Introduction to Prime Numbers

Brendan Mullen

Introduction

Prime numbers are a critical topic to mathematics and are essentially the building blocks of natural numbers because of their certain characteristics.

They play a crucial role in mathematics and have been studied by mathematicians for centuries. The curiosity and study of prime numbers originates back to ancient civilizations. Circa 300 BC, Euclid's theorem was discovered and proves that infinitely many prime numbers exist. Prime numbers have remained a central topic in number theory and are continuing to be used to this day.

The formal definition of a prime number is such that an integer is prime if it is greater than 1 and has no divisors other than 1 and itself. A composite number is an integer that can be divided evenly by numbers other than 1 and itself (i.e. not prime). The Fundamental Theorem of Arithmetic states that all positive integers greater than 1 can be written as a product of prime numbers in only one distinct way.

Prime numbers are extremely important in modern fields of science such as cryptography, computer science, and security. The relative use of prime numbers demonstrates the fact that they are not only theoretically interesting but practically very useful and necessary. Fully exploring the qualities and attributes of prime numbers can lead to further insights and problem-solving.

The structure of this paper will introduce prime numbers, provide clear definitions, and reveal critical proofs. Later sections will provide deeper analyzation of definitions and proofs related. The overall objective is to make the topic of prime numbers as understandable as possible yet highlighting the fundamental significance.

Consequently, prime numbers and a key element in many studies of modern and historical science and have helped shape our world today. Throughout the following sections, we will explore and prove various essential properties of prime numbers and build upon these ideas.

1 Basic Concepts and Definitions

It is important to understand some fundamental definitions in order to fully explore prime numbers.

Definition 1 (Prime Number)**.** A prime number is defined as an integer that is greater than 1 and has no positive divisors other than 1 and itself. For instance,

$$2, \quad 3, \quad 5, \quad 7$$

are examples of prime numbers.

Definition 2 (Composite Number)**.** A composite number is defined as an integer that is greater than 1 and not prime; that is, it can be divided evenly by numbers other than 1 and itself. For instance,

$$4, \quad 6, \quad 8$$

are all examples of composite numbers because they have factors that are different from either 1 or itself.

Definition 3 (The Fundamental Theorem of Arithmetic)**.** The Fundamental Theorem of Arithmetic states that any positive integer greater than 1 can be further expressed as a product of prime numbers in a distinct way, up to the order of the factors.

> **Margin note:** A paragraph is not one line.

> **Margin note:** was discovered and proves have a small tense agreement issue, although Eudlid's Theorem does continue to prove there are an infinite number of primes.

> **Margin note:** Maybe this should be an example and not in the defintion?

2 Key Proofs in Prime Number Theory

Several proofs in number theory truly highlight the intriguing characteristics of prime numbers. Here are three classic proofs:

Lemma 1 (Euclid's Theorem: Infinitude of Primes)**.** *There are infinitely many prime numbers.*

Proof. Assume there exists a finite list of all prime numbers

$$p_1, p_2, p_3, ..., p_n$$

Observe the number

$$N = p_1 \times p_2 \times p_3 \times ... \times p_n + 1$$

We observe that, N is not divisible by any p_i because such division of any p_i leaves a remainder of 1, due to the basic construction of N. Thus, N must either be a prime number or divisible by some prime outside of the initial finite list of all prime numbers. We observe this contradiction of the initial premise and conclude that there must exist infinitely many prime numbers. □

Remark 1. This classical proofs demonstrates that no finite list exits that can hold all the prime numbers.

Lemma 2 (Uniqueness of 2 as an Even Prime)**.** *The number 2 is the only even prime number.*

Proof. By definition, a prime number, P, generally has exactly two distinct positive divisors:

$$1 \text{ and } P$$

If there exists an even number x that is greater than 2, we see that this x will divisible by 2. Observe that this now introduces at least one additional divisor besides the initial 1 and the number itself (namely, 2).

Consequently, this contradicts the definition of a prime number and therefore 2 is the only even prime number. □

Remark 2. This proof highlights a certain property of 2 and shows the uniqueness of 2 among all the other prime numbers.

Lemma 3 (Prime Factor of a Composite Number)**.** *Every composite number greater than 1 has at least one prime factor.*

Proof. Let $n > 1$ and let it be a composite number. By definition, n has a divisor d such that

$$1 < d < n$$

If d is prime, then the proof is complete.
If d is composite, then d itself has a divisor d_1 with

$$1 < d_1 < d$$

If this process is continued, it will yield a strictly decreasing sequence of positive integers. This sequence must eventually terminate in a prime number. We now observe that every composite number has a prime factor. □

Remark 3. This lemma proves that every integer greater than 1 can be uniquely factored into primes. We can see that this proof serves as an introduction and building step toward the Fundamental Theorem of Arithmetic.