

An Introduction to Number Theory

Abstract

Number theory is a fascinating branch of mathematics that deals with the properties and relationships of numbers, especially integers. This article introduces foundational concepts in number theory, explores examples, and provides detailed explanations to help readers develop a deep understanding of this field.

Contents

1	Introduction	1
2	Divisibility and the Euclidean Algorithm	2
2.1	Divisibility	2
2.2	Greatest Common Divisor (GCD)	2
2.3	The Euclidean Algorithm	2
3	Prime Numbers and Factorization	2
3.1	Prime Numbers	2
3.2	Fundamental Theorem of Arithmetic	2
3.3	Applications in Cryptography	3
4	Modular Arithmetic	3
4.1	Definition	3
4.2	Congruences	3
4.3	Applications	3
5	Fermat's Little Theorem and Euler's Totient Function	3
5.1	Fermat's Little Theorem	3
5.2	Euler's Totient Function	3
6	Conclusion	4

1 Introduction

Number theory is one of the oldest and most beautiful areas of mathematics. It focuses on understanding the properties of integers, prime numbers, divisibility, and related concepts. Applications of number theory range from cryptography to computer science and pure mathematical research.

2 Divisibility and the Euclidean Algorithm

2.1 Divisibility

An integer a is said to divide another integer b if there exists an integer k such that $b = ak$. This is denoted by $a \mid b$. For example, $3 \mid 12$ because $12 = 3 \times 4$, but $5 \nmid 12$.

2.2 Greatest Common Divisor (GCD)

The greatest common divisor of two integers a and b , denoted $\gcd(a, b)$, is the largest integer that divides both a and b . For example:

- $\gcd(18, 24) = 6$.
- $\gcd(7, 13) = 1$ (these numbers are coprime).

2.3 The Euclidean Algorithm

The Euclidean Algorithm is an efficient method for computing the GCD of two integers. It is based on the principle that $\gcd(a, b) = \gcd(b, a \bmod b)$. Here is an example:

Example: Find $\gcd(252, 105)$.

$$252 = 105 \times 2 + 42,$$

$$105 = 42 \times 2 + 21,$$

$$42 = 21 \times 2 + 0.$$

Thus, $\gcd(252, 105) = 21$.

3 Prime Numbers and Factorization

3.1 Prime Numbers

A prime number is an integer greater than 1 that has no positive divisors other than 1 and itself. Examples include 2, 3, 5, 7, 11, and 13. Prime numbers play a central role in number theory.

3.2 Fundamental Theorem of Arithmetic

The Fundamental Theorem of Arithmetic states that every integer greater than 1 can be expressed uniquely as a product of prime numbers, up to the order of the factors. For example:

- $84 = 2^2 \cdot 3 \cdot 7$.
- $360 = 2^3 \cdot 3^2 \cdot 5$.

3.3 Applications in Cryptography

Prime numbers are the foundation of many cryptographic algorithms, such as RSA encryption. The difficulty of factoring large numbers into their prime components ensures the security of these systems.

4 Modular Arithmetic

4.1 Definition

Modular arithmetic involves integers under a "clock-like" system. For an integer a and a positive integer n , $a \bmod n$ is the remainder when a is divided by n . For example:

- $17 \bmod 5 = 2$.
- $20 \bmod 6 = 2$.

4.2 Congruences

We write $a \equiv b \pmod{n}$ if $a \bmod n = b \bmod n$. For example:

- $17 \equiv 2 \pmod{5}$.
- $20 \equiv 2 \pmod{6}$.

4.3 Applications

Modular arithmetic is crucial in areas such as cryptography, computer science, and solving Diophantine equations. For example, it is used in hashing functions and cyclic redundancy checks (CRC).

5 Fermat's Little Theorem and Euler's Totient Function

5.1 Fermat's Little Theorem

If p is a prime number and a is an integer not divisible by p , then:

$$a^{p-1} \equiv 1 \pmod{p}.$$

For example, if $p = 7$ and $a = 3$:

$$3^6 \equiv 1 \pmod{7}.$$

5.2 Euler's Totient Function

Euler's Totient Function $\phi(n)$ counts the number of integers between 1 and n that are coprime with n . For example:

- $\phi(9) = 6$ (the numbers 1, 2, 4, 5, 7, 8 are coprime with 9).
- $\phi(10) = 4$ (the numbers 1, 3, 7, 9 are coprime with 10).

6 Conclusion

Number theory is a rich and diverse field with profound theoretical and practical implications. From understanding the nature of integers to applications in modern cryptography, the study of number theory continues to inspire mathematicians and scientists worldwide.

Acknowledgements

Special thanks to the mathematical community for developing the beautiful theories and applications discussed in this article.