



REPUBLIC OF IRAQ
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH
AL- MUSTAQBAL UNIVERSITY
COLLAGE OF SCIENCE - DEPARTMENT OF MEDICAL PHYSICS

1st 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	1
1.1	Historical Background	1
1.2	Applications of Number Theory	1
1.3	The Beauty of Numbers	2
2	Algebra Preliminaries	4
2.1	Sets	4
2.2	Integer and Natural Numbers	4
2.2.1	Basic Properties of Natural Numbers	5
2.2.2	Basic Properties of Integer Numbers	6
2.2.3	Laws of Exponents	7
2.2.4	Properties of Inequalities	8
2.3	Even and Odd Numbers	8
3	Divisibility and Prime Numbers	9
3.1	Divisibility	9
3.2	Prime Numbers	12
3.3	Exercises of Divisibility and Prime Numbers	14
4	Great Common Divisor and Euclidean Algorithm	15
4.1	Great Common Divisor	15
4.2	Euclidean Algorithm	16
4.3	Exercises of Great Common Divisor and Euclidean Algorithm	19
5	Prime Numbers	20

5.1	Lists of primes by type	22
5.2	Exercises of Prime Numbers	24
6	Mersenne Primes	25
7	The Group, Ring, and Field	27
7.1	Groups	27
7.2	Rings	31
7.3	Field	32
7.4	Exercises of The Group, Ring, and Field	33
8	Theory of Congruence's	34
8.1	Exercises of Theory of Congruence's	38
9	Congruent Modulo	39
9.1	Exercises of Congruent modulo	43
10	Divisibility Tests	44
10.1	Exercises of Divisibility Tests	47
11	More Properties of Congruences	48
11.1	Finding Modular Inverses Using the Extended Euclidean Algorithm	49
11.2	Exercises of More Properties of Congruences	51
12	Residue Classes	52
12.1	\mathbb{Z}_m and Complete Residue Systems	54
12.2	Addition and Multiplication in \mathbb{Z}_m	55
13	Theorems of Euler, Fermat and Carmichael	59

14 The Chinese Remainder Theorem	65
15 Finite Galois Field	70
16 Discrete Logarithm Problem	72
16.1 Definition of the Discrete Logarithm Problem	72
16.2 Applications in Cryptography	72
17 Public-key cryptography	73
17.1 Introduction	73
17.2 Basic Concept	73
17.3 Mathematical Foundation	74
17.4 Diffie-Hellman Key Exchange (DHKE)	74
17.4.1 Example of Diffie-Hellman Key Exchange	75
17.4.2 Diffie-Hellman Key Exchange Analysis	75
17.5 ElGamal Cryptosystem	76
17.5.1 Example of ElGamal Cryptosystem	76
17.5.2 ElGamal Analysis	78
17.6 RSA Cryptosystem	78
17.6.1 Example of RSA Public Key Cryptosystem	80
17.6.2 RSA Analysis	81



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

$$1 = 1$$

$$1 + 3 = 4$$

$$1 + 3 + 5 = 9$$

$$1 + 3 + 5 + 7 = 16$$

$$1 + 3 + 5 + 7 + 9 = 25$$

$$1 + 3 + 5 + 7 + 9 + 11 = 36$$

$$1 + 3 + 5 + 7 + 9 + 11 + 13 = 49$$

Palindromic Multiplication

$$1 \cdot 1 = 1$$

$$11 \cdot 11 = 121$$

$$111 \cdot 111 = 12321$$

$$1111 \cdot 1111 = 1234321$$

$$11111 \cdot 11111 = 123454321$$

$$111111 \cdot 111111 = 12345654321$$

$$1111111 \cdot 1111111 = 1234567654321$$

$$11111111 \cdot 11111111 = 123456787654321$$

$$111111111 \cdot 111111111 = 12345678987654321$$

