1. Factorization

1.1. Divisibility in $\mathbb{Z}$.

Definition 1.1.1. *Let $a, b \in \mathbb{Z}$. Then we say that a divides b and write $a|b$ if $b = ac$ for some $c \in \mathbb{Z}$:*

$$a|b \iff \exists c \in \mathbb{Z} : b = ac.$$

Alternatively, we may say that "b is a multiple of a". If $a \neq 0$ this is equivalent to the statement that the rational number b/a is an integer c. If a does not divide b we write $a \not| b$.

Lemma 1.1.2. *[Easy facts about divisibility] For all a, b, $\ldots \in \mathbb{Z}$:*

(1) $a|b \implies a|kb \ \ (\forall k \in \mathbb{Z})$;
(2) $a|b_1$, $a|b_2 \implies a|b_1 \pm b_2$; *hence if b_1 and b_2 are multiples of a, then so are all integers of the form $k_1b_1 + k_2b_2$.*
(3) $a|b$, $b|c \implies a|c$;
(4) $a|b$, $b|a \iff a = \pm b$;
(5) $a|b$, $b \neq 0 \implies |a| \leq |b|$; *so nonzero integers have only a finite number of divisors;*
(6) *If $k \neq 0$ then $a|b \iff ka|kb$;*
(7) *Special properties of ± 1: $\pm 1|a \ \ (\forall a \in \mathbb{Z})$, and $a| \pm 1 \iff a = \pm 1$;*
(8) *Special properties of 0: $a|0 \ \ (\forall a \in \mathbb{Z})$, and $0|a \iff a = 0$.*

Proposition 1.1.3 (Division Algorithm in $\mathbb{Z}$)**.** *Let $a, b \in \mathbb{Z}$ with $a \neq 0$. There exist unique integers q, r such that*

$$b = aq + r \qquad \text{with} \qquad 0 \leq r < |a|.$$

Notation: the set of all multiples of a fixed integer a is denoted (a) or $a\mathbb{Z}$:

$$(a) = a\mathbb{Z} = \{ka \mid k \in \mathbb{Z}\}.$$

Then we have $a|b \iff b \in (a) \iff (a) \supseteq (b)$: "to contain is to divide". From Lemma 1.1.2(4) we have $(a) = (b) \iff a = \pm b$.

An *ideal* in a commutative ring R is a subset I of R satisfying

(i) $0 \in I$;
(ii) $a, b \in I \implies a \pm b \in I$;
(iii) $a \in I$, $r \in R \implies ra \in I$.

Notation: $I \triangleleft R$. For example, the set of all multiples of a fixed element a of R is the *principal ideal* denoted (a) or aR. We say that a *generates* the principal ideal (a). The other generators of (a) are the *associates* of a: elements $b = ua$ where u is a unit of R.

Proposition 1.1.4. *Every ideal in $\mathbb{Z}$ is principal.*

Definition 1.1.5. *A Principal Ideal Domain or PID is a (nonzero) commutative ring R such that*

(i) $ab = 0 \iff a = 0$ *or* $b = 0$;
(ii) *every ideal of R is principal.*

So $\mathbb{Z}$ is a principal ideal domain. Every nonzero ideal of $\mathbb{Z}$ has a unique positive generator.

1.2. Greatest Common Divisors in $\mathbb{Z}$.

Theorem 1.2.1. *Let $a, b \in \mathbb{Z}$.*

(1) *There exists a unique integer d satisfying*
  (i) $d|a$ *and* $d|b$;

(ii) *if* $c|a$ *and* $c|b$ *then* $c|d$;
(iii) $d \geq 0$.
(2) *The integer* d *can be expressed in the form* $d = au + bv$ *with* $u, v \in \mathbb{Z}$.

Definition 1.2.2. *For* $a, b \in \mathbb{Z}$ *we define the* Greatest Common Divisor *(or GCD) of* a *and* b *to be the integer* d *with the properties given in the theorem. Notation:* $\gcd(a, b)$*, or sometimes just* (a, b)*. Integers* a *and* b *are said to be* coprime *(or relatively prime) if* $\gcd(a, b) = 1$.

So integers are coprime if they have no common factors other than ± 1. The identity $\gcd(a, b) = au + bv$ is sometimes called *Bezout's identity*.

Corollary 1.2.3. *[Basic Properties of* $\gcd$*] For all* $a, b, k, m \in \mathbb{Z}$*:*
(1) a *and* b *are coprime iff there exist* $u, v \in \mathbb{Z}$ *such that* $au + bv = 1$;
(2) $\gcd(a, b) = \gcd(b, a) = \gcd(|a|, |b|)$;
(3) $\gcd(ka, kb) = |k| \gcd(a, b)$;
(4) $\gcd(a, 0) = |a|$; $\gcd(a, 1) = 1$;
(5) $\gcd(a, b) = \gcd(a, b + ka)$ *for all* $k \in \mathbb{Z}$;
(6) *if* $\gcd(a, m) = \gcd(b, m) = 1$ *then* $\gcd(ab, m) = 1$;
(7) *if* $\gcd(a, b) = 1$ *then* $\gcd(a^k, b^l) = 1$ *for all* $k, l \in \mathbb{N}$.

Lemma 1.2.4. *[Euler's Lemma] If* $a|bc$ *and* $\gcd(a, b) = 1$ *then* $a|c$.

If $a_1, a_2, \ldots, a_n$ is any finite sequence of integers then we similarly find that the ideal they generate, $I = (a_1, a_1, \ldots, a_n) = \{k_1a_1 + k_2a_2 + \cdots + k_na_n \mid k_1, k_2, \ldots, k_n \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}$, hence $I = (d)$ for a unique $d \geq 0$, and we define $d = \gcd(a_1, a_2, \ldots, a_n)$. We say that

$a_1, a_2, \ldots, a_n$ are *coprime* if $\gcd(a_1, a_2, \ldots, a_n) = 1$. This is weaker than the condition that $\gcd(a_i, a_j) = 1$ for all $i \neq j$: for example, $\gcd(6, 10, 15) = 1$ since $6 + 10 - 15 = 1$, but no pair of $6, 10, 15$ is coprime. When $\gcd(a_i, a_j) = 1$ for all $i \neq j$, we say that the a_i are *pairwise coprime*.

Our proofs have been non-constructive. A very important computational tool is the Euclidean Algorithm, which computes $d = \gcd(a, b)$ given a and $b \in \mathbb{Z}$, and its extended form which also computes the (non-unique) u, v such that $d = au + bv$.

1.3. **The Euclidean Algorithm in $\mathbb{Z}$.** The Euclidean Algorithm is an efficient method of computing $\gcd(a, b)$ for any two integers a and b, without having to factorize them. It may also be used to compute the coefficients u and v in the identity $d = \gcd(a, b) = au + bv$.

The basic idea is this. We may assume $b > a > 0$ (see the Basic Properties above). Write $r = b - aq$ with $0 \leq r < a$; then $\gcd(a, b) = \gcd(r, a)$ and we have reduced the problem to a smaller one. After a finite number of steps we reach 0, and the last positive integer in the sequence $a, b, r, \ldots$ is the $\gcd$.

Example: $(963, 657) = (657, 963) = (306, 657) = (45, 306) = (36, 45) = (9, 36) = (0, 9) = 9$. Here we have used $963 - 657 = 306$, $657 - 2 \cdot 306 = 45$, $306 - 6 \cdot 45 = 36$, $45 - 36 = 9$.

To solve $9 = 963u + 657v$ we can back-substitute in these equations: $9 = 45 - 36 = 45 - (306 - 6 \cdot 45) = 7 \cdot 45 - 306 = 7 \cdot (657 - 2 \cdot 306) - 306 = 7 \cdot 657 - 15 \cdot 306 = 7 \cdot 657 - 15(963 - 657) = 22 \cdot 657 - 15 \cdot 963$, so $u = -15$ and $v = 22$.

There is a simpler way of keeping track of all these coefficients while reducing the amount which needs to be written down, using some auxiliary variables, which leads to the Euclidean algorithm. We give it in a form which keeps all the auxiliary variables positive which is easier to carry out in practice.

Extended Euclidean Algorithm: Given positive integers a and b, this algorithm computes (d, u, v) such that $d = \gcd(a, b) = au + bv$:

(1) Set $a_1 = a$, $a_2 = b$; $x_1 = 1$, $x_2 = 0$; $y_1 = 0$, $y_2 = 1$.
(2) Let $q = [a_1/a_2]$.
(3) Set $a_3 = a_1 - qa_2$; $x_3 = x_1 + qx_2$; $y_3 = y_1 + qy_2$.
(4) Set $a_1 = a_2$, $a_2 = a_3$; $x_1 = x_2$, $x_2 = x_3$; $y_1 = y_2$, $y_2 = y_3$.
(5) If $a_2 > 0$ loop back to Step 2.
(6) If $ax_1 - by_1 > 0$ return $(d, u, v) = (a_1, x_1, -y_1)$, else return $(d, u, v) = (a_1, -x_1, y_1)$.

Example: In the previous example, the a_i sequence is

$$963, 657, 306, 45, 36, 9, 0$$

using quotients

$$q = 1, 2, 6, 1, 4.$$

So the x_i sequence is

$$1, 0, 1, 2, 13, 15, 73$$

and the y_i sequence is

$$0, 1, 1, 3, 19, 22, 107.$$

Using the last x_i and y_i provides a check:

$$73a - 107b = 73 \cdot 963 - 107 \cdot 657 = 0$$

and the preceding values give the solution:

$$15a - 22b = 15 \cdot 963 - 22 \cdot 657 = -9.$$

So we may take $u = -15$, $v = 22$.

1.4. **Primes and unique factorization.**

Definition 1.4.1. *A prime number (or prime for short) is an integer $p > 1$ whose only divisors are ± 1 and $\pm p$; the set of primes is denoted $\mathbb{P}$:*

$$p \in \mathbb{P} \iff p > 1 \quad \text{and} \quad p = ab \implies a = \pm 1 \quad \text{or} \quad b = \pm 1.$$

For example $2, 3, 5, 7, 11$ are primes. Integers $n > 1$ which are not prime are called *composite*. If a is any integer then either $p|a$, in which case $\gcd(p, a) = p$, or $p \not| a$, in which case $\gcd(p, a) = 1$.

Lemma 1.4.2. *Let p be a prime and $a, b \in \mathbb{Z}$. If $p|ab$ then either $p|a$ or $p|b$ (or both).*

This property of primes is very important, and the uniqueness of prime factorization relies on it. (It is easy to see that composite numbers do not have this property.) More generally:

Corollary 1.4.3. *Let p be a prime and $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. Then*

$$p|a_1 a_2 \ldots a_n \implies p|a_i \quad \text{for some } i.$$

Theorem 1.4.4 (Fundamental Theorem of Arithmetic)**.** *Every positive integer n is a product of prime numbers, and its factorization into primes is unique up to the order of the factors.*

Note that this includes $n = 1$ which is an "empty" product, and primes themselves with only one factor in the product. Collecting together any powers of primes which occur in a prime factorization, we obtain

Corollary 1.4.5. *Every positive integer n may be expressed uniquely in the form*

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$$

where $p_1, \dots, p_k$ are primes with $p_1 < p_2 < \cdots < p_k$ and each $e_i \geq 1$. Alternatively, every positive integer n may be expressed uniquely in the form

$$n = \prod_{p \in \mathbb{P}} p^{e_p}$$

where the product is over all *primes, each $e_p \geq 0$, but only a* finite *number of $e_p > 0$.*

The exponent e_p which appears in this standard factorization of n is denoted $\mathrm{ord}_p(n)$; it is characterized by the following property:

$$e = \mathrm{ord}_p(n) \iff p^e | n \quad \text{and} \quad p^{e+1} \nmid n.$$

For example, $700 = 2^2 \cdot 5^2 \cdot 7$, so $\mathrm{ord}_2(700) = \mathrm{ord}_5(700) = 2$, $\mathrm{ord}_7(700) = 1$, and $\mathrm{ord}_p(700) = 0$ for primes $p \neq 2, 5, 7$. Every positive integer n is uniquely determined by the sequence of exponents $\mathrm{ord}_p(n)$.

This standard factorization of positive integers into primes may be extended to negative integers by allowing a factor ± 1 in front of the product, and to nonzero rational numbers by allowing the exponents to be negative. We may accordingly extend the function ord_p to $\mathbb{Q}^*$, by setting $\mathrm{ord}_p(-n) = \mathrm{ord}_p(n)$ and $\mathrm{ord}_p(n/d) = \mathrm{ord}_p(n) - \mathrm{ord}_p(d)$ for nonzero rationals n/d. [You should check that this is well-defined, independent of the representation of the fraction n/d.] Then we have the following extension of the main theorem on unique factorization:

Corollary 1.4.6. *Every nonzero rational number x may be uniquely expressed in the form*

$$x = \pm \prod_{p \in \mathbb{P}} p^{\mathrm{ord}_p(x)}.$$

For example, $-72/91 = -2^3 3^2 7^{-1} 13^{-1}$.

Many facts about integers may easily be proved using their unique factorization into primes. For example:

Proposition 1.4.7. *Let $m, n \in \mathbb{Z}$ be nonzero. Then*

$$m = \pm n \iff \mathrm{ord}_p(m) = \mathrm{ord}_p(n) \quad \forall p \in \mathbb{P}.$$

The function ord_p works rather like a logarithm. The following is easy to check:

Proposition 1.4.8. *Let $m, n \in \mathbb{Z}$ be nonzero. Then $\mathrm{ord}_p(mn) = \mathrm{ord}_p(m) + \mathrm{ord}_p(n)$.*

The previous result looks elementary enough, but it is sufficient to imply the uniqueness of prime factorization: for if $n = \prod p^{e_p}$ is *any* factorization of n in to primes, applying ord_q to both sides (where q is some fixed prime) and using the Proposition gives

$$\mathrm{ord}_q(n) = \sum e_p \mathrm{ord}_q(p) = e_q,$$

since $\mathrm{ord}_q(q) = 1$ and $\mathrm{ord}_q(p) = 0$ when $p \neq q$. It follows that the exponents e_p are uniquely determined.

Proposition 1.4.9. *Let $n \in \mathbb{Z}$ be nonzero. Then n is a perfect square if and only if $n > 0$ and $\mathrm{ord}_p(n)$ is even for all primes p.*

We end this section with a famous and ancient result of Euclid.

Theorem 1.4.10. *[Euclid] The number of primes is infinite.*

Note that this proof actually shows how to construct a "new" prime from any given finite set of known primes. Variations of this proof can show that there are infinitely many primes of various special forms: see the Exercises.

1.5. **Unique Factorization Domains.** Theorem 1.4.4 (extended to include negative integers) may be expressed succinctly by the statement that $\mathbb{Z}$ is a *Unique Factorization Domain* or UFD. Roughly speaking, a UFD is a ring in which every element has an essentially unique factorization as a unit times a product of "prime" elements. Every PID is a UFD (but not conversely: $\mathbb{Z}[X]$ is a UFD but not a PID), and an important source of PIDs is rings which have a "division algorithm" similar to the one for $\mathbb{Z}$. Such rings are called Euclidean Domains, and we start by defining these.

Definition 1.5.1. (a) *A nonzero ring R is an* Integral Domain *if, for $a, b \in R$,*

$$ab = 0 \iff (a = 0 \quad \textit{or} \quad b = 0).$$

(b) *A nonzero ring R is a* Euclidean Domain *or ED if it is an integral domain equipped with a function $\lambda : R - \{0\} \to \mathbb{N}_0$ such that, for $a, b \in R$ with $a \neq 0$, there exist $q, r \in R$ such that*

$$b = aq + r \qquad \textit{with either } r = 0 \textit{ or } \lambda(r) < \lambda(a).$$

Examples:

- $\mathbb{Z}$ is an ED with $\lambda(n) = |n|$: this is what Proposition 1.1.3 states (though note that the definition of an ED does not require q and r to be unique).
- Any field F is an ED with $\lambda(x) = 0$ for all $x \neq 0$; this is a degenerate example since we may always take $r = 0$ in division.
- If F is a field then the polynomial ring $F[X]$ is an ED, using the degree function $\lambda(f(X)) = \deg(f(X))$. The required division property is well-known, being just the usual long division for polynomials.

  It is important that F is a field here: for example, $\mathbb{Z}[X]$ is *not* Euclidean (exercise).
- The ring $\mathbb{Z}[i]$ of *Gaussian Integers* is defined as

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\};$$

  it is a subring of $\mathbb{C}$. We will study this in some detail as it gives another example of a Euclidean Domain which is of interest in number theory, both for its own sake and also for proving some properties of the ordinary or "rational" integers $\mathbb{Z}$. The Euclidean function λ on $\mathbb{Z}[i]$ is usually called the *norm* and denoted N:

$$N(\alpha) = \alpha\overline{\alpha} = a^2 + b^2 \qquad \text{for } \alpha = a + bi \in \mathbb{Z}[i].$$

Theorem 1.5.2. *The ring $\mathbb{Z}[i]$ of Gaussian Integers is a Euclidean Domain.*

Lemma 1.5.3. *The norm function N on $\mathbb{Z}[i]$ has the following properties:*

(1) *Multiplicativity: for all α, $\beta \in \mathbb{Z}[i]$, $N(\alpha\beta) = N(\alpha)N(\beta)$;*

(2) *Positivity:* $N(0) = 0$, $N(\alpha) \geq 1$ *for* $\alpha \neq 0$;
(3) *Units:* $N(\alpha) = 1 \iff \alpha \in U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$.

Recall that for a ring R, the group of *units* (invertible elements) is denoted $U(R)$. Elements of an integral domain are called *associate* if one is a unit times the other, or (equivalently) if each divides the other.

Example: Take $\alpha = 3 + 4i$ and $\beta = 10 + 11i$. Then

$$\frac{10+11i}{3+4i} = \frac{(10+11i)(3-4i)}{25} = \frac{74-7i}{25} = 3 + \frac{-1-7i}{25},$$

so the quotient is 3 and remainder $(10 + 11i) - 3(3 + 4i) = 1 - i$. Check: $N(1 - i) = 2$ is less than $N(3 + 4i) = 25$.

Just as we did for $\mathbb{Z}$, we can now prove that every ED is a PID:

Theorem 1.5.4. *Let R be a Euclidean Domain. Then R is a Principal Ideal Domain.*

In a PID we have $\gcd$s just as in $\mathbb{Z}$, and Bezout's identity. In general we do not have uniqueness of $\gcd$s, only uniqueness up to associates (multiplication by a unit). (In $\mathbb{Z}$ we avoided this non-uniqueness by insisting that all $\gcd$s were non-negative.)

Definition 1.5.5. *In a ring R, a $\gcd$ of two elements a and b is an element d satisfying*
(i) $d|a$ *and* $d|b$;
(ii) *if* $c|a$ *and* $c|b$ *then* $c|d$.

Lemma 1.5.6. *If $\gcd(a, b)$ exists then it is unique up to associates.*

Because of this non-uniqueness we cannot talk about *the* $\gcd$, only *a* $\gcd$ of a and b. In specific rings, one may impose an extra condition to ensure uniqueness: in $\mathbb{Z}$ we insisted that $\gcd(a,b) \geq 0$; in the polynomial ring $F[X]$ (with F a field) one usually insists that $\gcd(a(X), b(X))$ is *monic* (with leading coefficient 1).

Proposition 1.5.7. *In a PID, the* $\gcd$ *of two elements* a *and* b *exists, and may be expressed in the form* $au + bv$.

So in a PID, whether Euclidean or not, the $\gcd$ always exists. However, it is only in a ED that computing $\gcd$s is easily possible via the Euclidean Algorithm.

Example: Take $\alpha = 3 + 4i$ and $\beta = 10 + 11i$. Then from the previous example we have $\beta - 3\alpha = 1 - i$. Similarly, $\alpha - 3i(1-i) = i$, and lastly $1 - i = i(-1-i)$ with zero remainder. The last nonzero remainder was i which is therefore a $\gcd$ of α and β; one would normally adjust this since i is a unit and say that $\gcd(\alpha, \beta) = 1$. Back-substitution gives $i = \alpha - 3i(\beta - 3\alpha) = (1+9i)\alpha - 3i\beta$, so finally $1 = (9 - i)\alpha - 3\beta$.

The next step is to show that every PID is also a unique factorization domain. In the case of $\mathbb{Z}$, we used the Euclidean property again, and not just the PID property, for this step, but since there are rings which are PIDs but not Euclidean we give a proof which works for all PIDs.

Definition 1.5.8. *In an integral domain* R, *an element* p *is called* irreducible *if it is neither* 0 *nor a unit and* $p = ab$ *implies that either* a *or* b *is a unit;* p *is called* prime *if it is neither* 0 *nor a unit and* $p|ab$ *implies that either* $p|a$ *or* $p|b$.

Lemma 1.5.9. *Every prime is irreducible. In a PID, every irreducible is prime.*

The last property will be crucial in proving the uniqueness of factorizations into irreducibles, but for the existence we need to do some more preparation. The following lemma is called the "ascending chain condition" or ACC for ideals in a PID.

Lemma 1.5.10. *Let R be a PID. Let $(a_i)_{i\in\mathbb{N}}$ be a sequence of elements of R with $(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \dots$. (So each a_i is a multiple of the next). Then there exists k such that $(a_k) = (a_{k+1}) = (a_{k+2}) = \dots$, so the chain of ideals stabilizes. Hence any strictly ascending chain of ideals $(a_1) \subset (a_2) \subset (a_3) \subset \dots$ must be finite.*

This lemma is used to replace induction in the proof of the existence of factorizations into irreducibles, which was used for $\mathbb{Z}$.

Proposition 1.5.11. *Let R be a PID. Every element of R which is neither 0 nor a unit is a product of irreducibles.*

Finally, we use the fact that in a PID irreducibles are prime to prove that the factorizations of any given nonzero non-unit are essentially the same, up to reordering the factors and replacing irreducibles by associates.

Definition 1.5.12. *An Integral Domain R is a* Unique Factorization Domain *or UFD if*

(i) *every nonzero element may be expressed as a unit times a product of irreducibles;*
(ii) *the factorization in (i) is unique up to the order of the factors and replacing the irreducibles by associates; that is, if $a \in R$ is nonzero and*

$$a = up_1p_2\dots p_r = vq_1q_2\dots q_s$$

with u, v units and all p_i, q_j irreducibles, then $r = s$, and after permuting the q_j if necessary, there are units v_j for $1 \leq j \leq r$ such that $q_j = v_j p_j$ and $u = v v_1 v_2 \dots v_r$.

Theorem 1.5.13. *Let R be a PID. Then R is a UFD.*

Example (continued): Since the ring $\mathbb{Z}[i]$ of Gaussian Integers is Euclidean, it is a PID and a UFD. We have already determined that its units are the four elements ± 1 and $\pm i$, but what are its primes/irreducibles?

(1) If $\pi \in \mathbb{Z}[i]$ is prime then π divides some ordinary "rational" prime p, since if $n = N(\pi) = \pi\overline{\pi}$ then $\pi | n$ so by primality of π, π divides at least one prime factor p of n.

(2) If $N(\pi) = p$ is prime, then π is irreducible: for if $\pi = \alpha\beta$ then $p = N(\pi) = N(\alpha)N(\beta)$, so one of α, β has norm 1 and is a unit. For example, $1 + i$, $2 + i$, $3 + 2i$, $4 + i$ are prime since their norms are 2, 5, 13, 17.

(3) If a rational prime p is a sum of two squares, $p = a^2 + b^2$, then setting $\pi = a + bi$ gives $p = N(\pi) = N(\overline{\pi})$, so π and $\overline{\pi}$ are both Gaussian primes. We will prove later, in Theorem 2.4.2, that every rational prime p of the form $4k + 1$ can be expressed in this way; the factors π and $\overline{\pi}$ are not associate (exercise).

(4) However, rational primes q of the form $4k + 3$ can *not* be expressed as sums of two squares, since squares all leave remainder of 0 or 1 when divided by 4, so all numbers of the form $a^2 + b^2$ leave a remainder of 0, 1 or 2 on division by 4. Such primes q remain prime in $\mathbb{Z}[i]$. For if $q = \alpha\beta$ with neither α nor β a unit, then $q^2 = N(\alpha)N(\beta)$ with both $N(\alpha)$, $N(\beta) > 1$, so (by unique factorization in $\mathbb{Z}$) we must have $N(\alpha) = N(\beta) = q$, so q would be a sum of two squares.

We sum up this example as follows; we have proved everything stated here except for the fact that all primes of the form $4k+1$ are sums of two squares (Theorem 2.4.2), and the remark about associates (exercise).

Theorem 1.5.14. *The ring $\mathbb{Z}[i]$ of Gaussian Integers is a Euclidean Domain and hence also a Principal Ideal Domain and a Unique Factorization Domain. Its units are the four elements ± 1, $\pm i$. Its primes are as follows (together with their associates):*

(1) $1+i$, *of norm* 2;
(2) *each rational prime p of the form $4k+1$ is a sum of two squares, $p=a^2+b^2$, and p factorizes in $\mathbb{Z}[i]$ as $p=\pi\overline{\pi}$ where $\pi=a+bi$ and $\overline{\pi}=a-bi$ are non-associate Gaussian primes of norm p;*
(3) *each rational prime q of the form $4k+3$ is also a Gaussian prime.*

For example, here are some Gaussian factorizations: $123+456i = 3\cdot(1+2i)\cdot(69+14i)$ (the last factor has prime norm 4957), $2000=(1+i)^8(1+2i)^3(1-2i)^3$.

```
sage: Qi.<i> = QQ.extension(x^2+1)
sage: 2018.factor()
2 * 1009
sage: Qi(2018).factor()
(i) * (15*i - 28) * (i + 1)^2 * (15*i + 28)
sage: (123+456*i).norm().factor()
3^2 * 5 * 4957
sage: (123+456*i).factor()
(-1) * (-14*i - 69) * (2*i + 1) * 3
```

There are other "number rings" similar to $\mathbb{Z}[i]$, but not many which are known to have unique factorization. A complete study requires more algebra, and is done in Algebraic Number Theory. Here are some further examples.

Example: The ring $R = \mathbb{Z}[\sqrt{-2}]$ is also Euclidean and hence a UFD. The proof is almost identical to the one given above for $\mathbb{Z}[i]$, using the norm $N(\alpha) = \alpha\overline{\alpha}$, so that $N(a + b\sqrt{-2}) = a^2 + 2b^2$. The key fact which makes R Euclidean via the norm is that every point in the complex plane is at distance less than 1 from the nearest element of R, as was the case with $\mathbb{Z}[i]$. Factorization of primes p now depends on $p \pmod 8$.

Example: The ring $R = \mathbb{Z}[\sqrt{-3}]$ is **not** Euclidean, and neither a PID nor a UFD. For example, $4 = 2 \cdot 2 = (1 + \sqrt{-3}) \cdot (1 - \sqrt{-3})$ with all factors on the right irreducible in R. Also: the ideal $(2, 1 + \sqrt{-3})$ is not principal; and the element 2 is irreducible but not prime (as the previous equation shows, since neither $1 \pm \sqrt{-3}$ are divisible by 2 in R). However, if we enlarge the ring by including numbers of the form $(a+b\sqrt{-3})/2$ where a and b are both odd, we obtain the larger ring $S = \mathbb{Z}[\omega]$, where $\omega = (-1 + \sqrt{-3})/2$, satisfying $\omega^2 + \omega + 1 = 0$, which is Euclidean and hence a UFD. The norm is again $N(\alpha) = \alpha\overline{\alpha}$; with $\alpha = a + b\omega$ one computes that $N(\alpha) = a^2 - ab + b^2$, and $4N(\alpha) = (2a - b)^2 + 3b^2$. This ring turns out to be useful in the solution of the Fermat equation $x^3 + y^3 = z^3$.

Example: As in the previous example, the ring $\mathbb{Z}[\sqrt{-19}]$ is not Euclidean. Enlarging it to $R = \mathbb{Z}[\omega]$, where now $\omega = (-1 + \sqrt{-19})/2$, satisfying $w^2 + w + 5 = 0$, we find a ring which is still not Euclidean, but is a PID and hence a UFD. This example shows that not every PID is Euclidean. We omit the details.