Chapter 1

Basics of elementary number theory

1.1 Divisibility

Definition 1.1 (Divisibility)**.** *Let $m, n \in \mathbb{Z}$. We say m* ***divides*** *n and write $m \mid n$ if there exists some integer q such that $n = qm$. If m divides n, we say n is a* ***multiple*** *of m and say m is a* ***divisor*** *or a* ***factor*** *of n.*

Definition 1.2 (Congruence)**.** *Let $a, b \in \mathbb{Z}$, $q \in \mathbb{N}^*$. If $q \mid (a - b)$, we say a and b are* ***congruent*** *modulo q and write*

$$a \equiv b \pmod{q}.$$

Definition 1.3 (Greatest common divisor and least common multiple)**.** *Let $m, n \in \mathbb{Z}$, not both zero. The* ***greatest common divisor*** *(g.c.d. for short) of m and n, denoted by (m, n) or $\gcd(m, n)$, is the largest positive integer d such that $d \mid m$ and $d \mid n$.*

Let $m, n \in \mathbb{Z} \setminus \{0\}$. The ***least common multiple*** *(l.c.m. for short) of m and n, denoted by $[m, n]$ or $\operatorname{lcm}(m, n)$, is the smallest positive integer d such that $m \mid d$ and $n \mid d$. If $mn = 0$, we define $[m, n] = 0$.*

Similarly, we can iteratively define the g.c.d. or l.c.m. of multiple integers.

Theorem 1.1 (Euclidean division theorem)**.** *Let a be an integer and let b be a positive integer. Then there is a unique pair of integers q and r such that*

$$a = bq + r, \quad 0 \le r < b.$$

*The integer q is called the **quotient** and r is called the **remainder** when b is divided by a.*

Proof. Take q to be the largest integer with $bq \leq a$ and set $r = a - bq$. Then r satisfies $0 \leq r < b$ since otherwise $q' = q + 1$ will be a larger integer satisfying $bq' \leq a$. □

Remark. Theorem 1.1 imples that $\mathbb{Z}$ is a euclidean domain hence is a principal ideal domain. So any non-zero ideal $\mathfrak{a}$ of $\mathbb{Z}$ is of the form $m\mathbb{Z}$ with $m \in \mathbb{N}^*$. Let $m\mathbb{Z}$ be a non-zero ideal of $\mathbb{Z}$, we have the natural homomorphism of rings

$$\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} : a \mapsto a + m\mathbb{Z}.$$

For $a \in \mathbb{Z}$, we usually denote the image of a under the above homomorphism by $\bar{a}$ or $a \pmod{m}$. The concepts of divisibility and congruences can be described in the language of ring theory:

- $a \mid b \quad \Leftrightarrow \quad b \in a\mathbb{Z} \quad \Leftrightarrow \quad \bar{b} = \bar{0}$ in $\mathbb{Z}/a\mathbb{Z}$.
- $a \equiv b \pmod{m} \quad \Leftrightarrow \quad a + m\mathbb{Z} = b + m\mathbb{Z} \quad \Leftrightarrow \quad \bar{a} = \bar{b}$ in $\mathbb{Z}/a\mathbb{Z}$.

In order to obtain the greatest common divisor, we can use the following **euclidean algorithm**: Let a and b be positive integers. By repeatedly applying Theorem 1.1, we find the sequence of equations:

$$\begin{aligned}
a &= bq_1 + r_1, \quad 0 < r_1 < b, \\
b &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1, \\
r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2, \\
&\cdots \\
r_{n-1} &= r_n q_{n+1} + r_{n+1}, \quad 0 < r_{n+1} < r_n \\
r_n &= r_{n+1} q_{n+2}.
\end{aligned}$$

This process must terminate in finitely many steps since the decreasing sequence $b, r_1, r_2, \dots$ can not contain more than b positive integers. Clearly, we have

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_n, r_{n+1}) = r_{n+1}.$$

Example 1.1. *We apply the euclidean algorithm to evaluate $(525, 231)$:*

$$\begin{aligned}
525 &= 231 \cdot 2 + 63, \\
231 &= 63 \cdot 3 + 42, \\
63 &= 42 \cdot 1 + 21, \\
42 &= 21 \cdot 2.
\end{aligned}$$

So we find $(525, 231) = 21$.

1.2 The prime numbers

Definition 1.4 (Prime number)**.** *An integer p is a **prime number** if it satisfies the following equivalent conditions:*

i) $p = ab$ *with* $a, b \in \mathbb{Z} \quad \Rightarrow \quad a \in \mathbb{Z}^\times$ *or* $b \in \mathbb{Z}^\times$.

ii) $p \mid ab$ *with* $a, b \in \mathbb{Z} \quad \Rightarrow \quad p \mid a$ *or* $p \mid b$.

The set of positive prime numbers is denoted by $\mathbb{P}$. Positive integers larger than 1 *which are not prime are called **composite**.*

Convention. Unless otherwise stated, when we say "prime number", we mean "positive prime number". The lowercase letter p, with or without subscripts, is considered as a prime number, unless otherwise stated. This convention is usually used when p appears as a variable in $\sum$ or $\prod$. For example, the notation

$$\sum_{p \le x} \frac{1}{p}$$

means summing over all prime numbers not exceeding x.

Theorem 1.2 (Fundamental theorem of arithmetic)**.** *Every integer $n > 1$ can be uniquely represented as a product of prime numbers, up to the order of factors.*

Definition 1.5 (Prime factorization)**.** *By the fundamental theorem of arithmetic, we have the **prime factorization** for each integer $n > 1$:*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

where $p_1, \ldots, p_k$ are distinct prime numbers and $\alpha_1, \ldots, \alpha_k$ are positive integers.

Definition 1.6 (p-adic valuation)**.** *Let p be a prime number and let $n \in \mathbb{Z} \setminus \{0\}$. Then there exists a unique non-negative integer α such that $p^\alpha \mid n$ but $p^{\alpha+1} \nmid n$. We denote this case as $p^\alpha \parallel n$. The exponent α is called the p**-adic valuation** of n and is denoted by $v_p(n)$. Set $v_p(0) = +\infty$.*

Remark. Clearly, for any $m, n \in \mathbb{Z} \setminus \{0\}$, we have

$$v_p(mn) = v_p(m) + v_p(n). \tag{1.1}$$

That is, $v_p(n)$ is a completely additive function (ref. Definition 2.1).

Theorem 1.3 (The infinity of prime numbers)**.** *There are infinitely many prime numbers.*

Proof I. Suppose on the contrary that there are only finitely many prime numbers, say, $p_1, \ldots, p_k$. Then any prime factor of $p_1 \cdots p_k + 1$ is a prime number differing from $p_1, \ldots, p_k$. This is a contradiction. □

Proof II. Suppose on the contrary that there are only finitely many prime numbers, say, $p_1, \ldots, p_k$. Let N be an arbitrarily large integer. By Theorem 1.2, every positive integer $n \leq N$ can be uniquely represented as

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

with $\alpha_j \in \mathbb{N}$, $j = 1, 2, \ldots, k$. Moreover, since $n \leq N$, we have

$$p_j^{\alpha_k} \leq n \leq N \quad \Rightarrow \quad \alpha_j \leq \frac{\log N}{\log p_j} \leq \frac{\log N}{\log 2}.$$

So the number of possible choices of $(\alpha_1, \ldots, \alpha_k)$ is at most

$$\left(\frac{\log N}{\log 2} + 1 \right)^k.$$

But for sufficiently large N, we have

$$\left(\frac{\log N}{\log 2} + 1 \right)^k < N.$$

This is a contradiction. □

In analytic number theory, we are more concerned with quantitative behavior. For $x \geq 1$, we define the **prime counting function** $\pi(x)$ by

$$\pi(x) = \left| \mathbb{P} \cap [1, x] \right|.$$

In other words, $\pi(x)$ is the number of prime numbers not exceeding x. Actually, our proof of Theorem 1.3 provides a (very weak) lower bound for $\pi(x)$. Let p_n denote the n-th prime. From the first proof, it is not hard to obtain the inequality

$$p_n \leq 2^{2^n},$$

which implies the lower bound (provided that x is sufficiently large)

$$\pi(x) \geq \frac{\log\log x}{\log 2} - \left(\frac{\log\log 2}{\log 2} + 1\right).$$

The second proof provides a better bound:

$$\pi(x) \geq \frac{\log x}{\log\log x}.$$

But these bounds are far from the best since we have the following well-known prime number theorem.

Theorem 1.4 (Prime number theorem)**.** *As $x \to +\infty$, we have $\pi(x) \sim x/\log x$, i.e.*

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

Proving the prime number theorem is one of the main goals of this course.

1.3 The functions $[x]$ and $\{x\}$

Let $[x]$ denote the "rounding down" function, i.e.

$$[x] = \text{the largest integer not exceeding } x.$$

Clearly, for $n \in \mathbb{Z}$,

$$[x] = n \quad \Leftrightarrow \quad n \leq x < n+1.$$

Let $\{x\} = x - [x]$ denote the fractional part of x. The following facts about these two functions can be easily checked.

Proposition 1.5. *i) For any $x \in \mathbb{R}$, we have $0 \leq \{x\} < 1$.*

ii) For $x \in \mathbb{R}$ and $n \in \mathbb{Z}$, we have $[x+n] = [x] + n$ and $\{x+n\} = \{x\}$.

iii) For $x, y \in \mathbb{R}$, $[x] + [y] \leq [x+y]$.

Proposition 1.6. *Let $d \in \mathbb{N}^*$ and $x \in \mathbb{R}^+$. The number of positive integers not exceeding x which are divisible by d is $[x/d]$.*

Proof. The set of positive integers not exceeding x divisible by d can be represented as

$$\{d, 2d, \ldots, kd\},$$

where k is the largest positive integer such that $kd \le x$. But

$$kd \le x \quad \Leftrightarrow \quad k \le \frac{x}{d}.$$

So $k = [x/d]$. □

Theorem 1.7. *Let $n \in \mathbb{N}^*$ and let $p \in \mathbb{P}$. We have*

$$v_p(n!) = \sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right].$$

Proof. By (1.1), we have

$$v_p(n!) = \sum_{m=1}^{n} v_p(m) = \sum_{m=1}^{n} \sum_{k \le v_p(m)} 1 = \sum_{k=1}^{\infty} \sum_{\substack{m \le n \\ v_p(m) \ge k}} 1.$$

Notice that

$$v_p(m) \ge k \quad \Leftrightarrow \quad p^k \mid m.$$

So by Proposition 1.6, the last summation is

$$\sum_{\substack{m \le n \\ v_p(m) \ge k}} 1 = \sum_{\substack{m \le n \\ p^k \mid m}} 1 = \left[\frac{n}{p^k}\right].$$

This completes the proof. □

Theorem 1.8. *Let $m, n \in \mathbb{N}^*$ with $m \le n$. Then the bionomial number*

$$\binom{n}{m} = \frac{n(n-1)\cdots(n-m+1)}{m!} = \frac{n!}{m!(n-m)!}$$

is an integer.

Proof. It is sufficient to show that for any prime number p, the p-adic valuation of the denominator does not exceed that of the numerator. By Theorem 1.7 and iii) of Proposition 1.5, we have

$$v_p(n!) = \sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right] \ge \sum_{k=1} \left(\left[\frac{m}{p^k}\right] + \left[\frac{n-m}{p^k}\right]\right) = v_p(m!(n-m)!).$$

□

Theorem 1.9 (Dirichlet's approximation theorem). *Let $Q \geq 1$ be a positive integer. Then for any real number α, there exist integers a, q with $1 \leq q \leq Q$ and $(a, q) = 1$, such that*

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{qQ}.$$

Proof. Consider the following $(Q+1)$ points in $[0, 1)$:

$$0, \{\alpha\}, \{2\alpha\}, \ldots, \{Q\alpha\}.$$

By the pigeonhole principle, there are two points whose distance is less that $1/Q$. That is, there exist $0 \leq m_1 < m_2 \leq Q$ such that

$$|\{m_2\alpha\} - \{m_1\alpha\}| < \frac{1}{Q}.$$

We have

$$\{m_2\alpha\} - \{m_1\alpha\} = (m_2 - m_1)\alpha - ([m_2\alpha] - [m_1\alpha]).$$

Take

$$\frac{a}{q} = \frac{[m_2\alpha] - [m_1\alpha]}{m_2 - m_1}$$

and the desired result follows. □

Remark. In fact, the requirement "Q is an integer" is not necessary. The same result holds for real $Q \geq 1$. One could prove this slightly stronger version by slightly modifying the above proof. We leave it as an exercise.

Corollary 1.10. *Let α be an irrational number. Consider the irrational rotation on the unit circle*

$$\begin{aligned} T_\alpha : \mathbb{T}^1 &\to \mathbb{T}^1 \\ x &\mapsto x + \alpha \end{aligned}$$

where

$$\mathbb{T}^1 = \mathbb{R}/\mathbb{Z} = \{x \,(\mathrm{mod}\, 1) \,|\, x \in \mathbb{R}\}.$$

Then for any $x \in \mathbb{T}$, the orbit $\{T_\alpha^n x\}_{n=1}^{+\infty}$ is dense in $\mathbb{T}$.

Proof. It suffices to show that

$$U \cap \{T_\alpha^n x\}_{n=1}^{+\infty} \neq \emptyset$$

for any interval U. In fact, suppose that the length of U is ε. By Theorem 1.9, there exist integers a, q with $q \geq 1$ such that

$$\left|\alpha - \frac{a}{q}\right| < \frac{\varepsilon}{q} \quad \Rightarrow \quad |q\alpha - a| < \varepsilon.$$

Let $\delta = q\alpha - a$. Then $|\delta| < \varepsilon$ and

$$T_\alpha^q x = x + q\alpha \pmod 1 = x + \delta \pmod 1.$$

for any $x \in \mathbb{T}$. Therefore, under the repeated action of T_α^q, x will eventually enter U. $\square$