Unique Factorization in Quadratic Fields

Timothy Cho

June 2024

1. Prologue: Three Nice Properties of the Integers

The ring of integers, $\mathbb{Z}$, is nice — that is why number theory cares about it. For example, we can divide with remainder, which we learned in grade school, and is ubiquitous across all of number theory:

Theorem 1.1 (Division Algorithm)**.** *Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then there exist unique $q, r \in \mathbb{Z}$, with $0 \leq r < b$, with $a = bq + r$.*

Recall that given a ring R, an ideal I is an additive subgroup of R such that $ra, ar \in I$ for all $a \in I$ and $r \in R$, and we write $I \trianglelefteq R$. This gives us another nice thing about the integers: every ideal of $\mathbb{Z}$ is generated by one element. We prove this by using the division algorithm.

Proposition 1.2. *Let $I \trianglelefteq \mathbb{Z}$ be an ideal. Then $I = n\mathbb{Z}$ for some $n \in \mathbb{Z}$.*

Proof. If $I = \{0\}$ this is trivial. Otherwise, I contains a nonzero integer a, so it contains $1 \cdot a$ and $-1 \cdot a = -a$. One of these is positive, so I contains a positive element, so take $d \in \mathbb{Z}^+$ to be the smallest positive integer that is contained in I. We claim $I = d\mathbb{Z}$. To see this, clearly $d\mathbb{Z} \subseteq I$ because $d \in I$, so take $b \in I$. By the division algorithm, write $b = qd + r$ for $q, r \in \mathbb{Z}$ with $0 \leq r < b$. It suffices to show $b = 0$; for contradiction suppose $b > 0$. Then $r = b - qd \in I$, contradicting the minimality of d. Hence $I = d\mathbb{Z}$. □

Finally, the most famous property of the integers is that every integer has a unique prime factorization. We will give a proof of this later, when we deduce something more general.

Theorem 1.3 (Fundamental Theorem of Arithmetic)**.** *Let $n \geq 2$ be an integer. Then n can be factored into a product of primes $n = p_1 p_2 \cdots p_r$, and this factorization is unique, in that if $n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$, where the p_i and q_j are prime, then $r = s$ and up to some rearrangement of the primes, we have $p_i = q_i$ for all $1 \leq i \leq r = s$.*

These are fairly convenient properties. However, are there any other rings other than $\mathbb{Z}$ which satisfy such nice properties? Also, are any of these stronger than the others? To answer these questions, let us make a few definitions.

Definition 1.4. Let R be a ring. We say that a function $N : R \to \mathbb{N}$ is a *norm* on R if $N(0) = 0$. If $N(a) > 0$ whenever $a \neq 0$, we say that N is a *positive norm*.

Intuitively, the norm is a measure of "size" on the ring R, though it need not satisfy any nice properties at all. However, having a norm means we can state that some elements are "smaller" than others, which may help us introduce a division algorithm on a general ring R. Recall that a unital ring R is an integral domain if the *zero-product property* holds, i.e., if $a, b \in R$ satisfy $ab = 0$, then either $a = 0$ or $b = 0$.

Definition 1.5. Let R be an integral domain. We say that R is an *Euclidean domain* if there exists a norm $N : R \to \mathbb{N}$ such that for any two elements $a, b \in R$, there exist $q, r \in R$ with

$$a = bq + r, \text{ where } N(b) < N(r) \text{ or } r = 0.$$

That is, an Euclidean domain is simply an environment where we can do a division algorithm. To give our prototypical example, $\mathbb{Z}$, with respect to the usual norm (absolute value), is Euclidean. Another familiar Euclidean domain is $\mathbb{R}[x]$, the ring of polynomials with real coefficients. Here, the norm is given by taking the degree of a polynomial, and the division algorithm is our familiar polynomial long division. We will see more examples, but let us examine the other two properties of $\mathbb{Z}$ more closely first.

Definition 1.6. Let R be a ring. We say that an ideal $I \trianglelefteq R$ is *principal* if I is generated by one element: i.e., $I = (a)$ for some $a \in I$. An integral domain R whose ideals are all principal is called a *principal ideal domain*, or *PID* for short.

It turns out that being Euclidean is being stronger than being a PID. The proof is essentially the same as it was for integers, except for our minimality arguments, we use the norm instead.

Proposition 1.7. *Every Euclidean domain is a principal ideal domain.*

Proof. Let R be a Euclidean domain with respect to some norm N. Take $I \trianglelefteq R$. If $I = \{0\}$, this is obvious, so suppose I is nonzero. Since the codomain of the norm N is the set of natural numbers $\mathbb{N}$, take a nonzero element of minimal norm, and call it d. We claim $I = (d)$. Again, we clearly have $I \supseteq (d)$, so we just need to show the other inclusion. Take $b \in I$. Then by the division algorithm on R, write $b = qd + r$ for $q, r \in R$ with $N(r) < N(d)$. If $r \neq 0$, then $r = b - qd \in I$, which contradicts the minimality of d with respect to the norm, so we must have $r = 0$. Hence $I \subseteq (d)$, so $I = (d)$ and thus I is principal. □

However, not every principal ideal domain is a Euclidean domain — [1], Section 8.2 gives the gnarly example $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$, with an equally gnarly proof. The reason why someone might care about this will be made evident later, but it is not of primary importance.

2. Primes, Irreducibles, and Factorization

The most interesting property of $\mathbb{Z}$ is its unique factorization. Technically, we only stated unique factorization for integers $n \geq 2$: when $n = 1, 0$ there is nothing to do, but negative numbers are slightly problematic. For example,

$$-12 = (-2) \times 2 \times 3 = (-2) \times (-2) \times (-3) = 1 \times (-2) \times 2 \times 3 = (-1) \times 2 \times 2 \times 3 = \cdots,$$

but clearly, these "alterations" are immaterial — multiplying by ± 1 does nothing except for "change the sign" in $\mathbb{Z}$, and replacing p with $-p$ also does the same thing. However, these notions over $\mathbb{Z}$ are difficult to generalize because it deals with the idea of *sign*, which requires the idea of an *ordering* on a ring. To get around this, notice that ± 1 are the only integers with integer multiplicative inverses. This suggests a more careful codification of what we just discussed, in precise terms:

Definition 2.1. Let R be an integral domain.

1. We say that $u \in R$ is a *unit* if it has a multiplicative inverse in R, i.e., there is some $v \in R$ with $uv = 1$.
2. We say $r, s \in R$ are *associate* if there is a unit $u \in R$ such that $s = ru$, and we write $r \sim s$.

It is readily checked that $\sim$ is an equivalence relation on R. Now, we define what it means for an element to be "prime" in an integral domain. Unfortunately, there are two competing notions, which may or may not be the same in a general integral domain:

Definition 2.2. Let R be an integral domain.

1. Let $a, b \in R$. We say a *divides* b if $b = ka$ for some $k \in R$, and write $a \mid b$.
2. If $p \in R \setminus \{0\}$ is not a unit, we say that p is *prime* if whenever $p \mid ab$, then $p \mid a$ or $p \mid b$. Alternatively, p is prime if (p) is a prime ideal.
3. If $r \in R \setminus \{0\}$ is not a unit, we say that r is *irreducible* if whenever $r = ab$ for $a, b \in R$, then either a or b is a unit.

These definitions should be completely natural to us, though the definition of "prime" is not what we are used to seeing — for the integers $\mathbb{Z}$, it is Euclid's Lemma. However, it is taken for definition in an arbitrary integral domain. We now see the relationship between these two definitions of "prime."

Proposition 2.3. *In an integral domain, all prime elements are irreducible.*

Proof. Let R be an integral domain and take $p \in R \setminus \{0\}$ to be a non-unit. Suppose $p = ab$ for $a, b \in R$. Since p is prime, either $p \mid a$ or $p \mid b$. Without loss of generality, write $a = pk$ for some $k \in R$, so $p = ab = pkb$. Cancelling $p \neq 0$, we have $1 = kb$, so k is a unit and b is a unit. Hence, p is irreducible. □

However, not all irreducible elements are prime, and we will exhibit an example later. However, for PIDs, the reverse inclusion actually holds, though we will also see this later. But with these definitions, we now state what it means for an integral domain to have unique factorization.

Definition 2.4. A *unique factorization domain*, or *UFD* for short, is an integral domain R in which every nonzero, non-unit element $r \in R$ has a factorization $r = p_1 p_2 \cdots p_t$, where the p_i are irreducibles in R, and this factorization is unique, in that if $r = p_1 p_2 \cdots p_t = q_1 q_2 \cdots q_s$ for irreducibles $p_i, q_j \in R$, we have $t = s$ and up to some reordering of the irreducibles, we have $p_i \sim q_i$ for all $1 \leq i \leq t = s$.

That is, a UFD is any environment where the "Fundamental Theorem of Arithmetic" holds — notice that we have the slightly weaker condition $p_i \sim q_i$, but being associate is analogous to two numbers "differing in sign" in $\mathbb{Z}$.

Example 2.5. Consider the ring $\mathbb{Z}[2i] = \{a + 2bi : a, b \in \mathbb{Z}\}$. We claim that $\mathbb{Z}[2i]$ is not a UFD. Notice that 2 and $2i$ are irreducibles, and $2 \not\sim 2i$ (notice $i \notin \mathbb{Z}[2i]$), yet $4 = 2(2) = (2i)(-2i)$ gives distinct factorizations. Hence, $\mathbb{Z}[2i]$ is not a UFD.

The next result tells us that primes and irreducibles are the same — at least in a UFD. Hence, after we prove this result, we will only use the word "prime" unless we are explicitly working with a ring that is not a UFD.

Proposition 2.6. *In a UFD, an element is prime if and only if it is irreducible.*

Proof. We know that prime elements are irreducible, so take $r \in R$, and suppose $p \mid ab$ for some $a, b \in R$. Hence, we may write $ab = pk$ for some $k \in R$. Now, we may factor a, b into irreducibles, say $a = p_1 p_2 \cdots p_t$ and $b = q_1 q_2 \cdots q_s$, for irreducibles $p_i, q_j \in R$, so that

$$pk = p_1 p_2 \cdots p_t q_1 q_2 \cdots q_s.$$

Since p is irreducible, it follows that p must be associate to one of the p_i or the q_j. Without loss of generality, just suppose $p \sim p_1$, so $p = up_1$ for some unit $u \in R$. It follows that $pu^{-1} = p_1$, so $a = p_1 p_2 \cdots p_r = (u^{-1}p)p_2 p_3 \cdots p_r$, so $p \mid a$ and we are done. □

Next, we prove that every PID is a UFD. But to do this, we need the following lemma, which tells us about primes and irreducibles in PIDs. It might seem strange that we are proving this separately, but the proof that "PID implies UFD" uses this lemma.

Lemma 2.7. *In a PID, an element is prime if and only if it is irreducible.*

Proof. Again, we just need to show all irreducibles are prime. Let R be a PID and let $p \in R$ be irreducible. We show that $P := (p) \trianglelefteq R$ is a prime ideal. In fact, we show something stronger: P is a maximal ideal. Let M be any ideal containing P; since R is a PID, we set $M := (m)$. Certainly, $p \in M$ so that $p = km$ for some $k \in R$. But since p is irreducible, either k is a unit or m is a unit. If m is a unit, then $(m) = R$, but if k is a unit, we have $m \sim p$ and thus $(m) = (p)$. Hence (p) is maximal, and hence prime. □

Now, we finally prove our main theorem, which will give us this chain of inclusions:

$$\text{Euclidean domains} \subsetneq \text{PIDs} \subsetneq \text{UFDs} \subsetneq \text{Integral domains}.$$

Theorem 2.8. *Every PID is a UFD.*

Proof. The proof of this may be boiled down into two words: just factor. Let R be a PID, and take $r \in R \setminus \{0\}$ to be a non-unit. By Lemma 2.7, we can replace every instance of the word "irreducible" with prime in the following text. If r is prime, we are done. If not, write $r = r_1 r_2$. Then, look at r_1 and r_2 and factor them if they are prime: for example, $r_1 = r_3 r_4$. Now, look at r_3 and factor it if needed: $r_3 = r_5 r_6$. Doing so, we get many divisibility relations

$$\cdots \mid r_{2k+1} \mid \cdots \mid r_7 \mid r_5 \mid r_3 \mid r_1 \mid r.$$

The only thing we need to do is to make sure that this process terminates. If this process never terminates, then we always have "proper" factorizations, corresponding to proper ideal inclusions

$$(r) \subsetneq (r_1) \subsetneq (r_3) \subsetneq (r_5) \subsetneq \cdots .$$

We show that such a strictly increasing chain of ideals does not exist in a PID in general.[1] Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq R$ be an increasing chain of ideals, and consider the ideal $I := \bigcup_{k=1}^{\infty} I_k$. Since R is a PID, write $I = (a)$, so that $a \in I_n$ for some $n \in \mathbb{Z}^+$. But now this forces $I = I_n = I_{n+1} = \cdots$, so the chain stabilizes. Hence, our factorization algorithm must terminate, and so a factorization into primes exists.

Now, we need to demonstrate that this factorizations are unique. We proceed by the number of prime factors of r. If r has one prime factor, this is obvious, and assume inductively that unique factorization holds for all elements with less than n factors. Let $r = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_s$, where $p_i, q_j \in R$ are primes. Since all irreducibles in a PID are prime, we see that $p_1 \mid q_1 q_2 \cdots q_s$ implies $p_1 \mid q_j$ for some j; without loss of generality, take $j = 1$. But since p_1 and q_1 are both prime, so $p_1 \sim q_1$, so write $q_1 = up_1$. Cancelling, we see $p_2 p_3 \cdots p_n = q_2 q_3 \cdots q_s$. This is an element with $n-1$ factors on the left, which forces $n = s$ and, up to rearrangement, $p_i \sim q_i$. This completes the proof. □

Example 2.9. Are all UFDs necessarily PIDs? No — take the polynomial ring $\mathbb{Z}[x]$. We are familiar with the fact that polynomials with integer coefficients factor uniquely (though we will not prove this), but the ideal $(2, x)$ is not principal — if it were, then $(2, x) = (f(x))$ for some $f(x) \in \mathbb{Z}[x]$, so $2 = a(x)f(x)$ and $x = b(x)f(x)$. The first equation forces $f(x)$ to be a constant, so we have $f(x) = \pm 1, \pm 2$. Clearly, $f(x) \neq \pm 1$, so we must have $f(x) = \pm 2$, but solving yields $b(x) = \pm \frac{1}{2} x \notin \mathbb{Z}[x]$, a contradiction.

3. Quadratic Fields and Quadratic Integers

Now, with all of the theoretical framework, we introduce the main objects we will work with.

Definition 3.1. Let $D \neq 0, \pm 1$ be a squarefree integer. We define the *quadratic field* $\mathbb{Q}(\sqrt{D})$ to be the set

$$\mathbb{Q}(\sqrt{D}) := \left\{ a + b\sqrt{D} : a, b \in \mathbb{Q} \right\} \subseteq \mathbb{C},$$

where the field addition is regular addition and the field multiplication is regular multiplication.

It is readily verified that $\mathbb{Q}(\sqrt{D})$ is actually a field, and we leave this to the reader, and whenever we mention $\mathbb{Q}(\sqrt{D})$ as a quadratic field, we will assume $D \neq 0, \pm 1$ and D is squarefree. To every quadratic number field, we associate the following three important functions.

Definition 3.2. Let $\mathbb{Q}(\sqrt{D})$ be a quadratic field. If $\alpha = a + b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$, we define the following:

1. The *conjugate* $\bar{\alpha}$ is given by $\bar{\alpha} = a - b\sqrt{D}$.
2. The *field norm* $N(\alpha)$ is given by $N(\alpha) := \alpha\bar{\alpha} = a^2 - Db^2$.
3. The *trace* $T(\alpha)$ is given by $T(\alpha) := \alpha + \bar{\alpha} = 2a$.

We should not confuse the field norm with the norm used to define Euclidean domains — for example, the field norm is allowed to go negative! However, they do coincide at times. We now give some examples.

Example 3.3. Let $x = 3 + \sqrt{3}$ and $y = -1 + 7\sqrt{3}$ in $\mathbb{Q}(\sqrt{3})$. Then we may compute

$$\begin{aligned} xy &= (3 + \sqrt{3})(-1 + 7\sqrt{3}) = 18 + 20\sqrt{3}, \\ N(x) &= 3^2 - 3 \cdot 1^2 = 6 = (3 + \sqrt{3})(3 - \sqrt{3}), \\ N(y) &= (-1)^2 - 3 \cdot 7^2 = -146 = (-1 + 7\sqrt{3})(-1 - 7\sqrt{3}), \\ N(xy) &= 18^2 - 3 \cdot 20^2 = -876. \end{aligned}$$

We notice that $-876 = -146 \cdot 6$. This is in fact something that holds in general, and is actually a result that was known since antiquity (though, of course, they never referred to it using norms of quadratic fields):

[1] That is, a PID is a *Noetherian* ring.

Proposition 3.4 (Brahmagupta–Fibonacci Identity)**.** *Let $\mathbb{Q}(\sqrt{D})$ be a quadratic field. Then the field norm N is multiplicative: $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in \mathbb{Q}(\sqrt{D})$.*

Proof. Let $\alpha = a + b\sqrt{D}$ and $\beta = c + d\sqrt{D}$, where $a, b, c, d \in \mathbb{Q}$. Then

$$N(\alpha)N(\beta) = (a^2 - Db^2)(c^2 - Dd^2) = (a^2c^2 + b^2d^2D^2) - (b^2c^2 - a^2d^2)D.$$

On the other hand, $\alpha\beta = (a + b\sqrt{D})(c + d\sqrt{D}) = (ac + bdD) + (bc + ad)\sqrt{D}$, so

$$\begin{aligned} N(\alpha\beta) &= (ac + bdD)^2 - D(bc + ad)^2 \\ &= a^2c^2 + 2abcdD + b^2d^2D^2 - D\left[b^2c^2 + 2abcd + a^2d^2\right] \\ &= a^2c^2 + \cancel{2abcdD} + b^2d^2D^2 - b^2c^2D - \cancel{2abcdD} - a^2d^2D \\ &= (a^2c^2 + b^2d^2D^2) - (b^2c^2 + a^2d^2)D, \end{aligned}$$

which matches the expression we got for $N(\alpha)N(\beta)$, so the proof is complete. □

In this new environment, quadratic fields play the role of rational numbers, which are nice and all, but they could not be as nice as the integers. Hence, we now try to define what it means for a number to be a "quadratic integer." To do this, we take a look at the rational numbers again. Algebraically, all rational numbers are roots to linear polynomials $ax + b$ with coefficients $a, b \in \mathbb{Z}$, with $a \neq 0$:

$$ax + b = 0 \implies x = -\frac{b}{a}.$$

This is not too big of a surprise, and if $a = 1$ (i.e., the linear polynomial is *monic*), we get an integer solution. Similarly, it is not too hard to see that every quadratic integer is a root of a quadratic with integer coefficients. Notice that if $\alpha \in \mathbb{Q}(\sqrt{D})$, then we multiply

$$(x - \alpha)(x - \bar{\alpha}) = x^2 - (\alpha + \bar{\alpha})x + \alpha\bar{\alpha} = x^2 - T(\alpha)x + N(\alpha).$$

Certainly, $T(\alpha)$ and $N(\alpha)$ are *rational numbers*, so clearing denominators if necessary tells us that α is a root of some quadratic $ax^2 + bx + c$, with $a, b, c \in \mathbb{Z}$ and $a \neq 0$. We define quadratic integers analogously:

Definition 3.5. Let $\alpha \in \mathbb{C}$. We say that α is a *quadratic integer* if α is the root of a monic polynomial with integer coefficients; i.e., there exist $b, c \in \mathbb{Z}$ such that $x^2 + bx + c$ has α as a root.

In fact, our work above tells us that if α is a quadratic integer, then $b = T(\alpha)$ and $c = N(\alpha)$; to say this differently, *if α is quadratic integer, then $T(\alpha) \in \mathbb{Z}$ and $N(\alpha) \in \mathbb{Z}$*. This allows us to prove the following:

Theorem 3.6 (Characterization of Quadratic Integers)**.** *Let $\mathbb{Q}(\sqrt{D})$ be a quadratic number field. Then the quadratic integers in $\mathbb{Q}(\sqrt{D})$, denoted $\mathcal{O}$, are exactly*

$$\mathcal{O} = \begin{cases} \left\{a + b\sqrt{D} : a, b \in \mathbb{Z}\right\} & m \equiv 2, 3 \bmod 4 \\ \left\{\frac{a+b\sqrt{D}}{2} : a, b \in \mathbb{Z} \text{ and } a \equiv b \bmod 2\right\} & m \equiv 1 \bmod 4. \end{cases}$$

Proof. Fix some quadratic number field $\mathbb{Q}(\sqrt{D})$, and take $\alpha = r + s\sqrt{D}$ with $r, s \in \mathbb{Q}$ to be a quadratic integer. Then we saw that $T(\alpha) = 2r \in \mathbb{Z}$ and $N(\alpha) = r^2 - Ds^2 \in \mathbb{Z}$. Multiplying the second equation by 4, we see $4N(\alpha) = (2r)^2 - 4Ds^2$ implies $4Ds^2 \in \mathbb{Z}$, and since D is squarefree by assumption, $4s^2 \in \mathbb{Z}$, and taking square roots, $2s \in \mathbb{Z}$. Hence, let $a := 2r$ and $b := 2s$, so that $a, b \in \mathbb{Z}$. Since $N(\alpha) = r^2 - Ds^2$ is an integer, multiplying everything by 4 again gives $4N(\alpha)a^2 - Db^2$, and reducing modulo 4 gives $0 \equiv a^2 - Db^2 \iff a^2 \equiv Db^2 \pmod 4$. At this point, take cases modulo 4.

Case I: $D \equiv 1 \pmod 4$. In this case, $a^2 \equiv b^2 \pmod 4$, so either $a \equiv b \equiv 0 \pmod 2$ or $a \equiv b \equiv 1 \pmod 2$. In either case, $a \equiv b \pmod 2$, so back-substituting, we see that algebraic integers take the form $\frac{1}{2}(a+b\sqrt{D})$, where $a \equiv b \pmod 2$. We check that these are indeed quadratic integers: if $x = \frac{1}{2}(a+b\sqrt{D})$, then $2x = a+b\sqrt{D}$ implies $2x-a = b\sqrt{D}$. Squaring yields $4x^2-4ax+a^2 = b^2D \iff 4x^2-4ax+(a^2-b^2D) = 0$,

and now note $a^2 - b^2 D \equiv 0 \pmod 4$, so we may divide out by 4 to obtain a polynomial $x^2 + Bx + C$, where $B, C \in \mathbb{Z}$.

Case II: $D \equiv 2 \pmod 4$. In this case, $a^2 \equiv 2b^2 \pmod 4$, which is only possible if a and b are both even. Hence, r and s are both integers, so quadratic integers take the form $r + s\sqrt{D}$, for $r, s \in \mathbb{Z}$. We leave it to the reader to verify that these are indeed integers.

Case III: $D \equiv 3 \pmod 4$. In this case, $a^2 \equiv 3b^2 \equiv -b^2 \pmod 4$, but this is only possible again if a and b are both even, so this reduces to Case II. This completes the casework, and thus the proof. □

Corollary 3.7. *Let $\mathbb{Q}(\sqrt{D})$ be a quadratic number field. Then $\mathcal{O}$ is a subring of $\mathbb{Q}(\sqrt{D})$ with $\mathcal{O} = \mathbb{Z}[\omega]$, where*

$$\omega = \begin{cases} \sqrt{D} & D \equiv 2, 3 \bmod 4 \\ \frac{1+\sqrt{D}}{2} & D \equiv 1 \bmod 4. \end{cases}$$

Proof. This is clear if $D \equiv 2, 3 \pmod 4$, so assume $D \equiv 1 \pmod 4$. We can check that $\mathcal{O}$ is closed under addition and multiplication directly, but we circumvent this by showing the equality $\mathcal{O} = \mathbb{Z}[\omega]$ first. Take $\frac{a+b\sqrt{D}}{2} \in \mathcal{O}$, so $a \equiv b \pmod 2$. Then $\frac{a+b\sqrt{D}}{2} = \frac{a-b}{2} + b\left(\frac{1+\sqrt{D}}{2}\right) \in \mathbb{Z}[\omega]$ as $\frac{1}{2}(a-b)$ is an integer. Similarly, if $x + y\omega \in \mathbb{Z}[\omega]$, we check that $x + y\omega = x + y\left(\frac{1+\sqrt{D}}{2}\right) = \frac{(2x+y)+y\sqrt{D}}{2}$, and certainly $2x + y \equiv y \pmod 2$ so $x + y\omega \in \mathcal{O}$, so $\mathbb{Z}[\omega] = \mathcal{O}$. Now, $\mathbb{Z}[\omega]$ is a ring: it is obviously closed under addition, and if $a + b\omega, c + d\omega \in \mathbb{Z}[\omega]$, we have $(a + b\omega)(c + d\omega) = ac + (bc + ad)\omega + bd\omega^2$, but now it is not too hard to check $\omega^2 = \frac{D^2+1+2\sqrt{D}}{4} = \frac{D-1}{4} + \omega \in \mathbb{Z}[\omega]$ as $D \equiv 1 \pmod 4$. □

Now that we have quadratic integers, we can ask about divisibility relationships among different integers: given a quadratic integer ring $\mathcal{O}$, which elements are prime or irreducible, and which are units? We first observe the following proposition, which demonstrates the importance of the field norm N:

Lemma 3.8. *Let $\mathcal{O}$ be a quadratic integer ring. If $\alpha \mid \beta$ in $\mathcal{O}$, then $N(\alpha) \mid N(\beta)$ in $\mathbb{Z}$.*

Proof. Suppose $\alpha \mid \beta$ in $\mathcal{O}$. Then $\beta = \alpha\gamma$ for some $\gamma \in \mathcal{O}$. But now the norm is multiplicative: $N(\beta) = N(\alpha\gamma) = N(\alpha)N(\gamma)$, so that $N(\alpha) \mid N(\beta)$. □

The next proposition follows painlessly:

Proposition 3.9. *Let $\mathcal{O}$ be a quadratic integer ring. Then $\alpha \in \mathcal{O}$ is a unit if and only if $N(\alpha) = \pm 1$.*

Proof. Suppose α is a unit in $\mathcal{O}$, and let $\beta \in \mathcal{O}$ be its multiplicative inverse. Then $1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta)$, and since $N(\alpha)$ and $N(\beta)$ are integers, we see $N(\alpha) = \pm 1$. Conversely, suppose $N(\alpha) = 1$. Then by definition of the norm, $N(\alpha) = \alpha\bar{\alpha} = 1$, so $\bar{\alpha} = \alpha^{-1}$ and α is a unit. □

The classification of prime and irreducible elements is slightly more tricky. To this end, we state the following result.

Proposition 3.10. *Let $\mathcal{O}$ be a quadratic integer ring, and take $\pi \in \mathcal{O}$. If $N(\pi)$ is a prime number in $\mathbb{Z}$, then π is irreducible in $\mathcal{O}$.*

Proof. Suppose $\pi = \alpha\beta$, so by multiplicativity of the norm, $N(\pi) = N(\alpha)N(\beta)$. But $N(\pi)$ is prime, so either $N(\alpha) = \pm 1$ or $N(\beta) = \pm 1$, i.e., one of α or β is a unit. This implies π is irreducible. □

We now view some examples.

Example 3.11. Consider the quadratic field $\mathbb{Q}(\sqrt{3})$ again. Evidently, $3 \equiv 3 \pmod 4$, so we have the ring of integers $\mathcal{O} = \mathbb{Z}[\sqrt{3}]$. Let us consider the units in $\mathbb{Z}[\sqrt{3}]$, which are precisely the elements $a + b\sqrt{3}$ with $a^2 - 3b^2 = 1$, where $a, b \in \mathbb{Z}$. We know how to solve this — this is Pell's equation (with its negative) for $D = 3$. We take care of the case $a^2 - 3b^2 = -1$ first; notice that reducing modulo 3 yields $a^2 \equiv -1 \pmod 3$, which has no solutions. Hence, the units in $\mathbb{Z}[\sqrt{3}]$ can be classified by all solutions to the Pell equation $a^2 - 3b^2 = 1$. Guessing at small integers, we see $(a, b) = (2, 1)$ is a solution, and it is not too hard to see that it is the solution with the smallest integer solution. Hence, a whole infinite set of units is given by $(2 + \sqrt{3})^k$ as well as the conjugates $(2 - \sqrt{3})^k$.

Generalizing this, it follows that if $\mathbb{Q}(\sqrt{D})$ is a real quadratic field, then Pell's Equation Theorem tells us that its associated ring of integers $\mathbb{Z}[\omega]$ has infinitely many units.

Example 3.12. Let $D = -5$, and consider the imaginary quadratic field $\mathbb{Q}(\sqrt{-5}) = \mathbb{Q}(i\sqrt{5})$. Since $-5 \equiv 3 \pmod 4$, we have the ring of integers $\mathcal{O} = \mathbb{Z}[i\sqrt{5}]$. Again, let us consider the units in $\mathcal{O}$, which are precisely the elements $a + bi\sqrt{5}$ with $a^2 + 5b^2 = 1$, where $a, b \in \mathbb{Z}$. We can just guess at the solutions: $(a, b) = (\pm 1, 0)$, so it follows that there are only two units in $\mathbb{Z}[i\sqrt{5}]$, namely ± 1.

Another interesting thing about $\mathbb{Z}[i\sqrt{5}]$ is the fact that it is not a UFD. For example, 6 has two factorizations into irreducibles:

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

These two factorizations are indeed genuinely different, as 2 is not associate to either $1 + i\sqrt{5}$ or $1 - i\sqrt{5}$. We verify that, for example, $1 + i\sqrt{5}$ is indeed irreducible. First, notice that $N(1 + i\sqrt{5}) = 6$, so if $1 + i\sqrt{5} = \alpha\beta$ for $\alpha, \beta \in \mathbb{Z}[i\sqrt{5}]$, we must have $6 = N(\alpha)N(\beta)$. Clearly, $N \geq 0$ here, and it is easily checked that the equations $x^2 + 5y^2 = 2, 3$ have no solutions. Hence, we either have $N(\alpha) = 1$ or $N(\beta) = 1$, i.e., either α or β is a unit. Hence, $1 + i\sqrt{5}$ is indeed irreducible. Also, we remark that 2 is irreducible yet not prime: we have $2 \mid (1 + i\sqrt{5})(1 - i\sqrt{5})$, yet $2 \nmid 1 \pm i\sqrt{5}$.

Example 3.13. The idea of using the multiplicativity of the norm to our advantage is helpful in factoring things into irreducibles. For example, consider the quadratic integer ring $\mathbb{Z}[i\sqrt{2}]$, which we accept on faith is a UFD. Notice that the norm $N(a + bi\sqrt{2}) = a^2 + 2b^2$ is always non-negative, so that the units are exactly the elements with norm 1, which are only ± 1. Say that we want to factor the quadratic integer $-10 + 7i\sqrt{2}$ into irreducibles. First, note $N(-10 + 7i\sqrt{2}) = 198 = 2 \cdot 3^2 \cdot 11$. If we have $-10 + 7i\sqrt{2} = \alpha\beta$, then $N(\alpha), N(\beta) \mid (-10 + 7i\sqrt{2})$. It is easily verified that there are no elements of norm 2 in $\mathbb{Z}[i\sqrt{2}]$. We try an element of order 3 (which is irreducible), like $-1 + i\sqrt{2}$:

$$\frac{-10 + 7i\sqrt{2}}{-1 + i\sqrt{2}} = 8 + i\sqrt{2},$$

so indeed $-1 + i\sqrt{2} \mid -10 + 7i\sqrt{2}$. Now, $N(8 + i\sqrt{2}) = 198/3 = 66 = 2 \cdot 3 \cdot 11$, so we again try $-1 + i\sqrt{2}$ again to get $8 + i\sqrt{2} = (-1 + i\sqrt{2})(-2 - 3i\sqrt{2})$, with $N(-2 - 3i\sqrt{2}) = 66/3 = 22 = 2 \cdot 11$. We claim that we are done: if $-2 - 3i\sqrt{2}$ were reducible, then we have $-2 - 3i\sqrt{2} = \gamma\delta$ where $N(\gamma) = 2$ and $N(\delta) = 11$, but there are no elements of norm 2, so $-2 - 3i\sqrt{2}$ is irreducible. Hence, the full prime factorization is

$$-10 + 7i\sqrt{2} = -(1 - i\sqrt{2})^2(2 + 3i\sqrt{2}),$$

where we have taken the liberty of flipping signs as we wish.

Of course, we remark that this method is not very helpful if the norm of a given quadratic integer has a lot of prime factors, or is very large.

4. An Application: Gaussian Integers and Sums of Squares

In this section, we present an extended study of the ring $\mathbb{Z}[i]$, also known as the *Gaussian integers*, and we will prove a familiar result. First, we claim that $\mathbb{Z}[i]$ is a Euclidean domain and hence it is a UFD:

Theorem 4.1. *The Gaussian integers $\mathbb{Z}[i]$ form a Euclidean domain with respect to its field norm $N(a+bi) = a^2 + b^2$.*

Proof. Take $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$. We claim that there exists elements $q, r \in \mathbb{Z}[i]$ such that $\alpha = q\beta + r$, where $N(r) < N(b)$. It suffices to find $\gamma \in \mathbb{Z}[i]$ such that $N(\alpha - \beta\gamma) < N(\beta)$, after replacing γ for q and moving everything to one side. Now, dividing over by $N(\beta)$ gives

$$N\left(\frac{\alpha - \beta\gamma}{\beta}\right) < N(1) = 1 \iff N\left(\frac{\alpha}{\beta} - \gamma\right) < 1,$$

so take $\xi := \alpha/\beta \in \mathbb{Q}(i)$. [Notice that we are now working over the entire field, not just the ring of integers]. If we can find such a ξ, then we are done, as all of these steps are reversible. But now, if $\xi = x + yi$, where $x, y \in \mathbb{Q}$, just round x and y to respective closest integers u, v, so that if we set $\gamma := u + vi \in \mathbb{Z}[i]$, we have that

$$N(\xi - \gamma) = N\big((x - u) + (y - v)i\big) = (x - u)^2 + (y - v)^2 \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2} < 1.$$

This shows that $\mathbb{Z}[i]$ is Euclidean. □

Example 4.2. To see an example of the division algorithm, let us divide $1+12i$ by $7+4i$, with remainder. First, as in our proof, we compute the division in $\mathbb{Q}(i)$ and then round,

$$\frac{1+12i}{7+4i} = \frac{(1+12i)(7-4i)}{7^2+4^2} = \frac{7+48+(84-4)i}{65} = \frac{11+16i}{13} \approx 1+i,$$

so we get $1+12i = (1+i)(7+4i)+(-2+i)$. Indeed, $N(-2+i) = 5 < 65 = N(7+4i)$, which tells us that we did something right.

Now, recall that the we proved the result about sums of squares for primes first; that is, we asked, which primes p take the form $p = a^2+b^2$, for $a, b \in \mathbb{Z}$? Now, we can rephrase this question by factoring over $\mathbb{Z}[i]$: which primes can be factored $p = (a+bi)(a-bi)$? Alternatively stated, we are really asking whether a regular integer prime $p \in \mathbb{Z}$ "stays prime" in the larger ring $\mathbb{Z}[i]$. If p does not stay prime, then we say that p *splits*[2] and thus gives us a solution to $p = a^2+b^2$. If p remains prime in $\mathbb{Z}[i]$, we say that p is *inert* and thus $p \neq a^2+b^2$. Hence, to solve the two-squares problem, it suffices to determine the prime (= irreducible) elements in $\mathbb{Z}[i]$. To do this, we need the help of the following three lemmas.

Lemma 4.3. *The units in $\mathbb{Z}[i]$ are ± 1 and $\pm i$.*

Proof. This is obvious. □

Lemma 4.4 (Quadratic Reciprocity, First Supplement)**.** *Let p be an odd prime. Then -1 is a quadratic residue modulo p if and only if $p \equiv 1 \pmod 4$.*

For a (boring) number-theoretic proof of this statement, refer to [3]. For fun, we present a purely algebraic proof, due to [1].

Proof. Suppose -1 is a quadratic residue modulo p. Then viewing everything in $\mathbb{F}_p$, there exists $n \in \mathbb{F}_p$ with $n^2 = -1$, so $n^4 = 1$. Hence, n has order 4 in $\mathbb{F}_p^\times$, so by Lagrange's Theorem, $4 \mid |\mathbb{F}_p^\times| = p-1$.

Conversely, suppose $p \equiv 1 \pmod 4$, so $4 \mid p-1$. First, -1 is the unique element of multiplicative order 2 in $\mathbb{F}_p$, as the polynomial $x^2-1 \in \mathbb{F}_p[x]$ has exactly two roots, namely ± 1. Now, consider the quotient group $\mathbb{F}_p^\times / \langle -1 \rangle$, which has order $\frac{1}{2}(p-1)$. By assumption, $\frac{1}{2}(p-1)$ is even, so by Cauchy's Theorem, $\mathbb{F}_p^\times / \langle -1 \rangle$ has a subgroup of order 2. By the correspondence (or lattice) isomorphism theorem, this subgroup takes the form $H / \langle -1 \rangle$, where $H \leq \mathbb{F}_p^\times$ has order $2 \cdot 2 = 4$. There are two groups of order 4: either $H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $H \cong \mathbb{Z}/4\mathbb{Z}$. Since -1 is the unique element of multiplicative order 2, we must have $H \cong \mathbb{Z}/4\mathbb{Z}$, so a generator a for H has order 4, i.e., $a^2 = -1$ in $\mathbb{F}_p$, completing the proof. □

Lemma 4.5. *Let $\mathbb{Q}(\sqrt{D})$ be a quadratic field, and $\mathcal{O} := \mathbb{Z}[\omega]$ be its associated quadratic integer ring. If $n, a, b \in \mathbb{Z}$, then $n \mid (a+b\omega)$ in $\mathcal{O}$ if and only if $n \mid a, b$ in $\mathbb{Z}$.*

Proof. One direction of this is trivial, so suppose $n \mid a+b\omega$. Then $a+b\omega = n(c+d\omega)$ for $c, d \in \mathbb{Z}$. Distributing, we see $a+b\omega = nc+nd\omega$, and matching up like terms, we have $a = nc$ and $b = nd$ (as ω is not an integer, this is legal). That is, $n \mid a, b$. □

Now, we state and prove the main result.

Theorem 4.6 (Gaussian Prime Theorem)**.** *Let $p \in \mathbb{Z}^+$ be a rational prime*[3] *number. Then these are all of the primes in $\mathbb{Z}[i]$:*

1. *When $p = 2$, then $2 = -i(1+i)^2$, and $\pi := 1+i$ is the only prime (up to associates) dividing 2, and 2 is not prime in $\mathbb{Z}[i]$.*
2. *When $p \equiv 3 \pmod 4$, then p is inert.*
3. *When $p \equiv 1 \pmod 4$, then $p = \pi\bar{\pi}$ for primes $\pi = a+bi$ and $\bar{\pi} = a-bi$ in $\mathbb{Z}[i]$, and the primes $\pi, \bar{\pi}$ are not associate.*

[2] There is, however, one special case, namely $p = 2$, the "oddest" of all primes. Notice $2 = (1+i)(1-i)$, but $1+i$ and $1-i$ are really "the same" prime, as they are associate: $1-i = -i(1+i)$, and $-i$ is a unit in $\mathbb{Z}[i]$. For an odd prime p, this does not happen, as we shall see.

[3] That is, a normal, ordinary, integer prime, like 43.

Proof. Point (1) is trivial: notice that $2 = (1-i)(1+i) = -i(1+i)^2$, and we have $N(1+i) = 2$, which establishes the claim. For (2), suppose for contradiction that $p \equiv 3 \pmod 4$ and p were reducible; in particular, since p is an integer, $p = \alpha\bar{\alpha} = N(\alpha)$ for some $\alpha = a+bi$, a non-unit. But now $p = a^2+b^2$, which is impossible, as the squares modulo 4 are 0 and 1; no combination of these gives 3 modulo 4.

For (3), suppose $p \equiv 1 \pmod 4$. By Euler's Criterion, we know that $(-1)^{\frac{1}{2}(p-1)} \equiv \left(\frac{-1}{p}\right)$, but now $p-1$ is divisible by 4 so $\frac{1}{2}(p-1)$ is even, so $\left(\frac{-1}{p}\right) = 1$. Hence, we may pick $x \in \mathbb{Z}^+$ with $x^2 \equiv -1 \pmod p$. Hence, factoring over $\mathbb{Z}[i]$, we have $p \mid (x-i)(x+i)$. None of these factors $x \pm i$ divide p by applying Lemma 4.5, which means that p is not prime in $\mathbb{Z}[i]$. Hence, p must be reducible, so $p = \pi\bar{\pi}$ for some $\pi := a+bi$, which has prime norm and thus is prime.

Finally, we show that π and $\bar{\pi}$ are distinct up to associates. Suppose for contradiction otherwise, so that $u\pi = \bar{\pi}$ for some unit u. Now

$$u = \frac{\bar{\pi}}{\pi} = \frac{\bar{\pi}^2}{p} = \frac{a^2-b^2+2abi}{p}$$

is a Gaussian integer, so applying Lemma 4.5 again, we have $p \mid a^2-b^2$ and $p \mid ab$. By Euclid's Lemma, $p \mid a$ or $p \mid b$, but now $p \mid a^2-b^2 = \pi$. Taking norms, we have $p^2 \mid N(\pi)$, which is illegal by assumption.

The fact that these are all of the primes in $\mathbb{Z}[i]$ comes from the correspondence between factorizations in $\mathbb{Z}[i]$ and sums of integer squares. □

Corollary 4.7 (Fermat's Two-Squares Theorem)**.** *The prime p is a sum of two integer squares if and only if $p \equiv 2$ or $p \equiv 1 \pmod 4$.*

Proof. This is merely a repackaging of the Gaussian Prime Theorem. □

Using $\mathbb{Z}[i]$ also gives us a fast way to count the number of representations as a sum of squares.

Corollary 4.8. *A positive integer n can be written as the sum of two squares if and only if every prime divisor of n congruent to 3 modulo 4 divides n an even number of times. Now, if n is the sum of two squares and*

$$n = 2^k p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s},$$

where the $p_i \equiv 1 \pmod 4$ and $q_j \equiv 3 \pmod 4$ are primes (with all the b_i even), then n can be written as a sum of two integer squares in exactly $4(a_1+1)(a_2+1)\cdots(a_r+1)$ ways.

Proof. Write $n = A^2+B^2 = (A+Bi)(A-Bi)$, factoring over $\mathbb{Z}[i]$. Evidently, we see $N(A \pm Bi) = n$. Now, take n and factor it over $\mathbb{Z}[i]$, using the Gaussian Prime Theorem so that $2^k = u(1+i)^{2k}$ for some unit $u \in \mathbb{Z}[i]$ and $p_i = \pi_i\bar{\pi}_i$ for Gaussian primes $\pi_i, \bar{\pi}_i$:

$$n = u(1+i)^{2k} \prod_{i=1}^{r} \pi_i^{a_i} \bar{\pi}_i^{a_i} \prod_{j=1}^{s} q_j^{b_j} = N(A+Bi) = N(A-Bi).$$

Now, it is not too hard to see that (this looks scarier than it actually is)

$$A+Bi = u'(1+i)^k \prod_{i=1}^{r} \pi_i^{a_{i,1}} \bar{\pi}_i^{a_{i,2}} \prod_{j=1}^{s} q_j^{b_j/2},$$

where we have $a_{i,1}+a_{i,2} = a_i$ and u' is a unit. That is, the primes are "evenly distributed" between $A+Bi$ and $A-Bi$ in terms of norm — one of the $A \pm Bi$ can "take more" of the conjugates $\pi_i, \bar{\pi}_i$ than the other, but this is balanced out. Hence, our choice of $A+Bi$ which has norm n, is completely dependent on u' and what $a_{i,1}$ is. Now, $a_{i,1} \in \{0, 1, 2, \ldots, a_i\}$ and we have four units in $\mathbb{Z}[i]$, for a total of $4(a_1+1)(a_2+1)\cdots(a_n+1)$ choices of $A+Bi$. This completes the proof. □

Example 4.9. The number $63 = 3^2 \cdot 7$ is not a sum of two squares, as the prime 7 is a prime congruent to 3 modulo 4 occurs once in its prime factorization. In contrast, $2691325 = 5^2 \cdot 7^2 \cdot 13^3$ has three distinct prime factors, and prime factor congruent to 3 (mod 4), namely 7, occurs an even number of times. Hence, 2691325 is a sum of two squares, and it has $4(2+1)(3+1) = 48$ representations as a sum of two squares.

5. Epilogue: An Introduction to the Class Group

In the last section, we examined the unique factorization property of $\mathbb{Z}[i]$, which is the quadratic integer ring for $\mathbb{Q}(i)$, and how determining the primes in $\mathbb{Z}[i]$ instantly implies Fermat's Two-Square Theorem. However, it is usually not the case that a quadratic integer ring is a UFD, and we have already seen the infamous example of $\mathbb{Z}[i\sqrt{5}]$:

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

However, this "bad" factorization is actually indicative of the ideal structure of $\mathbb{Z}[i\sqrt{5}]$ in the background. Ideals in a ring may be "multiplied" using the product we define below:

Definition 5.1. Let R be a commutative ring. The *product* of two ideals $A, B \trianglelefteq R$ is defined by the collection of all finite sums of the form ab, where $a \in A$ and $b \in B$:

$$AB := \{a_1b_1 + \cdots + a_nb_n : n \in \mathbb{Z}^+, a_i \in A, b_i \in B\}.$$

In the case that A and B are finitely generated, we have the following proposition, which can be proved by basic subset inclusion.

Proposition 5.2. *Let $A = (a_1, \ldots, a_m)$ and $B = (b_1, \ldots, b_n)$ be two finitely-generated ideals in a commutative ring. Then $AB = (a_1b_1, a_1b_2, \ldots, a_mb_n)$: that is, AB is generated by the elements of the form a_ib_j, where $1 \le i \le m$ and $1 \le j \le n$.*

This corollary also follows:

Corollary 5.3. *Let $A, B, C \trianglelefteq R$ be finitely generated, where R is a commutative unital ring. Then $AB = BA$, $(AB)C = A(BC)$, and $AR = A \cdot (1) = A$.*

Hence, ideal multiplication is closed, is associative, and has an identity — this seems very familiar to us. We first view a computational example.

Example 5.4. Let $\mathcal{O} = \mathbb{Z}[i\sqrt{5}]$, and take[4] $\mathfrak{a} = \left(2, 1 + i\sqrt{5}\right)$, $\mathfrak{b} = \left(3, 1 + i\sqrt{5}\right)$, and $\mathfrak{c} = \left(3, 1 - i\sqrt{5}\right)$. We compute the following products:

$$\begin{aligned}
\mathfrak{a}^2 = \mathfrak{a}\mathfrak{a} &= \left(2 \cdot 2, 2(1 + i\sqrt{5}), (1 + i\sqrt{5})2, (1 + i\sqrt{5})^2\right) \\
&= \left(4, 2 + 2i\sqrt{5}, -4 + 2i\sqrt{5}\right) \\
&= (2) \cdot \left(2, 1 + i\sqrt{5}, -2 + i\sqrt{5}\right).
\end{aligned}$$

Now, the second ideal contains $1 + i\sqrt{5} - (-2 + i\sqrt{5}) = 3$, and thus also $3 - 2 = 1$, so we just have $\mathfrak{a}^2 = (2) \cdot \mathcal{O} = (2)$.

Similarly, we compute

$$\begin{aligned}
\mathfrak{b}\mathfrak{c} &= \left(3 \cdot 3, (1 + i\sqrt{5})(1 - i\sqrt{5}), 3(1 + i\sqrt{5}), 3(1 - i\sqrt{5})\right) \\
&= \left(9, 6, 3 + 3i\sqrt{5}, 3 - 3i\sqrt{5}\right) \\
&= (3) \cdot \left(3, 2, 1 + i\sqrt{5}, 1 - i\sqrt{5}\right) = (3)
\end{aligned}$$

(the last step: $\left(3, 2, 1 + i\sqrt{5}, 1 - i\sqrt{5}\right) = \mathcal{O}$)

and

$$\begin{aligned}
\mathfrak{b}^2 = \mathfrak{b}\mathfrak{b} &= \left(3 \cdot 3, 3(1 + i\sqrt{5}), (1 + i\sqrt{5})^2\right) \\
&= \left(9, 3 + 3i\sqrt{5}, -4 + 2i\sqrt{5}\right).
\end{aligned}$$

[4] When ideals in quadratic integer rings are discussed, we commonly use Gothic letters to denote them, as per tradition. The reason for doing this will be evident later.

From here, observe that all three factors are divisible by $2 - i\sqrt{5}$, so factoring it out, we get

$$\mathfrak{b}^2 = \left(2 - i\sqrt{5}\right) \cdot \left(2 + i\sqrt{5}, -1 + i\sqrt{5}, -2\right) = \left(2 - i\sqrt{5}\right) \cdot \mathcal{O}.$$

This sheds some light into the factorization

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

we have seen before. Taking ideals of everything, we observe

$$(2) \cdot (3) = \left(1 + i\sqrt{5}\right) \cdot \left(1 - i\sqrt{5}\right),$$

but now $(2) = \mathfrak{a}^2$ and $(3) = \mathfrak{bc}$. Hence $(6) = \mathfrak{a}^2\mathfrak{bc}$. Switching the order of the factors, we may check $(6) = (\mathfrak{ab})(\mathfrak{ac}) = \left(1 + i\sqrt{5}\right)\left(1 - i\sqrt{5}\right)$, which we will verify in the exercises. Hence, the two different factorizations on the number level actually correspond to two different representation of the same ideal factorization.

Now that we have a notion of "multiplication" among ring ideals, we can also inquire about divisibility:

Definition 5.5. Let R be a commutative ring, and $A, B \trianglelefteq R$. We say that A *divides* B, and write $A \mid B$, if there exists an ideal C with $B = AC$.

This is fairly substantial, because of the following theorem we will state, but not prove. We will remark, however, that the proof is very much like the Fundamental Theorem of Arithmetic and that of "PID implies UFD," so clearly, there is something going on here.

Theorem 5.6 (Fundamental Theorem of Quadratic Ring Ideals)**.** *Let $\mathcal{O}$ be a ring of quadratic integers. If $\mathfrak{a} \trianglelefteq \mathcal{O}$ is nonzero, then $\mathfrak{a}$ is a product of nonzero prime ideals, and this factorization is unique up to reordering of the ideals.*

Hence, even in very "ill-behaved" rings like $\mathbb{Z}[i\sqrt{5}]$, there is still some notion of unique factorization — just not for the elements themselves, but for the ideals they generate. We might ask, "are some quadratic integer rings more well-behaved than others?" This is a valid, though vague, question, with a precise answer.

The problem with $\mathbb{Z}[i\sqrt{5}]$ is the existence of non-principal ideals such as $(2, 1 + i\sqrt{5})$; in fact, this is always the problem with a quadratic integer ring that is not a UFD — it may be deduced from Theorem 5.6 that a quadratic integer ring is a PID if and only if it is a UFD. To this end, our question may be completely rephrased: given a quadratic field F with associated integer ring $\mathcal{O}$, we should classify its ideals based on its relationship to the collection of principal ideals of $\mathcal{O}$. One way to go about this is to note that ideal multiplication is closed, is associative, and has an identity, as we have mentioned before. This would imply that the set of nonzero ideals of $\mathcal{O}$ is a group, provided that we find a suitable way of "inverting" ideals. Luckily, the construction of this is not too difficult, and we refer the reader to [2] to see how *fractional ideals* are constructed. Then, the set of nonzero fractional ideals $\mathcal{I}$ forms an abelian group under ideal multiplication, and it has a subgroup, $\mathcal{P}$, consisting of the *principal fractional ideals* (whatever that means). The quotient group $\mathrm{Cl}(F) := \mathcal{I}/\mathcal{P}$ is the *ideal class group* of the field F, and the order of $\mathrm{Cl}(F)$ is the *class number*, usually denoted h. The class group satisfies the following:

Theorem 5.7. *Let $F := \mathbb{Q}(\sqrt{D})$ be a quadratic field. Then $\mathcal{O}$ is a PID if and only if F has class number* 1.

Using our previous discussion, we see that $\mathcal{O}$ has unique factorization if and only if $h = 1$. Hence, very roughly speaking, the class number could be used to measure the failure of unique factorization: the higher the class number, the more complex the relationships between the non-principal ideals in $\mathcal{O}$. However, the class number is never infinite, at least for quadratic integer rings:

Theorem 5.8. *Let $F := \mathbb{Q}(\sqrt{D})$ be a quadratic field. Then the ideal class group $\mathrm{Cl}(F)$ is finite.*

In fact, we have some fairly tight bounds on the class number when given the quadratic field $\mathbb{Q}(\sqrt{D})$, though we will not mention them here. Finally, we remark that ideal class groups can also be generalized far outside of quadratic number fields, and still remain an important area of study in modern algebraic number theory, with many questions still left open.

References

[1] David S. Dummit and Richard M. Foote. *Abstract Algebra*. Third. John Wiley & Sons, Inc., Hoboken, NJ, 2004, pp. xii+932. ISBN: 0-471-43334-9.

[2] Franz Lemmermeyer. *Quadratic Number Fields*. Springer Undergraduate Mathematics Series. Translated from the 2017 German original. Springer, Cham, 2021, pp. xi+343. ISBN: 978-3-030-78651-9. DOI: 10.1007/978-3-030-78652-6. URL: https://doi.org/10.1007/978-3-030-78652-6.

[3] Joseph Hillel Silverman. *A Friendly Introduction to Number Theory*. Pearson Modern Classics. Pearson, 2018, pp. x+409. ISBN: 978-0-13-468946-3.