# 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 how to prove the FTA. Knowledge of the material that is already in the textbook (AoPS Volume 1) or in class examples is assumed.

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

## 1.1 Every positive integer is a product of primes

The fact that there is *a* prime factorization requires no additional theory.

**Theorem 1.1.** *Every positive integer (greater than 1) is prime or can be written as a product of primes.*

*Proof.* Suppose otherwise, and let $n > 1$ be the smallest counterexample to the statement. Then $n$ cannot be prime itself, so we can write $n = ab$ where neither $a$ nor $b$ is 1. This means that $a, b < n$, so $a$ and $b$ can be written as products of primes. Joining these products together shows $n$ is a product of primes, contradiction. □

*Remark.* For those familiar with mathematical induction, the proof is a little smoother by using strong induction instead of contradiction.

What remains is to prove that there is only one prime factorization (aside from rearrangement), and the rest of the handout is dedicated to this goal.

## 1.2 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 1.2** (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 $b$.

## 1.3 Common divisors

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 1.3.** *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:

$$\begin{aligned}\gcd(582133, 268381) &= \gcd(313752, 268381) = \gcd(45371, 268381)\\ &= \gcd(45371, 223010) = \gcd(45371, 177639) = \gcd(45371, 132268)\\ &= \gcd(45371, 86897) = \gcd(45371, 41526) = \gcd(3845, 41526)\\ &= \gcd(3845, 37681) = \gcd(3845, 33836) = \cdots\\ &= \gcd(3845, 3076) = \gcd(769, 3076) = \gcd(769, 2307)\\ &= \gcd(769, 1538) = \gcd(769, 769) = \boxed{769}.\end{aligned}$$

Subtracting the same number over and over again can be done in one line by using division with remainder (Proposition 1.2) instead:

$$\begin{aligned}\gcd(582133, 268381) &= \gcd(45371, 268381) & 582133 &= 2 \cdot 268381 + 45371\\ &= \gcd(45371, 41526) & 268381 &= 5 \cdot 45371 + 41526\\ &= \gcd(3845, 41526) & 45371 &= 1 \cdot 41526 + 3845\\ &= \gcd(3845, 3076) & 41526 &= 10 \cdot 3845 + 3076\\ &= \gcd(769, 3076) & 3845 &= 1 \cdot 3076 + 769\\ &= \gcd(769, 0) & 3076 &= 4 \cdot 769 + 0\\ &= \boxed{769}.\end{aligned}$$

## 1.4 Bézout's lemma

When running the euclidean algorithm by division with remainder, the last non-zero remainder will always be the GCD. We can repeatedly "back-substitute" to write, in the previous example,

$$\begin{aligned}769 &= 1 \cdot 3845 - 1 \cdot 3076 = 1 \cdot 3845 - (41526 - 10 \cdot 3845)\\ &= 11 \cdot 3845 - 1 \cdot 41526 = 11 \cdot (45371 - 1 \cdot 41526) - 1 \cdot 41526\\ &= 11 \cdot 45371 - 12 \cdot 41526 = 11 \cdot 45371 - 12 \cdot (268381 - 5 \cdot 45371)\\ &= 71 \cdot 45371 - 12 \cdot 268381 = 71 \cdot (582133 - 2 \cdot 268381) - 12 \cdot 268381\\ &= 71 \cdot 582133 - 154 \cdot 268381.\end{aligned}$$

In general, we can write the GCD as a "linear combination" of the original numbers by running this procedure. The fact we can always do this is known as *Bézout's lemma*.

**Lemma 1.4** (Bézout)**.** *Let $a, b$ be numbers, not both 0. There exist integers $m, n$ such that*

$$am + bn = \gcd(a, b).$$

## 1.5 Prime numbers

A number $p$ is *prime* if $p \neq 1$ and the equation $p = ab$, where $a$ and $b$ are numbers, implies that $a = 1$ or $b = 1$. Equivalently, a prime number has exactly two distinct divisors: 1 and itself.

**Proposition 1.5.** *Let $p$ be a prime number and let $a, b$ be numbers. If $p \mid ab$, then $p \mid a$ or $p \mid b$.*

*Proof.* It is equivalent to show that if $p \mid ab$ but $p$ does not divide $a$ (written $p \nmid a$), then $p \mid b$. Since the only divisors of $p$ are 1 and $p$, we must then have $\gcd(a, p) = 1$. By Bézout's lemma (1.4), there exist integers $m, n$ such that $am + pn = 1$. Multiplying through by $b$,

$$(ab)m + p(bn) = b.$$

Both terms on the left hand side are divisible by $p$, so the right hand side $b$ is divsible by $p$. □

## 1.6 Prime factorization is unique