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

A central concept in number theory is *divisibility*.

Consider the integers $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$. For $a, b \in \mathbb{Z}$, we say that a **divides** b if $az = b$ for some $z \in \mathbb{Z}$. If a divides b, we write $a \mid b$, and we may say that a is a **divisor** of b, or that b is a **multiple** of a, or that b is **divisible by** a. If a does not divide b, then we write $a \nmid b$.

We first state some simple facts about divisibility:

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) $a \mid b$ *if and only if* $-a \mid b$ *if and only if* $a \mid -b$;

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

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

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

We make a simple observation: if $a \mid b$ and $b \neq 0$, then $1 \leq |a| \leq |b|$. Indeed, if $az = b \neq 0$ for some integer z, then $a \neq 0$ and $z \neq 0$; it follows that $|a| \geq 1$, $|z| \geq 1$, and so $|a| \leq |a||z| = |b|$.

Theorem 1.2. *For all $a, b \in \mathbb{Z}$, we have $a \mid b$ and $b \mid a$ if and only if $a = \pm b$. In particular, for every $a \in \mathbb{Z}$, we have $a \mid 1$ if and only if $a = \pm 1$.*

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 the other must be zero as well. So assume that neither is zero. By the above observation, $a \mid b$ implies $|a| \leq |b|$, and $b \mid a$ implies $|b| \leq |a|$; thus, $|a| = |b|$, and so $a = \pm b$. That proves the first statement. The second statement follows from the first by setting $b := 1$, and noting that $1 \mid a$. □

The product of any two non-zero integers is again non-zero. This implies the usual **cancellation law**: if a, b, and c are integers such that $a \neq 0$ and $ab = ac$, then we must have $b = c$; indeed, $ab = ac$ implies $a(b - c) = 0$, and so $a \neq 0$ implies $b - c = 0$, and hence $b = c$.

Primes and composites. Let n be a positive integer. Trivially, 1 and n divide n. If $n > 1$ and no other positive integers besides 1 and n divide n, then we say n is **prime**. If $n > 1$ but n is not prime, then we say that n is **composite**. The number 1 is not considered to be either prime or composite. Evidently, n 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

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

While it is possible to extend the definition of prime and composite to negative integers, we shall not do so in this text: *whenever we speak of a prime or composite number, we mean a positive integer.*

A basic fact is that every 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 $p_1, \ldots, p_r$ are distinct primes and $e_1, \ldots, e_r$ 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.

The theorem intuitively says that the primes act as the "building blocks" out of which all non-zero integers can be formed by multiplication (and negation). The reader may be so familiar with this fact that he may feel it is somehow "self evident," requiring no proof; however, this feeling is simply a delusion, and most of the rest of this section and the next are devoted to developing a proof of this theorem. We shall give a quite leisurely proof, introducing a number of other very important tools and concepts along the way that will be useful later.

To prove Theorem 1.3, 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. Assume, then, that n is composite, so that 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 the hard part. An essential ingredient in this proof is the following:

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

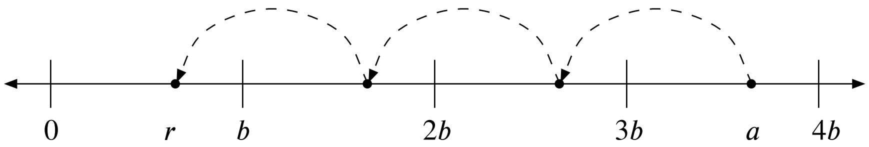
Proof. Consider the set S of non-negative integers of the form $a - bt$ with $t \in \mathbb{Z}$. This set is clearly non-empty; indeed, if $a \geq 0$, set $t := 0$, and if $a < 0$, set $t := a$. Since every non-empty set of non-negative integers contains a minimum, we define r to be the smallest element of S. By definition, r is of the form $r = a - bq$ for some $q \in \mathbb{Z}$, and $r \geq 0$. Also, we must have $r < b$, since otherwise, $r - b$ would be an element of S smaller than r, contradicting the minimality of r; indeed, if $r \geq b$, then we would have $0 \leq r - b = a - b(q + 1)$.

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

$$r' - r = b(q - q').$$

Thus, $r' - r$ is a multiple of b; however, $0 \leq r < b$ and $0 \leq r' < b$ implies $|r' - r| < b$; therefore, the only possibility is $r' - r = 0$. Moreover, $0 = b(q - q')$ and $b \neq 0$ implies $q - q' = 0$. □

Theorem 1.4 can be visualized as follows:



Starting with a, we subtract (or add, if a is negative) the value b until we end up with a number in the interval $[0, b)$.

Floors and ceilings. Let us briefly recall the usual **floor** and **ceiling** functions, denoted $\lfloor\cdot\rfloor$ and $\lceil\cdot\rceil$, respectively. These are functions from $\mathbb{R}$ (the real numbers) to $\mathbb{Z}$. For $x \in \mathbb{R}$, $\lfloor x\rfloor$ is the greatest integer $m \leq x$; equivalently, $\lfloor x\rfloor$ is the unique integer m such that $m \leq x < m + 1$, or put another way, such that $x = m + \varepsilon$ for some $\varepsilon \in [0, 1)$. Also, $\lceil x\rceil$ is the smallest integer $m \geq x$; equivalently, $\lceil x\rceil$ is the unique integer m such that $m - 1 < x \leq m$, or put another way, such that $x = m - \varepsilon$ for some $\varepsilon \in [0, 1)$.

The mod operator. Now let $a, b \in \mathbb{Z}$ with $b > 0$. If q and r are the unique integers from Theorem 1.4 that satisfy $a = bq + r$ and $0 \leq r < b$, we define

$$a \bmod b := r;$$

that is, $a \bmod b$ denotes the remainder in dividing a by b. It is clear that $b \mid a$ if and only if $a \bmod b = 0$. Dividing both sides of the equation $a = bq + r$ by b, we obtain $a/b = q + r/b$. Since $q \in \mathbb{Z}$ and $r/b \in [0, 1)$, we see that $q = \lfloor a/b\rfloor$. Thus,

$$(a \bmod b) = a - b\lfloor a/b\rfloor.$$

One can use this equation to extend the definition of $a \bmod b$ to all integers a and b, with $b \neq 0$; that is, for $b < 0$, we simply define $a \bmod b$ to be $a - b\lfloor a/b\rfloor$.

Theorem 1.4 may be generalized so that when dividing an integer a by a positive integer b, the remainder is placed in an interval other than $[0, b)$. Let x be any real number, and consider the interval $[x, x + b)$. As the reader may easily verify, this interval contains precisely b integers, namely, $\lceil x\rceil, \ldots, \lceil x\rceil + b - 1$. Applying Theorem 1.4 with $a - \lceil x\rceil$ in place of a, we obtain:

Theorem 1.5. *Let $a, b \in \mathbb{Z}$ with $b > 0$, and let $x \in \mathbb{R}$. Then there exist unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $r \in [x, x + b)$.*

EXERCISE 1.1. Let $a, b, d \in \mathbb{Z}$ with $d \neq 0$. Show that $a \mid b$ if and only if $da \mid db$.

EXERCISE 1.2. Let n be a composite integer. Show that there exists a prime p dividing n, with $p \leq n^{1/2}$.

EXERCISE 1.3. Let m be a positive integer. Show that for every real number $x \geq 1$, the number of multiples of m in the interval $[1, x]$ is $\lfloor x/m\rfloor$; in particular, for every integer $n \geq 1$, the number of multiples of m among $1, \ldots, n$ is $\lfloor n/m\rfloor$.

EXERCISE 1.4. Let $x \in \mathbb{R}$. Show that $2\lfloor x\rfloor \leq \lfloor 2x\rfloor \leq 2\lfloor x\rfloor + 1$.

EXERCISE 1.5. Let $x \in \mathbb{R}$ and $n \in \mathbb{Z}$ with $n > 0$. Show that $\lfloor \lfloor x \rfloor / n \rfloor = \lfloor x/n \rfloor$; in particular, $\lfloor \lfloor a/b \rfloor / c \rfloor = \lfloor a/bc \rfloor$ for all positive integers a, b, c.

EXERCISE 1.6. Let $a, b \in \mathbb{Z}$ with $b < 0$. Show that $(a \bmod b) \in (b, 0]$.

EXERCISE 1.7. Show that Theorem 1.5 also holds for the interval $(x, x+b]$. Does it hold in general for the intervals $[x, x+b]$ or $(x, x+b)$?

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 closed 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

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

Besides its utility in proving Theorem 1.3, the notion of an ideal is quite useful in a number of contexts, which will be explored later.

It is easy to see that every ideal I contains 0: since $a \in I$ for some integer a, we have $0 = a \cdot 0 \in I$. Also, note that if an ideal I contains an integer a, it also contains $-a$, since $-a = a \cdot (-1) \in I$. Thus, if an ideal contains a and b, it also contains $a - b$. 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 every $z \in \mathbb{Z}$, we have $z = 1 \cdot z \in I$, 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 multiples of a. If $a = 0$, then clearly $a\mathbb{Z} = \{0\}$; otherwise, $a\mathbb{Z}$ consists of the distinct integers

$$\ldots, -3a, -2a, -a, 0, a, 2a, 3a, \ldots.$$

It is easy to see that $a\mathbb{Z}$ is an ideal: for all $az, az' \in a\mathbb{Z}$ 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 ideal $a\mathbb{Z}$ is called the **ideal generated by** a, and an ideal of the form $a\mathbb{Z}$ for some $a \in \mathbb{Z}$ is called a **principal ideal**.

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

Suppose I_1 and I_2 are ideals. Then it is not hard to see that the set

$$I_1 + I_2 := \{a_1 + a_2 : a_1 \in I_1, a_2 \in I_2\}$$

is also an ideal. Indeed, suppose $a_1 + a_2 \in I_1 + I_2$ and $b_1 + b_2 \in I_1 + I_2$. Then we have $(a_1 + a_2) + (b_1 + b_2) = (a_1 + b_1) + (a_2 + b_2) \in I_1 + I_2$, and for every $z \in \mathbb{Z}$, we have $(a_1 + a_2)z = a_1 z + a_2 z \in I_1 + I_2$.

Example 1.1. Consider the principal ideal $3\mathbb{Z}$. This consists of all multiples of 3; that is, $3\mathbb{Z} = \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\}$. □

Example 1.2. Consider the ideal $3\mathbb{Z} + 5\mathbb{Z}$. This ideal contains $3 \cdot 2 + 5 \cdot (-1) = 1$. Since it contains 1, it contains all integers; that is, $3\mathbb{Z} + 5\mathbb{Z} = \mathbb{Z}$. □

Example 1.3. Consider the ideal $4\mathbb{Z} + 6\mathbb{Z}$. This ideal contains $4 \cdot (-1) + 6 \cdot 1 = 2$, and therefore, it contains all even integers. It does not contain any odd integers, since the sum of two even integers is again even. Thus, $4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$. □

In the previous two examples, we defined an ideal that turned out upon closer inspection to be a principal ideal. This was no accident: the following theorem says that all ideals of $\mathbb{Z}$ are principal.

Theorem 1.6. *Let I be an ideal of $\mathbb{Z}$. Then 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 $a \in I$ then so is $-a$. 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 a be any element in I. It suffices to show that $d \mid a$. Using the division with remainder property, write $a = dq + r$, where $0 \leq r < d$. Then by the closure properties of ideals, one sees that $r = a - dq$ is also an element of I, and by the minimality of the choice of d, we must have $r = 0$. Thus, $d \mid a$.

We have shown that $I \subseteq d\mathbb{Z}$. The fact that $d\mathbb{Z} \subseteq I$ follows from the fact that $d \in I$. Thus, $I = d\mathbb{Z}$.

That proves the existence part of the theorem. For uniqueness, note that if $d\mathbb{Z} = e\mathbb{Z}$ for some non-negative integer e, then $d \mid e$ and $e \mid d$, from which it follows by Theorem 1.2 that $d = \pm e$; since d and e are non-negative, we must have $d = e$. □

Greatest common divisors. 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 1.7. *For all $a, b \in \mathbb{Z}$, 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 some $a', b', d' \in \mathbb{Z}$. 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. For uniqueness, note that if e is a greatest common divisor of a and b, then $d \mid e$ and $e \mid d$, and hence $d = \pm e$; since both d and e are non-negative by definition, we have $d = e$. □

For $a, b \in \mathbb{Z}$, we write $\gcd(a, b)$ for the greatest common divisor of a and b. 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.

The following is essentially just a restatement of Theorem 1.7, but we state it here for emphasis:

Theorem 1.8. *Let $a, b, r \in \mathbb{Z}$ and let $d := \gcd(a, b)$. Then there exist $s, t \in \mathbb{Z}$ such that $as + bt = r$ if and only if $d \mid r$. In particular, a and b are relatively prime if and only if there exist integers s and t such that $as + bt = 1$.*

Proof. We have

$$\begin{aligned} & as + bt = r \text{ for some } s, t \in \mathbb{Z} \\ \iff & r \in a\mathbb{Z} + b\mathbb{Z} \\ \iff & r \in d\mathbb{Z} \quad \text{(by Theorem 1.7)} \\ \iff & d \mid r. \end{aligned}$$

That proves the first statement. The second statement follows from the first, setting $r := 1$. □

Note that as we have defined it, $\gcd(0, 0) = 0$. Also note that when at least one of a or b are non-zero, $\gcd(a, b)$ may be characterized as the *largest* positive integer that divides both a and b, and as the *smallest* positive integer that can be expressed as $as + bt$ for integers s and t.

Theorem 1.9. *Let $a, b, c \in \mathbb{Z}$ such that $c \mid ab$ and $\gcd(a, c) = 1$. Then $c \mid b$.*

Proof. Suppose that $c \mid ab$ and $\gcd(a, c) = 1$. Then since $\gcd(a, c) = 1$, by Theorem 1.8 we have $as + ct = 1$ for some $s, t \in \mathbb{Z}$. Multiplying this equation by

b, we obtain

$$abs + cbt = b. \tag{1.1}$$

Since c divides ab by hypothesis, and since c clearly divides cbt, it follows that c divides the left-hand side of (1.1), and hence that c divides b. □

Suppose that p is a prime and a is any integer. As the only divisors of p are ± 1 and $\pm p$, we have

$$\begin{aligned} p \mid a &\implies \gcd(a, p) = p, \text{ and} \\ p \nmid a &\implies \gcd(a, p) = 1. \end{aligned}$$

Combining this observation with the previous theorem, we have:

Theorem 1.10. *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 $p \mid ab$. If $p \mid a$, we are done, so assume that $p \nmid a$. By the above observation, $\gcd(a, p) = 1$, and so by Theorem 1.9, we have $p \mid b$. □

An obvious corollary to Theorem 1.10 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 1.10, either $p \mid a_1$ or $p \mid a_2 \cdots a_k$; if $p \mid a_1$, we are done; otherwise, by induction, p divides one of $a_2, \ldots, a_k$.

Finishing the proof of Theorem 1.3. We are now in a position to prove the uniqueness part of Theorem 1.3, which we can state as follows: if $p_1, \ldots, p_r$ are primes (not necessarily distinct), and $q_1, \ldots, q_s$ are primes (also not necessarily distinct), such that

$$p_1 \cdots p_r = q_1 \cdots q_s, \tag{1.2}$$

then $(p_1, \ldots, p_r)$ is just a reordering of $(q_1, \ldots, q_s)$. 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 obviously divides the left-hand side of (1.2), it must also divide the right-hand side of (1.2); that is, $p_1 \mid q_1 \cdots q_s$. It follows from (the corollary to) Theorem 1.10 that $p_1 \mid q_j$ for some $j = 1, \ldots, s$, and moreover, since q_j is prime, we must have $p_1 = q_j$. Thus, we may cancel p_1 from the left-hand side of (1.2) and q_j from the right-hand side of (1.2), and the statement now follows from the induction hypothesis. That proves the uniqueness part of Theorem 1.3.

EXERCISE 1.8. Let I be a non-empty set of integers that is closed under addition (i.e., $a+b \in I$ for all $a, b \in I$). Show that I is an ideal if and only if $-a \in I$ for all $a \in I$.

EXERCISE 1.9. Show that for all integers a, b, c, we have:

(a) $\gcd(a, b) = \gcd(b, a)$;

(b) $\gcd(a, b) = |a| \iff a \mid b$;

(c) $\gcd(a, 0) = \gcd(a, a) = |a|$ and $\gcd(a, 1) = 1$;

(d) $\gcd(ca, cb) = |c| \gcd(a, b)$.

EXERCISE 1.10. Show that for all integers a, b with $d := \gcd(a, b) \neq 0$, we have $\gcd(a/d, b/d) = 1$.

EXERCISE 1.11. Let n be an integer. Show that if a, b are relatively prime integers, each of which divides n, then ab divides n.

EXERCISE 1.12. Show that two integers are relatively prime if and only if there is no one prime that divides both of them.

EXERCISE 1.13. Let $a, b_1, \ldots, b_k$ be integers. Show that $\gcd(a, b_1 \cdots b_k) = 1$ if and only if $\gcd(a, b_i) = 1$ for $i = 1, \ldots, k$.

EXERCISE 1.14. Let p be a prime and k an integer, with $0 < k < p$. Show that the binomial coefficient

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

which is an integer (see §A2), is divisible by p.

EXERCISE 1.15. An integer a is called **square-free** if it is not divisible by the square of any integer greater than 1. Show that:

(a) a is square-free if and only if $a = \pm p_1 \cdots p_r$, where the p_i's are distinct primes;

(b) every positive integer n can be expressed uniquely as $n = ab^2$, where a and b are positive integers, and a is square-free.

EXERCISE 1.16. For each positive integer m, let I_m denote $\{0, \ldots, m-1\}$. Let a, b be positive integers, and consider the map

$$\begin{aligned} \tau : \quad & I_b \times I_a \to I_{ab} \\ & (s, t) \mapsto (as + bt) \bmod ab. \end{aligned}$$

Show τ is a bijection if and only if $\gcd(a, b) = 1$.

EXERCISE 1.17. Let a, b, c be positive integers satisfying $\gcd(a, b) = 1$ and $c \geq (a-1)(b-1)$. Show that there exist *non-negative* integers s, t such that $c = as + bt$.

EXERCISE 1.18. For each positive integer n, let D_n denote the set of positive divisors of n. Let n_1, n_2 be relatively prime, positive integers. Show that the sets $D_{n_1} \times D_{n_2}$ and $D_{n_1 n_2}$ are in one-to-one correspondence, via the map that sends $(d_1, d_2) \in D_{n_1} \times D_{n_2}$ to $d_1 d_2$.

1.3 Some consequences of unique factorization

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

Theorem 1.11. *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 $M := \prod_{i=1}^{k} p_i$ and $N := M + 1$. 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's, since if it did, then p would divide M, and hence also divide $N - M = 1$, 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 each prime p, we may define the function ν_p, mapping non-zero integers to non-negative integers, as follows: for every 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; although syntactically this is an infinite product, all but finitely many of its terms are equal to 1, and so this expression makes sense.

Observe that if a and b are non-zero integers, then

$$\nu_p(a \cdot b) = \nu_p(a) + \nu_p(b) \ \text{ for all primes } p, \tag{1.3}$$

and

$$a \mid b \iff \nu_p(a) \leq \nu_p(b) \ \text{ for all primes } p. \tag{1.4}$$

From this, it is clear that

$$\gcd(a, b) = \prod_{p} p^{\min(\nu_p(a), \nu_p(b))}.$$

Least common multiples. 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. It is easy to see that the least common multiple exists and is unique, and we denote the least common multiple of a and b by $\operatorname{lcm}(a, b)$. Indeed, for all $a, b \in \mathbb{Z}$, if either a or b are zero, the only common multiple of a and b is 0, and so $\operatorname{lcm}(a, b) = 0$; otherwise, if neither a nor b are zero, we have

$$\operatorname{lcm}(a, b) = \prod_p p^{\max(\nu_p(a), \nu_p(b))},$$

or equivalently, $\operatorname{lcm}(a, b)$ may be characterized as the smallest positive integer divisible by both a and b.

It is convenient to extend the domain of definition of ν_p to include 0, defining $\nu_p(0) := \infty$. If we interpret expressions involving "∞" appropriately (see Preliminaries), then for arbitrary $a, b \in \mathbb{Z}$, both (1.3) and (1.4) hold, and in addition,

$$\nu_p(\gcd(a, b)) = \min(\nu_p(a), \nu_p(b)) \text{ and } \nu_p(\operatorname{lcm}(a, b)) = \max(\nu_p(a), \nu_p(b))$$

for all primes p.

Generalizing gcd's and lcm's to many integers. It is easy to generalize the notions of greatest common divisor and least common multiple from two integers to many integers. Let $a_1, \ldots, a_k$ be integers. 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. The greatest common divisor of $a_1, \ldots, a_k$ is denoted $\gcd(a_1, \ldots, a_k)$ and is the unique non-negative integer d satisfying

$$\nu_p(d) = \min(\nu_p(a_1), \ldots, \nu_p(a_k)) \text{ for all primes } p.$$

Analogously, we call $m \in \mathbb{Z}$ a common multiple of $a_1, \ldots, a_k$ if $a_i \mid m$ for all $i = 1, \ldots, k$; moreover, such an m is called the least common multiple of $a_1, \ldots, a_k$ if m divides all common multiples of $a_1, \ldots, a_k$. The least common multiple of $a_1, \ldots, a_k$ is denoted $\operatorname{lcm}(a_1, \ldots, a_k)$ and is the unique non-negative integer m satisfying

$$\nu_p(m) = \max(\nu_p(a_1), \ldots, \nu_p(a_k)) \text{ for all primes } p.$$

Finally, we say that the family $\{a_i\}_{i=1}^k$ is **pairwise relatively prime** if for all indices i, j with $i \neq j$, we have $\gcd(a_i, a_j) = 1$. Certainly, if $\{a_i\}_{i=1}^k$ is pairwise relatively prime, and $k > 1$, then $\gcd(a_1, \ldots, a_k) = 1$; however, $\gcd(a_1, \ldots, a_k) = 1$ does not imply that $\{a_i\}_{i=1}^k$ is pairwise relatively prime.

Rational numbers. Consider the rational numbers $\mathbb{Q} = \{a/b : a, b \in \mathbb{Z},\ b \neq 0\}$. Given any rational number a/b, if we set $d := \gcd(a, b)$, and define the integers $a_0 := a/d$ and $b_0 := b/d$, then we have $a/b = a_0/b_0$ and $\gcd(a_0, b_0) = 1$. Moreover, if $a_1/b_1 = a_0/b_0$, then we have $a_1 b_0 = a_0 b_1$, and so $b_0 \mid a_0 b_1$; also, since $\gcd(a_0, b_0) = 1$, we see that $b_0 \mid b_1$; writing $b_1 = b_0 c$, we see that $a_1 = a_0 c$. Thus, we can represent every rational number as a fraction in **lowest terms**, which means a fraction of the form a_0/b_0 where a_0 and b_0 are relatively prime; moreover, the values of a_0 and b_0 are uniquely determined up to sign, and every other fraction that represents the same rational number is of the form $a_0 c/b_0 c$, for some non-zero integer c.

EXERCISE 1.19. Let n be an integer. Generalizing Exercise 1.11, show that if $\{a_i\}_{i=1}^k$ is a pairwise relatively prime family of integers, where each a_i divides n, then their product $\prod_{i=1}^k a_i$ also divides n.

EXERCISE 1.20. Show that for all integers a, b, c, we have:

(a) $\operatorname{lcm}(a, b) = \operatorname{lcm}(b, a)$;

(b) $\operatorname{lcm}(a, b) = |a| \iff b \mid a$;

(c) $\operatorname{lcm}(a, a) = \operatorname{lcm}(a, 1) = |a|$;

(d) $\operatorname{lcm}(ca, cb) = |c| \operatorname{lcm}(a, b)$.

EXERCISE 1.21. Show that for all integers a, b, we have:

(a) $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = |ab|$;

(b) $\gcd(a, b) = 1 \implies \operatorname{lcm}(a, b) = |ab|$.

EXERCISE 1.22. Let $a_1, \ldots, a_k \in \mathbb{Z}$ with $k > 1$. Show that:

$$\gcd(a_1, \ldots, a_k) = \gcd(a_1, \gcd(a_2, \ldots, a_k)) = \gcd(\gcd(a_1, \ldots, a_{k-1}), a_k);$$
$$\operatorname{lcm}(a_1, \ldots, a_k) = \operatorname{lcm}(a_1, \operatorname{lcm}(a_2, \ldots, a_k)) = \operatorname{lcm}(\operatorname{lcm}(a_1, \ldots, a_{k-1}), a_k).$$

EXERCISE 1.23. Let $a_1, \ldots, a_k \in \mathbb{Z}$ with $d := \gcd(a_1, \ldots, a_k)$. Show that $d\mathbb{Z} = a_1\mathbb{Z} + \cdots + a_k\mathbb{Z}$; in particular, there exist integers $z_1, \ldots, z_k$ such that $d = a_1 z_1 + \cdots + a_k z_k$.

EXERCISE 1.24. Show that if $\{a_i\}_{i=1}^k$ is a pairwise relatively prime family of integers, then $\operatorname{lcm}(a_1, \ldots, a_k) = |a_1 \cdots a_k|$.

EXERCISE 1.25. Show that every 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's are distinct primes and the e_i's are non-zero integers, and that this expression in unique up to a reordering of the primes.

EXERCISE 1.26. Let n and k be positive integers, and suppose $x \in \mathbb{Q}$ such that $x^k = n$ for some $x \in \mathbb{Q}$. Show that $x \in \mathbb{Z}$. In other words, $\sqrt[k]{n}$ is either an integer or is irrational.

EXERCISE 1.27. Show that $\gcd(a+b, \operatorname{lcm}(a,b)) = \gcd(a,b)$ for all $a, b \in \mathbb{Z}$.

EXERCISE 1.28. Show that for every positive integer k, there exist k consecutive composite integers. Thus, there are arbitrarily large gaps between primes.

EXERCISE 1.29. Let p be a prime. Show that for all $a, b \in \mathbb{Z}$, we have $\nu_p(a+b) \geq \min\{\nu_p(a), \nu_p(b)\}$, and $\nu_p(a+b) = \nu_p(a)$ if $\nu_p(a) < \nu_p(b)$.

EXERCISE 1.30. For a given 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 $\nu_p(a/b) := \nu_p(a) - \nu_p(b)$. Show that:

(a) 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) for all $x, y \in \mathbb{Q}$, we have $\nu_p(xy) = \nu_p(x) + \nu_p(y)$;

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

(d) 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 are equal to 1;

(e) for all $x \in \mathbb{Q}$, we have $x \in \mathbb{Z}$ if and only if $\nu_p(x) \geq 0$ for all primes p.

EXERCISE 1.31. Let n be a positive integer, and let 2^k be the highest power of 2 in the set $S := \{1, \ldots, n\}$. Show that 2^k does not divide any other element in S.

EXERCISE 1.32. Let $n \in \mathbb{Z}$ with $n > 1$. Show that $\sum_{i=1}^{n} 1/i$ is not an integer.

EXERCISE 1.33. Let n be a positive integer, and let C_n denote the number of pairs of integers (a, b) with $a, b \in \{1, \ldots, n\}$ 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 1.34. 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 1.6, we know that $I \cap J = m\mathbb{Z}$ for some uniquely determined non-negative integer m. Show that $m = \operatorname{lcm}(a, b)$.