FACTORIZATION

JULIET OLIVER

Abstract. A previous paper from this REU by Xinyu Liu[1] gave a proof of the unique factorization of ideals in a Dedekind domain. This paper will describe one "backstory" of this problem by motivating the concept of ideals as a tool for solving Diophantine equations. The content is focused on details rather than breadth or complexity in hopes of being more accessible to those without a great deal of background knowledge.

Contents

1. Motivation: Diophantine Equations and the Fundamental Theorem of Arithmetic

Definition 1.1. Let $f(x_1, x_2, \cdots, x_n)$ be a polynomial with integer coefficients. An equation of the form $f(x_1, \ldots, x_n) = 0$ is called *Diophantine* if we allow only integer solutions $x_1, \cdots, x_n \in \mathbb{Z}$.

Consider the Diophantine equation

$$y^2 = x^3 + 4.$$

Readers with their fair share of middle school arithmetic and algebra likely won't have any trouble solving it. However, we are not interested in the solution so

Date: 22 August 2023.

much as its structure. To motivate the problem of this paper, let us solve the equation by factoring, paying particular attention to the assumptions made at each step.

1.1. **The Structure of our Approach: Solving $y^2 = x^3 + 4$.**

The first thing to notice is that $4 = 2^2$ is a square in the integers. Thus the above equation is equivalent to $y^2 - 4 = (y-2)(y+2) = x^3$. We will first prove a lemma.

Lemma 1.2. *If y is odd, then $(y-2)$ and $(y+2)$ are coprime in $\mathbb{Z}$.*

Proof. Let y be an odd integer. Suppose $m \in \mathbb{Z}$ is a common divisor of $(y-2)$ and $(y+2)$, i.e. $m|(y-2)$ and $m|(y+2)$. Then, m must also divide their difference, so $m|(y+2-(y-2))$ and thus $m|4$. However, 4 is a power of two while both $(y-2)$ and $(y+2)$ are odd, so it must be the case that $|m| = 1$. Since $(y-2)$ and $(y+2)$ share no common factors other than 1 and -1, they must be coprime. □

Now, we take advantage of a useful propery of $\mathbb{Z}$: the Fundamental Theorem of Arithmetic.

Theorem 1.3 (Fundamental Theorem of Arithmetic)**.** *Every integer greater than* 1 *can be represented uniquely as the product of primes, up to reordering.*

Claim 1.1. *If $(y-2)$ and $(y+2)$ are coprime integers and their product is a cube of an integer, then $(y-2)$ and $(y+2)$ are both cubes.*

Proof. Let $x^3 = (y-2)(y+2)$ for $(y-2)$, $(y+2)$ coprime. Since x is assumed to be an integer, by Theorem 1.3, we can factor x as

$$x = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$$

for some primes $p_1, \cdots, p_n \in \mathbb{Z}$. We assume without loss of generality that $p_1, \cdots, p_n$ are distinct. Our equation gives $(y-2)(y+2) = p_1^{3e_1} \cdots p_n^{3e_n}$.

Let $i \in \{1, \cdots, n\}$. Since p_i is prime, p_i must divide either $(y-2)$ or $(y+2)$. Suppose, without loss of generality, that p_i is a factor of $(y-2)$. Then since $(y-2)$ and $(y+2)$ are coprime, p_i cannot be a factor of $(y+2)$. By uniqueness of the prime factorization of $x^3 = (y-2)(y+2)$, we must have $\left(p_i^{e_i}\right)^3 \mid (y-2)$. This is true for all $i \in \{1, \cdots, n\}$, so we can write each of $(y-2)$, $(y+2)$ as the product of cubes of prime integers of the form $\left(p_i^{e_i}\right)^3$. Hence, $(y-2)$ and $(y+2)$ must both be cubes of integers. □

Now, let $y - 2 = a^3$ and $y + 2 = b^3$ for some $a, b \in \mathbb{Z}$. This gives

$$4 = b^3 - a^3 = (b-a)(b^2 + ab + a^2).$$

There are finitely many factors of 4 so all that remains is case work to find a and b from which we can derive solutions for x and y. However, we said at the beginning that the solution is not what we're after. So, what was the point of this exercise?

Recall the steps that we took. First, we noticed that 4 is a square in $\mathbb{Z}$ and used this fact to rewrite the left hand side of the original equation as the difference of squares. A natural question we might ask is: what if our equation doesn't factor so nicely in $\mathbb{Z}$? For instance, what if we wanted to solve the equation $y^2 = x^3 - 4$? To use our method of factorization, we need to construct a ring in which -4 is a square.

2. Unique Factorization Domains

2.1. Adjoining Algebraic Integers to $\mathbb{Z}$.

Up until this point we have been relying on readers' intuitive understanding of the integers. Before proceeding, let us add clarity with a few definitions.

Definition 2.1. A ring $(R, +, \cdot)$ is a set R equipped with two binary operations $+$ and $\cdot$ satisfying the following axioms.

(1) $(R, +)$ is a commutative group.
(2) There exists an element $1 \in R$ such that for all $r \in R$, $r1 = 1r = r$. We refer to 1 as the *multiplicative identity* of R.
(3) For all $a, b, c \in R$, we have:
   (a) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,
   (b) $a \cdot (b + c) = a \cdot b + a \cdot c$,
   (c) $(a + b) \cdot c = a \cdot c + b \cdot c$.

If additionally, for every $a, b \in R$, we have $a \cdot b = b \cdot a$, then R is called a *commutative ring.*

A *subring* of $(R, +, \cdot)$ is a subset $H \ni 1$ such that $(H, +|_{H \times H}, \cdot|_{H \times H})$ is a ring with multiplicative identity 1. We write $H \leq R$.

Remark 2.2. Observe that the set of complex numbers $\mathbb{C}$ forms a commutative ring under usual addition and multiplication. In this paper, for simplicity, we will work only with subrings of $\mathbb{C}$.

Back to our second Diophantine equation $y^2 + 4 = x^3$. To imitate our previous approach, we want to work with the "smallest" subring of $\mathbb{C}$ in which -4 (and hence -1) is a square. Equivalently, we want to work with the "smallest" subring of $\mathbb{C}$ containing $i = \sqrt{-1}$. To talk about such rings formally, we need the following definition.

Definition 2.3. Let S be a subset of $\mathbb{C}$. *The subring of* $\mathbb{C}$ *generated by* S, denoted $\mathbb{Z}[S]$, is defined as the intersection of all subrings of $\mathbb{C}$ containing S. (Note that the intersection of subrings of $\mathbb{C}$ is again subring of $\mathbb{C}$.) We also call $\mathbb{Z}[S]$ the subring of $\mathbb{C}$ obtained by *adjoining* S to $\mathbb{Z}$.

When $S = \{s\}$ is a simpleton set, we write $\mathbb{Z}[s]$ instead of $\mathbb{Z}[\{s\}]$.

Example 2.4. It is not hard too see that $\mathbb{Z}[i] = \{f(i) \mid f \in \mathbb{Z}[x]\}$. One can further show that $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ i.e. elements of $\mathbb{Z}[i]$ are exactly linear combinations of 1 and i with integer coefficients.

Over $\mathbb{Z}[i]$, the left hand side of our second Diophantine equation factors as

$$y^2 - (-4) = (y - 2i)(y + 2i)$$

. Thus the equation gives two factorization $(y - 2i)(y + 2i) = x^3$ of the same element of $\mathbb{Z}[i]$. To continue imitating our approach in the previous case, we want to generalize the notions of *prime* and *coprime* in $\mathbb{Z}$ to an arbitrary subring of $\mathbb{C}$.

2.2. Primes and Irreducibles in Subrings of $\mathbb{C}$.

In this section we will discuss various notions related to factorization and divisibility.

Remark 2.5. Note that while we restrict our attention to subrings of $\mathbb{C}$ for concreteness, the definitions and propositions below hold more generally for any *integral domains.* Recall that an *integral domain* R is a commutative ring in which the product of any two nonzero elements is nonzero. Consequently, one can perform "cancellation" in R: for every $a, b, c \in R$, if $ab = ac$ and $a \neq 0$ then $b = c$.

To begin with, we define divisibility and use this to formalize the notion of a unit.

Definition 2.6. Let $R \leq \mathbb{C}$. Take $a, b \in R$, $a \neq 0$. We say that a *divides* b in R and use the notation $a \mid_R b$ if there exists $c \in R$ such that $ac = b$.

Notation 2.7. For ease of reading, we will drop the subscript R in $\mid_R$ when there is no risk of confusion.

Definition 2.8. Let $R \leq \mathbb{C}$ and take $a, b \in R$. An element $g \in R$ is called a *greatest common divisor* of a and b, if for all $r \in R$, $r \mid_R a$ and $r \mid_R b$ if and only if $r \mid_R g$. We write $g = \gcd(a, b)$. (Note that this is an abuse of notation, since g is not necessarily unique.)

Definition 2.9. Let $R \leq \mathbb{C}$. The set of *units* of R, denoted R^*, consist of all $u \in R$ for which there exists $v \in R$ such that $uv = 1$. Equivalently, the units of R are exactly the elements of R that divide 1.

An element $a \in R$ is said to be *associated* to an element $b \in R$ if $a = bu$ for some $u \in R^*$. Observe that a is associated to b iff b is associated to a, in which case we call a and b *associates*.

Example 2.10. $\mathbb{Z}^* = \{\pm 1\}$.

Now we have the tools to define a prime element and irreducible elements of a subring of $\mathbb{C}$. These are two distinct generalizations of the concept of integer primes.

Definition 2.11. Let $R \leq \mathbb{C}$. We say that $\pi \in R$ is *prime* if $\pi \notin R^*$ and for every $a, b \in R$, $\pi | ab$ iff $\pi | a$ or $\pi | b$.

Definition 2.12. Let $R \leq \mathbb{C}$. We say that $\pi \in R$ is *irreducible* if $\pi \notin R^*$ and for every $a, b \in R$, $\pi = ab$ implies that at least one of a or b must be a unit.

In the case of the integers, these two notions coincide (see Proposition 2.18 below). However, for a general ring $R \leq \mathbb{C}$, only one of the implications necessarily holds.

Property 2.13. Let $R \leq \mathbb{C}$. If $\pi \in R$ is prime, then π is irreducible.

Proof. Let R be a subring of $\mathbb{C}$ and let $\pi \in R$ be prime. Suppose $\pi = ab$ for some $a, b \in R$. Then, $\pi | ab$, so $\pi | a$ or $\pi | b$. Suppose, without loss of generality, that $\pi | a$. Then, there exists $c \in R$ such that $\pi c = a$, so $\pi = ab = \pi cb$. As R is an integral domain and $\pi \neq 0$ (by definition of prime), we can "cancel" π from both sides to obtain $cb = 1$. In particular, b is a unit. Thus, π is irreducible. □

The converse of the above proposition does not hold in general. In Example 2.16 below, we show that $\mathbb{Z}[\sqrt{-5}]$ contains an irreducible that is not prime. To that end, we introduce the *norm* function.

Definition 2.14. Let D be a squarefree integer congruent to 3 modulo 4. On $\mathbb{Z}[\sqrt{D}]$, we can define the *norm* function $N : \mathbb{Z}[\sqrt{D}] \to \mathbb{Z}$ by

$$N(a + b\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2$$

for all $a, b \in \mathbb{Z}$.

Observation 2.15. It is easy to check that the norm function N satisfies the following properties:

1. N is multiplicative;
2. $N(u) = 1$ iff $u \in R^*$;
3. if $N(\pi)$ is an integer prime then π must be irreducible in R.

Example 2.16. We claim that 2 is irreducible but not prime in $\mathbb{Z}[\sqrt{-5}]$.

Indeed, to see that 2 is irreducible in $\mathbb{Z}[\sqrt{-5}]$, suppose $2 = (a+b\sqrt{-5})(c+d\sqrt{-5})$ for some $a, b, c, d \in \mathbb{Z}$. By multiplicativity of N, we have

$$4 = N(2) = N(a + b\sqrt{-5})N(c + d\sqrt{-5}) = (a^2 + 5b^2)(c^2 + 5d^2).$$

By examining the integer factors of 4, one can show that either (a^2+5b^2) or (c^2+5d^2) must be a unit.

Now, suppose for contradiction that 2 is a prime in $\mathbb{Z}[\sqrt{-5}]$. Then, as 2 divides $6 = (1 - \sqrt{-5})(1 + \sqrt{-5})$, 2 must divide either $1 - \sqrt{-5}$ or $1 + \sqrt{-5}$. Equivalently, one of (and hence both of) $\frac{1}{2} \pm \frac{1}{2}\sqrt{-5}$ must lie in $\mathbb{Z}[\sqrt{-5}]$. In particular, there exist $m, n \in \mathbb{Z}$ such that $m + n\sqrt{-5} = \frac{1}{2} + \frac{1}{2}\sqrt{-5}$, i.e. $\left(\frac{1}{2} - m\right) + \left(\frac{1}{2} - n\right)\sqrt{-5} = 0$. As 1 and $\sqrt{-5}$ are linearly independent over $\mathbb{Q}$, this implies $m = n = \frac{1}{2}$, contradicting the assumption that $m, n \in \mathbb{Z}$. Thus, 2 is not prime in $\mathbb{Z}[\sqrt{-5}]$.

On the other hand, as previously mentioned, over $\mathbb{Z}$, the concepts of irreducibility and primeness are equivalent. To prove this, we first recall the following consequence of the Euclidean Algorithm for the integers.

Lemma 2.17 (Bezout's Lemma)**.** *Let $a, b \in \mathbb{Z}$ have greatest common divisor c. Then, there exist integers $x, y \in \mathbb{Z}$ such that $ax + by = c$.*

Proof. A proof is given in [2, page 6]. □

Proposition 2.18. *An integer $\pi \in \mathbb{Z}$ is prime iff it is irreducible.*

Proof. By Proposition 2.13, it suffices to show that irreducible integers are prime. Let $\pi \in \mathbb{Z}$ be irreducible. Suppose that $\pi | ab$ for some $a, b \in \mathbb{Z}$ but $\pi \nmid a$. We let $g = \gcd(a, \pi)$. Then, $g|\pi$, so there exists $c \in \mathbb{Z}$ such that $gc = \pi$.

We claim that g is a unit. Indeed, suppose by contradiction that g is not a unit. Then $c \in \mathbb{Z}^* = \{\pm 1\}$, by irreducibility of π. Thus $\pi = gc = \pm g$ must divide a, contradicting our assumption.

By Lemma 2.17, there exist $x, y \in \mathbb{Z}$ such that $ax + \pi y = g = \pm 1$. Multiplying both sides by b gives $abx + \pi by = \pm b$. Since $\pi | ab$, we can write $ab = \pi d$ for some $d \in \mathbb{Z}$. Thus $\pm b = abx + \pi by = \pi(dx + by)$, so $\pi | b$. This shows that π is prime. □

Observe that, given an appropriate definition of greatest common divisors, the above proof works for any ring $R \leq \mathbb{C}$ for which Bezout's Lemma hold. This turns out to be the case when R is a *unique factorization domain*, which is the topic of the next section.

2.3. **Properties of Unique Factorization Domains.**

Definition 2.19. A *unique factorization domain* (henceforth abbreviated as UFD) is an integral domain R such that all nonzero elements $x \in R$ factor uniquely as $x = up_1 \cdots p_n$ for some unit u, irreducibles p_i, and $n \geq 0$. Uniqueness here means that if $x = wq_1 \cdots q_m$ for some unit w, irreducibles q_i, and $m \geq 0$, then $m = n$ and there exists a bijection $\phi : \{1, \cdots, n\} \to \{1, \cdots, m\}$ such that p_i is associated to $q_{\phi(i)}$ for $i \in \{1, \cdots, n\}$. We call each p_i a *prime factor* of x. Note that the prime factors of x are uniquely determined, up to associates.

Proposition 2.20. *$\mathbb{Z}[i]$ is a UFD.*

Proof. A very readable proof of this fact is given in [2, 41-44]. □

Recall where we left our most recent Diophantine equation, $y^2 = x^3 - 4$. We factor over $\mathbb{Z}[i]$ to get $(y - 2i)(y + 2i) = x^3$. In the very first example, we used the Fundamental Theorem of Arithmetic to show that $(y - 2)$ and $(y + 2)$ must both be cubes. We can use this same technique in $\mathbb{Z}[i]$ because it is a UFD.

Definition 2.21. Let R be a UFD and $a, b \in R$. We call a and b *coprime* if they have no common prime factors.

Proposition 2.22. *Let R be a UFD. Let $a, b \in R$. Then a and b are coprime if and only if* $\gcd(a, b)$ *is a unit.*

Proof. Suppose a and b are coprime. We show that every common divisor of a and b must be a unit. To this end, let g be an element of R dividing both a and b. Since R is a UFD, we can write $a = u \cdot p_1 \cdots p_s$ and $b = w \cdot q_1 \cdots q_t$ for primes p_i, q_j and units u, w of R. Because $g|a$, there exists $c \in R$ such that $gc = a = p_1 \cdots p_s$.

We show that $p_i \mid c$ for all i. Indeed, fix $i \in \{1, \ldots, s\}$. Since a and b are coprime, p_i cannot divide b. Thus $p_i \nmid g$ as $g \mid b$. As p_i is prime, this implies that $p_i \mid c$. As this holds for all prime factors p_i of a, we must have $a \mid c$, so that $c = ha$ for some $h \in R$. Cancelling $a \neq 0$ from both sides of $gha = gc = a$ gives $gh = 1$. Thus g is a unit.

The other direction is somewhat more straightforward. Suppose $u = \gcd(a, b)$ is a unit. Suppose for contradiction that a, b have a common prime factor π. Then, $\pi \mid u$ by definition of the gcd. Since u is a unit, there exists $w \in R$ such that $wu = 1$. However, $\pi \mid u$ implies that there exists $c \in R$ such that $wc\pi = u$ and thus $wc\pi = wu = 1$. In particular, π must be a unit, contradicting the assumption that π is prime. Hence, a and b are coprime. □

Theorem 2.23. *Let R be a UFD. Let $a_1, \cdots, a_s \in R$ be pairwise coprime. Suppose $a_1 \cdots a_s = b^n$ for some $b \in R$. Then, a_i are associated to n-powers in R. In other words, for all $i \in \{1, \cdots, s\}$, there exist $l_i \in R$ and $u_i \in R^*$ such that $a_i = u_i l_i^n$.*

Proof. The same argument as in the proof Claim 1.1 applies. □

Now we finally have the tools to solve $(y - 2i)(y + 2i) = x^3$ just as we solved its counterpart in the integers. Using the norm we can show for odd y that $(y - 2i)$ and $(y + 2i)$ must be coprime. This proof also follows similarly to its counterpart, Lemma 1.2, but the use of the norm makes it an instructive example so it is included.

Claim 2.1. *Let y be an odd integer. Then, $(y - 2i)$ and $(y + 2i)$ are coprime in $\mathbb{Z}[i]$.*

Observation 2.24. By considering the common prime factors, it is not hard to show that every pair of elements in a UFD has a greatest common divisor.

Proof. Let y be an odd integer. Let $(a+bi), a, b \in \mathbb{Z}$ be a greatest common divisor of $y-2i$ and $y+2i$ in $\mathbb{Z}[i]$. Then, $(a+bi)$ divides their difference, which is $4i$. Taking norms gives $(a^2+b^2)|(y^2+4)$ and $(a^2+b^2)|16$ in $\mathbb{Z}$. By assumption, y is odd and hence so is y^2+4. But 16 is a power of two and thus $N(a+bi) = a^2+b^2 = 1$. By Observation 2.15, $(a+bi)$ is a unit. Thus, by Proposition 2.22, $(y-2i)$ and $(y+2i)$ are coprime, as claimed. □

Now, Theorem 2.23, implies that $(y-2i)$ and $(y+2i)$ are cubes in $\mathbb{Z}[i]$. In particular, we can write $y+2i = (a+bi)^3$ for some $a, b \in \mathbb{Z}$. Expanding the right hand side gives

$$\begin{aligned} y + 2i &= (a+bi)^3 \\ &= a^3 + 3a^2bi + 3ab^2(-1) + b^3(-i) \\ &= a^3 - 3ab^2 + (3a^2b - b^3)i. \end{aligned}$$

Since 1 and i are linearly independent over $\mathbb{Q}$, we can then conclude that $y = a^3 - 3ab^2$ and $2 = 3a^2b - b^3 = (3a^2 - b^2)b$. By enumerating the finitely many integer factors of 2, we can solve for a and b, and consequently for x and y.

We have now been able to solve two Diophantine equations using factorization and some nice properties of UFDs. But, as we saw in Example 2.16, not all subrings of $\mathbb{C}$ are UFDs. What are we to do if we are presented with a Diophantine equation such as $y^2 = x^3 - 5$, where $y^2 + 5$ can only be factored in $\mathbb{Z}[\sqrt{-5}]$? We have seen that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD because not all irreducibles are primes, so how might we solve this? Studying problems such that this is what inspired Ernst Kummer's notion of ideals numbers which were later formalized as *ideals*.

3. Ideals

3.1. **What is an ideal?**

The balance of the paper will be guided in part by solving our final Diophantine equation, $y^2 = x^3 - 5$, which, as mentioned above, can be factored as

$$x^3 = (y - \sqrt{-5})(y + \sqrt{-5})$$

in $\mathbb{Z}[\sqrt{-5}]$. But, elements of this ring may have multiple distinct factorizations into irreducibles

Example 3.1. Consider $6 \in \mathbb{Z}[\sqrt{-5}]$. We can write the factors of 6 in $\mathbb{Z}[\sqrt{-5}]$ as $6 = 2 \cdot 3 = (1-\sqrt{-5})(1+\sqrt{-5})$, both of which are factorizations into irreducibles in $\mathbb{Z}[\sqrt{-5}]$. Since $N(2) = 4$, $N(3) = 9$, $N(1-\sqrt{-5}) = N(1+\sqrt{-5}) = 6$, we see that these two factorizations are distinct.

Before formalizing the notion of ideals, we must first give a few definitions.

Definition 3.2. Let R be a ring. An R-module is an additive group $(M, +)$ together with a "scalar multiplication" map $R \times M \to M$ such that for all $a, b \in R$ and $\mathbf{x}, \mathbf{y}, \mathbf{z} \in M$, the following properties hold (here we denote the image of (r, m) by rm):

$$\begin{array}{cc} \mathbf{x} + \mathbf{y} = \mathbf{y} + \mathbf{x} & (ab)\mathbf{x} = a(b\mathbf{x}) \\ \mathbf{x} + (\mathbf{y} + \mathbf{z}) = (\mathbf{x} + \mathbf{y}) + \mathbf{z} & 1\mathbf{x} = \mathbf{x} \\ \mathbf{x} + \mathbf{0} = \mathbf{x} & \mathbf{x}(a+b) = a\mathbf{x} + b\mathbf{x} \\ \mathbf{x} + -\mathbf{x} = \mathbf{0} & a(\mathbf{x} + \mathbf{y}) = a\mathbf{x} + a\mathbf{y} \end{array}$$

An R-*submodule* of M is an R-subgroup of M that is an R-module under the restriction of the scalar multiplication map on M.

With this, we can now define ideals and some of their properties. We will use the formal definition given below, but it is perhaps more intuitive to think of an ideal as a module, so keep the above definition in mind.

Definition 3.3. Let R be a ring. Then R can be viewed as a module over itself. An *ideal* of R is simply an R-submodule of R. In other words, a subgroup $\mathcal{I}$ of $(R, +)$ is called an *ideal* of R if it is closed under multiplication by elements of R, i.e., for all $r \in R$, $r \cdot \mathcal{I} \subseteq \mathcal{I}$.

Notation 3.4. As in the definition above, script capitals (e.g. $\mathcal{A}, \mathcal{B}, \mathcal{I}, \mathcal{P}$) will be used to denote ideals.

Definition 3.5. Let $S \subset R$. We define the *ideal of R generated by S*, denote $\langle S\rangle$ as the intersection if all ideals of R containing S. Equivalently, $\langle S\rangle$ is the smallest ideal of R containing S, if we order ideals of R by inclusion.

We denote the ideal generated by elements $a_1, \cdots, a_n \in R$ by $\langle a_1, \cdots, a_n\rangle$. A *principal ideal* is an ideal that can be generated by a single element.

Notation 3.6. Let R be a domain.

Example 3.7.

$$\langle 2\rangle = 2\mathbb{Z} = \{\cdots, -6, -4, -2, 0, 2, 4, 6, \cdots\}$$
$$\langle 4, 6\rangle = 6\mathbb{Z} + 4\mathbb{Z} = \{4m + 6n \mid m, n \in \mathbb{Z}\} = \{\cdots, -6, -4, -2, 0, 2, 4, 6, \cdots\}$$

Notice that $\langle 2\rangle = \langle 4, 6\rangle$. This is in fact because $2 = \gcd(4, 6)$. We will see that the ideal is a nice generalization of the concept of gcd. Next, we will find out what it means for ideals to be prime and coprime.

3.2. **Prime and Coprime Ideals.**

First, we define the product of ideals and use this to define a prime ideal.

Definition 3.8. Let $\mathcal{A}$ and $\mathcal{B}$ be ideals of a ring R.

The *product* $\mathcal{AB}$ of $\mathcal{A}$ and $\mathcal{B}$ is defined as the ideal generated by elements of the form ab for some $a \in \mathcal{A}$ and $b \in \mathcal{B}$. In other words,

$$\mathcal{AB} = \{a_1b_1 + \cdots + a_nb_n \mid a_i \in \mathcal{A}, b_i \in \mathcal{B}, n \in \mathbb{N}\}.$$

The *sum* $\mathcal{A} + \mathcal{B}$ of $\mathcal{A}$ and $\mathcal{B}$ is defined as the ideal generated by elements of the form $a + b$ for some $a \in \mathcal{A}$ and $b \in \mathcal{B}$.

Definition 3.9. Let R be a ring. We call an ideal $\mathcal{P} \subseteq R$ a *prime ideal* if $\mathcal{P} \neq R$ and for all $\mathcal{I}, \mathcal{J} \subseteq R$, $\mathcal{P} \supseteq \mathcal{IJ}$ implies $\mathcal{P} \supseteq \mathcal{I}$ or $\mathcal{P} \supseteq \mathcal{J}$.

Notice that this definition is similar to that of primes in a UFD but with "divides" replaced by "contains." When it comes to ideals, "to divide is to contain" captures the intuition behind this definition. Let's look at an example in the integers.

Example 3.10. Observe that in $\mathbb{Z}$, $d|m$ iff $\langle d\rangle \ni m$ or $\langle d\rangle \supseteq \langle m\rangle$.

Proposition 3.11. *Let $\mathcal{P} = \langle p \rangle$ be a principle ideal of a ring R generated by some prime element $p \in R$. Then $\mathcal{P}$ is a prime ideal.*

Proof. Let $\mathcal{A}, \mathcal{B} \subseteq R$ be such that $\mathcal{AB} \subseteq \mathcal{P}$. Suppose by contradiction that neither $\mathcal{A}$ nor $\mathcal{B}$ is contained in $\mathcal{P}$, i.e. there exist $a \in \mathcal{A} \backslash \mathcal{P}$ and $b \in \mathcal{B} \backslash \mathcal{P}$. Thus $p \nmid a$ and $p \nmid b$, so $p \nmid ab$, as p is prime. Thus ab is an element of $\mathcal{AB}$ not contained in $\mathcal{P}$, contradicting our assumption.

□

As before, now that we have a notion of prime ideals, we want to expand this to formulate the notion of coprime ideals. Previously, we did this using the gcd, and now we get to see the very nice relationship between ideals and gcd mentioned earlier.

In Example 3.7 we saw that the ideal generated by 2 is equal to that generated by 4 and 6 since we can express 2 as $4m + 6n$ for some $m, n \in \mathbb{Z}$. We saw in Lemma 2.17 that this is a property of the gcd, and in fact, the gcd of two ideals is just their sum! Let's formalize this.

Definition 3.12. Let $\mathcal{I}$ and $\mathcal{J}$ be ideals of a ring R. An ideal $\mathcal{A}$ of R is said to be a *greatest common divisor* of $\mathcal{I}$ and $\mathcal{J}$, denoted $\gcd(\mathcal{I}, \mathcal{J})$, if for all ideals $\mathcal{B}$ of R, we have $\mathcal{B} \supset \mathcal{I}$ and $\mathcal{B} \supset \mathcal{J}$ iff $\mathcal{B} \supset \mathcal{A}$.

Theorem 3.13. *Let $\mathcal{I}, \mathcal{J}$ be ideals of a ring R. Then, $\gcd(\mathcal{I}, \mathcal{J}) = \mathcal{I} + \mathcal{J}$. In other words, $\mathcal{I} + \mathcal{J}$ is the smallest ideal of R containing both $\mathcal{I}$ and $\mathcal{J}$.*

Proof. Clear. □

Definition 3.14. Two ideals $\mathcal{I}, \mathcal{J}$ of a ring R are *coprime* if $\mathcal{I} + \mathcal{J} = R = \langle 1 \rangle$.

Recall that two integers are coprime if their gcd is equal to 1. Consider how this is analogous to the definition of coprime ideals; we have seen previously that the sum of two ideals of a ring R of algebraic integers is equal to their gcd, so if their sum is $\langle 1 \rangle$, i.e. the entire ring, then they are coprime!

Before proceeding to the next section, we will formally define what it means for an ideal to divide another ideal and from this give an alternate but equivalent definition of coprime. To do so, we first give an overview of the notion of a Dedekind domain.

Definition 3.15. Let R be a ring. Then R is called a *Dedekind domain* if R contains a nontrivial ideal (i.e. a nonzero ideal that is not the whole of R) and if for all ideals $\mathcal{I}$ and $\mathcal{J}$ of R, we have $\mathcal{I} \subseteq \mathcal{J}$ if and only if, $\mathcal{I} = \mathcal{J}\mathcal{J}'$ for some ideal $\mathcal{J}' \subseteq R$.

Theorem 3.16. *Let R be a Dedekind domain. Then, every nonzero ideal $\mathcal{I}$ of R factors as a product of nonzero prime ideals $\mathcal{I} = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_n^{e_n}$ with $e_1, \cdots, e_n \in \mathbb{Z}_{\geq 0}$ and this factorization is unique up to reordering. We call $\mathcal{P}_i$'s the* prime factors *of $\mathcal{I}$.*

Proof. This is the subject of the paper referenced in the abstract by Xinyu Liu [1]. See below. □

3.3. **Dedekind Domains.** In order to continue solving our Diophantine equation, we will need to use some properties not just of the commutative rings we have been discussing, but of a *Dedekind Domain.* The definition and proofs of properties of a Dedekind domain as they relate to our use of ideals require exposition beyond the scope of this paper and are covered in another paper from this REU by Xinyu Liu[1], as well as in Stillwell[2]. The goal of this paper is to see why such properties are useful rather than to repeat their exposition.

3.4. nth Power Law for Ideals.

Let's check in with our latest Diophantine equation, $x^3 = (y - \sqrt{-5})(y + \sqrt{-5})$. We find by a similar argument to Claim 2.1 that $(y - \sqrt{-5})$ and $(y + \sqrt{-5})$ must be coprime. So, our next step is to prove something akin to the nth power law (Theorem 2.23) for ideals. But first, a few more results about ideals.

Lemma 3.17. *Let $\mathcal{I}_1$ and $\mathcal{I}_2$ be pairwise coprime ideals of a Dedekind domain R. If a prime ideal $\mathcal{P} \supseteq I_1$ of R, then $\mathcal{P} \not\supseteq \mathcal{I}_2$.*

Proof. Suppose by contradiction that $\mathcal{P} \supseteq \mathcal{I}_2$. Then, since $\mathcal{P}$ is closed under addition, $\mathcal{P} \supset \mathcal{I}_1 + \mathcal{I}_2 = R$ (contradiction). □

Theorem 3.18 (nth Power Law for Ideals)**.** *Let $\mathcal{I}_1, \cdots, \mathcal{I}_s$ be coprime ideals of a Dedekind domain R. Suppose $\mathcal{I}_1 \cdots \mathcal{I}_s = \mathcal{J}^n$ for some ideal $\mathcal{J}$ of R. Then each $\mathcal{I}_j$ must be an nth power of some ideal of R.*

Proof. Since R is a Dedekind domain, we can factor $\mathcal{J}$ as $\mathcal{J} = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_t^{e_t}$ for some distinct prime ideals $\mathcal{P}_1, \cdots, \mathcal{P}_t$ of R.

We show that $\mathcal{I}_1$ is the n-th power of some ideals of R. The same argument applies for the rest of the $\mathcal{I}_j$. By uniqueness of the prime factorization of $\mathcal{J}^n$ (cf. Theorem 3.16), all the prime factors of $\mathcal{I}_1$ must appear amongst the $\mathcal{P}_j$. By relabeling, assume that $\mathcal{P}_1, \ldots, \mathcal{P}_s$, $s \leq t$ are the prime factors of $\mathcal{I}_1$. By Lemma 3.17, $\mathcal{P}_1, \ldots, \mathcal{P}_s$ do not contain $\mathcal{I}_j$ for any $j \neq 1$. In particular, they do not appear in the prime factorizations of $\mathcal{I}_j$ for any $j \neq 1$. Again by uniqueness of the prime factorization of $\mathcal{J}^n$, we must have that $\mathcal{I}_1 = \mathcal{P}_1^{ne_1} \cdots \mathcal{P}_s^{ne_2} = (\mathcal{P}_\infty{}^{e_1} \cdots \mathcal{P}_\int{}^{e_s})^n$ is an n-th power, as claimed.

□

Definition 3.19. Let R be a domain. We call an ideal $\mathcal{I}$ of R *maximal* if it is contained only by the domain and itself. Returning once again to the intuition "to divide is to contain," we would say that the only divisors of $\mathcal{I}$ are $R = \langle 1 \rangle$ and $\mathcal{I}$.

Remark 3.20. Note that maximal ideals are prime. Consult [2] for a proof.

Example 3.21. Consider the domain $\mathbb{Z}$. The maximal ideals of $\mathbb{Z}$ are all of the ideals generated by prime elements of $\mathbb{Z}$. For example, $\langle 5 \rangle$ is a principle ideal because the only divisors of 5 are units and 5 itself.

Lemma 3.22. *Let $\mathcal{I}_1$ and $\mathcal{I}_2$ be ideals of a domain R such that $\mathcal{I}_1$ and $\mathcal{I}_2$ have no common factor. Then, $\mathcal{I}_1$ and $\mathcal{I}_2$ are coprime.*

Proof. Let $\mathcal{I}_1$ and $\mathcal{I}_2$ be ideals of a domain R such that $\mathcal{I}_1$ and $\mathcal{I}_2$ have no common factor. Suppose $\mathcal{I}_1 + \mathcal{I}_2 \neq R$. Then, there exists a maximal ideal $\mathcal{P} \subseteq R$ such that $\mathcal{I}_1 + \mathcal{I}_2 \subseteq \mathcal{P}$.[1] However, recall that the gcd of two ideals is their sum and $\mathcal{I}_1$ and $\mathcal{I}_2$ have no common factor, so $\mathcal{I}_1 + \mathcal{I}_2 \not\subseteq \mathcal{P}$. Hence, $\mathcal{I}_1 + \mathcal{I}_2 = R$, that is to say, $\mathcal{I}_1$ and $\mathcal{I}_2$ are coprime. □

[1] this fact is not obvious and requires some additional background knowledge which is not particularly useful for the rest of the paper and is thus ommitted. Consult [2] or [3].

Now, we return to the equation $x^3 = y^2 + 5$. Recall that we factored $y^2 + 5$ in $\mathbb{Z}[\sqrt{-5}]$ and now we replace these factors with ideals to get

$$\langle y + \sqrt{-5}\rangle\langle y - \sqrt{-5}\rangle = \langle x\rangle^3.$$

What remains is to show that $\langle y + \sqrt{-5}\rangle$ and $\langle y - \sqrt{-5}\rangle$ are coprime.

Claim 3.1. *Let $\langle y + \sqrt{-5}\rangle\langle y - \sqrt{-5}\rangle = \langle x\rangle^3$. Then, $\langle y + \sqrt{-5}\rangle$ and $\langle y - \sqrt{-5}\rangle$ are coprime.*

Proof. Let $\langle y + \sqrt{-5}\rangle\langle y - \sqrt{-5}\rangle = \langle x\rangle^3$. Suppose, for contradiction, that there exists a prime ideal $\mathcal{P} \subseteq \mathbb{Z}[\sqrt{-5}]$ such that $\mathcal{P} \supseteq \langle y - \sqrt{-5}\rangle$ and $\mathcal{P} \supseteq \langle y + \sqrt{-5}\rangle$. Then, $\mathcal{P} \ni x$ and $\mathcal{P} \ni 2\sqrt{-5}$. Because $\mathcal{P}$ is closed under addition and multiplication by scalars, $\mathcal{P} \ni 2\sqrt{-5}\sqrt{-5} = -10$ and thus $\mathcal{P} \supseteq \langle -10, x\rangle$. We find that x must be odd, so $1 = \gcd(-10, x)$ (we can find by casework that $x \neq 5$ and $x \neq -5$). Since $\mathcal{P} \supseteq \langle -10, x\rangle$, this implies $\mathcal{P} \supseteq \langle 1\rangle$ and thus $\mathcal{P} = R$ (contradiction). Thus, $\langle y + \sqrt{-5}\rangle$ and $\langle y - \sqrt{-5}\rangle$ have no common factors so by Lemma 3.22, they are coprime. □

Finally, we can show that $\langle y + \sqrt{-5}\rangle$ and $\langle y - \sqrt{-5}\rangle$ are cubes in $\mathbb{Z}[\sqrt{-5}]$ using the nth power law for ideals, Theorem 3.18. With that, we have found analogous tools to those used to solve our very first Diophantine equation, $y^2 = x^3+4$, to solve the similarly simple-looking but much trickier equation $y^2 = x^3-5$. It happens that this equation and the ring in which it factors are special cases that have simplified our task, but delving into these topics (in particular, class groups) is beyond the scope of this paper. However, there is much to be gained by studying this special case! With any luck, this paper has given you a deeper appreciation for some properties of the integers which we may take for granted, a concrete motivation for the construction of the ideals, and a glimpse of one of the many ways in which they can be useful.

Acknowledgments

It is my immense pleasure to thank my mentor, Zana Tran, for so many things: her time and dedication to guiding me through many topics before I knew what I wanted to write about, her clear and thoughtful lectures and mentorship meetings, her adaptability to my various interests and backgrounds, and her bottomless enthusiasm for answering any question I might ask. She is an exceptional teacher and I am truly grateful to have worked with her. Next I would like to thank my mentorship group: Ray, Richard, Oliver, and Will, for struggling through problems with me and for their patience when explaining their solutions. Thank you to Professor Rudenko and Professor Babai for their excellent courses in the REU Apprentice Program–their instruction laid the foundation for my understanding much of the material for this paper–and to Professor May for organizing the program as a whole and for advocating for math exposition.

References

[1] Xinyu Liu. Unique Factorization of Ideals in a Dedekind Domain, University of Chicago REU.

[2] John Stillwell. Algebraic Number Theory for Beginners, Cambridge University Press, https://doi.org/10.1017/9781009004138.

[3] Saban Alaca. Introduction to Algebraic Number Theory, Cambridge University Press.

[4] Kazuya Kato. Number Theory 1, American Mathematical Society.