MSCM Number Theory

Alan Zhou

2024-25

Contents

1 Proving the Fundamental Theorem of Arithmetic

The **fundamental theorem of arithmetic** (FTA) states that every positive integer can be written as a product of primes, and that moreover, there is only one way to do this (aside from rearranging the primes in the product). For example, 2024 and 2025 can be written as

$$2024 = 2 \cdot 2 \cdot 2 \cdot 11 \cdot 23 \quad \text{and} \quad 2025 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 5.$$

For a given positive integer, the corresponding product of primes is its *prime factorization.*

This handout develops the number theory needed to prove the FTA from (more-or-less) first principles. Along the way, we will encounter some other useful tools, in particular the *euclidean algorithm* for calculating the greatest common divisor (GCD).

Convention. Unless otherwise specified, “number” means “non-negative integer.”

These notes are also available at https://azhou5849.github.io/teaching/.

1.1 Divisibility

Given two numbers a and b, we say that a *is divisible by* b, or that b *divides* a, if there is a number c such that $a = bc$. If this is the case, we can write $b \mid a$. For example:

$$3 \mid 6, \quad 17 \mid 51, \quad 13 \mid 91, \quad 23 \mid 2024, \quad 1 \mid 7, \quad 7 \mid 7, \quad 6 \mid 0.$$

1.2 The division algorithm

Integers can be added, subtracted, and multiplied without issue, but division does not always produce an integer result. However, we can stay within the integers by introducing remainders.

Proposition 1.1 (Division algorithm)**.** *Let a and b be positive integers, with $b \neq 0$. There are unique non-negative integers q and r, with $0 \leq r < b$, such that $a = bq + r$.*

Using the notation of the statement, q is the *(integer) quotient* when dividing a by b, while r is the *remainder* when dividing a by b.

Proof. Consider the set $\mathcal{R}$ of *all* non-negative integers that can be written in the form $a - bn$, where n is a non-negative integer. This set is non-empty, as $a - b \cdot 0 = a$ is in $\mathcal{R}$, so it has a minimal element $r \geq 0$, which we can write as $r = a - bq$ for some non-negative integer q. We claim that $r < b$ as well. If $r \geq b$, then $r' = r - b \geq 0$, and we can write

$$r' = r - b = (a - bq) - b = a - b(q + 1). \tag{1}$$

This shows that $r' \in \mathcal{R}$, but $r' < r$, contradicting minimality of r. Hence we must have $r < b$, so we have shown that the non-negative integers q and r in the proposition must exist.

For uniqueness, suppose we can write $a = bq + r$ and $a = bq' + r'$, with $0 \leq r, r' < b$. Then

$$b(q - q') = r' - r, \tag{2}$$

so $r' - r$ is divisible by b. Since $0 \leq r, r' < b$, the only way this can happen is to have $r' - r = 0$, in which case $r' = r$. Then, since $b \neq 0$, we must have $q - q' = 0$, so $q = q'$. □