1

Basic properties of the integers

This chapter discusses some of the basic properties of the integers, including the notions of divisibility and primality, unique factorization into primes, greatest common divisors, and least common multiples.

1.1 Divisibility and primality

Consider the integers $\mathbb{Z} := \{\ldots, -2, -1, 0, 1, 2, \ldots\}$. For $a, b \in \mathbb{Z}$, we say that b **divides** a, or alternatively, that a is **divisible by** b, if there exists $c \in \mathbb{Z}$ such that $a = bc$. If b divides a, then b is called a **divisor** of a, and we write $b \mid a$. If b does not divide a, then we write $b \nmid a$.

We first state some simple facts:

Theorem 1.1. *For all $a, b, c \in \mathbb{Z}$, we have*

(i) $a \mid a$, $1 \mid a$, *and* $a \mid 0$;

(ii) $0 \mid a$ *if and only if* $a = 0$;

(iii) $a \mid b$ *and* $a \mid c$ *implies* $a \mid (b + c)$;

(iv) $a \mid b$ *implies* $a \mid -b$;

(v) $a \mid b$ *and* $b \mid c$ *implies* $a \mid c$.

Proof. These properties can be easily derived from the definition using elementary facts about the integers. For example, $a \mid a$ because we can write $a = a \cdot 1$; $1 \mid a$ because we can write $a = 1 \cdot a$; $a \mid 0$ because we can write $0 = a \cdot 0$. We leave it as an easy exercise for the reader to verify the remaining properties. □

Another simple but useful fact is the following:

Theorem 1.2. *For all $a, b \in \mathbb{Z}$, we have $a \mid b$ and $b \mid a$ if and only if $a = \pm b$.*

Proof. Clearly, if $a = \pm b$, then $a \mid b$ and $b \mid a$. So let us assume that $a \mid b$ and $b \mid a$, and prove that $a = \pm b$. If either of a or b are zero, then part (ii) of the previous theorem implies that the other is zero. So assume that neither is zero. Now, $b \mid a$ implies $a = bc$ for some $c \in \mathbb{Z}$. Likewise, $a \mid b$ implies $b = ad$ for some $d \in \mathbb{Z}$. From this, we obtain $b = ad = bcd$, and canceling b from both sides of the equation $b = bcd$, we obtain $1 = cd$. The only possibility is that either $c = d = -1$, in which case $a = -b$, or $c = d = 1$, in which case $a = b$. □

Any integer n is trivially divisible by ± 1 and $\pm n$. We say that an integer p is **prime** if $p > 1$ and the only divisors of p are the trivial divisors ± 1 and $\pm p$. Conversely, an integer n is called **composite** if $n > 1$ and it is not prime. So an integer $n > 1$ is composite if and only if $n = ab$ for some integers a, b with $1 < a < n$ and $1 < b < n$. The first few primes are

$$2, 3, 5, 7, 11, 13, 17, \ldots.$$

The number 1 is not considered to be either prime or composite. Also, we do not consider the negative of a prime (e.g., -2) to be prime (although one can, and some authors do so).

A basic fact is that any non-zero integer can be expressed as a signed product of primes in an essentially unique way. More precisely:

Theorem 1.3 (Fundamental theorem of arithmetic). *Every non-zero integer n can be expressed as*

$$n = \pm p_1^{e_1} \cdots p_r^{e_r},$$

where the p_i are distinct primes and the e_i are positive integers. Moreover, this expression is unique, up to a reordering of the primes.

Note that if $n = \pm 1$ in the above theorem, then $r = 0$, and the product of zero terms is interpreted (as usual) as 1.

To prove this theorem, we may clearly assume that n is positive, since otherwise, we may multiply n by -1 and reduce to the case where n is positive.

The proof of the existence part of Theorem 1.3 is easy. This amounts to showing that every positive integer n can be expressed as a product (possibly empty) of primes. We may prove this by induction on n. If $n = 1$, the statement is true, as n is the product of zero primes. Now let $n > 1$, and assume that every positive integer smaller than n can be expressed as a product of primes. If n is a prime, then the statement is true, as n is the

product of one prime; otherwise, n is composite, and so there exist $a, b \in \mathbb{Z}$ with $1 < a < n$, $1 < b < n$, and $n = ab$; by the induction hypothesis, both a and b can be expressed as a product of primes, and so the same holds for n.

The uniqueness part of Theorem 1.3 is by no means obvious, and most of the rest of this section and the next section are devoted to developing a proof of this. We give a quite leisurely proof, introducing a number of other very important tools and concepts along the way that will be useful later. An essential ingredient in this proof is the following:

Theorem 1.4 (Division with remainder property). *For $a, b \in \mathbb{Z}$ with $b > 0$, there exist unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$.*

Proof. Consider the set S of non-negative integers of the form $a - zb$ with $z \in \mathbb{Z}$. This set is clearly non-empty, and so contains a minimum. Let r be the smallest integer in this set, with $r = a - qb$ for $q \in \mathbb{Z}$. By definition, we have $r \geq 0$. Also, we must have $r < b$, since otherwise, we would have $0 \leq r - b < r$ and $r - b = a - (q + 1)b \in S$, contradicting the minimality of r.

That proves the existence of r and q. For uniqueness, suppose that $a = bq + r$ and $a = bq' + r'$, where $0 \leq r < b$ and $0 \leq r' < b$. Then subtracting these two equations and rearranging terms, we obtain

$$r' - r = b(q - q'). \tag{1.1}$$

Now observe that by assumption, the left-hand side of (1.1) is less than b in absolute value. However, if $q \neq q'$, then the right-hand side of (1.1) would be at least b in absolute value; therefore, we must have $q = q'$. But then by (1.1), we must have $r = r'$. □

In the above theorem, it is easy to see that $q = \lfloor a/b \rfloor$, where for any real number x, $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x. We shall write $r = a \bmod b$; that is, $a \bmod b$ denotes the remainder in dividing a by b. It is clear that $b \mid a$ if and only if $a \bmod b = 0$.

One can generalize the notation $a \bmod b$ to all integers a and b, with $b \neq 0$: we define $a \bmod b := a - bq$, where $q = \lfloor a/b \rfloor$.

In addition to the "floor" function $\lfloor \cdot \rfloor$, the "ceiling" function $\lceil \cdot \rceil$ is also useful: for any real number x, $\lceil x \rceil$ is defined as the smallest integer greater than or equal to x.

Exercise 1.1. Let n be a composite integer. Show that there exists a prime p dividing n, such that $p \leq |n|^{1/2}$.

EXERCISE 1.2. For integer n and real x, show that $n \leq x$ if and only if $n \leq \lfloor x \rfloor$.

EXERCISE 1.3. For real x and positive integer n, show that $\lfloor \lfloor x \rfloor / n \rfloor = \lfloor x/n \rfloor$. In particular, for positive integers a, b, c, $\lfloor \lfloor a/b \rfloor / c \rfloor = \lfloor a/(bc) \rfloor$.

EXERCISE 1.4. For real x, show that $2\lfloor x \rfloor \leq \lfloor 2x \rfloor \leq 2\lfloor x \rfloor + 1$.

EXERCISE 1.5. For positive integers m and n, show that the number of multiples of m among $1, 2, \ldots, n$ is $\lfloor n/m \rfloor$. More generally, for integer $m \geq 1$ and real $x \geq 0$, show that the number of multiples of m in the interval $[1, x]$ is $\lfloor x/m \rfloor$.

EXERCISE 1.6. For integers a, b with $b < 0$, show that $b < a \bmod b \leq 0$.

1.2 Ideals and greatest common divisors

To carry on with the proof of Theorem 1.3, we introduce the notion of an **ideal of** $\mathbb{Z}$, which is a non-empty set of integers that is closed under addition, and under multiplication by an arbitrary integer. That is, a non-empty set $I \subseteq \mathbb{Z}$ is an ideal if and only if for all $a, b \in I$ and all $z \in \mathbb{Z}$, we have

$$a + b \in I \quad \text{and} \quad az \in I.$$

Note that for an ideal I, if $a \in I$, then so is $-a$, since $-a = a \cdot (-1) \in I$. It is easy to see that any ideal must contain 0: since an ideal I must contain some element a, and by the closure properties of ideals, we must have $0 = a + (-a) \in I$. It is clear that $\{0\}$ and $\mathbb{Z}$ are ideals. Moreover, an ideal I is equal to $\mathbb{Z}$ if and only if $1 \in I$—to see this, note that $1 \in I$ implies that for all $z \in \mathbb{Z}$, $z = 1 \cdot z \in I$, and hence $I = \mathbb{Z}$; conversely, if $I = \mathbb{Z}$, then in particular, $1 \in I$.

For $a \in \mathbb{Z}$, define $a\mathbb{Z} := \{az : z \in \mathbb{Z}\}$; that is, $a\mathbb{Z}$ is the set of all integer multiples of a. It is easy to see that $a\mathbb{Z}$ is an ideal: for $az, az' \in a\mathbb{Z}$ and $z'' \in \mathbb{Z}$, we have $az + az' = a(z + z') \in a\mathbb{Z}$ and $(az)z'' = a(zz'') \in a\mathbb{Z}$. The set $a\mathbb{Z}$ is called the **ideal generated by** a, and any ideal of the form $a\mathbb{Z}$ for some $a \in \mathbb{Z}$ is called a **principal ideal**.

We observe that for all $a, b \in \mathbb{Z}$, we have $a \in b\mathbb{Z}$ if and only if $b \mid a$. We also observe that for any ideal I, we have $a \in I$ if and only if $a\mathbb{Z} \subseteq I$. Both of these observations are simple consequences of the definitions, as the reader may verify. Combining these two observations, we see that $a\mathbb{Z} \subseteq b\mathbb{Z}$ if and only if $b \mid a$.

We can generalize the above method of constructing ideals. For

$a_1, \ldots, a_k \in \mathbb{Z}$, define

$$a_1\mathbb{Z} + \cdots + a_k\mathbb{Z} := \{a_1z_1 + \cdots + a_kz_k : z_1, \ldots, z_k \in \mathbb{Z}\}.$$

That is, $a_1\mathbb{Z} + \cdots + a_k\mathbb{Z}$ consists of all linear combinations, with integer coefficients, of $a_1, \ldots, a_k$. We leave it to the reader to verify that $a_1\mathbb{Z} + \cdots + a_k\mathbb{Z}$ is an ideal and contains $a_1, \ldots, a_k$; it is called the **ideal generated by** $a_1, \ldots, a_k$. In fact, this ideal is the "smallest" ideal containing $a_1, \ldots, a_k$, in the sense that any other ideal that contains $a_1, \ldots, a_k$ must already contain this ideal (verify).

***Example* 1.1.** Let $a := 3$ and consider the ideal $a\mathbb{Z}$. This consists of all integer multiples of 3; that is, $a\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$. □

***Example* 1.2.** Let $a_1 := 3$ and $a_2 := 5$, and consider the ideal $a_1\mathbb{Z} + a_2\mathbb{Z}$. This ideal contains $2a_1 - a_2 = 1$. Since it contains 1, it contains all integers; that is, $a_1\mathbb{Z} + a_2\mathbb{Z} = \mathbb{Z}$. □

***Example* 1.3.** Let $a_1 := 4$ and $a_2 := 6$, and consider the ideal $a_1\mathbb{Z} + a_2\mathbb{Z}$. This ideal contains $a_2 - a_1 = 2$, and therefore, it contains all even integers. It does not contain any odd integers, since the sum of two even integers is again even. □

The following theorem says that all ideals of $\mathbb{Z}$ are principal.

Theorem 1.5. *For any ideal $I \subseteq \mathbb{Z}$, there exists a unique non-negative integer d such that $I = d\mathbb{Z}$.*

Proof. We first prove the existence part of the theorem. If $I = \{0\}$, then $d = 0$ does the job, so let us assume that $I \neq \{0\}$. Since I contains non-zero integers, it must contain positive integers, since if $z \in I$ then so is $-z$. Let d be the smallest positive integer in I. We want to show that $I = d\mathbb{Z}$.

We first show that $I \subseteq d\mathbb{Z}$. To this end, let c be any element in I. It suffices to show that $d \mid c$. Using the division with remainder property, write $c = qd + r$, where $0 \leq r < d$. Then by the closure properties of ideals, one sees that $r = c - qd$ is also an element of I, and by the minimality of the choice of d, we must have $r = 0$. Thus, $d \mid c$.

We next show that $d\mathbb{Z} \subseteq I$. This follows immediately from the fact that $d \in I$ and the closure properties of ideals.

That proves the existence part of the theorem. As for uniqueness, note that if $d\mathbb{Z} = d'\mathbb{Z}$, we have $d \mid d'$ and $d' \mid d$, from which it follows by Theorem 1.2 that $d' = \pm d$. □

For $a, b \in \mathbb{Z}$, we call $d \in \mathbb{Z}$ a **common divisor** of a and b if $d \mid a$ and

$d \mid b$; moreover, we call such a d a **greatest common divisor** of a and b if d is non-negative and all other common divisors of a and b divide d.

Theorem 1.6. *For any $a, b \in \mathbb{Z}$, there exists a unique greatest common divisor d of a and b, and moreover, $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.*

Proof. We apply the previous theorem to the ideal $I := a\mathbb{Z} + b\mathbb{Z}$. Let $d \in \mathbb{Z}$ with $I = d\mathbb{Z}$, as in that theorem. We wish to show that d is a greatest common divisor of a and b. Note that $a, b, d \in I$ and d is non-negative.

Since $a \in I = d\mathbb{Z}$, we see that $d \mid a$; similarly, $d \mid b$. So we see that d is a common divisor of a and b.

Since $d \in I = a\mathbb{Z} + b\mathbb{Z}$, there exist $s, t \in \mathbb{Z}$ such that $as + bt = d$. Now suppose $a = a'd'$ and $b = b'd'$ for $a', b', d' \in \mathbb{Z}$. Then the equation $as + bt = d$ implies that $d'(a's + b't) = d$, which says that $d' \mid d$. Thus, any common divisor d' of a and b divides d.

That proves that d is a greatest common divisor of a and b. As for uniqueness, note that if d'' is a greatest common divisor of a and b, then $d \mid d''$ and $d'' \mid d$, and hence $d'' = \pm d$, and the requirement that d'' is non-negative implies that $d'' = d$. □

For $a, b \in \mathbb{Z}$, we denote by $\gcd(a, b)$ the greatest common divisor of a and b. Note that as we have defined it, $\gcd(a, 0) = |a|$. Also note that when at least one of a or b are non-zero, $\gcd(a, b)$ is the largest positive integer that divides both a and b.

An immediate consequence of Theorem 1.6 is that for all $a, b \in \mathbb{Z}$, there exist $s, t \in \mathbb{Z}$ such that $as + bt = \gcd(a, b)$, and that when at least one of a or b are non-zero, $\gcd(a, b)$ is the smallest positive integer that can be expressed as $as + bt$ for some $s, t \in \mathbb{Z}$.

We say that $a, b \in \mathbb{Z}$ are **relatively prime** if $\gcd(a, b) = 1$, which is the same as saying that the only common divisors of a and b are ± 1. It is immediate from Theorem 1.6 that a and b are relatively prime if and only if $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$, which holds if and only if there exist $s, t \in \mathbb{Z}$ such that $as + bt = 1$.

Theorem 1.7. *For $a, b, c \in \mathbb{Z}$ such that $c \mid ab$ and $\gcd(a, c) = 1$, we have $c \mid b$.*

Proof. Suppose that $c \mid ab$ and $\gcd(a, c) = 1$. Then since $\gcd(a, c) = 1$, by Theorem 1.6 we have $as + ct = 1$ for some $s, t \in \mathbb{Z}$. Multiplying this equation by b, we obtain

$$abs + cbt = b. \tag{1.2}$$

Since c divides ab by hypothesis, and since c clearly divides cbt, it follows that c divides the left-hand side of (1.2), and hence that c divides b. □

As a consequence of this theorem, we have:

Theorem 1.8. *Let p be prime, and let $a, b \in \mathbb{Z}$. Then $p \mid ab$ implies that $p \mid a$ or $p \mid b$.*

Proof. Assume that $p \mid ab$. The only divisors of p are ± 1 and $\pm p$. Thus, $\gcd(p, a)$ is either 1 or p. If $p \mid a$, we are done; otherwise, if $p \nmid a$, we must have $\gcd(p, a) = 1$, and by the previous theorem, we conclude that $p \mid b$. □

An obvious corollary to Theorem 1.8 is that if $a_1, \ldots, a_k$ are integers, and if p is a prime that divides the product $a_1 \cdots a_k$, then $p \mid a_i$ for some $i = 1, \ldots, k$. This is easily proved by induction on k. For $k = 1$, the statement is trivially true. Now let $k > 1$, and assume that statement holds for $k - 1$. Then by Theorem 1.8, either $p \mid a_1$ or $p \mid a_2 \cdots a_{k-1}$; if $p \mid a_1$, we are done; otherwise, by induction, p divides one of $a_2, \ldots, a_{k-1}$.

We are now in a position to prove the uniqueness part of Theorem 1.3, which we can state as follows: if $p_1, \ldots, p_r$ and $p'_1, \ldots, p'_s$ are primes (with duplicates allowed among the p_i and among the p'_j) such that

$$p_1 \cdots p_r = p'_1 \cdots p'_s, \tag{1.3}$$

then $(p_1, \ldots, p_r)$ is just a reordering of $(p'_1, \ldots, p'_s)$. We may prove this by induction on r. If $r = 0$, we must have $s = 0$ and we are done. Now suppose $r > 0$, and that the statement holds for $r - 1$. Since $r > 0$, we clearly must have $s > 0$. Also, as p_1 is obviously divides the left-hand side of (1.3), it must also divide the right-hand side of (1.3); that is, $p_1 \mid p'_1 \cdots p'_s$. It follows from (the corollary to) Theorem 1.8 that $p_1 \mid p'_j$ for some $j = 1, \ldots, s$, and indeed, since p_i and p'_j are both prime, we must have $p_i = p'_j$. Thus, we may cancel p_i from the left-hand side of (1.3) and p'_j from the right-hand side of (1.3), and the statement now follows from the induction hypothesis. That proves the uniqueness part of Theorem 1.3.

Exercise 1.7. Let I be a non-empty set of integers that is closed under addition, that is, $a + b \in I$ for all $a, b \in I$. Show that the condition

$$-a \in I \quad \text{for all } a \in I$$

holds if and only if

$$az \in I \quad \text{for all } a \in I,\ z \in \mathbb{Z}.$$

EXERCISE 1.8. Let a, b, c be positive integers, with $\gcd(a, b) = 1$ and $c \geq ab$. Show that there exist *non-negative* integers s, t such that $c = as + bt$.

EXERCISE 1.9. Show that for any integers a, b with $d := \gcd(a, b) \neq 0$, we have $\gcd(a/d, b/d) = 1$.

1.3 Some consequences of unique factorization

The following theorem is a consequence of just the existence part of Theorem 1.3:

Theorem 1.9. *There are infinitely many primes.*

Proof. By way of contradiction, suppose that there were only finitely many primes; call them $p_1, \ldots, p_k$. Then set $n := 1 + \prod_{i=1}^{k} p_i$, and consider a prime p that divides n. There must be at least one such prime p, since $n \geq 2$, and every positive integer can be written as a product of primes. Clearly, p cannot equal any of the p_i, since if it did, then p would divide $n - \prod_{i=1}^{k} p_i = 1$, which is impossible. Therefore, the prime p is not among $p_1, \ldots, p_k$, which contradicts our assumption that these are the only primes. □

For a prime p, we may define the function ν_p, mapping non-zero integers to non-negative integers, as follows: for integer $n \neq 0$, if $n = p^e m$, where $p \nmid m$, then $\nu_p(n) := e$. We may then write the factorization of n into primes as

$$n = \pm \prod_p p^{\nu_p(n)},$$

where the product is over all primes p, with all but finitely many of the terms in the product equal to 1.

It is also convenient to extend the domain of definition of ν_p to include 0, defining $\nu_p(0) := \infty$. Following standard conventions for arithmetic with infinity (see Preliminaries), it is easy to see that for all $a, b \in \mathbb{Z}$, we have

$$\nu_p(a \cdot b) = \nu_p(a) + \nu_p(b) \quad \text{for all } p. \tag{1.4}$$

From this, it follows that for all $a, b \in \mathbb{Z}$, we have

$$b \mid a \quad \text{if and only if} \quad \nu_p(b) \leq \nu_p(a) \quad \text{for all } p, \tag{1.5}$$

and

$$\nu_p(\gcd(a, b)) = \min(\nu_p(a), \nu_p(b)) \quad \text{for all } p. \tag{1.6}$$

For $a, b \in \mathbb{Z}$ a **common multiple** of a and b is an integer m such that

$a \mid m$ and $b \mid m$; moreover, such an m is the **least common multiple** of a and b if m is non-negative and m divides all common multiples of a and b. In light of Theorem 1.3, it is clear that the least common multiple exists and is unique, and we denote the least common multiple of a and b by $\mathrm{lcm}(a, b)$. Note that as we have defined it, $\mathrm{lcm}(a, 0) = 0$, and that when both a and b are non-zero, $\mathrm{lcm}(a, b)$ is the smallest positive integer divisible by both a and b. Also, for all $a, b \in \mathbb{Z}$, we have

$$\nu_p(\mathrm{lcm}(a, b)) = \max(\nu_p(a), \nu_p(b)) \quad \text{for all } p, \tag{1.7}$$

and

$$\gcd(a, b) \cdot \mathrm{lcm}(a, b) = |ab|. \tag{1.8}$$

It is easy to generalize the notions of greatest common divisor and least common multiple from two integers to many integers. For $a_1, \ldots, a_k \in \mathbb{Z}$, with $k \geq 1$, we call $d \in \mathbb{Z}$ a common divisor of $a_1, \ldots, a_k$ if $d \mid a_i$ for $i = 1, \ldots, k$; moreover, we call such a d the greatest common divisor of $a_1, \ldots, a_k$ if d is non-negative and all other common divisors of $a_1, \ldots, a_k$ divide d. It is clear that the greatest common divisor of $a_1, \ldots, a_k$ exists and is unique, and moreover, we have

$$\nu_p(\gcd(a_1, \ldots, a_k)) = \min(\nu_p(a_1), \ldots, \nu_p(a_k)) \quad \text{for all } p. \tag{1.9}$$

Analogously, for $a_1, \ldots, a_k \in \mathbb{Z}$, with $k \geq 1$, we call $m \in \mathbb{Z}$ a common multiple of $a_1, \ldots, a_k$ if $a_i \mid m$ for $i = 1, \ldots, k$; moreover, such an m is called the least common multiple of $a_1, \ldots, a_k$ if m divides all common multiples of $a_1, \ldots, a_k$. It is clear that the least common multiple of $a_1, \ldots, a_k$ exists and is unique, and moreover, we have

$$\nu_p(\mathrm{lcm}(a_1, \ldots, a_k)) = \max(\nu_p(a_1), \ldots, \nu_p(a_k)) \quad \text{for all } p. \tag{1.10}$$

We say that integers $a_1, \ldots, a_k$ are **pairwise relatively prime** if $\gcd(a_i, a_j) = 1$ for all i, j with $i \neq j$. Note that if $a_1, \ldots, a_k$ are pairwise relatively prime, then $\gcd(a_1, \ldots, a_k) = 1$; however, $\gcd(a_1, \ldots, a_k) = 1$ does not imply that $a_1, \ldots, a_k$ are pairwise relatively prime.

Consider now the rational numbers $\mathbb{Q} := \{a/b : a, b \in \mathbb{Z},\ b \neq 0\}$. Because of the unique factorization property for $\mathbb{Z}$, given any rational number a/b, if we set $d := \gcd(a, b)$, and define the integers $a' := a/d$ and $b' := b/d$, then we have $a/b = a'/b'$ and $\gcd(a', b') = 1$. Moreover, if $\tilde{a}/\tilde{b} = a'/b'$, then we have $\tilde{a}b' = a'\tilde{b}$, and so $b' \mid a'\tilde{b}$, and since $\gcd(a', b') = 1$, we see that $b' \mid \tilde{b}$; if $\tilde{b} = \tilde{d}b'$, it follows that $\tilde{a} = \tilde{d}a'$. Thus, we can represent every rational number as a fraction in **lowest terms**, that is, a fraction of the form a'/b'

where a' and b' are relatively prime; moreover, the values of a' and b' are uniquely determined up to sign, and every other fraction that represents the same rational number is of the form $(\tilde{d}a')/(\tilde{d}b')$, for some non-zero integer $\tilde{d}$.

EXERCISE 1.10. Let n be a positive integer. Show that if a, b are relatively prime integers, each of which divides n, then ab divides n. More generally, show that if $a_1, \ldots, a_k$ are pairwise relatively prime integers, each of which divides n, then their product $a_1 \cdots a_k$ divides n.

EXERCISE 1.11. For positive integer n, let $\mathcal{D}(n)$ denote the set of positive divisors of n. For relatively prime, positive integers n_1, n_2, show that the sets $\mathcal{D}(n_1) \times \mathcal{D}(n_2)$ and $\mathcal{D}(n_1 \cdot n_2)$ are in one-to-one correspondence, via the map that sends $(d_1, d_2) \in \mathcal{D}(n_1) \times \mathcal{D}(n_2)$ to $d_1 \cdot d_2$.

EXERCISE 1.12. Let p be a prime and k an integer $0 < k < p$. Show that the binomial coefficient

$$\binom{p}{k} = \frac{p!}{k!(p-k)!},$$

which is an integer, of course, is divisible by p.

EXERCISE 1.13. An integer $a \in \mathbb{Z}$ is called **square-free** if it is not divisible by the square of any integer greater than 1. Show that any integer $n \in \mathbb{Z}$ can be expressed as $n = ab^2$, where $a, b \in \mathbb{Z}$ and a is square-free.

EXERCISE 1.14. Show that any non-zero $x \in \mathbb{Q}$ can be expressed as

$$x = \pm p_1^{e_1} \cdots p_r^{e_r},$$

where the p_i are distinct primes and the e_i are non-zero integers, and that this expression in unique up to a reordering of the primes.

EXERCISE 1.15. Show that if an integer cannot be expressed as a square of an integer, then it cannot be expressed as a square of any rational number.

EXERCISE 1.16. Show that for all integers a, b, and all primes p, we have $\nu_p(a+b) \geq \min\{\nu_p(a), \nu_p(b)\}$, and that if $\nu_p(a) < \nu_p(b)$, then $\nu_p(a+b) = \nu_p(a)$.

EXERCISE 1.17. For a prime p, we may extend the domain of definition of ν_p from $\mathbb{Z}$ to $\mathbb{Q}$: for non-zero integers a, b, let us define $\nu_p(a/b) := \nu_p(a) - \nu_p(b)$.

(a) Show that this definition of $\nu_p(a/b)$ is unambiguous, in the sense that it does not depend on the particular choice of a and b.

(b) Show that for all $x, y \in \mathbb{Q}$, we have $\nu_p(xy) = \nu_p(x) + \nu_p(y)$.

(c) Show that for all $x, y \in \mathbb{Q}$, we have $\nu_p(x+y) \geq \min\{\nu_p(x), \nu_p(y)\}$, and that if $\nu_p(x) < \nu_p(y)$, then $\nu_p(x+y) = \nu_p(x)$.

(d) Show that for all non-zero $x \in \mathbb{Q}$, we have

$$x = \pm \prod_p p^{\nu_p(x)},$$

where the product is over all primes, and all but a finite number of terms in the product is 1.

Exercise 1.18. Let n be a positive integer, and let C_n denote the number of pairs of integers (a, b) such that $1 \leq a \leq n$, $1 \leq b \leq n$ and $\gcd(a, b) = 1$, and let F_n be the number of *distinct* rational numbers a/b, where $0 \leq a < b \leq n$.

(a) Show that $F_n = (C_n + 1)/2$.

(b) Show that $C_n \geq n^2/4$. Hint: first show that $C_n \geq n^2(1 - \sum_{d \geq 2} 1/d^2)$, and then show that $\sum_{d \geq 2} 1/d^2 \leq 3/4$.

Exercise 1.19. This exercise develops a characterization of least common multiples in terms of ideals.

(a) Arguing directly from the definition of an ideal, show that if I and J are ideals of $\mathbb{Z}$, then so is $I \cap J$.

(b) Let $a, b \in \mathbb{Z}$, and consider the ideals $I := a\mathbb{Z}$ and $J := b\mathbb{Z}$. By part (a), we know that $I \cap J$ is an ideal. By Theorem 1.5, we know that $I \cap J = m\mathbb{Z}$ for some uniquely determined non-negative integer m. Show that $m = \operatorname{lcm}(a, b)$.

Exercise 1.20. For $a_1, \ldots, a_k \in \mathbb{Z}$, with $k > 1$, show that

$$\gcd(a_1, \ldots, a_k) = \gcd(\gcd(a_1, \ldots, a_{k-1}), a_k)$$

and

$$\operatorname{lcm}(a_1, \ldots, a_k) = \operatorname{lcm}(\operatorname{lcm}(a_1, \ldots, a_{k-1}), a_k).$$

Exercise 1.21. Show that for any $a_1, \ldots, a_k \in \mathbb{Z}$, if $d := \gcd(a_1, \ldots, a_k)$, then $d\mathbb{Z} = a_1\mathbb{Z} + \cdots + a_k\mathbb{Z}$; in particular, there exist integers $s_1, \ldots, s_k$ such that

$$d = a_1 s_1 + \cdots + a_k s_k.$$

Exercise 1.22. Show that for all integers a, b, we have

$$\gcd(a + b, \operatorname{lcm}(a, b)) = \gcd(a, b).$$

EXERCISE 1.23. Show that for integers $c, a_1, \ldots, a_k$, we have

$$\gcd(ca_1, \ldots, ca_k) = |c| \gcd(a_1, \ldots, a_k).$$