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 discusses the number theory needed to prove the FTA. Knowledge of the material that is already in the textbook (AoPS Volume 1) is assumed.

Convention. Unless otherwise specified, "number" means "non-negative integer" in this chapter.

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 if there is a number c such that $a = bc$. When $b \neq 0$, this is equivalent to saying that a/b is an integer. Synonymously, we say that a *is a multiple of* b, that b *divides* a, and that b *is a divisor of* a. This can be written as $b \mid a$.

When a is divisible by b, we can calculate $c = a/b$ using the usual division method(s) taught in school. Even when a is not divisible by b, long division gets us

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

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

1.2 Common divisors

Suppose that a and b are numbers with $a \neq 0$. We know that 1 divides both a and b and that there are only finitely many numbers which divide a, so the set of *common divisors* of a and b, i.e. the numbers which divide both a and b, is non-empty and finite. This means that there is a *greatest* common divisor of a and b, which we denote by $\gcd(a, b)$. If $\gcd(a, b) = 1$, we say that a and b are *relatively prime* or *coprime.*

One way to compute $\gcd(a, b)$ is simply to list out all of the divisors of a and b and look for the largest one that appears in both lists. For larger numbers, a better idea uses the following.

Proposition 1.2. *If a and b are numbers, $a \neq 0$, and $a \geq b$, then $\gcd(a, b) = \gcd(a - b, b)$.*

Proof. We prove the stronger statement that *any* common divisor of a and b is also a common divisor of b and $a - b$, and vice versa. Suppose d is a common divisor of a and b, so $a = da'$ and $b = db'$ for some numbers a' and b'. Then $a - b = d(a' - b')$, so d is a divisor of $a - b$ as well, hence a common divisor of b and $a - b$. A similar argument shows that any common divisor of b and $a - b$ is also a divisor of a; this is left as an exercise. □

Repeatedly using this result to calculate GCD is the *euclidean algorithm.* For example:

$$\begin{aligned}\gcd(582\,133, 268\,381) &= \gcd(313\,752, 268\,381) = \gcd(45\,371, 268\,381)\\ &= \gcd(45\,371, 223\,010) = \gcd(45\,371, 177\,639) = \gcd(45\,371, 132\,268)\\ &= \gcd(45\,371, 86\,897) = \gcd(45\,371, 41\,526) = \gcd(3845, 41\,526)\\ &= \gcd(3845, 37\,681) = \gcd(3845, 33\,836) = \cdots\\ &= \gcd(3845, 3076) = \gcd(769, 3076) = \gcd(769, 2307)\\ &= \gcd(769, 1538) = \gcd(769, 769) = \boxed{769}.\end{aligned}$$

Subtracting the same number over and over again can be done in one line by using division with remainder (Proposition 1.1) instead:

$$\begin{aligned}\gcd(582\,133, 268\,381) &= \gcd(45\,371, 268\,381) & 582\,133 &= 2\cdot 268\,381 + 45\,371\\ &= \gcd(45\,371, 41\,526) & 268\,381 &= 5\cdot 45\,371 + 41\,526\\ &= \gcd(3845, 41\,526) & 45\,371 &= 1\cdot 41\,526 + 3845\\ &= \gcd(3845, 3076) & 41\,526 &= 10\cdot 3845 + 3076\\ &= \gcd(769, 3076) & 3845 &= 1\cdot 3076 + 769\\ &= \gcd(769, 0) & 3076 &= 4\cdot 769 + 0\\ &= \boxed{769}.\end{aligned}$$

1.3 Bézout's lemma