[MA276] Number Theory Introduction

Rose-Hulman Institute of Technology

David Sachmanyan
February 20, 2026

This topic will not be discussed on exams but might make a slight appearance on the final. We will just go over some basic topics within the field of number theory.

Definition 0.1 (The Division Algorithm)**.** For all $n, m \in \mathbb{N}$, if $m > 0$ there exists a $q, r \in \mathbb{N}$ such that $n = qm + r$ and $r < m$. The number q is called the quotient and the number r is called the remainder.

Definition 0.2 (Divisor)**.** The divisors of $a \in \mathbb{Z}^+$ are the positive integers that divide a. Let

$$D(a) = \{d \mid d|a\} = \{d \mid k \in \mathbb{Z}(a = kd)\}. \tag{0.1}$$

Then, if $a, b \in \mathbb{Z}^+$, we have that $D(a) \cap D(b)$ is the set of common divisors. The *greatest common divisor* of a, b is the largest element of the set of common divisors.

Theorem 0.1. *Let $a, b \in \mathbb{Z}^+$ with $a \geq b$. Let r be the remainder when we divide a by b. If $r = 0$, then $\gcd(a, b) = b$, and if $r > 0$, then $\gcd(a, b) = \gcd(b, r)$.*

Proof. Assume $a = qb + r$ where $- < r < b$. So $0 < r = a - qb$. Let $d \in D(a) \cup D(b)$ be a common divisor of a and b. So $d|a$ and $d|b$, therefore, $a = jd$ and $b = kd$ for some $j, k \in \mathbb{Z}$. I forgot. □

Theorem 0.2 (Fundamental Theorem of Arithmetic)**.** *For every integer $n > 1$, there exist unique prime numbers $p_1, p_2, \ldots, p_k$ for some $k \in \mathbb{Z}^+$ such that $p_1 \leq p_2 \leq \cdots \leq p_k$ and $n = p_1 p_2 \ldots p_k$.*

Proof. We will first prove *existence*. Let $\mathbb{Z} \ni n > 1$ and assume for any m such that $k < m < n$ that there are primes $p_1, \ldots p_k$ such that $m = p_1 \ldots p_k$. If n is prime, of course, there does exist a prime such that $n = p_i$, which is a product of primes. However, if n is not prime, it is what we call *composite*, meaning there are $a, b \in \mathbb{Z}^+$ with $q < a < n$ and $q < b < n$ so that $n = ab$. By our inductive hypothesis, there are primes $p_1, \ldots, p_{k_a}$ and $r_1, \ldots, r_{k_b}$ so that $a = p_1 \ldots p_{k_a}$ and $b = r_1 \ldots r_{k_b}$. This implies

$$ab = \prod p_i \prod r_i = (p_1 \ldots p_{k_a})(r_1 \ldots r_{k_b}) \tag{0.2}$$

which means that primes do exist. If we want, we can do a separate proof for uniqueness (which is also inductive) but we have only shown the proof for existence. □

Yes this is very short, but I shall take a proper number theory class later, this is just an interesting topic to cover because there are some interesting inductive proofs involved with number theory. Some practice problems can be found on the notes sheet but I suppose you might not have access to that.