we want a formula for $n(\pi)$ in general. In fact, there is a nice formula for $n(\alpha) = |(\mathbf{Z}[i]/(\alpha))|$ even when α is not prime.

Theorem 7.14. *If $\alpha \neq 0$ in $\mathbf{Z}[i]$, then $n(\alpha) = \mathrm{N}(\alpha)$. That is, the size of $\mathbf{Z}[i]/(\alpha)$ is $\mathrm{N}(\alpha)$.*

There is an analogy with the absolute value on $\mathbf{Z}$: $|(\mathbf{Z}/m)| = |m|$ when $m \neq 0$ and now $|(\mathbf{Z}[i]/(\alpha))| = \mathrm{N}(\alpha)$ when $\alpha \neq 0$. Our earlier lists of representatives for $\mathbf{Z}[i]/(1+2i)$, $\mathbf{Z}[i]/(2+2i)$, $\mathbf{Z}[i]/(3)$, and $\mathbf{Z}[i]/(3+i)$ are all consistent with this norm formula.

Perhaps we should point out why $n(\alpha)$ is finite (when $\alpha \neq 0$) before we prove the formula for it. Using division by α, every Gaussian integer is congruent modulo α to some Gaussian integer with norm less than $\mathrm{N}(\alpha)$. There are only finitely many Gaussian integers with norm below a given bound, so $n(\alpha)$ is finite.[1]

Before we prove Theorem 7.14 we establish a few lemmas about the n-function.

Lemma 7.15. *If $m \neq 0$ in $\mathbf{Z}$ then $n(m) = m^2$.*

Proof. The argument is the same as the case $m = 3$ done in Example 7.13. □

Lemma 7.16. *If $\alpha \neq 0$ in $\mathbf{Z}[i]$ then $n(\overline{\alpha}) = n(\alpha)$.*

Proof. Congruences modulo α and congruences modulo $\overline{\alpha}$ can be converted into one another by conjugating all terms:

$$x \equiv y \bmod \alpha \iff \overline{x} \equiv \overline{y} \bmod \overline{\alpha}.$$

Therefore a complete set of representatives modulo α becomes a complete set of representatives modulo $\overline{\alpha}$ by conjugating the representatives, so $n(\overline{\alpha}) = n(\alpha)$. □

The next lemma needs a bit more work.

Lemma 7.17. *The function n is multiplicative: if α and β are non-zero in $\mathbf{Z}[i]$, then $n(\alpha\beta) = n(\alpha)n(\beta)$.*

Proof. Let a complete set of representatives for $\mathbf{Z}[i]/(\alpha)$ be $x_1, x_2, \ldots, x_r$ and a complete set of representatives for $\mathbf{Z}[i]/(\beta)$ be $y_1, y_2, \ldots, y_s$. (That is, $r = n(\alpha)$ and $s = n(\beta)$.)

Given any $z \in \mathbf{Z}[i]$, we have $z \equiv x_i \bmod \alpha$ for some i. Then $z - x_i = \alpha t$ for some Gaussian integer t, and $t \equiv y_j \bmod \beta$ for some j. Writing $t = y_j + \beta w$, we have

$$z = x_i + \alpha y_j + \alpha\beta w \equiv x_i + \alpha y_j \bmod \alpha\beta.$$

Thus the rs numbers $x_i + \alpha y_j$ are a set of representatives for $\mathbf{Z}[i]/(\alpha\beta)$. To show they are complete (that is, no repetitions), suppose

$$x_i + \alpha y_j \equiv x_{i'} + \alpha y_{j'} \bmod \alpha\beta. \tag{7.1}$$

We want to show $i = i'$ and $j = j'$.

[1]This shows Gaussian integers with norm less than $\mathrm{N}(\alpha)$ fill up all congruence classes modulo α, but there could be different remainders which are congruent, unlike in $\mathbf{Z}$, so $n(\alpha)$ is actually smaller than the number of these remainders.

Reducing both sides of (7.1) modulo α, $x_i \equiv x_{i'} \bmod \alpha$. Since the x's are a complete set of representatives modulo α, this congruence must be equality: $x_i = x_{i'}$ (that is, $i = i'$). Then subtract the common x_i on both sides of (7.1) and divide through the congruence (including the modulus!) by α. We are left with $y_j \equiv y_{j'} \bmod \beta$. Since the y's are a complete set of representatives modulo β, we have $j = j'$. □

We are ready to prove Theorem 7.14. All the real work has been put into the lemmas, so the proof now will be a short and slick argument.

Proof. By Lemma 7.17, $n(\alpha\overline{\alpha}) = n(\alpha)n(\overline{\alpha})$. By Lemma 7.16, the right side is $n(\alpha)^2$. At the same time, since $\alpha\overline{\alpha} = \mathrm{N}(\alpha)$ is an integer, Lemma 7.15 says $n(\alpha\overline{\alpha}) = \mathrm{N}(\alpha)^2$. Thus $\mathrm{N}(\alpha)^2 = n(\alpha)^2$. Take positive square roots. □

There are two points worth noting about this argument:

(1) While we proved $n(\alpha)$ is a totally multiplicative function of α as a lemma, we did not use this to reduce the problem of calculating $n(\alpha)$ to the case of $n(\pi)$ for prime π. Usually when we know something is multiplicative, we take that as a clue to first compute on primes, then prime powers, and then in general by prime factorization. But the way multiplicativity of n got used in the proof of Theorem 7.14 completely sidestepped the special case of prime α.

(2) Our derivation of the formula for $n(\alpha)$ lets us count the size of $\mathbf{Z}[i]/(\alpha)$ without giving a method of listing a complete set of representatives. For instance, $n(2 + 2i) = \mathrm{N}(2 + 2i) = 8$, but this counting does not tell us a set of representatives for $\mathbf{Z}[i]/(2 + 2i)$ (it is *not* $0, 1, 2, \ldots, 7$, *e.g.*, $4 \equiv 0 \bmod 2 + 2i$). So the situation is unlike the integers, where we know $|(\mathbf{Z}/m)| = |m|$ because we actually made a list of representatives: $0, 1, 2, \ldots, |m| - 1$.

With an exact formula for $|(\mathbf{Z}[i]/(\pi))|$ in hand let's reformulate Theorem 7.12 as a more honest analogue of Fermat's little theorem:

$$\alpha \not\equiv 0 \bmod \pi \Longrightarrow \alpha^{\mathrm{N}(\pi)-1} \equiv 1 \bmod \pi. \tag{7.2}$$

Comparing this to $a^{p-1} \equiv 1 \bmod p$, we see more clearly from the Gaussian case that p was really playing two different roles in the integer case: the modulus is p and the number of incongruent integers for that modulus is p. The distinction between the modulus and the number of incongruent numbers in that modulus is more vivid in (7.2), where we see π in one place and $\mathrm{N}(\pi)$ in the other.

To formulate Euler's congruence in $\mathbf{Z}[i]$, we need the analogue of the φ-function. If you think about $\varphi(m)$ as the number of positive integers between 1 and m which are relatively prime to m, the correct generalization to $\mathbf{Z}[i]$ is not apparent. But if you think about $\varphi(m)$ as the number of invertible integers modulo m, then the generalization to $\mathbf{Z}[i]$ is (or should be) immediate.

Definition 7.18. For non-zero α in $\mathbf{Z}[i]$, set $\varphi(\alpha) = |(\mathbf{Z}[i]/(\alpha))^\times|$.

Example 7.19. When $\alpha = \pi$ is prime, every non-zero Gaussian integer modulo π is invertible, so $\varphi(\pi) = \mathrm{N}(\pi) - 1$. Notice the analogy to $\varphi(p) = p - 1$.

When we work with this φ-function on $\mathbf{Z}[i]$, we need to be careful when the argument is in $\mathbf{Z}$, because the Gaussian φ-function may not agree with the integral φ-function. For instance in $\mathbf{Z}$ we have $\varphi(3) = 2$, but in $\mathbf{Z}[i]$ we have $\varphi(3) = 8$. That is, $(\mathbf{Z}/3)^\times$ has 2 elements but $(\mathbf{Z}[i]/3)^\times$ has 8 elements. This might seem strange: didn't Theorem 7.10 tell us that

congruences with a modulus in $\mathbf{Z}$ are the same in $\mathbf{Z}[i]$ as in $\mathbf{Z}$? No. Theorem 7.10 was about congruences in $\mathbf{Z}[i]$ among ordinary integers to an ordinary integer modulus, which leaves out a lot of congruences among all the Gaussian integers to that ordinary integer modulus. Perhaps we should write $\varphi_{\mathbf{Z}[i]}$ to distinguish the Gaussian φ-function from the usual φ-function (which is now $\varphi_{\mathbf{Z}}$?), but nobody does this.

Euler's congruence for $\mathbf{Z}[i]$ looks like its counterpart over $\mathbf{Z}$, using the Gaussian φ-function:

Theorem 7.20. *If $(\alpha, \mu) = 1$ in $\mathbf{Z}[i]$, then $\alpha^{\varphi(\mu)} \equiv 1 \bmod \mu$.*

Proof. This is left as an exercise in translating the proof over $\mathbf{Z}$ into this new setting. □

How do we compute $\varphi(\mu)$? Let's recall the φ-formulas in $\mathbf{Z}$:

$$\varphi(p^k) = p^{k-1}(p-1), \quad \varphi(ab) = \varphi(a)\varphi(b) \text{ if } (a,b) = 1.$$

With these formulas, $\varphi(m)$ can be computed from the prime factorization of m. The analogous formulas for the Gaussian φ-function use norms in certain places, but otherwise are identical to the counterpart in $\mathbf{Z}$:

$$\varphi(\pi^k) = \mathrm{N}(\pi)^{k-1}(\mathrm{N}(\pi) - 1), \quad \varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta) \text{ if } (\alpha, \beta) = 1.$$

Example 7.21. What is $\varphi(3+4i)$? The Gaussian prime factorization is $3 + 4i = (2+i)^2$. Therefore $\varphi(3+4i) = \mathrm{N}(2+i)(\mathrm{N}(2+i) - 1) = 5 \cdot 4 = 20$.

Example 7.22. What is $\varphi(5)$? The Gaussian prime factorization is $5 = (1+2i)(1-2i)$, where $1+2i$ and $1-2i$ are relatively prime. Therefore $\varphi(5) = \varphi(1+2i)\varphi(1-2i) = (\mathrm{N}(1+2i) - 1)(\mathrm{N}(1-2i) - 1) = 16$.

8. Applications of $\mathbf{Z}[i]$ to the arithmetic of $\mathbf{Z}$

We are ready to give applications of the arithmetic of $\mathbf{Z}[i]$ to properties of $\mathbf{Z}$. All these applications are connected with sums of two squares. It is precisely the formula

$$a^2 + b^2 = (a + bi)(a - bi),$$

where a sum of two squares is on the left and a (special type of) factorization in $\mathbf{Z}[i]$ is on the right that explains why $\mathbf{Z}[i]$ is relevant to questions about sums of two squares in $\mathbf{Z}$.

Our applications will address the following issues:

- a prime number that is a sum of two squares is so in essentially just one way,
- classification of (primitive) Pythagorean triples,
- classification of (primitive) solutions to $a^2 + b^2 = c^3$.
- the only integer solution to $y^2 = x^3 - 1$ is $(x, y) = (1, 0)$,
- systematically finding integers which are sums of two squares in more than one way.

Theorem 8.1. *If a prime number p is a sum of two squares then it is so in essentially just one way: writing $p = a^2 + b^2$, the integers a and b are unique up to order and sign. (In particular, the squares a^2 and b^2 are unique up to order.)*

Notice the theorem says nothing explicitly about $\mathbf{Z}[i]$. It is a theorem about $\mathbf{Z}$ alone. We will find it very useful to use $\mathbf{Z}[i]$ in the proof, however.

Proof. Let $p = a^2 + b^2$, with $a, b \in \mathbf{Z}$. Then, in $\mathbf{Z}[i]$, p factors as

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

Since $a+bi$ and $a-bi$ both have norm p, which is prime in $\mathbf{Z}$, they are prime in $\mathbf{Z}[i]$ (Theorem 6.3). If there is a second representation $p = c^2 + d^2$, then

$$p = (c+di)(c-di),$$

and $c \pm di$ are prime in $\mathbf{Z}[i]$. By unique factorization in $\mathbf{Z}[i]$, we must have

$$a+bi = u(c+di) \quad \text{or} \quad a+bi = u(c-di)$$

for some unit u. The only difference between $c+di$ and $c-di$ is the sign of the coefficient of i, and we are aiming to show that a and b are determined up to order and sign, so there is no harm in treating only the case

$$a+bi = u(c+di).$$

If $u = 1$, then $c = a$ and $d = b$. If $u = -1$, then $c = -a$ and $d = -b$. If $u = i$, then $c = b$ and $d = -a$. If $u = -i$, then $c = -b$ and $d = a$. Thus c and d equal a and b up to order and sign. □

Theorem 8.1 is *not* saying that any integer which is a sum of two squares has only one representation in that form. It is only referring to primes which are sums of two squares. Two non-primes which are a sum of two squares in more than one way are $50 = 5^2 + 5^2 = 1^2 + 7^2$ and $65 = 1^2 + 8^2 = 4^2 + 7^2$. (We will find more examples at the end of this section.) Some primes which can be written as sums of two squares (necessarily uniquely) are

$$2 = 1^2 + 1^2, \quad 5 = 1^2 + 2^2, \quad 13 = 2^2 + 3^2, \quad 17 = 1^2 + 4^2, \quad 29 = 2^2 + 5^2.$$

Example 8.2. The fifth Fermat number $2^{2^5} + 1 = 4294967297$ is easily a sum of two squares: $2^{2^5} + 1 = (2^{16})^2 + 1^2$. Euler found it can be written as a sum of two squares in a different way:

$$(2^{16})^2 + 1^2 = 62264^2 + 20449^2.$$

This actually has an interesting consequence. Fermat guessed that the fifth Fermat number was a prime, but the fact that it can be written as a sum of two squares in two different ways proves it is not prime *without* telling us what a nontrivial factor might be! (Euler did find a nontrivial factor, 641: $2^{2^5} + 1 = 641 \cdot 6700417$.)

Our next application of $\mathbf{Z}[i]$ to ordinary arithmetic is the classification of Pythagorean triples, which are integral solutions to the equation

$$a^2 + b^2 = c^2.$$

If any two of a, b, and c have a common prime factor, it is also a factor of the third number (why?), so its square appears in all terms. Conversely, multiplying both sides by a square rescales a, b, and c by the same amount. Therefore, we focus our attention on the Pythagorean triples (a, b, c) where they share no common factor (equivalently, a and b alone share no common factor). Such triples are called *primitive*. Examples of primitive Pythagorean triples include $(3, 4, 5)$, $(5, 12, 13)$, and $(8, 15, 17)$, but not $(6, 8, 10)$. We will use unique factorization in $\mathbf{Z}[i]$ to obtain a formula for the primitive Pythagorean triples.

Before we give the formula, let's make a few observations about primitive triples (a, b, c). Since there is no common factor among the three numbers, *at most one* of them can be even (why?). Could c be even? If so, then a and b are odd, so $a^2 \equiv 1 \bmod 4$ and $b^2 \equiv 1 \bmod 4$. Then $c^2 = a^2 + b^2 \equiv 2 \bmod 4$. But no number squares to 2 mod 4. Therefore c is odd. Since

$a^2 + b^2$ is now known to be odd, a and b do not have the same parity. That is, one of them is odd and the other is even. Relabelling if necessary, we may assume that

$$a \text{ is odd and } b \text{ is even.}$$

With these preliminary observations out of the way, we are ready for the main result.

Theorem 8.3. *Every primitive Pythagorean triple (a, b, c) with a odd has the form*

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2,$$

where $m > n > 0$, $(m, n) = 1$, and $m \not\equiv n \bmod 2$. Conversely, for any such choice of m and n, the above formula is a primitive Pythagorean triple. Different choices of m and n give different primitive triples.

The table below gives some primitive Pythagorean triples from choices of m and n.

m	2	3	4	5	4
n	1	2	1	2	3
$a = m^2 - n^2$	3	5	15	21	7
$b = 2mn$	4	12	8	20	24
$c = m^2 + n^2$	5	13	17	29	25

Proof. We write the equation $a^2 + b^2 = c^2$ in the form

$$(a + bi)(a - bi) = c \cdot c. \tag{8.1}$$

Our proof will have three steps:

- use the primitivity of the triple to show $a+bi$ and $a-bi$ are relatively prime in $\mathbf{Z}[i]$,
- use unique factorization in $\mathbf{Z}[i]$ to show $a+bi$ is a square or i times a square in $\mathbf{Z}[i]$,
- use the evenness of b to show $a + bi$ is a square in $\mathbf{Z}[i]$, and then read off the consequences.

First we show $a+bi$ and $a-bi$ are relatively prime. This is going to follow from $(a, b) = 1$ and c being odd. Let δ be a common divisor of $a + bi$ and $a - bi$ in $\mathbf{Z}[i]$. It divides their sum and their difference:

$$\delta \mid 2a, \quad \delta \mid 2b. \tag{8.2}$$

(Strictly, δ dividing the difference means $\delta \mid 2bi$, but i is a unit so we can remove it.) Now we show δ is relatively prime to 2 in $\mathbf{Z}[i]$. Since $2 = -i(1 + i)^2$ and $1 + i$ is prime, this is equivalent to showing δ is not divisible by $1 + i$. By Corollary 2.5, $(1 + i) \mid \delta$ if and only if $\mathrm{N}(\delta)$ is even. Because $\delta^2 \mid c^2$, by (8.1), which implies $\mathrm{N}(\delta)^2 \mid c^4$, and c^4 is odd, we see $\mathrm{N}(\delta)$ is odd. That tells us $1 + i$ does not divide δ.

Now that we know δ is relatively prime to 2 in $\mathbf{Z}[i]$, (8.2) simplifies to

$$\delta \mid a, \quad \delta \mid b.$$

Because a and b are relatively prime in $\mathbf{Z}$, they are also relatively prime in $\mathbf{Z}[i]$ (just solve $ax + by = 1$ in $\mathbf{Z}$ and then view the equation in $\mathbf{Z}[i]$). Thus, their only common divisors in $\mathbf{Z}[i]$ are units, so at last we see δ is a unit.

In (8.1), we have a product of relatively prime Gaussian integers on the left and a perfect square on the right. If you think about it, the only way two relatively prime Gaussian integers can multiply to a square is if they are each squares. After all, think about how

their prime factors can combine to give a square, given that they are relatively prime and that $\mathbf{Z}[i]$ has unique factorization. Thus, from (8.1) we must have

$$a + bi = (m + ni)^2$$

for some Gaussian integer $m + ni$.

Alas, this reasoning is wrong! Two relatively prime Gaussian integers can multiply to a square without either factor being a square. In fact, this possibility already can happen in $\mathbf{Z}$:

$$36 = (-4)(-9).$$

Neither -4 nor -9 is a square in $\mathbf{Z}$, but their product is and they are relativey prime. Ah, the only sneaky thing here are the units. Remember, unique factorization always has an ambiguity due to units. (We tend to forget this in $\mathbf{Z}$ since we focus on factoring positive integers into positive factors, and the only positive unit is 1.) We can't forget about units!

Very well, we keep in mind the units in $\mathbf{Z}[i]$ when looking at (8.1). Since the two factors on the left are relatively prime and their product is a square, unique factorization in $\mathbf{Z}[i]$ tells us each factor is itself a square *up to unit multiple*. The units in $\mathbf{Z}[i]$ are ± 1 and $\pm i$. Since -1 is a perfect square, it can be absorbed into any square factor by writing it as i^2. Therefore, we can say

$$a + bi = (m + ni)^2 \quad \text{or} \quad a + bi = i(m + ni)^2$$

for some $m + ni \in \mathbf{Z}[i]$. Expanding these out and collecting real and imaginary parts, we have

$$a + bi = (m^2 - n^2) + (2mn)i \quad \text{or} \quad a + bi = (-2mn) + (m^2 - n^2)i.$$

Now we appeal to our convention that a is odd (and b is even). The second choice makes a even, so it is not correct. We thus must have

$$a + bi = (m + ni)^2, \tag{8.3}$$

so $a + bi$ is a perfect square after all. (The point is that we have now argued this *correctly*, rather than incorrectly as before.) The derivation of (8.3) from unique factorization in $\mathbf{Z}[i]$ is really the key step in this proof. The remainder of the proof will be just a matter of careful bookkeeping.

Identifying real and imaginary parts in (8.3) gives us

$$a = m^2 - n^2, \quad b = 2mn.$$

Therefore $c^2 = a^2 + b^2 = (m^2 - n^2)^2 + 4m^2n^2 = m^4 + 2m^2n^2 + n^4 = (m^2 + n^2)^2$. Since $c > 0$ we see that

$$c = m^2 + n^2.$$

Since $b > 0$, the formula for b shows m and n have the same sign: they are both positive or both negative. We can negate them both if necessary to assume m and n are positive without changing the values of a, b, or c. Since $a > 0$ we have $m^2 > n^2$, so $m > n$. Because a is odd, m and n have different parities. If m and n have a common factor, then we get a common factor in a, b, and c. Therefore primitivity of the triple (a, b, c) makes m and n relatively prime.

Now we show any triple $(m^2 - n^2, 2mn, m^2 + n^2)$ with m and n positive, relatively prime, of opposite parity, and $m > n$, is a primitive Pythagorean triple. Easily it is a Pythagorean triple: $(m^2 - n^2)^2 + (2mn)^2 = (m^2 + n^2)^2$. Suppose this triple is *not* primitive. Then some prime p divides each of $m^2 - n^2$, $2mn$, and $m^2 + n^2$. Since the first term is odd, $p \neq 2$. Then from $p \mid 2mn$ we have either $p \mid m$ or $p \mid n$. If $p \mid m$, then the relation $m^2 \equiv n^2 \bmod p$

implies $n^2 \equiv 0 \bmod p$, so $p \mid n$. Similarly, if $p \mid n$ then $p \mid m$. We are supposing $(m, n) = 1$, so we have a contradiction either way, and thus the triple is primitive.

As for the triple being uniquely determined by m and n, (8.3) tells us that the parameters m and n that describe the triple (a, b, c) are the coordinates of a square root of $a + bi$. As there are only two square roots, which just differ by a sign, the uniqueness falls out (since we take $m > 0$ and $n > 0$). □

This proof tells us how to produce Pythagorean triples on demand: take any Gaussian integer α (with non-zero real and imaginary parts) and square it, say $\alpha^2 = a + bi$. Then $(|a|, |b|, \mathrm{N}(\alpha))$ is a Pythagorean triple. For example, $(17+12i)^2 = 145+408i$ and $17^2+12^2 = 433$. Therefore $(145, 408, 433)$ is a Pythagorean triple (check it!). Moreover, since 17 and 12 are relatively prime, this triple is primitive.

To better appreciate this approach to $a^2 + b^2 = c^2$, let's apply it to $a^2 + b^2 = c^3$.

Theorem 8.4. *The integral solutions to $a^2 + b^2 = c^3$ with $(a, b) = 1$ are described by the parametric formula*

$$a = m^3 - 3mn^2, \quad b = 3m^2n - n^3, \quad c = m^2 + n^2,$$

where $(m, n) = 1$ and $m \not\equiv n \bmod 2$. Different choices of m and n give different solutions (a, b, c).

Proof. Since $(a, b) = 1$, a and b are not both even. If they were both odd then $c^3 \equiv 1 + 1 \equiv 2 \bmod 8$, but 2 is not a cube mod 8. Therefore one of a or b is even and the other is odd: $a \not\equiv b \bmod 2$ and c is odd.

In $\mathbf{Z}[i]$, we can rewrite $a^2 + b^2 = c^3$ as

$$(a + bi)(a - bi) = c^3.$$

Let's show $a+bi$ and $a-bi$ are relatively prime. If δ is a common divisor then $\delta \mid 2a$, $\delta \mid 2b$, and $\delta \mid c^3$. Taking norms, $\mathrm{N}(\delta)$ is a factor of $4a^2$, $4b^2$, and c^6. Since c is odd, $\mathrm{N}(\delta)$ is odd, so $\mathrm{N}(\delta)$ divides a^2 and b^2. The numbers a and b are relatively prime, so $\mathrm{N}(\delta) = 1$, and thus δ is ± 1 or $\pm i$. This proves $a + bi$ and $a - bi$ are relatively prime.

Because the product of $a + bi$ and $a - bi$ is a perfect cube in $\mathbf{Z}[i]$, and these numbers are relatively prime, unique factorization in $\mathbf{Z}[i]$ implies $a + bi$ and $a - bi$ are each cubes up to multiplication by a unit. Say $a + bi = u\alpha^3$ where $u \in \{\pm 1, \pm i\}$. However, every unit is itself a cube: $1 = 1^3$, $-1 = (-1)^3$, $i = (-i)^3$, and $-i = i^3$. Therefore we can absorb the unit factor into α^3, so $a + bi$ is in fact a perfect cube. Write $a + bi = (m + ni)^3$ for some integers m and n. Expanding the cube and equating real and imaginary parts, we get

$$a = m^3 - 3mn^2, \quad b = 3m^2n - n^3. \tag{8.4}$$

Any common factor of m and n would arise from these formulas as a common factor of a and b, so $(m, n) = 1$. If $m \equiv n \bmod 2$ then the parametric formulas would imply $a \equiv -2m^3 \equiv 0 \bmod 2$ and $b \equiv 2m^3 \equiv 0 \bmod 2$, but a and b are not both even. Thus $m \not\equiv n \bmod 2$. Moreover, $c^3 = (a + bi)(a - bi) = (m + ni)^3(m - ni)^3 = (m^2 + n^2)^3$, so $c = m^2 + n^2$.

Conversely, if $(m, n) = 1$ and $m \not\equiv n \bmod 2$, then defining a and b by (8.4), and $c = m^2 + n^2$, makes them satisfy $a^2 + b^2 = c^3$ and $a + bi = (m + ni)^3$. It is left as an exercise for the reader to check $(a, b) = 1$.

That the choice of m and n is unique for a and b follows from $a + bi = (m + ni)^3$: the only cube root of unity in $\mathbf{Z}[i]$ is 1, so if m', n' work in (8.4) for the same a and b then $(m + ni)^3 = (m' + n'i)^3$, which implies $m + ni = m' + n'i$, so $m = m'$ and $n = n'$. □

The table below gives some solutions to $a^2 + b^2 = c^3$ with $(a, b) = 1$.

m	1	2	4	7	9
n	0	1	3	2	5
$a = m^3 - 2mn^2$	1	2	-44	259	54
$b = 3m^2n - n^3$	0	11	117	286	1090
$c = m^2 + n^2$	1	5	25	53	106

Unlike $a^2 + b^2 = c^2$, where every solution in integers is a multiple of a relatively prime (primitive) solution of the same equation, integral solutions of $a^2 + b^2 = c^3$ where $(a, b) > 1$ do not come from relatively prime solutions of the same equation because the exponents are not all equal. For example, three solutions of $a^2 + b^2 = c^3$ with $(a, b) > 1$ are (18, 26, 10), (5, 10, 5), and (30, 10, 10). Divide through each triple by their greatest common divisor to get (9, 13, 5), (1,2,1), and (3,1,1), and none of these satisfy $a^2 + b^2 = c^3$. They satisfy new equations: $a^2 + b^2 = 2c^3$, $a^2 + b^2 = 5c^3$, and $a^2 + b^2 = 10c^3$, respectively.

The next application uses $\mathbf{Z}[i]$ to show a perfect square in $\mathbf{Z}$ never comes right before a perfect cube, except for the pair 0 and 1.

Theorem 8.5. *The only $x, y \in \mathbf{Z}$ satisfying $y^2 = x^3 - 1$ is $(x, y) = (1, 0)$.*

Although the cubes are spread out more thinly than the squares in $\mathbf{Z}$, it is not obvious why they couldn't come within one of each other many times.

By the way, we know three examples where a cube precedes a square: -1 and 0, 0 and 1, and 8 and 9. However, this corresponds to the equation $x^3 = y^2 - 1$, which is not the one we are studying.

Proof. The integer pair $(x, y) = (1, 0)$ obviously fits the equation $y^2 = x^3 - 1$. We now show it is the only integral solution.

Write the equation in the form

$$x^3 = y^2 + 1,$$

which has the factored form

$$x^3 = (y + i)(y - i). \tag{8.5}$$

The same idea as in the proof of Theorem 8.3 suggests itself: if the two factors on the right side are relatively prime in $\mathbf{Z}[i]$, then since their product is a cube, each factor must be a cube up to unit multiple, by unique factorization in $\mathbf{Z}[i]$. Moreover, since every unit is a cube ($1 = 1^3$, $-1 = (-1)^3$, $i = (-i)^3$, $-i = i^3$), it can be absorbed into the cube. Thus, provided we show $y + i$ and $y - i$ are relatively prime, (8.5) tells us $y + i$ and $y - i$ are themselves cubes.

To see that $y + i$ and $y - i$ are relatively prime, let δ be a common divisor. Then δ divides their difference, so $\delta \mid 2i$. As $2i = (1 + i)^2$, unique factorization in $\mathbf{Z}[i]$ tells us that δ is 1, $1 + i$, or $(1 + i)^2$ up to units.

If δ is not a unit, it is divisible by $1 + i$, so $(1 + i) \mid x^3$. Taking norms, $2 \mid x^6$, so x is even. Then $y^2 + 1 = x^3 \equiv 0 \bmod 4$, so $y^2 \equiv -1 \bmod 4$. But $-1 \bmod 4$ is not a square. We have a contradiction, so δ is a unit.

Now that we know $y + i$ and $y - i$ are relatively prime, we must have (as argued already)

$$y + i = (m + ni)^3$$

for some $m, n \in \mathbf{Z}$. Expanding the cube and equating real and imaginary parts,

$$y = m^3 - 3mn^2 = m(m^2 - 3n^2), \quad 1 = 3m^2n - n^3 = n(3m^2 - n^2).$$

The equation on the right tells us $n = \pm 1$. If $n = 1$, then $1 = 3m^2 - 1$, so $3m^2 = 2$, which has no integer solution. If $n = -1$, then $1 = -(3m^2 - 1)$, so $m = 0$. Therefore $y = 0$, so $x^3 = y^2 + 1 = 1$. Thus $x = 1$. □

Remark 8.6. Using $\mathbf{Z}[i]$, in 1850 V. A. Lebesgue showed for all $d \geq 2$ that the equation $y^2 = x^d - 1$ has no solution in nonzero integers x and y.

We end this section by returning to the theme connected to our first application: sums of two squares. We saw that a prime is a sum of two squares in just one way. But other numbers can be sums of two squares in more than one way, such as 50 and 65. We now use arithmetic in $\mathbf{Z}[i]$ to *systematically* construct integers that are sums of two squares in more than one way. Consider the factorizations of 5 and 13:

$$5 = (1 + 2i)(1 - 2i), \quad 13 = (2 + 3i)(2 - 3i).$$

We can combine these factors in two ways:

$$5 \cdot 13 = ((1 + 2i)(2 + 3i))((1 - 2i)(2 - 3i)) = ((1 + 2i)(2 - 3i))((1 - 2i)(2 + 3i)).$$

After some algebra, this becomes

$$65 = (-4 + 7i)(-4 - 7i) = (8 + i)(8 - i).$$

Thus

$$65 = 4^2 + 7^2 = 8^2 + 1^2.$$

Different representations of an integer as a sums of two squares in $\mathbf{Z}$ correspond to *rearranging* prime factors in $\mathbf{Z}[i]$!

As another example, using $5 = (1 + 2i)(1 - 2i)$ and $10 = (1 + 3i)(1 - 3i)$, we can write down two different Gaussian integers with norm 50:

$$(1 + 2i)(1 + 3i) = -5 + 5i, \quad (1 + 2i)(1 - 3i) = 7 - i.$$

Taking the norm, we find $50 = 5^2 + 5^2 = 1^2 + 7^2$.

Let's find an integer which is a sum of two squares in *three* different ways. We use the primes 5, 13, and 17. In $\mathbf{Z}[i]$,

$$5 = (1 + 2i)(1 - 2i), \quad 13 = (2 + 3i)(2 - 3i), \quad 17 = (1 + 4i)(1 - 4i).$$

Consider the following products:

$$(1 + 2i)(2 + 3i)(1 + 4i) = -32 - 9i,$$

$$(1 - 2i)(2 + 3i)(1 + 4i) = 12 + 31i,$$

$$(1 + 2i)(2 - 3i)(1 + 4i) = 4 + 33i.$$

Their common norm is $5 \cdot 13 \cdot 17 = 1105$, so

$$1105 = 9^2 + 32^2 = 12^2 + 31^2 = 4^2 + 33^2.$$

Pursuing this theme further, you can try your hand at systematically (*i.e.*, without having to guess) constructing integers which are a sum of two squares in four, five, or more different ways.

9. Primes in $\mathbf{Z}[i]$

Theorem 6.3 gave a sufficient condition for a Gaussian integer to be prime: it has prime norm. We saw also that this condition was not necessary: 3 is prime but its norm is 9, which is not prime.

Our goal in this section is to classify the primes in $\mathbf{Z}[i]$. We don't mean this in an absolute sense, but rather in terms of the primes in $\mathbf{Z}$.

Lemma 9.1. *Let π be a prime in $\mathbf{Z}[i]$. For some prime p in $\mathbf{Z}^+$, $\pi \mid p$.*

The point of this lemma is that it tells us we can get a handle on all Gaussian primes by factoring every prime in $\mathbf{Z}^+$ in the Gaussian integers: each Gaussian prime is a factor of an ordinary prime.

Proof. It is always the case that π divides some positive integer, namely its norm: $\mathrm{N}(\pi) = \pi\overline{\pi}$, so $\pi \mid \mathrm{N}(\pi)$ in $\mathbf{Z}$. Since $\mathrm{N}(\pi) > 1$, we write $\mathrm{N}(\pi)$ as a product of primes in $\mathbf{Z}^+$:

$$\mathrm{N}(\pi) = p_1 p_2 \cdots p_r.$$

Since $\pi \mid \mathrm{N}(\pi)$ in $\mathbf{Z}[i]$, and π is prime in $\mathbf{Z}[i]$, we must have $\pi \mid p_j$ for some j by Lemma 6.5. □

As noted already, this lemma tells us the prime factors in $\mathbf{Z}[i]$ of the primes in $\mathbf{Z}^+$ will give us all Gaussian primes. Here are Gaussian prime factorizations of the first three prime numbers:

$$2 = (1+i)(1-i), \quad 3 = 3, \quad 5 = (1+2i)(1-2i).$$

For instance, by unique factorization, any other Gaussian prime factor of 5 is a unit multiple of $1+2i$ or $1-2i$, which gives one of the following numbers:

$$1+2i, \quad -1-2i, \quad -2+i, \quad 2-i, \quad 1-2i, \quad -1+2i, \quad -2-i, \quad 2+i.$$

Up to unit multiple, these eight numbers are really just two numbers: $1+2i$ and $1-2i$.

Theorem 9.2. *A prime p in $\mathbf{Z}^+$ is composite in $\mathbf{Z}[i]$ if and only if it is a sum of two squares.*

Thus, any prime p in $\mathbf{Z}^+$ which is *not* a sum of two squares is not composite in $\mathbf{Z}[i]$, so it stays prime in $\mathbf{Z}[i]$. Examples include 3, 7, 11, and 19.

Proof. If the prime p in $\mathbf{Z}^+$ is composite in $\mathbf{Z}[i]$, let a non-trivial factorization be $p = \alpha\beta$. Then, taking norms, $p^2 = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$. Since the factorization of p was nontrivial, and $p > 0$, we must have $\mathrm{N}(\alpha) = p$. Then, writing $\alpha = a + bi$, the norm equation tells us $p = a^2 + b^2$.

Conversely, suppose a prime p in $\mathbf{Z}^+$ is a sum of two squares, say $p = a^2 + b^2$. Then in $\mathbf{Z}[i]$ we get the non-trivial factorization

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

so p is composite in $\mathbf{Z}[i]$. □

The first primes in $\mathbf{Z}^+$ which are sums of two squares are $2, 5, 13, 17$, and 29:

$$2 = 1^2 + 1^2, \quad 5 = 1^2 + 2^2, \quad 13 = 2^2 + 3^2, \quad 17 = 1^2 + 4^2, \quad 29 = 2^2 + 5^2.$$

Therefore each of these prime numbers is composite in $\mathbf{Z}[i]$, *e.g.* $29 = (2+5i)(2-5i)$. This is a Gaussian prime factorization, since the factors have prime norm (and thus are

themselves prime in $\mathbf{Z}[i]$). The factorization of 2 is special, since its prime factors are unit multiples of *each other*: $1 - i = -i(1 + i)$. In other words,

$$2 = -i(1 + i)^2.$$

Corollary 9.3. *If a prime p in $\mathbf{Z}^+$ is composite, and $p \neq 2$, then up to unit multiple p has exactly two Gaussian prime factors, which are conjugate and have norm p.*

Proof. By Theorem 9.2, when p is composite we have

$$p = a^2 + b^2 = (a + bi)(a - bi)$$

for some $a, b \in \mathbf{Z}$. Since $a + bi$ and $a - bi$ have prime norm p, they are prime in $\mathbf{Z}[i]$. Could they be unit multiples? We consider all four ways this could happen and show each one leads to a contradiction.

If $a+bi = a-bi$, then $b = 0$ and $p = a^2$, which is a contradiction. If $a+bi = -(a-bi)$, then $a = 0$ and we get a contradiction again. If $a+bi = i(a-bi)$, then $b = a$ and $p = a^2+a^2 = 2a^2$, but $p \neq 2$. We have a contradiction. The final case, when $a + bi = -i(a - bi)$, again implies the contradiction $p = 2a^2$. □

Corollary 9.4. *If a prime p in $\mathbf{Z}^+$ satisfies $p \equiv 3 \bmod 4$, then it is not a sum of two squares in $\mathbf{Z}$ and it stays prime in $\mathbf{Z}[i]$.*

Proof. Once we show p is not a sum of two squares in $\mathbf{Z}$, it is prime in $\mathbf{Z}[i]$ by Theorem 9.2.

We consider the squares modulo 4: the only squares are 0 and 1. Adding them together modulo 4 gives us 0 $(= 0 + 0)$, 1$(= 1 + 0$ or $0 + 1)$, and 2$(= 1 + 1)$. We can't get 3, so any number which is $\equiv 3 \bmod 4$ is not a sum of two squares in $\mathbf{Z}$. □

We now know how 2 factors into Gaussian primes and how any prime p in $\mathbf{Z}^+$ with $p \equiv 3 \bmod 4$ factors in $\mathbf{Z}[i]$ (it doesn't factor). What about the primes $p \equiv 1 \bmod 4$? The first such primes are 5, 13, 17, and 29. These are primes we saw earlier among the sums of two squares, so they are all composite in $\mathbf{Z}[i]$ by Theorem 9.2 and they factor into conjugate Gaussian primes by Theorem 9.3. Is every prime $p \equiv 1 \bmod 4$ a sum of two squares? Numerical evidence suggests it is true, so we make the

Conjecture 9.5. *For a prime p in $\mathbf{Z}^+$, the following conditions are equivalent:*

(1) $p = 2$ *or* $p \equiv 1 \bmod 4$,
(2) $p = a^2 + b^2$ *for some* $a, b \in \mathbf{Z}$.

The easier condition to check in practice is (1). The more interesting condition, at least from the viewpoint of ordinary arithmetic, is (2). It is easy to see that (2) implies (1): if $p = a^2 + b^2$ for some a and b, then $p \bmod 4$ is a sum of two squares. The squares mod 4 are 0 and 1, so a sum of two squares mod 4 could be 0, 1, or 2. Therefore $p \equiv 0, 1, 2 \bmod 4$. The first choice is impossible (since p is prime) and the third only happens for $p = 2$. (This argument may look familiar. You already met it in the proof of Corollary 9.4.)

What about the proof that (1) implies (2) (which is the more interesting direction anyway)? It turns out to be convenient to insert an additional property in between them, involving a polynomial modulo p.

Theorem 9.6. *Let p be a prime in $\mathbf{Z}^+$. The following conditions are equivalent:*

(1) $p = 2$ *or* $p \equiv 1 \bmod 4$,
(2) *the congruence* $x^2 \equiv -1 \bmod p$ *has a solution.*
(3) $p = a^2 + b^2$ *for some* $a, b \in \mathbf{Z}$.

Proof. We have already shown (3) implies (1).

To show (1) implies (2), we may take $p \neq 2$. Consider the polynomial factorization

$$T^{p-1} - 1 = (T^{(p-1)/2} - 1)(T^{(p-1)/2} + 1) \tag{9.1}$$

with mod p coefficients. We are going to count roots of these polynomials modulo p. Recall that a polynomial of degree d has no more than d roots modulo p.

By Fermat's little theorem, the left side of (9.1) has $p-1$ different roots modulo p, namely the non-zero integers modulo p. The first polynomial on the right side of (9.1) has degree $(p-1)/2$, so it has at most $(p-1)/2$ roots modulo p. Therefore the second polynomial $T^{(p-1)/2}+1$ *must* have roots modulo p: some integer c satisfies $c^{(p-1)/2} \equiv -1 \bmod p$. Since $p \equiv 1 \bmod 4$, $(p-1)/2$ is an even integer: if $p = 4k+1$ then $(p-1)/2 = 2k$. Therefore $(c^k)^2 \equiv -1 \bmod p$, which proves (2).

To show (2) implies (3), we are going to show (2) implies p is composite in $\mathbf{Z}[i]$. Then Theorem 9.2 says p is a sum of two squares.

View the congruence in (2) as a divisibility relation in $\mathbf{Z}$. When $x^2 \equiv -1 \bmod p$ for some $x \in \mathbf{Z}$, $p \mid (x^2+1)$ in $\mathbf{Z}$. Now consider this divisibility in $\mathbf{Z}[i]$, where we can factor x^2+1:

$$p \mid (x+i)(x-i). \tag{9.2}$$

To show p is composite in $\mathbf{Z}[i]$, we argue by *contradiction*. If p is a Gaussian prime, then by (9.2) $p \mid (x+i)$ or $p \mid (x-i)$ in $\mathbf{Z}[i]$. Therefore some Gaussian integer $m+ni$ satisfies $p(m+ni) = x \pm i$, but look at the imaginary part: $pn = \pm 1$. This is impossible! We have a contradiction, which proves p is composite in $\mathbf{Z}[i]$, so p is a sum of two squares by Theorem 9.2. □

Be sure you make note of the way we used the condition $p \equiv 1 \bmod 4$ in the proof that (1) implies (2).

We can now summarize the factorization of primes in $\mathbf{Z}^+$ into Gaussian prime factors.

Theorem 9.7. *Let p be a prime in $\mathbf{Z}^+$. The factorization of p in $\mathbf{Z}[i]$ is determined by $p \bmod 4$:*

i) $2 = (1+i)(1-i) = -i(1+i)^2$.

ii) If $p \equiv 1 \bmod 4$ then $p = \pi\overline{\pi}$ is a product of two conjugate primes π, $\overline{\pi}$ which are not unit multiples.

iii) If $p \equiv 3 \bmod 4$ then p stays prime in $\mathbf{Z}[i]$.

Proof. Part i is a numerical check. Part ii is a consequence of Corollary 9.3 and Theorem 9.6. Part iii is Corollary 9.4. □

Example 9.8. The prime 61 satisfies $61 \equiv 1 \bmod 4$, so 61 has two conjugate Gaussian prime factors, coming from an expression of 61 as a sum of two squares. Since $61 = 5^2 + 6^2$, $61 = (5+6i)(5-6i)$.

Combining the factorizations in Theorem 9.7 with Lemma 9.1, we now have a description of all the Gaussian primes in terms of the primes in $\mathbf{Z}^+$.

Theorem 9.9. *Every prime in $\mathbf{Z}[i]$ is a unit multiple of the following primes:*

i) $1+i$

ii) π or $\overline{\pi}$, where $\mathrm{N}(\pi) = p$ is a prime in $\mathbf{Z}^+$ which is $\equiv 1 \bmod 4$.

iii) p, where p is a prime in $\mathbf{Z}^+$ with $p \equiv 3 \bmod 4$.

Proof. Lemma 9.1 tells us any Gaussian prime is a factor of a prime in $\mathbf{Z}^+$. Theorem 9.7 and unique factorization in $\mathbf{Z}[i]$ tell us how the primes in $\mathbf{Z}^+$ factor in $\mathbf{Z}[i]$ up to unit multiple. □

The Gaussian primes in parts i and ii of Theorem 9.9 have prime norm in $\mathbf{Z}$, while the primes occurring in part iii have norm p^2, where $p \equiv 3 \bmod 4$. Moreover, when $p \equiv 3 \bmod 4$, its unit multiples in $\mathbf{Z}[i]$ are $\pm p$ and $\pm ip$, which have real or imaginary part 0. Thus, although the converse to Theorem 6.3 is not strictly true, we see it is true for the "interesting" Gaussian integers, namely the ones with non-zero real and imaginary part: write $\alpha = a + bi$ and suppose a and b are both non-zero in $\mathbf{Z}$. Then α is prime in $\mathbf{Z}[i]$ if and only if $\mathrm{N}(\alpha)$ is prime in $\mathbf{Z}$!

Our classification of Gaussian primes tells us that a Gaussian prime has norm either p or p^2, where p is the prime in $\mathbf{Z}^+$ which the Gaussian prime divides. In particular, any Gaussian prime other than $1+i$ (and its unit multiples) has an odd norm. Thus, a Gaussian integer which is *not* divisible by $1+i$ must have a norm which is odd, so any Gaussian integer with an even norm must be divisible by $1 + i$. This is something we already checked, using simple algebra, back in Corollary 2.5. But now we understand why it is true from a higher point of view, in connection with unique factorization in $\mathbf{Z}[i]$: Corollary 2.5 is true because every Gaussian integer with norm greater than 1 is a product of Gaussian primes and $1 + i$ is the *only* Gaussian prime up to unit multiple with even norm.

As an application of Theorem 9.7, we now classify all the positive integers which are sums of two squares.

Theorem 9.10. *An integer greater than* 1 *is a sum of two squares exactly when any prime factor which is* $\equiv 3 \bmod 4$ *occurs with even multiplicity.*

Proof. First we show any integer having even multiplicity at its prime factors which are $\equiv 3 \bmod 4$ can be written as a sum of two squares.

We know sums of two squares are closed under multiplication (view them as norms of Gaussian integers and use multiplicativity of the norm). Any prime $p \equiv 1 \bmod 4$ is a sum of two squares by Theorem 9.6, as is 2. While a prime $p \equiv 3 \bmod 4$ is not a sum of two squares, any even power of it is (since an even power is itself a square). Therefore a product of 2, primes $\equiv 1 \bmod 4$, and even powers of primes $\equiv 3 \bmod 4$ is a sum of two squares.

Now we treat the converse direction: any $n > 1$ which is a sum of two squares has even multiplicity at any prime factor which is $\equiv 3 \bmod 4$. We argue by induction on n. The result is true when $n = 2$, as 2 is a sum of two squares and it has no prime factors that are $\equiv 3 \bmod 4$.

Assume $n \geq 3$, n is a sum of two squares, and the theorem has been checked for sums of two squares greater than 1 and less than n. If n has no prime factors which are $\equiv 3 \bmod 4$, then there is nothing to prove. Thus, we may assume n has a prime factor p with $p \equiv 3 \bmod 4$. Write $n = a^2 + b^2$, so $p \mid (a^2 + b^2)$ in $\mathbf{Z}$. In $\mathbf{Z}[i]$, we write this as

$$p \mid (a + bi)(a - bi). \tag{9.3}$$

Since $p \equiv 3 \bmod 4$, it is prime in $\mathbf{Z}[i]$. Therefore from (9.3) we know $p \mid (a+bi)$ or $p \mid (a-bi)$ in $\mathbf{Z}[i]$. Both cases imply $p \mid a$ and $p \mid b$ in $\mathbf{Z}$. (Why?) Write $a = pa'$ and $b = pb'$ for integers a' and b'. Then

$$n = p^2(a'^2 + b'^2).$$

If $n = p^2$ we are done, so we may suppose $n > p^2$. The integer $n' = n/p^2 = a'^2 + b'^2$ is a sum of two squares and it is greater than 1 and less than n. By our inductive hypothesis,

every prime factor of n' which is $\equiv 3 \bmod 4$ has even multiplicity. Since the only difference between n and n' is the even power p^2, we conclude that every prime factor of n which is $\equiv 3 \bmod 4$ has even multiplicity. That ends the inductive step. □

Example 9.11. The number $35 = 5 \cdot 7$ has a prime factor which is $\equiv 3 \bmod 4$, namely 7. This factor appears with multiplicity 1, so 35 is not a sum of two squares. Neither is $5^k \cdot 7^\ell$ for any odd exponent $\ell > 0$. But $5 \cdot 7^2 = 245$ is a sum of two squares: $245 = 7^2 + 14^2$.

Theorem 9.10 describes the sums of two squares in terms of a condition on the prime factors which are $\equiv 3 \bmod 4$. In particular, applying the condition in the theorem to decide whether n is a sum of two squares requires that we factor n.

References

[1] C. F. Gauss, Theoria Residuorum Biquadraticorum, Commentatio Secunda, pp. 93-148 in *Werke*, Band II, Koniglichen Gesellschaft der Wissenschaften, Göttingen, 1876. URL https://archive.org/details/117771763_002/page/n103/mode/2up