PART ONE

ELEMENTARY NUMBER THEORY

1

Prelude

Number theory deals with the properties of the positive integers, which were probably the first mathematical objects discovered by human beings. In this chapter we shall initially study the factorization of positive integers into primes, a basic result called the *fundamental theorem of arithmetic*. The possibly exaggerated title ‘Prelude’ refers to the second section, where we introduce Chebyshev’s theorem on the distribution of prime numbers. This result is remarkable and yet rather easy to understand, and it may encourage the reader to approach more advanced topics in number theory.

For the first part of this book we have used various references, including [3, 4, 6, 8, 9, 42, 46, 63, 68, 72, 76, 90, 93, 96, 101, 103, 108, 119, 120, 127, 128, 136, 145, 151, 165].

1.1 Prime numbers and factorization

We shall denote by $\mathbb{N} = \{1, 2, \ldots\}$ the set of natural numbers and by $\mathbb{Z}$ the set of integers. We shall say that $0 \neq b \in \mathbb{Z}$ divides $a \in \mathbb{Z}$ if there exists $c \in \mathbb{Z}$ such that $a = bc$. In this case we shall write $b \mid a$. If b does not divide a we shall write $b \nmid a$.

We know[1] that, given $a \in \mathbb{Z}$ and $b \in \mathbb{N}$, there exist (unique) $q, r \in \mathbb{Z}$ such that $a = bq + r$, with $0 \leq r < b$. We present the following consequence.

Theorem 1.1 *Let $b > 1$ be an integer. Then every $a \in \mathbb{N}$ can be written in one and only one way in base b :*

$$a = c_0 + c_1 b + c_2 b^2 + \ldots + c_n b^n \,, \tag{1.1}$$

[1] The set $\{a - xb : x \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\})$ is not empty and let $r = a - qb$ be its minimum. Observe that $(0 \leq) r < b$, otherwise we would have $r = a - qb \geq b$ and $0 \leq a - (q+1)\, b < r$, against the minimality of r. Now assume that $a = bq_1 + r_1 = bq_2 + r_2$, then $|r_1 - r_2| = b\,|q_2 - q_1|$. If $q_1 \neq q_2$ then $|r_1 - r_2| = b\,|q_2 - q_1| \geq b$, which is impossible since $0 \leq r_1, r_2 < b$.

where $n \geq 0$ *and* $0 \leq c_j < b$ *for* $j = 0, \dots, n-1$*, while* $1 \leq c_n < b$*.*

Proof Let us prove by induction that if $b^n \leq a < b^{n+1}$, then a can be written in base b. This is true for $n = 0$ and we assume that it is true for every $0 \leq m \leq n-1$. Since $b^n \leq a < b^{n+1}$ we have

$$a = c_n b^n + r \ ,$$

with $0 \leq r < b^n$ and $1 \leq c_n < b$. If $r = 0$, then a is written as in (1.1). If $r > 0$, we recall that $r < b^n$ and thus $b^m \leq r < b^{m+1}$ for some $m \leq n-1$. We now use the induction assumption to write

$$r = p_0 + p_1 b + p_2 b^2 + \dots + p_m b^m$$

with $0 \leq p_j < b$ for $j = 0, \dots, m$. Then

$$a = p_0 + p_1 b + p_2 b^2 + \dots + p_m b^m + c_n b^n \ .$$

Finally, we assume that there are two ways to write a in (1.1). By suitably subtracting them we obtain

$$0 = q_0 + q_1 b + q_2 b^2 + \dots + q_k b^k$$

with $q_k \geq 1$ ($k = 0$ gives a contradiction, so we assume that $k \geq 1$). For every $0 \leq j \leq k-1$ we have $\left|q_j\right| \leq b-1$. Then we have

$$q_k b^k = -\left(q_0 + q_1 b + q_2 b^2 + \dots + q_{k-1} b^{k-1}\right)$$

and

$$\begin{aligned} b^k \leq q_k b^k &\leq |q_0| + |q_1|\, b + |q_2|\, b^2 + \dots + |q_{k-1}|\, b^{k-1} \\ &\leq (b-1)\left(1 + b + b^2 + \dots + b^{k-1}\right) = b^k - 1 \ , \end{aligned}$$

which is impossible. □

The following theorem introduces the definition of greatest common divisor.

Theorem 1.2 *Let* a, b *be two integers not both zero. Then there exists a unique* $d \in \mathbb{N}$ *such that*

(i) there exist $x, y \in \mathbb{Z}$ *satisfying* $d = ax + by$*,*
(ii) $d \mid a$ *and* $d \mid b$*,*
(iii) if $k \in \mathbb{N}$ *divides* a *and* b*, then it also divides* d*.*

Proof Let

$$I := \{au + bv\}_{u,v \in \mathbb{Z}} \ .$$

Then $I \cap \mathbb{N}$ is not empty and let $d = \min(I \cap \mathbb{N})$. Observe that d trivially satisfies (i) and (iii). In order to show that d satisfies (ii), it is enough to prove that d divides every element in I. Indeed, let $au + bv = z \in I$, assume that $q \in \mathbb{Z}$ and $0 \leq r < d$ satisfy $z = dq + r$. Then

$$r = z - dq = au + bv - (ax + by)\,q = a\,(u - xq) + b\,(v - yq) \in I\ .$$

Since $0 \leq r < d = \min\,(I \cap \mathbb{N})$ we deduce that $r = 0$, thus d divides z. The uniqueness follows from (ii) and (iii). □

The number d is called the *greatest common divisor* (gcd) of a and b. We shall write[2]

$$d = (a, b)\ .$$

When $(a, b) = 1$ we shall say that a and b are coprime. Observe that $(a, b) = 1$ if and only if there exist integers x, y such that $ax + by = 1$.

Theorem 1.3 (Euclid's lemma) *Let a, b, c satisfy $a \mid bc$ and $(a, b) = 1$. Then $a \mid c$.*

Proof Let x and y satisfy $ax + by = 1$. Then $c = cax + cby$. Since $a \mid acx$ and $a \mid bcy$, we deduce that $a \mid c$. □

We are going to describe a famous method, called the *Euclidean algorithm*, which gives the gcd of two positive integers. We need a lemma.

Lemma 1.4 *Let $a, b, q, r \in \mathbb{N}$ satisfy $a = qb + r$. Then $(a, b) = (b, r)$.*

Proof If $t \mid b$ and $t \mid r$, then $t \mid a$. In particular, $(b, r) \mid a$. Since $(b, r) \mid b$ we deduce that $(b, r) \mid (a, b)$. In the same way we see that $(a, b) \mid (b, r)$. □

The Euclidean algorithm uses the previous lemma to compute the gcd of two integers $a \geq b > 0$. Indeed, let us write

$$\begin{array}{ll}
a = q_1 b + r_1 & \text{with } 0 < r_1 < b \\
b = q_2 r_1 + r_2 & \text{with } 0 < r_2 < r_1 \\
r_1 = q_3 r_2 + r_3 & \text{with } 0 < r_3 < r_2 \\
r_2 = q_4 r_3 + r_4 & \text{with } 0 < r_4 < r_3 \\
\vdots & \\
r_{n-3} = q_{n-1} r_{n-2} + r_{n-1} & \text{with } 0 < r_{n-1} < r_{n-2} \\
r_{n-2} = q_n r_{n-1}\ . &
\end{array}$$

By the previous lemma we have

$$(a, b) = (b, r_1) = (r_1, r_2) = (r_2, r_3) = \ldots = (r_{n-3}, r_{n-2}) = (r_{n-2}, r_{n-1}) = r_{n-1}\ .$$

[2] The symbol (a, b) already denotes the open interval $(a, b) = \{x \in \mathbb{R} : a < x < b\}$ and the pair $(a, b) \in \mathbb{Z}^2$, but there is actually no confusion.

Then the Euclidean algorithm says that $(a, b) = r_{n-1}$.

We apply the Euclidean algorithm to compute $(35777, 4123)$. We have

$$\begin{aligned} 35777 &= 4123 \cdot 8 + 2793 \\ 4123 &= 2793 \cdot 1 + 1330 \\ 2793 &= 1330 \cdot 2 + 133 \\ 1330 &= 133 \cdot 10\ . \end{aligned} \tag{1.2}$$

Hence $(35777, 4123) = 133$.

Remark 1.5 If we look at the numbers in the algorithm we can find x, y in Theorem 1.2. Indeed, if we rewrite the lines in (1.2) with $a = 35777$ and $b = 4123$ we have

$$\begin{aligned} a &= 8b + 2793 \\ b &= (a - 8b) \cdot 1 + 1330 \\ a - 8b &= [b - (a - 8b) \cdot 1] \cdot 2 + 133\ . \end{aligned}$$

Then we have

$$133 = 3a - 26b$$

or

$$(35777, 4123) = 3 \cdot 35777 - 26 \cdot 4123\ .$$

We now introduce the prime numbers.

Definition 1.6 An integer $p > 1$ is a *prime number* if it has only two positive divisors (namely 1 and p). We shall write $\mathcal{P}$ for the set of prime numbers. We shall say that an integer $n > 1$ is a *composite number* if $n \notin \mathcal{P}$.

Lemma 1.7 *Let $a, b \in \mathbb{N}$ and let p be a prime. If $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Proof $p \in \mathcal{P}$ and $p \nmid a$ imply $(a, p) = 1$. Then Theorem 1.3 gives $p \mid b$. □

By applying the previous lemma several times we obtain the following result.

Lemma 1.8 *Let $a_1, a_2, \ldots, a_k \in \mathbb{N}$ and let p be a prime. If $p \mid (a_1 a_2 \cdots a_k)$, then $p \mid a_j$ for some $j = 1, \ldots, k$.*

We can now introduce the *fundamental theorem of arithmetic*.

Theorem 1.9 (Fundamental theorem of arithmetic) *Every integer $n > 1$ can be written in a unique way (up to permutation) as*

$$n = p_1^{m_1} p_2^{m_2} \cdots p_N^{m_N} \ , \tag{1.3}$$

where the numbers p_j are prime and the numbers m_j are positive integers.

In certain cases it may be useful to write $n = p_1^{m_1} p_2^{m_2} \cdots p_N^{m_N} \cdots$ as an infinite product, where $\left\{p_j\right\}_{j=1}^{+\infty} = \mathcal{P}$ and all but a finite number of exponents m_j are zero. (1.3) is called the *canonical decomposition* (or *factorization*) of n.

Proof We shall use induction to prove that every integer $n \geq 2$ can be written as a product of prime numbers. This is true for 2 and we consider $n > 2$. Assume that every $2 \leq m \leq n - 1$ can be written as a product of prime numbers. If $n \in \mathcal{P}$, we are done. If not, let $n = n_1 n_2$. Then, by the induction assumption, n_1 and n_2 are products of prime numbers. Then the same is true for n. Now we shall prove the uniqueness of the decomposition. Let $\mathcal{A} \subset \mathbb{N}$ be the set of natural numbers with more than one canonical decomposition. Let $M = \min \mathcal{A}$. Then we may write

$$M = p_1 p_2 \cdots p_r = p'_1 p'_2 \cdots p'_s \ ,$$

where $p_1, p_2, \ldots, p_r$ and $p'_1, p'_2, \ldots, p'_s$ are prime numbers (possibly repeated), and the two products differ for at least one term. By Lemma 1.8 we deduce that $p_1 = p'_j$ for a suitable j. Then

$$\widetilde{M} = p_2 \cdots p_r = p'_1 \cdots p'_{j-1} p'_{j+1} \cdots p'_s$$

is smaller than M and admits two different canonical decompositions. □

See [20, 6.1] for a comment on the above theorem and its history. See also [61, Ch. 8] and [85].

The fundamental theorem of arithmetic allows us to write the gcd as follows. Let $a, b \in \mathbb{N}$. We may write $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ and $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$ (with the same prime numbers in the two products) as long as we allow some of the exponents to be zero. Then

$$(a, b) = p_1^{\min(\alpha_1,\, \beta_1)} p_2^{\min(\alpha_2,\, \beta_2)} \cdots p_s^{\min(\alpha_s,\, \beta_s)} \ .$$

Observe that the Euclidean algorithm does not need the fundamental theorem of arithmetic.

Euclid has proved the infinitude of primes.

Theorem 1.10 (Euclid) *There are infinitely many prime numbers.*

Proof Assume that $\mathcal{P} = \{p_1, p_2, \dots, p_N\}$. Then every other number should be a product of elements in $\mathcal{P}$. But this is impossible for $(p_1 p_2 \cdots p_N) + 1$. □

Here we can see the original proof.

> 'Prime numbers are more than any assigned multitude of prime numbers. Let A, B, and C be the assigned prime numbers. I say that there are more prime numbers than A, B, and C. Take the least number DE measured by A, B, and C. Add the unit DF to DE. Then EF is either prime or not. First, let it be prime. Then the prime numbers A, B, C, and EF have been found which are more than A, B, and C. Next, let EF not be prime. Therefore it is measured by some prime number. Let it be measured by the prime number G. I say that G is not the same with any of the numbers A, B, and C. If possible, let it be so. Now A, B, and C measure DE, therefore G also measures DE. But it also measures EF. Therefore G, being a number, measures the remainder, the unit DF, which is absurd. Therefore G is not the same with any one of the numbers A, B, and C. And by hypothesis it is prime. Therefore the prime numbers A, B, C, and G have been found which are more than the assigned multitude of A, B, and C. Therefore, prime numbers are more than any assigned multitude of prime numbers.'
>
> (Euclid, *Elements*, Book IX)

Observe that the above argument does not offer an instrument to find prime numbers. Indeed,

$$(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13) + 1 = 30031 = 59 \cdot 509$$

is a composite number.

The following result was proved by Euler in 1737.

Theorem 1.11 (Euler)

$$\sum_{p \in \mathcal{P}}^{+\infty} \frac{1}{p} = +\infty\ . \tag{1.4}$$

First proof For every real number $x \geq 2$ we write

$$P_x := \prod_{\mathcal{P} \ni p \leq x} \left(1 - \frac{1}{p}\right)^{-1} .$$

Since

$$\log(1 + \varepsilon) = \varepsilon - \frac{1}{2}\varepsilon^2 + \frac{1}{3}\varepsilon^3 - \frac{1}{4}\varepsilon^4 + \dots$$

for $-1 < \varepsilon < 1$, we have

$$\log P_x = -\sum_{\mathcal{P} \ni p \leq x} \log\left(1 - \frac{1}{p}\right) = \sum_{\mathcal{P} \ni p \leq x} \left(\frac{1}{p} + \frac{1}{2p^2} + \frac{1}{3p^3} + \frac{1}{4p^4} + \dots\right)$$

$$\leq \sum_{\mathcal{P}\ni p\leq x} \frac{1}{p}\left(1+\frac{1}{2^2}+\frac{1}{2^3}+\frac{1}{2^4}+\ldots\right)=\frac{3}{2}\sum_{\mathcal{P}\ni p\leq x}\frac{1}{p}\,.$$

To complete the proof we show that $P_x \to +\infty$ when $x \to +\infty$. Indeed, let $p_1 < p_2 < p_3 < \ldots < p_N$ be the prime numbers $\leq x$. Since

$$\left(1-\frac{1}{p}\right)^{-1}=\sum_{j=0}^{+\infty}p^{-j}$$

we have

$$\begin{aligned}
P_x &= \prod_{\mathcal{P}\ni p\leq x}\left(1-\frac{1}{p}\right)^{-1} \qquad (1.5)\\
&= \prod_{j=1}^{N}\left(1-\frac{1}{p_j}\right)^{-1}\\
&= \left(1+\frac{1}{p_1}+\frac{1}{p_1^2}+\ldots\right)\left(1+\frac{1}{p_2}+\frac{1}{p_2^2}+\ldots\right)\cdots\left(1+\frac{1}{p_N}+\frac{1}{p_N^2}+\ldots\right)\\
&= 1+\left(\frac{1}{p_1}+\frac{1}{p_2}+\ldots+\frac{1}{p_N}\right)+\left(\frac{1}{p_1^2}+\frac{1}{p_1p_2}+\frac{1}{p_2^2}+\frac{1}{p_1p_3}+\ldots\right)\\
&+\left(\frac{1}{p_1^3}+\frac{1}{p_1^2p_2}+\ldots\right)+\ldots\\
&= \sum_{\substack{n=p_1^{m_1}p_2^{m_2}\cdots p_N^{m_N},\\ p_1\leq x,\ p_2\leq x,\ \ldots\ p_N\leq x}}\frac{1}{n}\\
&\geq \sum_{k\leq x}\frac{1}{k}\longrightarrow +\infty
\end{aligned}$$

as $x \to +\infty$. □

An argument similar to the one in (1.5) shows that for every real number $s > 1$ we have

$$\sum_{n=1}^{+\infty}\frac{1}{n^s}=\prod_{p\in\mathcal{P}}\left(1-p^{-s}\right)^{-1}\ . \qquad (1.6)$$

The function

$$\zeta(s):=\sum_{n=1}^{+\infty}\frac{1}{n^s}$$

is called the *Riemann zeta function* and it plays a fundamental role in the study of prime numbers (see [102] or the short introductions in [8] or [10]).

Let us now see a different proof of (1.4), which we owe to Clarkson [56].

Second proof of Theorem 1.11 Let $p_1 < p_2 < p_3 < \ldots$ be all the prime numbers, and let us assume that $\sum_{p\in\mathcal{P}}^{+\infty} 1/p$ converges. Then there exists a positive integer k such that

$$\sum_{n>k} \frac{1}{p_n} < \frac{1}{2} \,. \tag{1.7}$$

Let $Q = p_1 p_2 \cdots p_k$. For no $\ell \in \mathbb{N}$ does there exist p_j (with $1 \leq j \leq k$) such that $p_j \mid (1 + \ell Q)$. Then the prime divisors of $1 + \ell Q$ must be found among $p_{k+1}, p_{k+2}, \ldots$ and, for every $N \geq 1$, we have

$$\sum_{\ell=1}^{N} \frac{1}{1+\ell Q} \leq \sum_{m=1}^{+\infty} \left(\sum_{n>k} \frac{1}{p_n} \right)^m \,. \tag{1.8}$$

In order to prove (1.8), we start by showing that every term $(1 + \ell Q)^{-1}$ in the LHS appears also in the RHS. Let

$$\frac{1}{1+\ell Q} \underset{\text{say}}{=} \frac{1}{p_{k+2}^3 \, p_{k+5} \, p_{k+9}^4} \,.$$

Then $\left(p_{k+2}^3 \, p_{k+5} \, p_{k+9}^4\right)^{-1}$ appears inside $\left(\sum_{n>k} \frac{1}{p_n}\right)^8$. In order to end the proof of (1.8) we observe that the terms $1 + \ell Q$ are distinct. Then (1.7) implies

$$\sum_{\ell=1}^{N} \frac{1}{1+\ell Q} \leq \sum_{m=1}^{+\infty} \left(\frac{1}{2} \right)^m = 1 \,.$$

This is impossible because $\sum_{\ell=1}^{+\infty} \frac{1}{1+\ell Q} = +\infty$. □

Remark 1.12 We now want to estimate the divergence of the series $\sum_{p\in\mathcal{P}}^{+\infty} 1/p$. We start by proving the inequality

$$\prod_{\mathcal{P}\ni p\leq x} \left(1 - \frac{1}{p}\right)^{-1} \leq \prod_{\mathcal{P}\ni p\leq x} e^{p^{-1}+p^{-2}} \,. \tag{1.9}$$

Indeed, let $f(t) = (1-t)\, e^{t+t^2}$. Then $f'(t) = t(1-2t)\, e^{t+t^2} \geq 0$ for every $t \in [0, 1/2]$. Since $f(0) = 1$, we have $f(t) \geq 1$, that is to say $\frac{1}{1-t} \leq e^{t+t^2}$ for every $t \in [0, 1/2]$. This implies (1.9). If we take logarithms on both sides, while recalling (1.5) and the inequalities[3]

$$\sum_{k\leq x} \frac{1}{k} = \sum_{k=1}^{[x]} \frac{1}{k} \geq \int_1^{[x]+1} \frac{1}{x}\, dx = \log([x]+1) > \log x \,,$$

[3] The integral part $[\alpha]$ of a real number α is the largest integer smaller than or equal to α, for example, $[5] = 5$, $[e] = 2$, $[-\pi] = -4$.