We assume that the reader is already familiar with the basics of set theory and how to write proofs. More concretely, the reader should have a good grasp on functions and relations. We do request that the reader know about equivalence relations. Therefore, we will not treat them in this book. (If there is sufficient demand I will add these in)

In this book, the naturals start from zero. That is, $\mathbb{N} = \{0, 1, 2, \dots\}$. We denote the set of integers by $\mathbb{Z}$, the set of real numbers by $\mathbb{R}$, the set of rational numbers by $\mathbb{Q}$ and the set of complex numbers by $\mathbb{C}$.

We first begin with an axiom. This will help us with proving the division algorithm (Theorem 0.2) and the fact that the GCD is a linear combination (Theorem 0.3).

**Axiom 0.1** (Well-ordering for naturals)**.** Let $S \subseteq \mathbb{N}$ be a nonempty set of natural numbers. Then, $S$ has a smallest element.

**Theorem 0.2** (Division algorithm)**.** Let $n, m \in \mathbb{Z}$ and $m > 0$. Then, there exists unique $q, r \in \mathbb{Z}$, where $0 \leq r < m$ such that $n = qm + r$.

*Proof.* Let

$$S = \{ n - qm : q \in \mathbb{Z}, n - qm \geq 0 \}.$$

Then $S$ is nonempty as $n \in S$, so it has a smallest element $r$. Clearly $r < m$, for if $r \geq m$ then it would not be the smallest. Then $n - r$ must divide $m$, so let $q$ be an integer such that $qm = n - r$. For uniqueness, suppose $q', r'$, where $0 \leq r' < m$ satisfies $n = q'm + r'$. Then, $qm + r = q'm + r'$, so $m(q - q') = r' - r$. Observe that $-m < r' - r < m$, so $q - q' = 0$, and thus $r = r'$ as well. □

In the proof above, $q$ is called the *quotient* and $r$ is called the *remainder*. If the remainder $r$ is zero, then $m$ is said to **divide** $n$, and we write $m \mid n$.

We now give some motivation for what is going on in the proof above. The set $S$ may seem mysterious, but let us quickly try to understand why it is defined as such. Let us suppose that we are dividing $n$ by $m$. Recall from elementary school that when performing long division, we are interested in the largest multiple of $m$, say $qm$ such that $n - qm$ is as small as possible. So $S$ should contain the minimum value of $n - qm$ possible. This would be the remainder.

**Theorem 0.3** (GCD is a linear combination)**.** Let $n, m \in \mathbb{Z}$ be nonzero integers. Then, there exists integers $s, t \in \mathbb{Z}$ such that $\gcd(n, m) = ns + mt$. Additionally, $\gcd(n, m)$ is the smallest positive integer of the form $ns + mt$.

*Proof.* Let

$$S = \{ na + mb : a, b \in \mathbb{Z}, na + mb > 0 \}.$$

Then $S$ is nonempty, so it has a smallest element $d$, which is of the form $ns + mt$. We claim $d = \gcd(n, m)$. First, we show $d$ divides both $n$ and $m$. By Theorem 0.2, $n = qd + r$, where $0 \leq r < d$. If $r > 0$ then we have $r = n - qd = n - q(ns + mt) = n(1 - qs) - m(qt)$. So $r \in S$ but $r < d$, a contradiction. A similar argument holds for $m$, so $d$ divides both $n$ and $m$. Let $d'$ divide both $n$ and $m$ too, we show $d'$ divides $d$ to establish that $d$ is in fact the gcd. Let $n = d'h$, and $m = d'k$. Then $d = (d'h)s + (d'k)t = d'(hs + kt)$ as desired. □

Once again we have constructed a rather mysterious looking set. However, such a set $S$ is natural because we are trying to show that the gcd is the *smallest* positive integer that is a linear combination of $n, m$.

We say that 2 numbers $n, m$ are **coprime** if $\gcd(n, m) = 1$. One corollary of this theorem is so important it is singled out.

**Corollary 0.4** (Bezout's lemma)**.** If $\gcd(n, m) = 1$, then there exists integers $s, t \in \mathbb{Z}$ such that $ns + mt = 1$.

And now a quick application of this corollary
**Lemma 0.5** (Euclid's Lemma)**.** *Let $p$ be a prime and $p \mid ab$. Then $p \mid a$ or $p \mid b$.*

*Proof.* Suppose $p$ does not divide $a$. Then, by Corollary 0.4, there are integers $s, t$ such that $as + pt = 1$, so $b = bas + bpt$. Then $p$ divides the right side of the equation, so it divides the left side too. □

This theorem tells us that we can factorize natural numbers into a product of primes in a unique way.

**Theorem 0.6** (Fundamental Theorem of Arithmetic)**.** Let $n \in \mathbb{N}$ and $n > 1$. Then $n$ is prime, or is a unique product of primes.

*Proof.* Exercise for the reader. Use Lemma 0.5 and strong induction. □

All the results here are rather important especially in the study of finite group theory. As we go deeper into the book, we will invoke them with no explicit mention, so the reader is highly encouraged to keep these in mind.

**Exercise 0.7** (Fundamental Theorem of Arithmetic)**.** Prove Theorem 0.6

**Exercise 0.8** (Generalized Euclid's lemma)**.** Prove that if $p \mid a_1 \cdots a_n$ then $p \mid a_i$ for some $a_i$.

**Exercise 0.9.** Prove that there are infinitely many primes.