In number theory one is interested in properties of the (rational) integers \( \mathbb{Z} \) and solving equations involving integers. In MATH 681 (algebraic number theory) we will look at certain structures that naturally crop up when considering such equations.

As an example, and to whet your appetite for what’s to come, suppose we are interested in equations that involve the sum of two squares: \( X^2 + Y^2 \). One thing that immediately comes to mind is to factor this sum as

\[
X^2 + Y^2 = (X + iY)(X - iY),
\]

where \( i \) is the usual “imaginary” complex number whose square is \(-1\). But already we’ve left the realm of integers and are now dealing with a particular subring \( \mathbb{Z}[i] \) of the complex numbers \( \mathbb{C} \). We are thus lead to studying this particular subring, called the Gaussian integers.

**Theorem:** Given \( \alpha, \beta \in \mathbb{Z}[i] \) with \( \beta \neq 0 \), there are \( \phi, \rho \in \mathbb{Z}[i] \) with

\[
\alpha = \phi \beta + \rho, \quad |\rho| \leq \frac{1}{\sqrt{2}} |\beta|,
\]

where \( |\cdot| \) denotes the usual modulus of a complex number. In particular, the Gaussian integers is a Euclidean domain.

**Proof:** Consider

\[
\{\phi \beta : \phi \in \mathbb{Z}[i]\} = \{a \beta + ib \beta : a, b \in \mathbb{Z}\},
\]

which is clearly a \( \mathbb{Z} \)-module contained in \( \mathbb{C} \), which we regard in the usual way as a (two-dimensional real) plane. This module has basis \( \beta \) and \( i \beta \), which we view as points in the plane. Connecting the dots, so to speak, of our module gives us a tiling of the plane which consists of non-overlapping squares of side length \( |\beta| \), whence of diameter \( \sqrt{2}|\beta| \). We now see that any \( \alpha \in \mathbb{C} \) is in one (or more!) of these squares, so that it is within \( \frac{\sqrt{2}}{2} |\beta| = \frac{1}{\sqrt{2}} |\beta| \) of the nearest vertex (i.e., point in our module).

**Application #1:** parametrizing the set of all Pythagorean triples: \( X, Y, Z \in \mathbb{Z} \) relatively prime and satisfying \( X^2 + Y^2 = Z^2 \).

Factor (uniquely!) \( Z^2 \in \mathbb{Z}[i] \) and write

\[
Z^2 = u \pi_1^{2e_1} \cdots \pi_n^{2e_n},
\]

where \( u \in \mathbb{Z}[i] \) is a unit, each \( \pi_j \in \mathbb{Z}[i] \) is irreducible, and \( e_j \) is a positive integer for all \( j \). Since \( Z^2 = (X + iY)(X - iY) \), each \( \pi_j \) divides at least one of these factors. We claim that, in fact, no \( \pi_j \) can divide both. To see why, suppose \( \pi_j |(X + iY) \) and \( \pi_j |(X - iY) \). Then it divides their sum: \( \pi_j |2X \). Thus \( \pi_j |2 \) or \( \pi_j |X \) since \( \pi_j \) is an irreducible element (a “prime”). But \( \pi_j |Z \), too. So \( \pi_j \) divides either the greatest common divisor of 2 and \( Z \) or the greatest common divisor of \( X \) and \( Z \) (in \( \mathbb{Z}[i] \)). Now \( X \) and \( Z \) are relatively prime rational integers, so that \( aX + bZ = 1 \) for some \( a, b \in \mathbb{Z} \). This implies that the greatest common divisor of \( X \) and \( Z \) as elements of the Gaussian integers is 1 as well. Therefore we can’t have \( \pi_j \) dividing \( X \). We are thus forced into the situation where 2 and \( Z \) are not relatively prime rational integers. But now \( 4 |Z^2 \) and we readily see that \( X^2 + Y^2 \) is congruent to 2 modulo 4 if both \( X \) and \( Y \) are odd (which must be the case if \( Z \) is even). This contradiction proves the validity of our claim.
Applying our claim, we see that there is some subset \( S \subseteq \{1, \ldots, n\} \) where \( \pi_j|(X + iY) \) if and only if \( j \in S \) and \( \pi_j|(X - iY) \) if and only if \( j \not\in S \). Suppose \( S \neq \emptyset \) (an entirely similar argument works otherwise); we have
\[
X + iY = u' \prod_{j \in S} \pi_j^{2e_j} = u' \alpha^2
\]
for some unit \( u' \) and \( \alpha = a + ib \in \mathbb{Z}[i] \). The units are easily seen to be \( \{1, -1, i, -i\} \). Without loss of generality, we see that
\[
X = a^2 - b^2, \quad Y = 2ab, \quad Z = a^2 + b^2
\]
for some non-negative relatively prime integers \( a, b \).

**Application #2:** Fermat’s Last Theorem for the exponent 4. This states that there are no non-trivial (meaning none of the variables may be zero) solutions in integers to the equation \( X^4 + Y^4 = Z^4 \). In fact, we’ll prove (as did Fermat so many years ago) that there are no non-trivial solutions in integers to the equation \( X^4 + Y^4 = Z^2 \).

We will prove this using the “method of descent;” essentially showing that a given solution can be used to produce a smaller solution, ultimately resulting in a contradiction since our solutions can’t “descend” ad infinitum.

Starting with a solution above, by our first application we may write
\[
X^2 = a^2 - b^2, \quad Y^2 = 2ab, \quad Z = a^2 + b^2
\]
for relatively prime positive integers \( a \) and \( b \). Now \( X^2 + b^2 = a^2 \), so that we may further write
\[
X = c^2 - d^2, \quad b = 2cd, \quad a = c^2 + d^2
\]
for relatively prime positive integers \( c \) and \( d \). We claim that \( a, c \) and \( d \) are all squares. Indeed, we have \( Y^2 = 2ab = 4acd \) where \( a, c \) and \( d \) are relatively prime. Writing \( c = (X')^2, d = (Y')^2 \) and \( a = (Z')^2 \), we have the sought-after smaller solution:
\[
(X')^4 + (Y')^4 = c^2 + d^2 = a = (Z')^2.
\]

**Theorem:** Given any \( \alpha, \beta \in \mathbb{Z}[\sqrt{-2}], \beta \neq 0 \), there are \( \phi, \rho \in \mathbb{Z}[\sqrt{-2}] \) with
\[
\alpha = \phi \beta + \rho, \quad |\rho| \leq \frac{\sqrt{3}}{2} |\beta|.
\]
In particular, \( \mathbb{Z}[\sqrt{-2}] \) is a Euclidean domain.

The proof is almost exactly the same as that for the Gaussian integers. This time our \( \mathbb{Z} \)-module in the complex plane has basis \( \beta \) and \( i\sqrt{2}\beta \). Instead of squares, we tile the plane with rectangles of diameter \( \sqrt{|\beta|^2 + |i\sqrt{2}\beta|^2} = \sqrt{3} |\beta| \).

Replacing \( \sqrt{-2} \) with \( \sqrt{-5} \) in the above argument won’t work, since now the rectangles have diameter \( \sqrt{|\beta|^2 + |i\sqrt{5}\beta|^2} = \sqrt{6} |\beta| > 2 |\beta| \). Indeed, the argument can’t work since \( \mathbb{Z}[\sqrt{-5}] \) isn’t even a unique factorization domain. The “proof” is almost trivial:
\[
6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).
\]
None of the above factors can be further factored. For example, if \(2 = \alpha \cdot \beta\) for \(\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]\), then \(|2|^2 = |\alpha|^2 |\beta|^2\) where now everything is a positive integer. But it’s simple to verify that no element \(\alpha\) of \(\mathbb{Z}[\sqrt{-5}]\) besides \(\pm 1\) has \(|\alpha|^2 < 4\).

That said, we can stretch things to the case \(\sqrt{-7}\). Here instead of looking at \(\mathbb{Z}[\sqrt{-7}]\) we consider the ring

\[
\mathbb{Z}[\alpha], \quad \alpha = \frac{1 + \sqrt{-7}}{2}.
\]

The geometric argument works once more (it’s a tad trickier since now we tile the plane with parallelograms). As to why we look at this ring rather than \(\mathbb{Z}[\sqrt{-7}]\), the answer leads us to one of the main items of investigation in MATH 681.

In this course (and in algebraic number theory in general) one is interested in the ring of integers of a number field. First, a number field is just a finite algebraic extension of the rational numbers \(\mathbb{Q}\); examples (from above) include \(\mathbb{Q}(\sqrt{-1})\) and \(\mathbb{Q}(\sqrt{-7})\). Second, the ring of integers inside such a field is the set of elements that are roots of monic polynomials with rational integer coefficients; examples (from above) include \(\sqrt{-1}\) and \(\frac{1 + \sqrt{-7}}{2}\). It’s not immediately obvious that this set is a ring. Clearly establishing that fact is an early priority.

When we consider the number field \(\mathbb{Q}(\sqrt{-3})\), we note that \(\omega = -\frac{1+\sqrt{-3}}{2}\) is an algebraic integer so, as with \(\sqrt{-7}\) above, we consider the ring \(\mathbb{Z}[\omega]\). In the exercises you prove that this ring is also a Euclidean domain, whence has unique factorization. We end our prologue with an application of this.

**Application:** Fermat’s last theorem for the exponent 3. In fact, we will show that there are no non-trivial (meaning all non-zero) solutions to

\[
\alpha^3 + \beta^3 + \zeta^3 = 0
\]

in \(\mathbb{Z}[\omega]\). (Obviously we may ask that a putative solution here be relatively prime, and we do.)

We start by considering the quotient ring \(\mathbb{Z}[\omega]/(1 - \omega)\), where \((1 - \omega)\) is the principal ideal generated by \(1 - \omega\). It’s not difficult to see that any unit \(u \in \mathbb{Z}[\omega]\) must have complex modulus 1, since all non-zero elements of our ring have complex modulus at least 1 (go back to the geometric argument if your faith is starting to weaken). Since \(|1 - \omega|^2 = 3\), obviously \(1 - \omega\) isn’t a unit; in fact, it is an irreducible element and we now write \(1 - \omega = \pi\) to help remind us of this fact. We see that our quotient ring is (isomorphic to) the field with three elements: \(\mathbb{Z}/3\mathbb{Z}\).

Now take a putative solution above and reduce modulo \(\pi\); we see that there must be exactly one of \(\alpha, \beta, \zeta\) divisible by \(\pi\) or all three congruent to 1 modulo \(\pi\) (if all three are congruent to \(-1\), just use \(-\alpha, -\beta\) and \(-\zeta\) instead). Suppose we have the latter case and write \(\alpha = 1 + \alpha' \pi\) for \(\alpha' \in \mathbb{Z}[\omega]\). Then (note \(1 - \omega^2 = \pi(1 + \omega) = -\pi\omega^2\))

\[
\alpha^3 - 1 = (\alpha - 1)(\alpha - \omega)(\alpha - \omega^2) = \alpha' \pi(\alpha' + 1 - \omega)(\alpha' + 1 - \omega^2) = \pi^3 \alpha' (\alpha' + 1)(\alpha' - \omega^2).
\]

Since \(\omega^2 \equiv 1 \mod \pi\), we see that one of \(\alpha', \alpha' + 1\), and \(\alpha' - \omega^2\) is divisible by \(\pi\), whence \(\alpha^3 \equiv 1 \mod \pi^4\). The same goes for \(\beta^3\) and \(\zeta^3\) if they are congruent to 1 modulo \(\pi\), so that

\[
0 = \alpha^3 + \beta^3 + \zeta^3 \equiv 1 + 1 + 1 \mod \pi^4.
\]

But by an assigned exercise \(\pi^2 = u3\) for some unit \(u \in \mathbb{Z}[\omega]\), so that \(\pi^4\) does not divide 3. We conclude that exactly one of \(\alpha, \beta, \) and \(\zeta\) is divisible by \(\pi\).
With the above in mind, we now write

$$\alpha^3 + \beta^3 + u\pi^{3n}\gamma^3 = 0, \quad (*)$$

where $\alpha, \beta$ and $\gamma$ are relatively prime, $u$ is a unit, and $n$ is a positive integer. We will do another descent argument: given a solution to (*) where $n > 1$, there is another with $n$ replaced by $n - 1$.

We write

$$-u\pi^{3n}\gamma^3 = \alpha^3 + \beta^3 = (\alpha + \beta)(\alpha + \omega\beta)(\alpha + \omega^2\beta).$$

Note that the differences of the factors on the right hand side are divisible by $\pi$ but not by $\pi^2$. Since $n \geq 2$, by unique factorization there is exactly one factor on the right hand side that is divisible by $\pi^2$; the other two are divisible by $\pi$. Without loss of generality (multiply by a unit if necessary) we have

$$\alpha + \beta = \pi^{3n-2}\delta_1, \quad \alpha + \omega\beta = \pi\delta_2, \quad \alpha + \omega^2\beta = \pi\delta_3,$$

where $\pi \nmid \delta_1\delta_2\delta_3$.

Now $\delta_2 - \delta_3 = \beta(\omega - \omega^2)/\pi = \omega\beta$ and $\omega\delta_3 - \omega^2\delta_2 = \alpha(\omega - \omega^2)/\pi = \omega\alpha$. Since $\omega$ is a unit and $\alpha, \beta$ are relatively prime, so are $\delta_2, \delta_3$. Similarly both $\delta_1, \delta_2$ and $\delta_1, \delta_3$ are pair-wise relatively prime. Therefore

$$-u\pi^{3n}\gamma^3 = \pi^{3n-2}\delta_1\pi\delta_2\pi\delta_3$$

$$-u\gamma^3 = \delta_1\delta_2\delta_3.$$

By unique factorization, each $\delta_i$ is some unit multiple of a cube:

$$\alpha + \beta = \pi^{3n-2}u_1\theta_1^3, \quad \alpha + \omega\beta = \pi u_2\theta_2^3, \quad \alpha + \omega^2\beta = \pi u_3\theta_3^3,$$

where the $u_i$s are units and the $\theta_i$s are relatively prime. A little algebra yields

$$\theta_1^3 + u_4\theta_2^3 + u_5\pi^{3n-3}\theta_3^3 = 0$$

for units $u_4$ and $u_5$.

To finish our descent argument, since neither $\theta_1$ nor $\theta_2$ is divisible by $\pi$, then as shown previously each of $\theta_1^3$ and $\theta_2^3$ are congruent to $\pm 1$ modulo $\pi^4$. But since $n \geq 2$ we have $\theta_1^3 + u_4\theta_2^3 \equiv 0 \mod \pi^2$, so that $\pm 1 \pm u_4 \equiv 0 \mod \pi^2$. Using an assigned exercise where you find all units, we conclude that $u_4 = \pm 1$. Replacing $\theta_2$ with $-\theta_2$ if necessary, we get our “smaller” solution to (*) as desired.

Finally, we complete our proof by showing that (*) can’t have a solution with $n = 1$. Indeed, we have

$$-u\pi^{3n}\gamma^3 = \alpha^3 + \beta^3 \equiv \pm 1 \pm 1 \mod \pi^4$$

by the same recycled argument above. If the signs are opposite here, we get $\pi^4|\pi^{3n}\gamma$, which implies that $n > 1$ since $\pi \nmid \gamma$. If the signs are the same we conclude that either $n > 1$ or $\pi|2$. Since the latter is not the case (just consider the modulus), we have $n > 1$ again.