Republic of Iraq
Ministry of Higher Education and Scientific Research
Al- Mustaqbal University
Collage of science - Department of Medical Physics

1^{st} class

2025- 2026

Number Theory

Asst. Lect. Huda Faris Albazy
huda.faris.abdulameer@uomus.edu.iq

الرياضيات :المرحلة الاولى

نظرية الاعداد

استاذ المادة: م.م هدى فارس

Cybersecurity Department
قسم الأمن السيبراني

اهداف المادة الدراسية

1. تنمية مهارات حل المشكلات وفهم نظرية الأعداد، وأهميتها في مجال أمن المعلومات.
2. إدراك دور نظرية الأعداد في علم التشفير وعلاقتها بأمن الحواسيب والأمن السيبراني.
3. يركز هذا المقرر على المفاهيم الأساسية للرياضيات في علم التشفير.
4. يُعد هذا المقرر أساسًا لفهم تقنيات التشفير وأساليب الأمن السيبراني.

المعرفة والفهم

1. تأهيل الطلاب لاستكشاف أهمية نظرية الأعداد وتطبيقاتها.
2. تمكين الطلاب من التعامل مع الأسس الرياضية لعلم التشفير.
3. تزويد الطلاب بالقدرة على حل مشكلات الأمان في بعض طرق التشفير باستخدام نماذج رياضية متخصصة في نظرية الأعداد.

المهارات المتخصصة بالمادة

1. تمكين الطلاب من تحديد النظريات الرياضية المستخدمة في أساليب التشفير.
2. تزويد الطلاب بالقدرة على ربط خوارزميات التشفير بنظرية الأعداد.
3. مساعدة الطلاب على فهم النظريات الرياضية لأساليب التشفير المتقدمة.

Contents

1 General Introduction

Number Theory is a branch of mathematics that deals with the properties and relationships of integers. It is one of the oldest and most fundamental areas of mathematics, often referred to as the Queen of Mathematics. The study of numbers has been central to mathematics since ancient times, with applications in cryptography, coding theory, and computer science.

1.1 Historical Background

The study of numbers dates back to ancient civilizations, with contributions from:

- **The Babylonians and Egyptians**, who used number systems for practical calculations.
- **The Greeks**, especially **Euclid**, who developed fundamental theorems on divisibility and prime numbers.
- **Pierre de Fermat**, known for Fermat's Little Theorem and his famous Last Theorem.
- **Leonhard Euler**, who expanded number theory through Euler's totient function.
- **Carl Friedrich Gauss**, who introduced modular arithmetic and developed the theory of congruences.

1.2 Applications of Number Theory

Although Number Theory was historically considered pure mathematics, it has found significant applications in modern areas, including:

- **Cryptography**: RSA encryption and elliptic curve cryptography rely on properties of prime numbers and modular arithmetic.
- **Computer Science**: Hash functions, random number generation, and error detection codes.
- **Coding Theory**: Applications in data transmission and error correction.

Number Theory is a rich and fascinating field that explores the properties of integers and their relationships. With deep theoretical foundations and modern applications, it continues to be an essential part of mathematical research and technological advancements.

1.3 The Beauty of Numbers

Sum of Odd Numbers Forms Perfect Squares

$$\begin{aligned}1&=1\\1+3&=4\\1+3+5&=9\\1+3+5+7&=16\\1+3+5+7+9&=25\\1+3+5+7+9+11&=36\\1+3+5+7+9+11+13&=49\end{aligned}$$

Palindromic Multiplication

$$\begin{aligned}1\cdot 1&=1\\11\cdot 11&=121\\111\cdot 111&=12321\\1111\cdot 1111&=1234321\\11111\cdot 11111&=123454321\\111111\cdot 111111&=12345654321\\1111111\cdot 1111111&=1234567654321\\11111111\cdot 11111111&=123456787654321\\111111111\cdot 111111111&=12345678987654321\end{aligned}$$

Factorial values

$$\begin{aligned}
1! &= 1\\
2! &= 1\times 2 = 2\\
3! &= 1\times 2\times 3 = 6\\
4! &= 1\times 2\times 3\times 4 = 24\\
5! &= 1\times 2\times 3\times 4\times 5 = 120\\
6! &= 1\times 2\times 3\times 4\times 5\times 6 = 720\\
7! &= 1\times 2\times 3\times 4\times 5\times 6\times 7 = 5,040\\
8! &= 1\times 2\times 3\times 4\times 5\times 6\times 7\times 8 = 40,320\\
9! &= 1\times 2\times 3\times 4\times 5\times 6\times 7\times 8\times 9 = 362,880\\
10! &= 1\times 2\times 3\times 4\times 5\times 6\times 7\times 8\times 9\times 10 = 3,628,800
\end{aligned}$$

$$\begin{aligned}
1 &= 1 && (1 = 1)\\
1+2+1 &= 2+2 && (121 \sim 22)\\
1+2+3+2+1 &= 3+3+3 && (12321 \sim 333)\\
1+2+3+4+3+2+1 &= 4+4+4+4 && (1234321 \sim 4444)
\end{aligned}$$

Pascal's Triangle

$$\begin{array}{c}
1\\
1 \quad 1\\
1 \quad 2 \quad 1\\
1 \quad 3 \quad 3 \quad 1\\
1 \quad 4 \quad 6 \quad 4 \quad 1\\
1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1\\
1 \quad 6 \quad 15 \quad 20 \quad 15 \quad 6 \quad 1\\
1 \quad 7 \quad 21 \quad 35 \quad 35 \quad 21 \quad 7 \quad 1\\
1 \quad 8 \quad 28 \quad 56 \quad 70 \quad 56 \quad 28 \quad 8 \quad 1
\end{array}$$