CHAPTER 1

Division and Factorization

1.1. Division

The oldest and most fundamental aspect of number theory is the study of the natural numbers and their relationship with each other.

Among the axioms that define the set $\mathbb{N} = \{1, 2, 3, \ldots\}$ of all natural numbers is the Well ordering principle, that every non-empty subset of $\mathbb{N}$ has a least element. This is equivalent to the Principle of induction.

The set $\mathbb{N}$ of all natural numbers can be extended to the set

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

of all integers. The Well ordering principle is then equivalent to the assertion that every non-empty subset of $\mathbb{Z}$ bounded below has a least element, and that every non-empty subset of $\mathbb{Z}$ bounded above has a greatest element. This is one of the most important tools that we need to establish some of the first results concerning the set of integers.

Suppose that $a, b \in \mathbb{Z}$ and $a \neq 0$. Then we say that a divides b, denoted by $a \mid b$, if there exists $c \in \mathbb{Z}$ such that $b = ac$. In this case, we also say that a is a divisor of b, or that b is a multiple of a.

THEOREM 1.1. *Suppose that $a \in \mathbb{N}$ and $b \in \mathbb{Z}$. Then there exist unique $q, r \in \mathbb{Z}$ such that $b = aq + r$ and $0 \leqslant r < a$.*

PROOF. We first show the existence of such numbers $q, r \in \mathbb{Z}$. To determine the value of r, we use an idea going back to school mathematics. If b is non-negative, then we subtract from it just enough multiples of a to ensure that what remains is less than a but still non-negative. We then extend this idea to the case when b is negative, but now add to it just enough multiples of a until the resulting number is non-negative but again less than a. Formally, consider the set

$$S = \{b - as \geqslant 0 : s \in \mathbb{Z}\}.$$

Then it is easy to see that S is a non-empty subset of $\mathbb{N} \cup \{0\}$. It follows from the Principle of induction that S has a smallest element. Let r be the smallest element of S, and let $q \in \mathbb{Z}$ such that $b - aq = r$. Clearly $r \geqslant 0$, so it remains to show that $r < a$. Suppose on the contrary that $r \geqslant a$. Then

$$b - a(q + 1) = (b - aq) - a = r - a \geqslant 0,$$

so that $b - a(q + 1) \in S$. Clearly $b - a(q + 1) < r$, contradicting that r is the smallest element of S.

Next we show that such numbers $q, r \in \mathbb{Z}$ are unique. Suppose that

$$b = aq_1 + r_1 = aq_2 + r_2.$$

Then

$$|r_1 - r_2| = a|q_2 - q_1|.$$

If $q_1 \neq q_2$, then it is easy to see that $a|q_2 - q_1| \geqslant a$, while $|r_1 - r_2| < a$, a contradiction. It follows that $q_1 = q_2$, and so $r_1 = r_2$ also. ◯

We next establish the existence of the greatest common divisor.

THEOREM 1.2. *Suppose that $a, b \in \mathbb{N}$. Then there exists a unique $d \in \mathbb{N}$ such that*

(i) *there exist $x, y \in \mathbb{Z}$ such that $d = ax + by$;*
(ii) *$d \mid a$ and $d \mid b$; and*
(iii) *for every $k \in \mathbb{N}$ such that $k \mid a$ and $k \mid b$, we have $k \mid d$.*

REMARK. Condition (ii) shows that d is a divisor of both a and b, whereas condition (iii) shows that it is the greatest such divisor. We include condition (i) here as it is a very convenient intermediate result in the course of the proof.

PROOF OF THEOREM 1.2. Consider the set

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

Then it is easy to see that I is a non-empty subset of $\mathbb{Z}$ which contains some positive integers. It follows from the Principle of induction that I has a least positive element. Let d be the least positive element of I, and let $x, y \in \mathbb{Z}$ such that $d = ax + by$. The conclusion (i) follows trivially. Also, d is uniquely defined.

Next, we show that d divides every integer in I. Suppose that $z = au + bv$ is any given integer in I. By Theorem 1.1, there exist $q, r \in \mathbb{Z}$ such that $z = dq + r$, where $0 \leqslant r < d$. Then

$$r = z - dq = a(u - xq) + b(v - yq) \in I.$$

If $r \neq 0$, then the requirement $0 < r < d$ contradicts the minimality of d. Hence $r = 0$, so that $z = dq$, whence d divides z.

Taking $u = 1$ and $v = 0$ gives $d \mid a$. Taking $u = 0$ and $v = 1$ gives $d \mid b$.

Finally, the conclusion (iii) is a simple consequence of (i). ◯

The number d in Theorem 1.2 is called the greatest common divisor of a and b, and denoted by $d = (a, b)$. Two numbers $a, b \in \mathbb{N}$ are said to be relatively prime, or coprime, if $(a, b) = 1$.

A practical way of finding the greatest common divisor of two natural numbers is given by the following result.

THEOREM 1.3. *Suppose that $a, b \in \mathbb{N}$, and that $a < b$. Suppose further that $q_1, \ldots, q_{n+1} \in \mathbb{Z}$ and $r_1, \ldots, r_n \in \mathbb{N}$ satisfy $0 < r_n < r_{n-1} < \ldots < r_1 < a$ and*

$$\begin{aligned} b &= aq_1 + r_1, \\ a &= r_1q_2 + r_2, \\ r_1 &= r_2q_3 + r_3, \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n, \\ r_{n-1} &= r_nq_{n+1}. \end{aligned}$$

Then $(a, b) = r_n$.

PROOF. We first of all prove that

$$(a, b) = (a, r_1). \tag{1.1}$$

Note that we have $(a, b) \mid a$ and $(a, b) \mid (b - aq_1) = r_1$, and so

$$(a, b) \mid (a, r_1).$$

On the other hand, we have $(a, r_1) \mid a$ and $(a, r_1) \mid (aq_1 + r_1) = b$, and so

$$(a, r_1) \mid (a, b).$$

Equality (1.1) follows. Similarly

$$(a, r_1) = (r_1, r_2) = (r_2, r_3) = \ldots = (r_{n-1}, r_n). \tag{1.2}$$

Note now that

$$(r_{n-1}, r_n) = (r_n q_{n+1}, r_n) = r_n. \tag{1.3}$$

The result follows on combining (1.1)–(1.3). ◯

EXAMPLE. Consider $(589, 5111)$. In our notation, we let $a = 589$ and $b = 5111$. Then we have

$$\begin{aligned} 5111 &= 589 \times 8 + 399, \\ 589 &= 399 \times 1 + 190, \\ 399 &= 190 \times 2 + 19, \\ 190 &= 19 \times 10. \end{aligned}$$

It follows that $(589, 5111) = 19$. On the other hand,

$$\begin{aligned} 19 &= 399 - 190 \times 2 \\ &= 399 - (589 - 399 \times 1) \times 2 \\ &= 589 \times (-2) + 399 \times 3 \\ &= 589 \times (-2) + (5111 - 589 \times 8) \times 3 \\ &= 5111 \times 3 + 589 \times (-26). \end{aligned}$$

It follows that $x = -26$ and $y = 3$ satisfy $589x + 5111y = (589, 5111)$.

A very useful result concerning divisors is the following.

THEOREM 1.4. *Suppose that $a, b \in \mathbb{N}$ and $(a, b) = 1$. Suppose further that $w \in \mathbb{N}$ satisfies $w \mid ab$. Then there exist unique $u, v \in \mathbb{N}$ such that $u \mid a$, $v \mid b$ and $w = uv$.*

PROOF. We first of all show that $u = (w, a)$ and $v = (w, b)$ satisfy the requirements. Consider the number $(w, a)(w, b)$. By Theorem 1.2, there exist $x_1, y_1, x_2, y_2 \in \mathbb{Z}$ such that $(w, a) = wx_1 + ay_1$ and $(w, b) = wx_2 + by_2$, so that

$$(w, a)(w, b) = (wx_1 + ay_1)(wx_2 + by_2) = w(wx_1x_2 + ay_1x_2 + bx_1y_2) + aby_1y_2.$$

It follows that

$$w \mid (w, a)(w, b). \tag{1.4}$$

On the other hand, since $(a, b) = 1$, it follows from Theorem 1.2 that there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$, so that $w = wax + wby$. Note now that $(w, a) \mid a$ and $(w, b) \mid w$, so that $(w, a)(w, b) \mid wax$. Note also that $(w, a) \mid w$ and $(w, b) \mid b$, so that $(w, a)(w, b) \mid wby$. It follows that

$$(w, a)(w, b) \mid w. \tag{1.5}$$

Combining (1.4) and (1.5), and noting that $w, (w, a), (w, b) \in \mathbb{N}$, we conclude that $w = (w, a)(w, b)$.

To show uniqueness, it suffices to show that if $u, v \in \mathbb{N}$ satisfy $u \mid a$, $v \mid b$ and $w = uv$, then $u = (w, a)$ and $v = (w, b)$. Since $u \mid w$ and $u \mid a$, it follows from Theorem 1.2 that $u \mid (w, a)$. Similarly $v \mid (w, b)$. Suppose on the contrary that $u \neq (w, a)$. Then $u < (w, a)$, so that $w = uv < (w, a)(w, b) = w$, a contradiction. A similar contradiction arises if $v \neq (w, b)$. ◯

1.2. Factorization

Suppose that $a \in \mathbb{N}$ and $a > 1$. Then we say that a is prime if it has exactly two positive divisors, namely 1 and a. We also say that a is composite if it is not prime. It is convenient to treat the integer 1 as neither prime nor composite. To find a good reason for not including 1 as a prime, see the Remark following Theorem 1.7.

Throughout this chapter, the symbol p, with or without suffices, denotes a prime.

THEOREM 1.5. *Suppose that $a, b \in \mathbb{Z}$, and $p \in \mathbb{N}$ is a prime. If $p \mid ab$, then $p \mid a$ or $p \mid b$.*

PROOF. Suppose that $p \nmid a$. Since p is prime, the only positive divisors of p are 1 and p. Hence we must have $(a, p) = 1$. It follows from Theorem 1.2 that there exist $x, y \in \mathbb{Z}$ such that $1 = ax + py$, so that $b = abx + pby$. Clearly $p \mid b$. ◯

Using Theorem 1.5 a finite number of times, we obtain immediately the following generalization.

THEOREM 1.6. *Suppose that $a_1, \ldots, a_k \in \mathbb{Z}$, and $p \in \mathbb{N}$ is a prime. If $p \mid a_1 \ldots a_k$, then $p \mid a_j$ for some $j = 1, \ldots, k$.*

THEOREM 1.7 (Fundamental theorem of arithmetic). *Every integer $n \geqslant 2$ is representable as a product of primes, uniquely up to the order of factors.*

REMARK. If the integer 1 were included as a prime, then we would have to rephrase the statement of the Fundamental theorem of arithmetic to allow for different representations like $6 = 2 \times 3 = 1 \times 2 \times 3$.

PROOF OF THEOREM 1.7. We first of all show by induction that every integer $n \geqslant 2$ is representable as a product of primes. Clearly 2 is a product of primes. Assume next that $n > 2$ and that every integer $m \in \mathbb{N}$ satisfying $2 \leqslant m < n$ is representable as a product of primes. If n is a prime, then it is obviously representable as a product of primes. If n is not a prime, then there exist $n_1, n_2 \in \mathbb{N}$ satisfying $2 \leqslant n_1 < n$ and $2 \leqslant n_2 < n$ such that $n = n_1 n_2$. By our induction hypothesis, both n_1 and n_2 are representable as products of primes, so that n must also be representable as a product of primes.

Next we show uniqueness. Suppose that

$$n = p_1 \ldots p_r = p'_1 \ldots p'_s, \tag{1.6}$$

where $p_1 \leqslant \ldots \leqslant p_r$ and $p'_1 \leqslant \ldots \leqslant p'_s$ are primes. Now $p_1 \mid p'_1 \ldots p'_s$, so it follows from Theorem 1.3 that $p_1 \mid p'_j$ for some $j = 1, \ldots, s$. Since p_1 and p'_j are both primes, we must then have $p_1 = p'_j$. On the other hand, $p'_1 \mid p_1 \ldots p_r$, so again it follows from Theorem 1.3 that $p'_1 \mid p_i$ for some $i = 1, \ldots, r$, so again we must have $p'_1 = p_i$. It now follows that $p_1 = p'_j \geqslant p'_1 = p_i \geqslant p_1$, so that $p_1 = p'_1$. Removing the factor $p_1 = p'_1$ from (1.6), we obtain

$$p_2 \ldots p_r = p'_2 \ldots p'_s.$$

Repeating this argument a finite number of times, we conclude that $r = s$ and $p_i = p'_i$ for every $i = 1, \ldots, r$. ◯

Grouping together equal primes, we can reformulate Theorem 1.7 as follows.

THEOREM 1.8. *Every natural number $n > 1$ is representable uniquely in the form*

$$n = p_1^{m_1} \ldots p_r^{m_r}, \tag{1.7}$$

where $p_1 < \ldots < p_r$ are primes, and where $m_j \in \mathbb{N}$ for every $j = 1, \ldots, r$.

The representation (1.7) in Theorem 1.8 is known as the canonical decomposition of the natural number n.

1.3. Some Elementary Properties of Primes

There are many consequences of the Fundamental theorem of arithmetic. The following is one which concerns primes.

THEOREM 1.9. *There are infinitely many primes.*

PROOF. Suppose on the contrary that $p_1 < \ldots < p_r$ are all the primes. Let

$$n = p_1 \ldots p_r + 1.$$

Then $n \in \mathbb{N}$ and $n > 1$. It follows from the Fundamental theorem of arithmetic that $p_j \mid n$ for some $j = 1, \ldots, r$, so that $p_j \mid (n - p_1 \ldots p_r) = 1$, a contradiction. ◯

Let $n \in \mathbb{N}$, and let p be a prime. It is an interesting problem to find the largest integer k such that $p^k \mid n!$. In order to describe the answer to this question, we need to define one of the most useful functions in number theory.

Suppose that $\alpha \in \mathbb{R}$. The number $[\alpha] \in \mathbb{Z}$ is defined to be the unique integer $m \in \mathbb{Z}$ satisfying $m \leqslant \alpha < m + 1$. We call $[\alpha]$ the integer part of α.

EXAMPLES. We have $[\pi] = 3$, $[5] = 5$ and $[-\pi] = -4$.

The integer part function has many interesting properties. The proof of the following results is left as an exercise.

REMARKS. Suppose that $\alpha, \beta \in \mathbb{R}$.
(i) We have $\alpha - 1 < [\alpha] \leqslant \alpha$ and $0 \leqslant \alpha - [\alpha] < 1$.
(ii) If $\alpha \geqslant 0$, then $[\alpha]$ counts the number of natural numbers not exceeding α. In other words,

$$[\alpha] = \sum_{1 \leqslant n \leqslant \alpha} 1.$$

(iii) For every $n \in \mathbb{Z}$, we have $[\alpha + n] = [\alpha] + n$.
(iv) We have $[\alpha] + [\beta] \leqslant [\alpha + \beta] \leqslant [\alpha] + [\beta] + 1$.
(v) If $\alpha \in \mathbb{Z}$, then $[\alpha] + [-\alpha] = 0$. If $\alpha \notin \mathbb{Z}$, then $[\alpha] + [-\alpha] = -1$.
(vi) The number $-[-\alpha]$ is the smallest integer not less than α.
(vii) If $n \in \mathbb{N}$, then $[[\alpha]/n] = [\alpha/n]$.
(viii) The number $[\alpha + \frac{1}{2}]$ is one of the two integers nearest to α. Furthermore, if these two integers both differ from α by the same value, then $[\alpha + \frac{1}{2}]$ is the larger of these two integers.
(ix) If $\alpha > 0$ and $n \in \mathbb{N}$, then $[\alpha/n]$ is the number of positive integers not exceeding α and which are multiples of n.

THEOREM 1.10. *Suppose that $n \in \mathbb{N}$ and p is a prime. Then the largest integer k such that $p^k \mid n!$ is given by*

$$k = \sum_{j=1}^{\infty} \left[\frac{n}{p^j} \right].$$

PROOF. Suppose that $m \in \mathbb{N}$ and $1 \leqslant m \leqslant n$. If $p^r \mid m$ and $p^{r+1} \nmid m$, we want to count a contribution of r. In other words, we count a contribution of 1 for every $j \in \mathbb{N}$ such that $p^j \mid m$. Hence

$$k = \sum_{m=1}^{n} \sum_{\substack{j=1 \\ p^j \mid m}}^{\infty} 1 = \sum_{j=1}^{\infty} \sum_{\substack{m=1 \\ p^j \mid m}}^{n} 1 = \sum_{j=1}^{\infty} \left[\frac{n}{p^j} \right],$$

in view of Remark (ix) above. ◯

If $m \in \mathbb{N}$ and p is prime, we sometimes write $p^r \parallel m$ if $p^r \mid m$ and $p^{r+1} \nmid m$.

EXAMPLE. Suppose that $3^k \parallel 150!$. Then

$$\begin{aligned} k &= \left[\frac{150}{3} \right] + \left[\frac{150}{3^2} \right] + \left[\frac{150}{3^3} \right] + \left[\frac{150}{3^4} \right] + \left[\frac{150}{3^5} \right] + \ldots \\ &= 50 + 16 + 5 + 1 + 0 + \ldots \\ &= 72. \end{aligned}$$

1.4. Some Results and Problems Concerning Primes

Given that there are infinitely many primes, a natural question that arises is to determine the number $\pi(X)$ of primes that do not exceed a given real number X. This was the subject of much investigation in the 1800's. For example, Legendre proposed in 1808 that there is a constant A such that for large values of X, the number $\pi(X)$ can be approximated by

$$\frac{X}{\log X - A}. \tag{1.8}$$

Gauss proposed the function

$$\frac{1}{\log x}$$

as an approximation to the average density of distribution of primes near any large real number x, and thus formulated the function

$$\int_2^X \frac{\mathrm{d}x}{\log x} \tag{1.9}$$

as an approximation to $\pi(X)$. Note that the dominating term in the integral is

$$\frac{X}{\log X}, \tag{1.10}$$

so perhaps

$$\lim_{X\to\infty} \frac{\pi(X)\log X}{X} = 1. \tag{1.11}$$

Indeed, Tchebycheff showed in 1848 that if the limit in (1.11) exists at all, then it must be equal to 1. Unfortunately, he and others were unable to show that the limit exists. Then in 1850, he showed that there exist positive constants c_1 and c_2 such that for every real number $X \geqslant 2$, we have

$$c_1 \frac{X}{\log X} < \pi(X) < c_2 \frac{X}{\log X}.$$

This confirms that the function (1.10) at least represents the correct order of magnitude of $\pi(X)$. We prove Tchebycheff's theorem in Chapter 6.

The crucial idea that finally led to the proof of (1.11) was introduced by Riemann in a monumental contribution in 1860. Riemann observed that the series

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \tag{1.12}$$

plays a crucial role in the study of the distribution of primes if one treats s as a complex variable. It follows that the distribution of primes can be studied by the use of methods in the theory of analytic functions. Riemann denoted the series (1.12) by $\zeta(s)$, and the function has since been known as the Riemann zeta function. Indeed, Riemann's work has also influenced greatly the development of the general theory of functions.

Riemann's ideas were studied in great depth in the late 1800's by von Mangoldt and Hadamard. This culminated in the proof of (1.11) in 1896 by Hadamard and de la Vallée Poussin, independently and almost simultaneously. In particularly, the work of de la Vallée Poussin showed that the integral (1.9) is a better approximation to $\pi(X)$ than the function (1.8) for any value of the constant A.

The result (1.11) is known nowadays as the Prime number theorem. As this is a course of lectures on elementary number theory, we shall not discuss here the analytic aspects described in the preceding two paragraphs.