1

Some preliminaries from number theory

In this chapter we provide the necessary prerequisites from multiplicative number theory regarding primes, divisibility and approximation by rationals.

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

The basic objects of our story are the set of natural numbers $\mathbb{N} = \{1, 2, 3, \dots\}$ and the set of integers $\mathbb{Z}$. In addition, we often deal with the set of *rationals* $\mathbb{Q}$ and the set of real numbers $\mathbb{R}$. An element of $\mathbb{R} \setminus \mathbb{Q}$ is called *irrational*. Shortly we will need the complex numbers $\mathbb{C}$ as well.

The set of integers $\mathbb{Z}$ forms a *ring* equipped with the usual addition and multiplication. The operation of division, the inverse to multiplication, applies to pairs (a, b) with $b \neq 0$. We say that a number $b \neq 0$ *divides* a (writing $b \mid a$) or, equivalently, b is a *divisor* of a or a is *divisible* by b or a is a *multiple* of b, if $a = bq$ holds for some integer q. The number q is called the *quotient* of a by b. The number 0 is divisible by any integer $b \neq 0$. If $a \neq 0$ then the number of its divisors is finite. We use the notation $b \nmid a$ to say that b does not divide a.

Let us list some simple properties of divisibility in $\mathbb{Z}$.

Lemma 1.1 *If $c \mid b$ and $b \mid a$ then $c \mid a$.*

Proof Since $b = cq_1$ and $a = bq_2$, we have $a = c(q_1q_2)$. □

Lemma 1.2 *If all terms in an equality $a_1 + \cdots + a_n = b_1 + \cdots + b_k$, except one, are multiples of a fixed integer c then the exceptional term is a multiple of c as well.*

Proof Writing all terms except b_k, say, in the form $a_i = c\widetilde{a}_i$ and $b_j = c\widetilde{b}_j$, we see that

$$b_k = c(\widetilde{a}_1 + \cdots + \widetilde{a}_n - \widetilde{b}_1 - \cdots - \widetilde{b}_{k-1}).$$

This means that b_k can be represented in the form $b_k = cb$ for some integer b, and hence b_k is a multiple of c. □

The *floor* or *greatest integer function* is denoted $\lfloor x \rfloor$ and is defined to be the greatest integer $\leq x$. Thus $\lfloor \pi \rfloor = 3$ and $\lfloor -e \rfloor = -3$. The *ceiling* or *least integer function* $\lceil x \rceil$ is defined, analogously, to be the least integer $\geq x$. Clearly $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$. We let $\{x\}$ denote the *fractional part* of x, that is, $x - \lfloor x \rfloor$; hopefully there will be no confusion with ordinary set notation.

Theorem 1.3 (Division with remainder) *For any integer a and any positive integer b, there exist integers q and r such that*

$$a = bq + r \qquad \text{and} \qquad 0 \leq r < b. \tag{1.1}$$

These numbers q and r are defined uniquely.

Proof The existence of such a pair q, r is clear; we take $q = \lfloor a/b \rfloor$. Then $q \leq a/b < q + 1$; hence $bq \leq a < b(q + 1)$ and so $0 \leq r = a - bq < b$.

Assuming two representations (1.1), the second being of the form

$$a = bq_1 + r_1 \qquad \text{and} \qquad 0 \leq r_1 < b, \tag{1.2}$$

we deduce from equations (1.1) and (1.2) that

$$0 = b(q - q_1) + (r - r_1) \qquad \text{and} \qquad |r - r_1| < b. \tag{1.3}$$

Hence b divides the difference $r - r_1$, which is possible only when $r = r_1$, by the inequality in (1.3). The equality $r = r_1$ implies $q = q_1$ by the equality in (1.3). □

An integer dividing each of the integers $a_1, a_2, \ldots, a_n$ is called their *common divisor*; the largest of the common divisors is called the *greatest common divisor* and denoted by $\gcd(a_1, a_2, \ldots, a_n)$. If $\gcd(a_1, \ldots, a_n) = 1$, the numbers $a_1, \ldots, a_n$ are called *coprime* (or *relatively prime*). If every pair of the set $\{a_1, \ldots, a_n\}$ is coprime then the set is called *pairwise coprime*. (The latter requirement is stronger, as the example of the set $\{6, 10, 15\}$ shows: these numbers are coprime but not pairwise coprime.)

The following two lemmas can be easily verified using the above definitions.

Lemma 1.4 *If a is a multiple of b then the set of common divisors of a and b coincides with the set of divisors of b; in particular,* $\gcd(a, b) = |b|$.

Lemma 1.5 *If $a = bq + r$ then the set of common divisors of a and b coincides with the set of common divisors of b and r; in particular,* $\gcd(a, b) = \gcd(b, r)$.

The last statement substantiates the following classical Greek algorithm for computing the greatest common divisor of two numbers $a, b \in \mathbb{Z}$:

EUCLIDEAN ALGORITHM Let $a, b \in \mathbb{Z}$ with $a \geq b > 0$. Defining $r_{-1} = a$ and $r_0 = b$, consider the following successive application of division with remainder (Theorem 1.3):

$$\begin{aligned} r_{-1} &= r_0 q_0 + r_1, & 0 < r_1 < r_0, \\ r_0 &= r_1 q_1 + r_2, & 0 < r_2 < r_1, \\ &\vdots & \\ r_{n-1} &= r_n q_n + r_{n+1}, & 0 < r_{n+1} < r_n, \\ r_n &= r_{n+1} q_{n+1}. \end{aligned} \tag{1.4}$$

Then the last nonzero remainder r_{n+1} is the greatest common divisor of a and b.

Critically, the procedure (1.4) terminates at some step in view of the following chain of inequalities:

$$r_0 > r_1 > \cdots > r_{n-1} > r_n > r_{n+1} > 0.$$

By (1.4) and Lemma 1.5 we get

$$\begin{aligned} \gcd(a, b) &= \gcd(r_{-1}, r_0) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots \\ &= \gcd(r_n, r_{n+1}) = \gcd(r_{n+1}, 0) = r_{n+1}. \end{aligned}$$

Hence the last nonzero remainder r_{n+1} in (1.4) is indeed the required greatest common divisor of a and b.

Lemma 1.6 *For any integer $m > 0$ we have* $\gcd(am, bm) = m \gcd(a, b)$.

Proof Multiply all equalities in (1.4) by m. □

Lemma 1.7 *Let δ be a common divisor of a and b. Then*

$$\gcd\left(\frac{a}{\delta}, \frac{b}{\delta}\right) = \frac{\gcd(a, b)}{|\delta|}$$

and, in particular,

$$\gcd\left(\frac{a}{\gcd(a, b)}, \frac{b}{\gcd(a, b)}\right) = 1.$$

Proof By Lemma 1.6 we obtain

$$\gcd(a, b) = \gcd\left(\frac{a}{\delta}\,\delta, \frac{b}{\delta}\,\delta\right) = \gcd\left(\frac{a}{\delta}, \frac{b}{\delta}\right)|\delta|.$$ □

We leave the proofs of Lemmas 1.8–1.10 below to the reader.

Lemma 1.8 *If* $\gcd(a, b) = 1$ *then* $\gcd(ac, b) = \gcd(c, b)$.

Lemma 1.9 *If* $\gcd(a, b) = 1$ *and* ac *is divisible by* b *then* c *is divisible by* b.

Lemma 1.10 *If each of the numbers* $a_1, \dots, a_n$ *is coprime with each of the numbers* $b_1, \dots, b_k$ *then the products* $a_1 \cdots a_n$ *and* $b_1 \cdots b_k$ *are coprime.*

An integer that is a multiple of all the numbers $a_1, \dots, a_n$ is called their *common multiple*. The smallest positive common multiple is called the *least common multiple* or *lcm* and denoted by $\operatorname{lcm}(a_1, \dots, a_n)$.

Lemma 1.11 *The set of common multiples of two given numbers coincides with the set of multiples of their least common multiple.*

Proof Let M denote a common multiple of the given integers a and b. Then $M = ak$ for $k \in \mathbb{Z}$, since M is a multiple of a, and the number $M/b = ak/b$ is an integer. Define $d = \gcd(a, b)$, $a = da_1$ and $b = db_1$; by Lemma 1.7 we have $\gcd(a_1, b_1) = 1$. By Lemma 1.9 the equality $M/b = a_1 k/b_1 \in \mathbb{Z}$ implies that k is divisible by b_1, that is, $k = b_1 t = bt/d$ for $t \in \mathbb{Z}$. Therefore

$$M = \frac{ab}{d}t = \frac{ab}{\gcd(a, b)}t, \qquad t \in \mathbb{Z}, \tag{1.5}$$

and, as can be seen, any such M is a multiple of both a and b. We get the least common multiple by specialization $t = \pm 1$: $\operatorname{lcm}(a, b) = |ab|/\gcd(a, b)$. Thus, formula (1.5) can be written in the required form $M = \operatorname{lcm}(a, b)t$ with $t \in \mathbb{Z}$. □

The previous lemma gives a simple and efficient algorithm for computing the least common multiple for a set $a_1, a_2, \dots, a_n$ of arbitrary length $n \geq 2$. Namely, we have the formula

$$\operatorname{lcm}(a_1, a_2, a_3, a_4, \dots, a_n) = \operatorname{lcm}(\operatorname{lcm}(\dots \operatorname{lcm}(\operatorname{lcm}(\operatorname{lcm}(a_1, a_2), a_3), a_4), \dots), a_n),$$

while the least common multiple of just two numbers is computed by

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

Exercise 1.12 Show that, for a pair of relatively prime integers a and b, the linear equation $ax - by = 1$ has infinitely many solutions in integers x, y.

Hint This can be split into two parts: First, show (using either an inductive argument or the Euclidean algorithm) that there exists at least one solution of the equation, say x_0, y_0, and, second, that the pair $x = x_0 + bt$, $y = y_0 + at$ is a solution for any $t \in \mathbb{Z}$. □

1.2 Primes

An integer exceeding 1 always has at least two distinct divisors, namely, 1 and itself. If these two divisors exhaust the list of all positive divisors of such an integer then the integer is called a *prime number*; otherwise, the integer (> 1) is called a *composite* number.

Lemma 1.13 *The least positive divisor, different from* 1*, of an integer* $a > 1$ *is a prime.*

Proof The set $A = \{2, 3, \ldots, a\}$ is not empty and finite and contains at least one divisor (namely, a) of the given integer a; thus we can choose the smallest such divisor, say b. If b is not prime then it has a divisor c such that $1 < c < b$, so that $c \in A$. But then Lemma 1.1 implies that c divides a, which contradicts our choice of b. □

The next lemma, while simple, is very potent.

Lemma 1.14 *The least positive divisor, different from* 1*, of a* composite *integer* $a > 1$ *does not exceed* $\sqrt{a}$.

Proof Let $b > 1$ be the least positive divisor of a. Write $a = bc$; since a is composite we have $b < a$, so that $c > 1$. As both b and c are divisors of a and b is the least divisor we have $b \le c = a/b$, implying that $b^2 \le a$. □

The next result, attributed to Euclid of Alexandria, circa 300 BCE, illustrates the sophistication of Greek number theory.

Theorem 1.15 (Euclid) *The set of primes is infinite.*

Proof If not, we could write the (nonempty) set of primes as

$$\{p_1 = 2, p_2 = 3, p_3, \ldots, p_n\}$$

and consider the least positive divisor, different from 1, of the number

$$p_1 p_2 \cdots p_n + 1.$$

The divisor is prime, by Lemma 1.13, and it is not on our list because it is relatively prime to each of $p_1, \ldots, p_n$. Thus, we arrive at a contradiction. □

An important property (as well as the main difficulty in use) of primes is their role as 'building blocks' or 'atoms' in the study of $\mathbb{Z}$ from the multiplicative point of view.

Lemma 1.16 *Every integer* a *is either a multiple of a given prime* p *or coprime with* p.

Proof Indeed, $\gcd(a, p)$ is p or 1, as a divisor of p. □

Lemma 1.17 *If a product of some terms is divisible by p then at least one of the terms is divisible by p.*

Proof Otherwise, each term is coprime with p by Lemma 1.16, while Lemma 1.10 implies that the product has to be coprime with p as well. □

Theorem 1.18 (Fundamental theorem of arithmetic) *Every integer greater than* 1 *may be decomposed into a product of primes* (*that is, factorised*)*, and this decomposition is unique* (*up to the ordering of the primes in it*)*.*

Proof *Existence*. This is shown by induction on $a > 1$. For the number $a = 2$, its factorisation is trivial (owing to the primality of 2). If $a > 2$ then it is either a prime (and hence its factorisation involves only the number itself) or composite. In the latter case it can be written in the form $a = pa_1$, where p is the prime divisor from Lemma 1.13, and for the number a_1, $\sqrt{a} \le a_1 < a$, we use the induction hypothesis.

Uniqueness. Assume, contrary to what we want to prove, that numbers with non-unique factorisation exist, and choose the least in the set of such numbers, say a:

$$a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_k, \tag{1.6}$$
$$p_1, p_2, \ldots, p_n \text{ and } q_1, q_2, \ldots, q_k \text{ are primes.}$$

On the one hand, the right-hand side of (1.6) is divisible by q_1, and hence at least one term on the left-hand side of (1.6) (say p_1, without loss of generality) is divisible by q_1 by Lemma 1.17. On the other hand, each term on the left-hand side of (1.6) is a prime and therefore p_1 has to coincide with q_1; after reduction by $p_1 = q_1$ in (1.6) we obtain

$$p_2 \cdots p_n = q_2 \cdots q_k. \tag{1.7}$$

At least one side of (1.7) involves a non-empty product (otherwise we would have $a = p_1 = q_1$, two identical prime factorisations of the number a, contradicting its choice above). Thus, (1.7) records two different factorisations of a number a_1 satisfying $1 < a_1 < a$. The latter contradicts the minimality of our choice of a. □

Two very important problems in number theory, with numerous applications to the theory and practice of information security and encryption, are deciding whether a given number is prime and finding large prime numbers. The latter problem is related to the distribution of primes in the set of positive integers. In

fact, it is not hard to show that there are arbitrarily long sequences of consecutive composite numbers (for example, the sequence $n! + i$ for $i = 2, 3, \ldots, n$). However, it is conjectured that there are infinitely many *twin primes*, that is, infinitely many pairs p, q of primes with $q - p = 2$. Very recent (2013) work by Zhang [173], as yet unpublished, has proved that there are infinitely many pairs of primes that differ by some $N < 70\,000\,000$; subsequently his methods were refined by the Polymath project to $N \leq 4680$ and by Maynard to $N \leq 600$. The latter number may seem feeble as a replacement for 2 but in fact it is an enormous accomplishment.

Another famous conjecture ('Goldbach's conjecture') states that any even integer greater than 2 is a sum of two primes. The recent work of Helfgott [73] reports on a proof of its weaker three-primes version.

The following result, known as the *prime number theorem*, is a fundamental theorem on the distribution of primes. It was almost guessed, from much numerical evidence, by Gauss in 1791; Chebyshev provided some evidence for it in 1850, and finally Hadamard and de la Vallée Poussin independently proved it in 1896 using methods of complex analysis. Chebyshev's work was good enough to prove *Bertrand's postulate*: there is a prime in the interval $[n - 1, 2n - 1]$ for each $n \geq 3$.

The main feature of the proofs of Hadamard and de la Vallée Poussin is the use of the Riemann zeta function $\zeta(s)$, defined in the complex half-plane $\operatorname{Re} s > 1$ by the (slowly convergent for small $s > 1$) series

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}. \tag{1.8}$$

Theorem 1.19 (Prime number theorem) *Let $\pi(x)$ be the number of primes less than or equal to x, for any real number x. Then*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1,$$

where $\log x = \ln x$ denotes the logarithm of x to the base e.

The details of this proof are a little tangential to our goals (the interested reader may find them in many places including [77, Chapter II]), but the following curious equivalent form of the prime number theorem will be useful later.

Theorem 1.20 (Rate of growth of lcm) *Let $d_n = \operatorname{lcm}(1, 2, \ldots, n)$ be the least common multiple of the first n consecutive natural numbers. Then*

$$\lim_{n\to\infty} \frac{\log d_n}{n} = 1.$$

It is clear that $n!$ is a common multiple of the numbers $1, 2, \ldots, n$, and it grows as $(n/e)^n\sqrt{2\pi n}(1 + o(1))$ according to *Stirling's asymptotic formula* (which can be replaced by rougher estimates that we will establish below in (2.37)). Theorem 1.20 tells us that the actual growth of the *least* common multiple in this case is, roughly speaking, e^n, which is of course asymptotically a better estimate than the one arising from $n!$.

Exercise 1.21 (see, for example, [77, Chapter I, Theorem 3]) Show the equivalence of Theorems 1.19 and 1.20.

1.3 Fibonacci numbers and the complexity of the Euclidean algorithm

The sequence of *Fibonacci numbers* $F_0, F_1, F_2, F_3, \ldots$ is defined by the simple linear recurrence relation

$$F_{n+2} = F_{n+1} + F_n \tag{1.9}$$

and the initial data $F_0 = 0$, $F_1 = 1$. It is a sequence on which the Euclidean algorithm (see the text after Lemma 1.5)

$$\begin{aligned} a &= bq_0 + r_1, & 0 < r_1 < b,\\ b &= r_1q_1 + r_2, & 0 < r_2 < r_1,\\ r_1 &= r_2q_2 + r_3, & 0 < r_3 < r_2,\\ &\vdots\\ r_{n-1} &= r_nq_n + r_{n+1}, & 0 < r_{n+1} < r_n,\\ r_n &= r_{n+1}q_{n+1} \end{aligned} \tag{1.10}$$

(here $a \geq b > 0$) works for more steps than might be expected: since the quotients $q_0, q_1, \ldots, q_{n+1}$ are integers greater than or equal to 1, the following estimates hold:

$$r_{n+1} \geq F_1, \quad r_n \geq F_2, \quad r_{n-1} \geq F_3, \quad \ldots, \quad r_1 \geq F_{n+1}, \quad b \geq F_{n+2}, \quad a \geq F_{n+3}.$$

Lemma 1.22 *If k is the number of steps (divisions with remainder) in the Euclidean algorithm then for given initial data $a \geq b > 0$ we have $a \geq F_{k+1}$ and $b \geq F_k$.*

Our immediate aim is to deduce a general form for the Fibonacci sequence.

This will allow us to give an upper bound on the number of steps in the Euclidean algorithm (the *complexity* of the algorithm) for arbitrary initial data $a \geq b > 0$.

EXERCISE 1.23 Before moving to the rest of this section, find and prove a closed-form expression for the Fibonacci numbers.

Now let $a_1(n), a_2(n), \ldots, a_m(n)$ be arbitrary functions of the nonnegative integer argument n. The recurrence equation

$$\phi(n+m) + a_1(n)\phi(n+m-1) + \cdots + a_{m-1}(n)\phi(n+1) + a_m(n)\phi(n) = 0 \quad (1.11)$$

is called a *linear homogeneous difference equation of order m*, and any function $\phi(n)$ satisfying (1.11) for all $n = 0, 1, 2, \ldots$ is called its *solution*. It is not difficult to see that the choice of *initial data*

$$\phi(0) = \phi_0, \quad \phi(1) = \phi_1, \quad \ldots, \quad \phi(m-1) = \phi_{m-1}$$

determines a solution $\phi(n)$, $n = 0, 1, 2, \ldots$, of (1.11) uniquely.

Lemma 1.24 *Let $\phi^{(1)}(n), \phi^{(2)}(n), \ldots, \phi^{(k)}(n)$ be k solutions of* (1.11)*. Then the function*

$$\phi(n) = c_1\phi^{(1)}(n) + c_2\phi^{(2)}(n) + \cdots + c_k\phi^{(k)}(n), \qquad n = 0, 1, 2, \ldots,$$

where $c_1, c_2, \ldots, c_k$ are arbitrary constants from the ground field (for example, $\mathbb{Q}$ or $\mathbb{R}$), is a solution of (1.11) *as well.*

Equivalently, the set of solutions of (1.11) forms a linear space. Furthermore, we can always construct m linearly independent solutions of the equation, $\phi^{(1)}(n), \phi^{(2)}(n), \ldots, \phi^{(m)}(n)$, by choosing the initial data in such a way that the m-vectors

$$\begin{pmatrix} \phi_0^{(1)} \\ \phi_1^{(1)} \\ \vdots \\ \phi_{m-1}^{(1)} \end{pmatrix}, \quad \begin{pmatrix} \phi_0^{(2)} \\ \phi_1^{(2)} \\ \vdots \\ \phi_{m-1}^{(2)} \end{pmatrix}, \quad \ldots, \quad \begin{pmatrix} \phi_0^{(m)} \\ \phi_1^{(m)} \\ \vdots \\ \phi_{m-1}^{(m)} \end{pmatrix}$$

are linearly independent.

Lemma 1.25 *A general solution of* (1.11) *can be written in the form*

$$\phi(n) = c_1\phi^{(1)}(n) + c_2\phi^{(2)}(n) + \cdots + c_m\phi^{(m)}(n), \qquad n = 0, 1, 2, \ldots,$$

where $\phi^{(1)}(n), \phi^{(2)}(n), \ldots, \phi^{(m)}(n)$ is a fixed basis (defined above) in the solution space, while $c_1, \ldots, c_m$ are arbitrary constants.

Proof Let $\phi(n)$, $n = 0, 1, 2, \ldots$, be a solution of (1.11). Then the constants $c_1, \ldots, c_m$ are determined by the system of linear equations

$$c_1 \begin{pmatrix} \phi_0^{(1)} \\ \phi_1^{(1)} \\ \vdots \\ \phi_{m-1}^{(1)} \end{pmatrix} + c_2 \begin{pmatrix} \phi_0^{(2)} \\ \phi_1^{(2)} \\ \vdots \\ \phi_{m-1}^{(2)} \end{pmatrix} + \cdots + c_m \begin{pmatrix} \phi_0^{(m)} \\ \phi_1^{(m)} \\ \vdots \\ \phi_{m-1}^{(m)} \end{pmatrix} = \begin{pmatrix} \phi(0) \\ \phi(1) \\ \vdots \\ \phi(m-1) \end{pmatrix}. \qquad \square$$

Exercise 1.26 Prove Lemma 1.24 and finalise the proof of Lemma 1.25.

From now on we switch to the simplest case, when the coefficients $a_1, \ldots, a_{m-1}, a_m$ of the difference equation do not depend on n and, in addition, the *characteristic polynomial*

$$\lambda^m + a_1\lambda^{m-1} + \cdots + a_{m-1}\lambda + a_m = 0 \tag{1.12}$$

of (1.11) has exactly m distinct *nonzero* roots $\lambda_1, \ldots, \lambda_m$. (For the case of repeated roots, we recommend [20].)

Theorem 1.27 (Solution to recursion with no repeated roots) *A general solution of the linear homogeneous difference equation with constant coefficients has the form*

$$\phi(n) = c_1\lambda_1^n + \cdots + c_m\lambda_m^n, \qquad n = 0, 1, 2, \ldots .$$

Proof Note that the functions $\phi^{(j)}(n) = \lambda_j^n$, where $j = 1, \ldots, m$, form a *fundamental solution system*, that is, a basis in the solution space. The fact that the solutions are linearly independent follows from the nonvanishing of a Vandermonde determinant (see, for example, [89, Section 2.1] for more information about the latter). $\square$

Lemma 1.28 *The Fibonacci numbers are also given by the explicit formula*

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}},$$

where $\alpha = (1 + \sqrt{5})/2$ *and* $\beta = (1 - \sqrt{5})/2$ *(with* $\alpha\beta = -1$*).*

Proof Indeed, the characteristic polynomial $\lambda^2 - \lambda - 1$ of the difference equation (1.9) has roots α, β. Letting

$$F_n = c_1\alpha^n + c_2\beta^n$$

and setting $n = 0$ and $n = 1$, we find $c_1 = -c_2 = 1/\sqrt{5}$. $\square$

Exercise 1.29 (Pell numbers) The Pell numbers satisfy the recurrence relation $P_{n+2} = 2P_{n+1} + P_n$ with initial conditions $P_0 = 0$ and $P_1 = 1$. Give a closed-form expression for the Pell numbers.