Chapter 4
Divisibility in Integral Domains

In this chapter we will study the notion of divisibility in general domains. We will restrict our attention to commutative domains R containing a unit[1] 1, i.e., an element with the property $1r = r$ for all $r \in R$. Recall that a ring R is called a *domain* if it does not contain any zero divisors, that is, if $ab = 0$ for elements $a, b \in R$ implies that $a = 0$ or $b = 0$. Subrings of fields are always domains, and every domain may be interpreted as a subring of its field of quotients (see Exercise 4.3). Our goal is the definition of units, primes, and irreducible elements and a first investigation of the question in which quadratic number rings the theorem of unique factorization holds.

4.1 Units, Primes, and Irreducible Elements

It is easy to transfer the notion of divisibility of integers in $\mathbb{Z}$ to arbitrary domains R: Given $a, b \in R$, we say that b divides a if there is a $c \in R$ such that $a = bc$, and we write $b \mid a$ in this case. More generally we write $a \equiv b \bmod mR$ if $m \mid (a - b)$ in R. Congruences in R have the usual properties; we leave the proofs as exercises (see Exercise 4.9).

Proposition 4.1 *Let R be a domain; for all $a, b, c, d, m, n \in R$, we have*

(a) $a \equiv b \bmod m$*,* $c \equiv d \bmod m \Longrightarrow a + c \equiv b + d \bmod m$*;*
(b) $a \equiv b \bmod m$*,* $c \equiv d \bmod m \Longrightarrow ac \equiv bd \bmod m$*; and*
(c) $n \mid m$ *und* $a \equiv b \bmod m \Longrightarrow a \equiv b \bmod n$*.*

The properties (a) and (b) are equivalent to the statement that $a \equiv b \bmod m$ implies $f(a) \equiv f(b) \bmod m$ for all polynomials $f \in \mathbb{Z}[x]$. The following result shows

[1] The standard example of a domain without 1 is the ring of even integers.

F. Lemmermeyer, *Quadratic Number Fields*, Springer Undergraduate
Mathematics Series, https://doi.org/10.1007/978-3-030-78652-6_4

that certain congruences in $\mathcal{O}_k$ imply congruences in $\mathbb{Z}$; it allows us to work in the bigger ring $\mathcal{O}_k$ and then pull back results from there to the ring of ordinary integers.

Proposition 4.2 *Let $a, b, m \in \mathbb{Z}$. Then $a \equiv b \bmod m$ in $\mathcal{O}_k$ if and only if $a \equiv b \bmod m$ in $\mathbb{Z}$.*

Proof The congruence $a \equiv b \bmod m$ in $\mathcal{O}_k$ is equivalent to $a - b = m\gamma$ for some $\gamma \in \mathcal{O}_k$. Since $\gamma = \frac{a-b}{m}$, we have $\gamma \in \mathcal{O}_k \cap \mathbb{Q}$, and now Proposition 2.4 shows that $\gamma \in \mathbb{Z}$, and hence $a \equiv b \bmod m\mathbb{Z}$ in $\mathbb{Z}$. The converse is trivial. □

The following result is also useful for computing with quadratic irrationalities; the simple proof is given in Exercise 4.10.

Proposition 4.3 *Let $\{1, \omega\}$ be an integral basis of a quadratic number field, and let $m \in \mathbb{Z}$ be an integer. Then $m \mid (a + b\omega)$ in $\mathcal{O}_k$ if and only if $m \mid a$ and $m \mid b$.*

Elements of a domain R that divide 1 are called *units* of R. The set $R^\times$ of all units forms a group with respect to multiplication; it is called the *unit group* of R. Examples of unit groups of some well-known rings are the following:

R	$\mathbb{Z}$	$\mathbb{Z}[x]$	$\mathbb{Q}[x]$	$\mathbb{Z}[\sqrt{-2}\,]$	$\mathbb{Z}[i]$	$\mathbb{Z}[\sqrt{2}\,]$
$R^\times$	$\{\pm 1\}$	$\{\pm 1\}$	$\mathbb{Q}^\times$	$\{\pm 1\}$	$\{\pm 1, \pm i\}$	$\{\pm(1+\sqrt{2}\,)^n\}$

The computation of units in number fields is often challenging; checking whether a given element is a unit is rather easy:

Proposition 4.4 *An element $\varepsilon \in \mathcal{O}_k$ is a unit if and only if $N\varepsilon = \pm 1$. If we write $\varepsilon = \frac{t+u\sqrt{m}}{2}$ for integers $t \equiv u \bmod 2$, then ε is a unit if and only if $t^2 - mu^2 = \pm 4$.*

Proof Let $\varepsilon \in \mathcal{O}_k$ be a unit; then $\varepsilon\eta = 1$ for some $\eta \in \mathcal{O}_k$, and taking the norm yields $N\varepsilon N\eta = N(1) = 1$. Since $N\varepsilon$ and $N\eta$ are integers whose product is 1, we either have $N\varepsilon = N\eta = 1$ or $N\varepsilon = N\eta = -1$. Conversely, $N\varepsilon = \pm 1$ for some $\varepsilon \in \mathcal{O}_k$ means $\pm\varepsilon\varepsilon' = 1$, and hence ε is a unit.

If $\varepsilon = \frac{t+u\sqrt{m}}{2}$ is a unit, then clearly $t^2 - mu^2 = \pm 4$. If conversely $t^2 - mu^2 = \pm 4$ and $m \equiv 2, 3 \bmod 4$, then it follows that t and u both must be even, and hence $\varepsilon = \frac{t}{2} + \frac{u}{2}\sqrt{m} \in \mathbb{Z}[\sqrt{m}\,]$. If $m \equiv 1 \bmod 4$, on the other hand, then $t \equiv u \bmod 2$. In both cases, ε is a unit in $\mathcal{O}_k$. □

It follows that the norm yields a group homomorphism $E_k \longrightarrow E_{\mathbb{Q}} = \{\pm 1\}$, where $E_k = \mathcal{O}_k^\times$ and $E_{\mathbb{Q}} = \mathbb{Z}^\times$ are the unit groups of $\mathcal{O}_k$ and $\mathbb{Z}$.

The unit groups in complex quadratic number fields can be described explicitly.

Theorem 4.5 *Let $m < 0$ be squarefree, $k = \mathbb{Q}(\sqrt{m}\,)$, and $R = \mathcal{O}_k$ the ring of integers in k. Then*

$$R^\times = \begin{cases} \langle i \rangle & \text{if } m = -1; \\ \langle -\rho \rangle & \text{if } m = -3; \\ \langle -1 \rangle & \text{otherwise.} \end{cases}$$

Here $i = \sqrt{-1}$ denotes a primitive fourth and $\rho = \frac{1}{2}(-1 + \sqrt{-3}\,)$ a primitive cube root of unity.

Proof Assume first that $m \equiv 1, 2 \bmod 4$, and let $\varepsilon = a + b\sqrt{-m}$ be a unit. Then $1 = N\varepsilon = a^2 + mb^2$ (the case $N\varepsilon = -1$ cannot occur since $m > 0$). For $m > 1$, this implies $a = \pm 1$ and $b = 0$, and hence $\varepsilon = \pm 1$ (and of course ± 1 are units). If $m = 1$, there are four possibilities, namely $a = \pm 1, b = 0$ and $a = 0, b = \pm 1$. All these units are powers of $i = \sqrt{-1}$.

If $m \equiv 3 \bmod 4$, we set $\varepsilon = \frac{1}{2}(a + b\sqrt{-m}\,)$ for integers a, b and find $4 = a^2 + mb^2$ as a necessary and sufficient condition for ε to be a unit. For $m > 3$, there are again only the trivial solutions corresponding to $\varepsilon = \pm 1$; if $m = 3$, then we obtain the units

$$\pm 1, \quad \pm\frac{-1 + \sqrt{-3}}{2}, \quad \pm\frac{1 + \sqrt{-3}}{2}.$$

Setting $\rho = \frac{-1+\sqrt{-3}}{2}$ (this is a cube root of unity since $\rho^3 = 1$), we find that E_k is generated by $-\rho$ (a primitive sixth root of unity). □

The determination of the unit group of rings of integers in real quadratic number fields boils down to solving the *Pell equation* $t^2 - mu^2 = \pm 4$; we will prove in Chap. 7 below that this equation has integral solutions whenever $m \geq 2$ is not a square. At this point we only observe that $\varepsilon = 1 + \sqrt{2}$ is a unit with infinite order in $\mathbb{Z}[\sqrt{2}\,]$ (see Theorem 2.7): If we had $(1 + \sqrt{2}\,)^n = \pm 1$ for some $n \geq 1$, then taking absolute values (after identifying $\sqrt{2}$ with the positive real square root of 2), we obtain $1 = |\pm 1| = |1 + \sqrt{2}\,|^n > 1$, and similarly $1 = |\pm 1| = |1 + \sqrt{2}\,|^n = |1 - \sqrt{2}\,|^{-n} < 1$ if $n \leq -1$. In particular, $\mathbb{Z}[\sqrt{2}\,]$ has infinitely many units.

John Pell (1611–1685) was an English mathematician. His name got attached to the Pell equation through a mistake by Euler, who apparently confused him with Lord William Brouncker. It was Brouncker who developed a method for solving such equations in integers in connection with Fermat's challenge in 1657 for the English mathematicians. The proof that Brouncker's method always leads to a solution was given much later by Lagrange.

A method for solving the Pell equation similar to Brouncker's had already been developed by Indian mathematicians, in particular Brahmagupta (ca. 598–670) and Bhaskara II (1114–1185); their contributions (see Plofker [104]) became known in Europe only during the nineteenth century. We will present a method for solving the Pell equation in Chap. 7.

Elements $a, b \in R$ are called *associated*, if there is a unit $e \in R^\times$ such that $a = be$; we write $a \sim b$ and verify easily that this defines an equivalence relation on R.

Irreducible and Prime Elements An element $a \in R \setminus R^\times$ is called *irreducible* if a has only trivial divisors, that is, units and associates. More exactly: a is irreducible in R if $a = bc$ implies that b or c is a unit. An element $p \in R \setminus R^\times$ is called *prime* if

$p \mid ab$ implies that $p \mid a$ or $p \mid b$. Observe that units are by definition neither prime nor irreducible.

Proposition 4.6 *Prime elements are irreducible.*

Proof Let a be prime. If we could factor a, there would exist $b, c \in R \setminus R^\times$ with $a = bc$. Now $a \mid bc$; if $a \mid b$, i.e., $b = ad$ for some $d \in R$, then $a = acd$, hence $1 = cd$, and c is a unit in contradiction to our assumption. □

A simple criterion for the primality of an element in a ring is the following:

Proposition 4.7 *An element $p \in R$ is prime if and only if the residue class ring R/pR of the residue classes modulo p is a domain.*

The proof is simple. The residue class ring modulo p does not have a zero divisor if $ab \equiv 0 \bmod p$ implies that $a \equiv 0 \bmod p$ or $b \equiv 0 \bmod p$. But this is just a version of the definition of a prime element, which states that an element is prime if $p \mid ab$ implies that $p \mid a$ or $p \mid b$.

4.1.1 Elements with Prime Norm Are Prime

We have already seen that elements $\pi \in \mathcal{O}_k$ for which $p = |N\pi|$ is a rational prime are always irreducible. As a matter of fact, such elements are always prime. This will follow easily from the theory of ideals that we will develop later; here we will give a direct proof based on Proposition 4.7.

Proposition 4.8 *If k is a quadratic number field with ring of integers $\mathcal{O}_k$, then each $\pi \in \mathcal{O}_k$ with prime norm is prime.*

This is easy to see if $\mathcal{O}_k$ is a unique factorization domain (see the next section): Elements with prime norm are irreducible, and in unique factorization domains, irreducible elements are prime. In order to prove this for general rings $\mathcal{O}_k$, we show that the residue class ring $\mathcal{O}_k/\pi\mathcal{O}_k$ does not have zero divisors. In fact, we will show that $\mathcal{O}_k/\pi\mathcal{O}_k \simeq \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is isomorphic to the field with p elements.

To this end, let $\{1, \omega\}$ be an integral basis of $\mathcal{O}_k$; then $\pi = a + b\omega$ for integers $a, b \in \mathbb{Z}$. We claim that b is not divisible by π (and thus not divisible by $p = |\pi\pi'|$). In fact, $\pi \mid b$ implies $\pi \mid a$ since $a = \pi - b\omega$, and taking norms, we find $p \mid a^2$ and $p \mid b^2$. Since p is prime, this implies that $p \mid a$ and $p \mid b$. But then $\pi = a + b\omega$ would be divisible by p, and hence π' would be a unit: a contradiction.

Thus there exists an integer $c \in \mathbb{Z}$ with $bc \equiv 1 \bmod p$, and in particular, we have $bc \equiv 1 \bmod \pi\mathcal{O}_k$. We find $b\omega \equiv -a \bmod \pi$, after multiplying through by c, thus $\omega \equiv -ac \bmod \pi\mathcal{O}_k$. If any $\gamma = r + s\omega \in \mathcal{O}_k$ is given, then we find $\gamma \equiv r - sac \bmod \pi\mathcal{O}_k$, and thus modulo π every element is congruent to an ordinary integer. Reducing this number modulo p (and p is a multiple of π), we find that γ is congruent to one of the numbers $0, 1, 2, \ldots, p-1$ modulo π.

Now it is easy to show that there are no zero divisors in the ring of residue classes: If we had $\alpha\beta \equiv 0 \bmod \pi$ and if $A, B \in \{0, 1, \dots, p-1\}$ are integers with $\alpha \equiv A \bmod \pi\mathcal{O}_k$ and $\beta \equiv B \bmod \pi\mathcal{O}_k$, then $\pi \mid AB$; taking norms yields $p \mid A^2B^2$, and hence $p \mid A$ or $p \mid B$. Thus $A = 0$ or $B = 0$, and therefore $\alpha \equiv A = 0 \bmod \pi$ or $\beta \equiv B = 0 \bmod \pi$.

Proposition 4.9 *Let p be an odd prime number and $\mathcal{O}_k$ the ring of integers in $k = \mathbb{Q}(\sqrt{m}\,)$. Then p is prime in $\mathcal{O}_k$ if and only if the congruence $x^2 \equiv m \bmod p$ is not solvable.*

Proof If $x^2 \equiv m \bmod p$ is solvable, then $p \mid (x+\sqrt{m}\,)(x-\sqrt{m}\,)$, but $p \nmid (x \pm \sqrt{m}\,)$. Thus p is not prime.

Now we show that p remains prime in $\mathcal{O}_k$ if $(\frac{m}{p}) = -1$. This case is not covered by Proposition 4.8 since here $N(p) = p^2$ is not prime. The idea for proving the result is the same as in the proof of Proposition 4.8: We show that the residue classes modulo p in $\mathcal{O}_k$ form a field.

We will give the proof in the case where $\mathcal{O}_k = \mathbb{Z}[\sqrt{m}\,]$. Here the residue classes modulo p in $\mathcal{O}_k$ are represented by the p^2 elements $a + b\sqrt{m}$ with $0 \le a, b < p$; clearly every $\alpha \in \mathcal{O}_k$ is congruent modulo p to one of these elements, and they are pairwise distinct. These residue classes form a ring, and we want to show that they form a field. This will follow if we can write down an inverse for each residue class $a + b\sqrt{m} \bmod p$ different from $0 \bmod p$. Now

$$\frac{1}{a+b\sqrt{m}} = \frac{a-b\sqrt{m}}{a^2-mb^2},$$

and the denominator is $\equiv 0 \bmod p$ if and only if a and b are divisible by p (otherwise m would be a quadratic residue modulo p). Since $0 \le a, b < p$, this implies $a = b = 0$. In fact, $a^2 \equiv mb^2 \bmod p$ implies either (if $b \ne 0$) that $(\frac{a}{b})^2 \equiv m \bmod p$, and then $x^2 \equiv m \bmod p$ is solvable and m is a quadratic residue modulo p, or (if $b = 0$) that $a^2 \equiv 0 \bmod p$ and hence $a = 0$. Thus for each nonzero residue class $a + b\sqrt{m} \bmod p$, the inverse is given by $\frac{a-b\sqrt{m}}{a^2-mb^2} \bmod p$.

In the case $m \equiv 1 \bmod 4$, the residue classes modulo p are represented by elements $a + b\omega$ with $0 \le a, b < p$; the rest of the proof is left to the readers as an exercise. □

For $p = 2$, there is a corresponding criterion that may be proved in a similar manner.

Proposition 4.10 *The element $p = 2$ is prime in the ring of integers $\mathcal{O}_k$ of the quadratic number field $k = \mathbb{Q}(\sqrt{m}\,)$ if and only if $m \equiv 5 \bmod 8$.*

We leave the proof as an exercise for the readers.

4.2 Unique Factorization Domains

A domain in which the theorem of unique factorization holds is called a unique factorization domain (UFD). More exactly, we demand

UFD–1. Each non-unit $\neq 0$ is a product of finitely many irreducible elements.
UFD–2. Irreducible elements are prime.

There are domains in which UFD–1 fails: In the domain A that is obtained by adjoining all 2^n-th roots of 2 to $\mathbb{Z}$, namely $A = \mathbb{Z}[\sqrt{2}, \sqrt[4]{2}, \sqrt[8]{2}, \ldots]$, the element 2 cannot be written as a finite product of irreducible elements since

$$2 = \sqrt{2}\sqrt{2} = \sqrt[4]{2}\,\sqrt[4]{2}\,\sqrt[4]{2}\,\sqrt[4]{2} = \ldots .$$

The defining property of unique factorization domains is that the factorization guaranteed by UFD–1 should be unique:

UFD–3. Let $a \in R \setminus \{0\}$ and $a = ep_1 \cdots p_s = e'q_1 \cdots q_t$, where $e, e' \in R^\times$ are units and where the p_j and q_j are irreducible elements in R. Then $s = t$, and we can rearrange the q_j in such a way that $p_i \sim q_i$ for $i = 1, \ldots, s$.

Clearly, UFD–3 holds in any unique factorization domain.

Proposition 4.11 *Conditions UFD–2 and UFD–3 are equivalent in every domain R in which UFD–1 holds.*

Proof UFD–2 $\Longrightarrow$ UFD–3: Since the p_i are irreducible, they are prime by assumption. In particular, p_1 divides one of the factors q_j, say q_1. Since q_1 is irreducible, we must have $p_1 \sim q_1$. Since R is a domain, p_1 may be canceled, and we obtain $e_1 p_2 \cdots p_s = e_1' q_2 \cdots q_t$. Induction now yields the claim.

UFD–3 $\Longrightarrow$ UFD–2: Let a be irreducible and $a \mid xy$, where $x, y \in R$. Then there exists an element $b \in R$ with $ab = xy$. Because of UFD–3, the decomposition into irreducible elements is unique up to order and units; thus an associate of a must occur in the factorization of x or y, and we find $a \mid x$ or $a \mid y$. Thus a is prime. □

Since $1 + \sqrt{-5}$ is irreducible in $R = \mathbb{Z}[\sqrt{-5}\,]$, but not prime, R is not a unique factorization domain. This fact also proves that the theorem of unique factorization in $\mathbb{Z}$, which often seems obvious to beginners in number theory, requires a proof.

We call an element d in some domain a common divisor of elements $a, b \in R$ if $d \mid a$ and $d \mid b$. How should we choose a "greatest" common divisor among these common divisors? In the ordinary integers, we can choose the greatest divisor with respect to the absolute value, but this is not a suitable definition for general domains R. What we want is a definition of the greatest common divisor in terms of divisibility alone: We call $d \in R$ a *greatest common divisor* of $a, b \in R$ and write $d \sim \gcd(a, b)$ if d has the following properties:

GCD–1. d is a common divisor of a and b, i.e., $d \mid a$ and $d \mid b$.

GCD–2. Every common divisor of a and b divides d, i.e., if $c \mid a$ and $c \mid b$ for some $c \in R$, then $c \mid d$.

Again we would like to emphasize the fact that this definition is well suited for building a theory of greatest common divisors but cannot easily be used for finding a greatest common divisor of two elements in some domain.

In unique factorization domains, the greatest common divisor of two elements can be written down explicitly. In fact, if $a = u \prod p^{\alpha_p}$ and $b = v \prod p^{\beta_p}$ are the prime factorizations of a and b (with units $u, v \in R^\times$), then we can easily show that $d = \prod p^{\min(\alpha_p, \beta_p)}$ is a greatest common divisor of a and b. One has to remark that even in the case of the ordinary integers, finding the prime factorization of two (large) integers can be very difficult.

Two elements a and b of some unique factorization domain R are called *coprime* (or relatively prime) if their greatest common divisor is a unit. Observe that we demand that R be a unique factorization domain. In fact, in domains without unique factorization, a greatest common divisor need not exist, and if it does, it need not have the properties we expect from a greatest common divisor, such as $\gcd(a, b)^2 = \gcd(a^2, b^2)$.

Proposition 4.12 *If R is a unique factorization domain, if $a, b \in R$ are coprime, and if $ab = ex^n$ $(n \geq 2)$ for some unit $e \in R^\times$ and some $x \in R$, then there exist units $e_1, e_2 \in R^\times$ and elements $c, d \in R$ such that $a = e_1c^n$ and $b = e_2d^n$, where $cd = x$ and $e_1e_2 = e$.*

Proof We prove this by induction on the number of prime factors of a. If a is a unit, then the claim follows with $c = 1$, $d = x$, $e_1 = a$, and $e_2 = ea^{-1}$.

Assume that the claim is true for all $a \in R$ with at most t different prime factors, and let $p \in R$ be a prime with $p \mid a$. Assume that $p^h \parallel a$ (we write $p^h \parallel a$ if $p^h \mid a$ and $p^{h+1} \nmid a$, i.e., if p^h is the largest power of p that divides a). Since $p^h \parallel x^n$ (here we use the fact that a and b are coprime), we must have $h = nk$ for some $k \in \mathbb{N}$ and $p^k \parallel x$. Thus $a = p^h a_1$, $x = p^k x_1$ and $a_1 b = ex_1^n$. By induction assumption, we have $a_1 = e_1c^n$ and $b = e_2d^n$, and now the claim follows since $a = e_1(cp^k)^n$. □

Corollary 4.13 *If R is a unique factorization domain, if $\gcd(a, b) = p$ for elements $a, b, p \in R$, where p is prime, and if $ab = ex^n$ $(n \geq 2)$ for some $e \in R^\times$ and $x \in R$, then there exist units $e_1, e_2 \in R^\times$ and $c, d \in R$ with $a = e_1pc^n$ and $b = e_2p^{n-1}d^n$ (after switching a and b, if necessary).*

Proof Exercise 4.28. □

4.3 Principal Ideal Domains

Principal ideal domains will play a minor role in this chapter, mainly as a link in the chain of inclusions

Euclidean Domains $\subset$ Principal Ideal Domains $\subset$ Unique Factorization Domains that we will use for constructing unique factorization domains. Both inclusions are proper; for rings of integers in quadratic number fields (and in fact of general number fields), the second inclusion is in fact an equality.

First we will have to explain the notion of a principal ideal domain. To this end, consider a domain R; a subring I of R is called an *ideal* of R if $I \cdot R \subseteq I$. Thus an ideal is a subset of a domain that is closed with respect to addition ($I + I \subseteq I$) as well as with respect to multiplication by arbitrary elements of the domain R.

Observe that I is a subring of R if the weaker condition $I \cdot I \subset I$ is satisfied. In the domain $R = \mathbb{Z}$, it can be shown that *each* subring is an ideal. The following example shows that this is not true for general domains: The set

$$M = \mathbb{Z} + 2\sqrt{m}\,\mathbb{Z} = \{a + 2b\sqrt{m} : a, b \in \mathbb{Z}\}$$

is a subring of $\mathbb{Z}[\sqrt{m}\,]$, but not an ideal. This is because $MR = R$; in fact, $1 \in M$ implies that each element of R is contained in MR. Since $\sqrt{m} \in R \setminus M$, the subring M is not an ideal.

It is very easy to write down examples of ideals. If we are given elements $a_1, \ldots, a_n \in R$, then the set of all R-linear combinations

$$I = (a_1, \ldots, a_n) := \{a_1 r_1 + \ldots + a_n r_n : r_j \in R\}$$

of these elements is an ideal called the ideal generated by $a_1, \ldots, a_n$. Clearly I is closed with respect to addition; thus it remains to verify that $IR \subseteq I$. But this is easy: Since $a = a_1 r_1 + \ldots + a_n r_n \in I$, clearly $ar = a_1(r_1 r) + \ldots + a_n(r_n r)$ is an element of I.

In our proofs we have to consider ideals generated by infinitely many elements $a_1, a_2, \ldots$ These ideals $I = (a_1, a_2, \ldots)$ are by definition the set of all *finite* R-linear combinations of the elements $a_i \in I$.

Remark In fields $R = K$, there are only two different ideals, namely the zero ideal (0) and the unit ideal $(1) = R$.

Ideals generated by a single element a are called *principal ideals*. These have the form $I = (a) = \{ar : r \in R\}$; occasionally, we will write $I = aR$. Principal ideals (a) consist of all multiples of a.

The transition from elements to principal ideals consists essentially in disregarding units.

Lemma 4.14 *For $a, b \in R$, the following assertions are equivalent:*

1. $(a) = (b)$;
2. *There is a unit $e \in R^\times$ with $a = be$.*

The proof is a simple exercise.

A domain in which each ideal is principal is called a *principal ideal domain* (PID). Clearly, the ring $\mathbb{Z}$ of ordinary integers is a PID; in fact, the ideal $(a_1, \ldots, a_n)$ is generated by the greatest common divisor $d = \gcd(a_1, \ldots, a_n)$. Not every unique factorization domain is a principal ideal domain; the best known example is the domain $\mathbb{C}[x, y]$ of polynomials in two variables with complex coefficients; here, (x, y) is not principal, as is easily seen.

Remark The fact that $\mathbb{C}[x, y]$ is a unique factorization domain follows from a well-known theorem in algebra: If R is a UFD, then so is the polynomial ring $R[y]$. Since $R = \mathbb{C}[x]$ is a UFD (this ring is even Euclidean—see Sect. 4.4), the claim follows.

Now we prove that principal ideal domains have unique factorization.

Theorem 4.15 *Principal ideal domains are unique factorization domains.*

Proof Assume that UFD–1 is not satisfied. Then there is an $a_1 \in R$ that cannot be written as a product of irreducible elements (in particular, a_1 is not irreducible). Thus, $a_1 = a_2b_2$ (for non-units $a_2, b_2 \in R \setminus R^\times$), where one of the factors, say a_2, is not a product of irreducible elements. Thus, $a_2 = a_3b_3$, etc., and we obtain a chain of elements $a_1, a_2, a_3 \ldots \in R$ with $a_2 \mid a_1, a_3 \mid a_2, \ldots$, where a_i and a_{i+1} are not associated.

Now consider the ideal $I = (a_1, a_2, \ldots)$ generated by the a_i. By assumption, there is an element $a \in R$ with $I = (a)$, and thus there exist $m \in \mathbb{N}$ and $r_i \in R$ such that $a = r_1a_1 + \ldots + r_ma_m$. Since $a_m \mid a_{m-1} \mid \cdots \mid a_1$, we have $a_m \mid a$. Since $a_{m+1} \in (a)$, there is an element $r \in R$ such that $a_m = ar$, i.e., with $a \mid a_{m+1}$. By construction of the a_i, we have $a_{m+1} \mid a_m$, and hence a_m and a_{m+1} are associated in contradiction to the construction of the a_i.

Now we show that irreducible elements are prime (UFD–2). To this end, let $a \in R$ be irreducible, and let $x, y \in R$ be given with $a \mid xy$ and $a \nmid x$; then we have to show that $a \mid y$. Now $(a, x) = (d)$ for some $d \in R$; thus $d \mid a$ and $d \mid x$. If we had $d \sim a$, it would follow that $a \mid x$ in contradiction to our assumption. Since a is irreducible, d must be a unit. Thus $d^{-1} \in R$, and therefore $1 = d^{-1}d \in (d) = (a, x)$, i.e., there exist $m, n \in R$ with $1 = ma + nx$. Multiplication by y yields $y = may + nxy$, and since $a \mid xy$, we find $a \mid y$. This is what we wanted to show. □

An important property of principal ideal domains is the fact that they are Bézout domains:[2] A domain R is called a *Bézout domain* if for all $a, b \in R$ there exists a $d \sim \gcd(a, b)$ such that $d = ar + bs$ is an R-linear combination of a and b. Principal ideal domains are always Bézout domains: Given $a, b \in R$, we form the ideal $I = (a, b)$; since R is a principal ideal domain, there is an element $d \in R$ with $(a, b) = (d)$. We claim that $d \sim \gcd(a, b)$. In fact, since $a \in (d)$, there is a $t \in R$ with $a = dt$; this shows that $d \mid a$, and similarly we find that $d \mid b$, and hence d is a common divisor of a and b. On the other hand, $d \in (a, b)$ implies that there are elements $r, s \in R$ with $d = ar + bs$; if e is any common divisor of a and b, then e

[2] Étienne Bézout (1730–1783) was a French mathematician, an author of textbooks. Bézout proved the existence of Bézout elements for polynomial rings; in the case of integers, they already occurred in the work of Bachet.

divides $ar + bs = d$, and hence d is a greatest common divisor of a and b. Observe that we have proved the Bézout property en passant.

4.4 Euclidean Domains

In his *Lectures on number theory* [31, p. 20], Dirichlet (actually we do not know how much of this is due to Dedekind) discusses the foundations of elementary number theory and then writes the following:

> It is now clear that the whole structure rests on a single foundation, namely the algorithm for finding the greatest common divisor of two numbers. [...] any analogous theory, for which there is a similar algorithm for the greatest common divisor, must also have consequences analogous to those in our theory.

In order to show that some domain R is a unique factorization domain, we will at first use the Euclidean algorithm. A function $f : R \longrightarrow \mathbb{N}_0$ is called a *Euclidean function* if it has the following properties:

EA–1. $f(a) = 0$ if and only if $a = 0$.
EA–2. For all $a \in R$ and $b \in R \setminus \{0\}$, there exists a $c \in R$ such that $f(a - bc) < f(b)$.

If there exists a Euclidean function on R, then R is called a *Euclidean domain*.

The ring of integers $\mathbb{Z}$ is Euclidean with respect to the absolute value $| \cdot |$. Other examples of Euclidean domains will be given in the Exercises section. The first domain $R \neq \mathbb{Z}$ that was shown to be Euclidean was the ring $\mathbb{Q}[X]$ of polynomials with rational (or real) coefficients. The existence of a Euclidean algorithm in this domain was proved by the Dutch mathematician Simon Stevin (1548–1620). Stevin wrote almost a dozen textbooks and helped to popularize the decimal system in Europe.

Theorem 4.16 *Euclidean domains are principal ideal domains.*

Proof Let f be a Euclidean function on R, and let $A \subseteq R$ be an ideal in R. Among the elements in $A \setminus \{0\}$, there is one, say a, for which f is minimal (in fact, the values of f are natural numbers). We claim that $A = (a)$. Since $a \in A$, we clearly have $(a) \subseteq A$; it remains to prove the reverse inclusion. To this end, take an arbitrary $b \in A$; by EA–2, there is a $q \in R$ with $f(b - aq) < f(a)$; since $f(a)$ was chosen minimal on $A \setminus \{0\}$, we have $f(b - aq) = 0$, and EA–2 implies that $b = aq$. Thus $b \in (a)$, and since $b \in A$ was arbitrary, we even have $A \subseteq (a)$. □

In particular, Euclidean domains have the Bézout property, i.e., given an ideal (a, b), an element $d \sim \gcd(a, b)$ can be written as $d = ar + bs$ with $r, s \in R$. The advantage of working in a Euclidean ring is that given $a, b \in R$, we can compute the greatest common divisor $d \sim \gcd(a, b)$ as well as the Bézout elements r and s using the Euclidean algorithm.

To this end, take elements $a, b \in R \setminus \{0\}$; applying the Euclidean algorithm, we find $q_0, r_1 \in R$ with $a - bq_0 = r_1$ and $f(r_1) < f(b)$. Similarly, there exist $q_1, r_2 \in R$ with $b - r_1 q_1 = r_2$ and $f(r_2) < f(r_1)$ (unless we already have $r_1 = 0$; in this case, $a = bq_1$ and $d = b = 0a + 1b$, so everything is trivial). Continuing in this way, we find a chain of equations

$$\begin{aligned}
a - bq_0 &= r_1 & f(r_1) &< f(b), \\
b - r_1 q_1 &= r_2 & f(r_2) &< f(r_1), \\
r_1 - r_2 q_2 &= r_3 & f(r_3) &< f(r_2), \\
&\vdots & &\vdots \\
r_{n-2} - r_{n-1} q_{n-1} &= r_n & f(r_n) &< f(r_{n-1}) \\
r_{n-1} - r_n q_n &= r_{n+1} & f(r_{n+1}) &< f(r_n).
\end{aligned}$$

Now the natural numbers $f(r_j)$ cannot become arbitrarily small; thus there exists an index $n \in \mathbb{N}$ with $r_{n+1} = 0$. We then claim that $r_n \sim \gcd(a, b)$. In fact, it follows from the last row that $r_n \mid r_{n-1}$, and then the next to last row gives $r_n \mid r_{n-2}$, and in this way we climb the ladder until we reach $r_n \mid r_1$, $r_n \mid b$ and $r_n \mid a$. Thus r_n is a common divisor of a and b.

Conversely, if d is any common divisor of a and b, then the first row tells us that $d \mid r_1$, the second $d \mid r_2$, etc., and eventually we reach $d \mid r_n$. In other words, r_n is a greatest common divisor.

It may be said that the definition of the greatest common divisor is chosen in such a way that the proof of this fundamental result on the Euclidean algorithm becomes essentially trivial.

We obtain the Bézout elements $r, s \in R$ as follows: We start with $r_n = r_{n-2} - r_{n-1} q_{n-1}$ and replace the r_j with the maximal index by the linear combination in the preceding row, in our case r_{n-1} by $r_{n-1} = r_{n-3} - r_{n-2} q_{n-2}$. Now we have written r_n as a linear combination of r_{n-2} and r_{n-3}. Next we replace r_{n-2} by $r_{n-2} = r_{n-4} - r_{n-3} q_{n-3}$, etc., until we finally have written r_n as an R-linear combination of a and b.

4.4.1 Summary

We have defined the following notions in quadratic number rings:

- divisibility and congruences,
- units and associate elements, and
- primes and irreducible elements.

Among the important results, we have obtained are the following:

- Primes are irreducible; the converse holds in unique factorization domains.
- We have the inclusions
  Unique Factorization Domains $\supset$ Principal ideal domains $\supset$ Euclidean domains.

Moreover we know that in unique factorization domains, there exist greatest common divisors $d = \gcd(a, b)$; in principal ideal domains, there exist Bézout elements: We can write the greatest common divisor as a $\mathbb{Z}$-linear combination of a and b: $d = am + bn$. Finally, in Euclidean domains, we have an algorithm for computing greatest common divisors as well as Bézout elements.

4.5 Exercises

4.1. In the ring $R = \mathbb{Z}[x]$ of polynomials, show that $x \mid f(x)$ for some $f \in R$ if and only if $f(0) = 0$. Show more generally that $(x - a) \mid f(x)$ if and only if $f(a) = 0$.

Show that these properties continue to hold in polynomial rings $R = K[x]$ over fields K. What about polynomial rings over domains or arbitrary rings?

4.2. Show that (1.12) is also a counterexample to the Four Numbers Theorem in $\mathbb{Z}[\sqrt{-5}\,]$, whereas (1.11) is compatible with the Four Numbers Theorem in $\mathbb{Z}[\sqrt{-2}\,]$.

4.3. Let R be a domain. Consider the set S of pairs (p, q) and define an equivalence relation on S by $(p, q) \sim (r, s)$ if and only if $ps = qr$. On the set K of equivalence classes, define addition and multiplication via

- $(p, q) + (r, s) = (ps + qr, qs)$;
- $(p, q) \cdot (r, s) = (pr, qs)$.

Show that this is well defined and that it makes K into a field with neutral elements (0, 1) for addition and (1, 1) for multiplication.

Show that the map $\iota : R \longrightarrow K : r \rightarrow (r, 1)$ is an injective ring homomorphism. The field K is called the quotient field of R, and we may regard R as a subring of K via the embedding ι.

4.4. Let $R \subseteq S$ be domains, and let $a, b, m \in R$. Does $a \equiv b \bmod m$ in R imply the same congruence in S? Is the converse true?

4.5. Each fraction in $\mathbb{Q}$ can be reduced to lowest terms in a unique way; in $\mathbb{Z}[\sqrt{-5}\,]$, on the other hand, $\frac{1+\sqrt{-5}}{2} = \frac{3}{1-\sqrt{-5}}$, and both fractions are reduced to lowest terms. Find more such examples.

4.6. Let $\alpha, \beta \in \mathcal{O}_k$; show that $\alpha \mid N\alpha$. If moreover $\alpha \mid \beta$, then $N\alpha \mid N\beta$ (even in $\mathbb{Z}$).

4.7. Show that if $\sqrt{-2} \mid y$ in $\mathbb{Z}[\sqrt{-2}]$ for some $y \in \mathbb{Z}$, then $2 \mid y$.

Show more generally that $\sqrt{m} \mid y$, where m is squarefree, always implies that $m \mid y$.

Find a counterexample to the claim that $\alpha \mid y$ always implies $N\alpha \mid y$.

4.8. Show that $a + bi \equiv a + b \bmod (1 + i)$ in $\mathbb{Z}[i]$.

4.9. Prove Proposition 4.1.

4.10. Prove Proposition 4.3.

4.11. Show that $a \mid b$ in $\mathbb{Z}$ implies $a \mid b$ in the ring of integers $\mathcal{O}_k$ in a quadratic number field k.

4.12. Show that the set of units $R^\times$ in some ring R is a group with respect to multiplication.

4.13. Show that if $R = K$ is a field, then $K^\times = K \setminus \{0\}$.

4.14. If R is a domain and $R[X]$ the ring of polynomials in one variable X with coefficients from R, then $R[X]^\times = R^\times$, that is, the units in this polynomial ring are all constant.

Show, on the other hand, that the polynomial $2X + 1$ in $(\mathbb{Z}/4\mathbb{Z})[X]$ is a unit.

4.15. Show that the unit groups of the domains $R = \mathbb{Z}[\sqrt{m}\,]$ for $m < -1$ are given by $R^\times = \{-1, +1\}$.

4.16. Let $\mathcal{O}_k$ be the ring of integers in a quadratic number field k, and let $E_k = \mathcal{O}_k^\times$ be its unit group. Show that E_k is a Gal $(k/\mathbb{Q})$-module (see Exercise 2.16).

4.17. Show: If R is a domain containing $\mathbb{Z}$, and if π is prime in R, then the smallest natural number divisible by π in R is a prime number.

4.18. Show that $N\alpha = 1$ for $\alpha = \frac{1+2i}{1-2i} \in \mathbb{Q}(i)$, but that α is not a unit in $\mathbb{Z}[i]$. Construct infinitely many such examples.

4.19. Show that $\mathbb{Z}$ is Euclidean with respect to the absolute value.

4.20. Show that the polynomial ring $K[x]$, where K is a field, is Euclidean with respect to $f(a) = 2^{\deg a}$, where $\deg a$ denotes the degree of $a \in K[x]$, and where we have set $\deg 0 = -\infty$ in order to have $2^{\deg 0} = 2^{-\infty} = 0$.

4.21. Discuss the examples $2 \cdot 3 = -\sqrt{-6} \cdot \sqrt{-6}$ in $\mathbb{Z}[\sqrt{-6}\,]$, $2 \cdot 3 = \sqrt{6} \cdot \sqrt{6}$ in $\mathbb{Z}[\sqrt{6}\,]$, and $2 \cdot 7 = (2 + \sqrt{-10}\,)(2 - \sqrt{-10}\,)$ in $\mathbb{Z}[\sqrt{10}\,]$ as in (1.12).

4.22. Consider the quadratic number field $k = \mathbb{Q}(\sqrt{m}\,)$; which of the rational prime numbers $p \in \{2, 3, 5\}$ in $\mathcal{O}_k$ with $m \in \{-5, -3, -2, -1, 2, 3, 5\}$ are irreducible and which are not?

4.23. Show that elements $\pi \in \mathcal{O}_k$ are irreducible if $N\pi$ is a rational prime.

4.24. Let R be a unique factorization domain. Show:

a. $\gcd(a^2, b^2) = (\gcd(a, b))^2$ for all $a, b \in R$.
b. If $\gcd(a, b) = 1$, then $\gcd(a^2, b) = 1$.
c. $\gcd(a + b, b) = \gcd(a, b)$.
d. $\gcd(ra, rb) = r \gcd(a, b)$.

4.25. Show that the elements $a = 1 + \sqrt{-5}$ and $b = 1 - \sqrt{-5}$ do not have a common divisor except ±1, but that 2 is a common divisor of a^2 and b^2.

4.26. Let S be the domain you obtain by adjoining the element $\omega = \frac{1}{2}(1+\sqrt{-5}\,)$ to $R = \mathbb{Z}[\sqrt{-5}\,]$. Show that $S = R[\frac{1}{2}]$ and $S \cap \mathbb{Q} = \mathbb{Z}[\frac{1}{2}]$.

Show moreover that the decomposition (1.12) is not an example for nonunique factorization into irreducible elements because $3 = \frac{1}{2}(1-\sqrt{-5}\,)(1+\sqrt{-5}\,)$ is a factorization of 3 into the unit $\frac{1}{2}$ and the two irreducible (and even prime) elements $1 \pm \sqrt{-5}$. Explain the equation $3 \cdot 3 = (2-\sqrt{-5}\,)(2+\sqrt{-5}\,)$ by giving a factorization into irreducible elements.

4.27. Solve the Diophantine equation $x^2 + 5y^2 = z^2$ by setting $x + y\sqrt{-5} = (r + s\sqrt{-5}\,)^2$ as Euler did, and show that the resulting parametrization $x = r^2 - 5s^2$, $y = 2rs$ does not yield all integral solutions of the equation.

Use the domain $S = \mathbb{Z}[\sqrt{-5}, \frac{1}{2}]$ from the preceding exercise for obtaining a complete parametrization of the solutions.

4.28. Prove Corollary 4.13. Hint: Try to obtain $a = pa_1$ and $b = p^{n-1}b_1$, and then apply Proposition 4.12 to a_1 and b_1.

4.29. Determine all integral points on the elliptic curve $4y^2 = x^3 + 1$, i.e., all pairs $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ satisfying this equation.

4.30. Find all ring homomorphisms κ from $\mathbb{Z}[\sqrt{-5}\,]$ to $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/5\mathbb{Z}$, and determine their kernels.

4.31. Show that the even integers $2\mathbb{Z}$ form an ideal in $\mathbb{Z}$. More generally, the sets $m\mathbb{Z}$ for arbitrary $m \in \mathbb{Z}$ are ideals in $\mathbb{Z}$.

4.32. Let (a) and (b) be principal ideals in some domain R. Show that $a \mid b$ if and only if $(a) \supseteq (b)$. Show moreover that this implies the equivalence of the following assertions:

a. $(a) = (b)$;
b. $a \mid b$ and $b \mid a$;
c. $a = be$ for some unit $e \in R^\times$.

4.33. Show that the set

$$T = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{Z} \right\}$$

is a subring of $R = M_2(\mathbb{Z})$, the ring of all 2×2-matrices with entries from $\mathbb{Z}$ (this ring is neither commutative nor a domain since it contains zero divisors), but that T is not an ideal in R. Hint: Consider the product of the identity matrix with a lower triangular matrix such as $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$.

4.34. Let $R \subseteq S$ be domains. Show that $I \cap R$ is an ideal in R if I is an ideal in S.

4.35. If I is a nonzero ideal in the ring of integers $\mathcal{O}_k$ of a quadratic number field k, then I contains a natural number $\neq 0$. (Hint: Take the norm). Show that, on the other hand, the ideal (X) in the polynomial rings $\mathbb{Z}[X]$ and $\mathbb{Q}[X]$ does not contain any natural number $\neq 0$.

4.36. Show that the polynomial ring $\mathbb{Z}[x]$ admits a lot more homomorphisms into simpler rings than the rings of integers $\mathcal{O}_k$; show in particular that the reductions π_p modulo p and π_x modulo x yield the following commutative diagram:

$$\begin{tikzcd}
\mathbb{Z}[x] \arrow[r, "\pi_p"] \arrow[d, "\pi_x"'] & \mathbb{F}_p[x] \arrow[d, "\pi_p"] \\
\mathbb{Z} \arrow[r, "\pi_p"] & \mathbb{F}_p
\end{tikzcd}$$

4.37. Let k be a quadratic number field. Show that $\mathbb{Z}$ is a subring of $\mathcal{O}_k$, but not an ideal in $\mathcal{O}_k$.

4.38. Show that the set $2\mathbb{Z} + \sqrt{2}\,\mathbb{Z}$ is an ideal in $\mathbb{Z}[\sqrt{2}\,]$ consisting of the multiples of $\sqrt{2}$. Show moreover that $\mathbb{Z} + 2\sqrt{2}\,\mathbb{Z}$ is a subring of $\mathbb{Z}[\sqrt{2}\,]$, but not an ideal.

4.39. An order $\mathcal{O}$ in some quadratic number field is a subring of $\mathcal{O}_k$ that properly contains $\mathbb{Z}$. Consider the set $\mathcal{F} = \{f \in \mathbb{Z} : f\omega \in \mathcal{O} \text{ for all } \omega \in \mathcal{O}_k\}$. Show that $\mathcal{F}$ is an ideal in $\mathbb{Z}$; the generator $f > 0$ of this ideal $\mathcal{F} = (f)$ is called the *conductor* of the order $\mathcal{O}$. Show that the maximal order $\mathcal{O}_k$ has conductor 1.

4.40. Show that $\gcd(2, x) = 1$ in the unique factorization domain $\mathbb{Z}[x]$ and that there do not exist associated Bézout elements, i.e., that there do not exist polynomials $p, q \in \mathbb{Z}[x]$ with $2p(x) + xq(x) = 1$.

Is $(2, x)$ a principal ideal in $\mathbb{Z}[x]$ or in $\mathbb{Q}[x]$?

4.41. Find ideals in $\mathbb{Z}[\sqrt{-6}\,]$, $\mathbb{Z}[\sqrt{-10}\,]$, and $\mathbb{Z}[\sqrt{10}\,]$ that are not principal.

4.42. Let R be the domain of all algebraic integers. Show that 2 does not possess a factorization into irreducible elements. Also show that the ideal $(2, \sqrt{2}, \sqrt[4]{2}, \sqrt[8]{2}, \ldots)$ is not principal in R and that it is not even finitely generated (this means that it is not generated by finitely many elements, i.e., it does not have the form $(a_1, \ldots, a_n)$ for suitable elements $a_j \in R$).

4.43. Let R be a domain containing $\mathbb{Z}$ (for example, $R = \mathcal{O}_k$). Show that if $a, b \in \mathbb{Z}$ are coprime in $\mathbb{Z}$, then they are also coprime in R. (Hint: Bézout).

4.44. Compute the Bézout elements for $\gcd(21, 15)$ in $\mathbb{Z}$.

4.45. For $n \geq 3$, compute the greatest common divisor of the polynomials $x^n + x^2 - 2$ and $x^2 - 1$ in $\mathbb{Z}[x]$ (the result will depend on n). How can the result that $x - 1$ is always a common divisor be verified in advance?

4.46. Let $\alpha, \beta \in \mathcal{O}_k$ and $(N\alpha, N\beta) = 1$ in $\mathbb{Z}$. Then $\gcd(\alpha, \beta) \sim 1$ in $\mathcal{O}_k$ even if $\mathcal{O}_k$ is not a unique factorization domain.

4.47. Bézout elements can be used for inverting residue classes. Assume for example that a and m are coprime integers; show how to find the inverse of the residue class a mod m in $(\mathbb{Z}/m\mathbb{Z})^\times$ (i.e., the element $b \in \mathbb{Z}$ such that $ab \equiv 1 \bmod m$). Compute $\frac{1}{2}$ mod 21 and $\frac{1}{5}$ mod 33.

4.48. Study the equation $y^2 = x^3 + 9$ in integers.

4.49. Use the factorization $(y - k)(y + k) = x^3$ to deduce results on the integral solutions of the Diophantine equation $y^2 = x^3 + k^2$ for a fixed integer k. This is more of an open problem than an exercise. Do not despair if you cannot find a complete solution (and look for an error if you do).

4.50. For integers k, study the Diophantine equation $y^2 = x^3 - k^2$. You should be able to prove that this equation is solvable for $k = b(3a^2 - b^2)$ or $k = 2(a^3 + 3a^2b - 3ab^2 - b^3)$. For $k = 88$, there are two different representations $k = b(3a^2 - b^2)$, and hence there are at least two solutions of the equation also $y^2 = x^3 - k^2$ in this case. Can the number of solutions become arbitrarily large?

4.51. Solve the Diophantine equation $(1 + 8i)x + (5 + 4i)y = 1$ in $\mathbb{Z}[i]$.