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

1st class

2024- 2025

Number Theory

Asst. Lect. Mohammed Jabbar
mohammed.jabbar.obaid@uomus.edu.iq

الرياضيات :المرحلة الاولى

نظرية الاعداد

استاذ المادة: م.م محمد جبار

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

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

2 Algebra Preliminaries

2.1 Sets

Definition 2.1. A **set** is a well-defined collection of distinct objects, called **elements**, enclosed in curly brackets $\{\}$.

Formal Definition: A set S is defined as $S = \{a, b, c, \dots\}$, where each element is unique and well-defined.

Examples of Sets

- **Finite Set:** $A = \{1, 2, 3, 4, 5\}$
- **Infinite Set:** $B = \{1, 2, 3, \dots\}$
- **Empty Set (Null Set):** $\emptyset = \{\}$ (A set with no elements)

Common Sets:

$\mathbb{N}$ - Natural numbers, $\mathbb{Z}$ - Integers, $\mathbb{Q}$ - Rational numbers, $\mathbb{R}$ - Real numbers, $\mathbb{C}$ - Complex numbers.

Relations and Membership:

- $x \in A$ (Element of A), $y \notin B$ (Not an element of B)
- $A \subseteq B$ (A is a Subset of B), $A \subset B$ (A is a Proper Subset of B), $A = B$ (Equality)

2.2 Integer and Natural Numbers

The set $\mathbb{Z}$ of all integers, consists of all positive and negative integers as well as 0. Thus $\mathbb{Z}$ is the set given by

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

While the set of all positive integers (Natural Numbers), denoted by $\mathbb{N}$, is defined by

$$\mathbb{N} = \{1, 2, 3, \dots\}.$$

2.2.1 Basic Properties of Natural Numbers

Addition in $\mathbb{N}$

- **Closure:** For any $a, b \in \mathbb{N}$, the sum $a + b$ is also in $\mathbb{N}$.
- **Associativity:** $(a + b) + c = a + (b + c)$ for all $a, b, c \in \mathbb{N}$.
- **Commutativity:** $a + b = b + a$ for all $a, b \in \mathbb{N}$.
- **Cancellation Law:** For any $a, b, c \in \mathbb{N}$, if $a + c = b + c$, then $a = b$.

Multiplication in $\mathbb{N}$

- **Closure:** For any $a, b \in \mathbb{N}$, the product $a \cdot b$ is also in $\mathbb{N}$.
- **Associativity:** $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in \mathbb{N}$.
- **Commutativity:** $a \cdot b = b \cdot a$ for all $a, b \in \mathbb{N}$.
- **Identity Element:** 1 serves as the multiplicative identity since $a \cdot 1 = a$ for every $a \in \mathbb{N}$.
- **Cancellation Law:** For any $a, b, c \in \mathbb{N}$, if $a \cdot c = b \cdot c$, then $a = b$.
- **Distributivity:** Multiplication is distributive over addition: For any $a, b, c \in \mathbb{N}$,

$$a(b + c) = ab + ac.$$

Subtraction and Division in $\mathbb{N}$

- **Subtraction:** The operation of subtraction is *not* always closed in $\mathbb{N}$. For example, $2 - 5$ is not a natural number.
- **Division:** Similarly, division is not generally closed in $\mathbb{N}$; for instance, $3 \div 2$ does not yield a natural number.

2.2.2 Basic Properties of Integer Numbers

Addition in $\mathbb{Z}$

- **Closure:** For any $a, b \in \mathbb{Z}$, the sum $a + b$ is also in $\mathbb{Z}$.
- **Associativity:** $(a + b) + c = a + (b + c)$ for all $a, b, c \in \mathbb{Z}$.
- **Commutativity:** $a + b = b + a$ for all $a, b \in \mathbb{Z}$.
- **Identity Element:** 0 is the additive identity since $a + 0 = a$ for every $a \in \mathbb{Z}$.
- **Inverses:** Every integer a has an inverse $-a$ such that $a + (-a) = 0$.

Subtraction in $\mathbb{Z}$

Subtraction is always defined in $\mathbb{Z}$ because for any $a, b \in \mathbb{Z}$, the difference $a - b = a + (-b)$ is also an integer.

Multiplication in $\mathbb{Z}$

- **Closure:** For any $a, b \in \mathbb{Z}$, the product $a \cdot b$ is in $\mathbb{Z}$.
- **Associativity:** $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in \mathbb{Z}$.
- **Commutativity:** $a \cdot b = b \cdot a$ for all $a, b \in \mathbb{Z}$.
- **Identity Element:** 1 is the multiplicative identity since $a \cdot 1 = a$ for every $a \in \mathbb{Z}$.
- **Cancellation Law:** For any $a, b, c \in \mathbb{Z}$, if $a \cdot c = b \cdot c$, then $a = b$.
- **Distributivity:** Multiplication is distributive over addition: For any $a, b, c \in \mathbb{Z}$,

$$a(b + c) = ab + ac.$$

Division in $\mathbb{Z}$

Division is not a closed operation in $\mathbb{Z}$. For example, $3 \div 2$ is not an integer.

Important Theorem

Theorem 2.1. *Let $a, b \in Z$, Then:*

1. $a \cdot 0 = 0 \cdot a = 0$
2. $(-a)b = a(-b) = -ab$
3. $(-a)(-b) = ab$

Proof. 1. $0 + 0 = 0$ (Identity element in $\mathbb{Z}$)

$\Rightarrow (0 + 0)a = 0a \Rightarrow 0a + 0a = 0a$

$\Rightarrow 0a + 0a + (-0a) = 0a + (-0a)$ (inverse in $\mathbb{Z}$)

$\Rightarrow 0a = 0$

Similarly $a0 = 0$

---

2. $b + (-b) = 0$ (inverse in $\mathbb{Z}$)

$\Rightarrow a(b + (-b)) = a0 = 0$ (From (1))

$\Rightarrow ab + a(-b) = ab + (-ab) \Rightarrow a(-b) = -ab$

---

3. $(-a)(-b) = ab$

In (2), replace a by $(-a) \Rightarrow (-a)(-b) = -((-a)b) = -(-ab) = ab$

□

2.2.3 Laws of Exponents

For $n, m \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, we have the following exponentiation rules:

1. **Product Rule:** $a^m \cdot a^n = a^{m+n}$
2. **Quotient Rule:** $\frac{a^m}{a^n} = a^{m-n}, \quad$ for $m \geq n,\ a \neq 0$
3. **Power of a Power:** $(a^m)^n = a^{m \cdot n}$
4. **Power of a Product:** $(ab)^n = a^n \cdot b^n$

2.2.4 Properties of Inequalities

For $a, b, c \in \mathbb{Z}$, the following properties hold:

1. **Transitivity:** If $a < b$ and $b < c$, then $a < c$.
2. **Addition Property:** If $a < b$, then $a + c < b + c$ for any $c \in \mathbb{Z}$.
3. **Multiplication by a Positive Number:** If $a < b$ and $c > 0$, then $ac < bc$.
4. **Multiplication by a Negative Number:** If $a < b$ and $c < 0$, then $ac > bc$ (the inequality sign reverses).

2.3 Even and Odd Numbers

Even Numbers

An integer n is called *even* if it is divisible by 2. That is, n is even if there exists an integer k such that:

$$n = 2k.$$

Examples: $2 = 2(1)$, $4 = 2(2)$, $10 = 2(5)$.

Odd Numbers

An integer n is called *odd* if it is not divisible by 2. Formally, n is odd if it can be expressed as:

$$n = 2k + 1,$$

where k is an integer.

Examples:

- $1 = 2(0) + 1$
- $3 = 2(1) + 1$
- $7 = 2(3) + 1$

3 Divisibility and Prime Numbers

3.1 Divisibility

Important Definition

Definition 3.1 (Divides)**.** For integers a and b, we say that a **divides** b (denoted $a \mid b$) if there exists an integer k such that:

$$b = a \cdot k.$$

For example:

$$3 \mid 15 \quad \text{since } 15 = 3 \times 5.$$

Remark 3.1. If a does not divide a, we write $a \nmid b$.

Properties of Divisibility

For integers a, b, c:

- If $a \mid b$ and $b \mid c$, then $a \mid c$ (Transitivity).
- If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$ and $a \mid (b - c)$.
- If $a \mid b$, then $a \mid kb$ for any integer k.

Theorem 3.1. *For integers a, b, c, the following hold:*

1. $a \mid 0,\ 1 \mid a,\ a \mid a$.
2. $a \mid 1$ *if and only if* $a = \pm 1$.
3. *If* $a \mid b$ *and* $c \mid d$, *then* $ac \mid bd$.
4. $a \mid b$ *and* $b \mid a$ *if and only if* $a = \pm b$.
5. *If* $a \mid b$ *and* $b \neq 0$, *then* $|a| \leq |b|$.
6. *If* $a \mid b$ *and* $a \mid c$, *then* $a \mid (bx + cy)$ *for arbitrary integers* x *and* y.

Division Algorithm

Theorem 3.2. *Let a, b be integers with $a \neq 0$. Then there exist unique integers q and r such that:*

$$b = aq + r, \quad 0 \leq r < |a|.$$

*where q is called the **quotient**, and r is called the **remainder**.*

Remark 3.2. Divisibility Condition: $a \mid b \iff r = 0$

Theorem 3.3. *For any integer $a \neq 0$ and any integer b, there exist unique integers q (quotient) and r (remainder) such that:*

$$b = aq + r, \quad \textit{where } 0 \leq r < |a|. \tag{1}$$

Proof. Let $(q_1, r_1), (q_2, r_2) \in \mathbb{Z}$, such that

$$b = aq_1 + r_1, \quad \text{where } 0 \leq r_1 < |a|, \tag{2}$$

$$b = aq_2 + r_2, \quad \text{where } 0 \leq r_2 < |a|, \tag{3}$$

From (2) and (3) $b = aq_1 + r_1 = aq_2 + r_2 \Rightarrow aq_1 - aq_2 = r_2 - r_1$.

$$a(q_1 - q_2) = r_2 - r_1. \tag{4}$$

Since $-|a| < -r_1 \leq 0, 0 \leq r_2 < |a|$, then

$$-|a| < r_2 - r_1 < |a|. \tag{5}$$

But from (4) $r_2 - r_1 = a(q_1 - q_2) \Rightarrow r_2 - r_1 = 0 \Rightarrow r_2 = r_1$

Since $a \neq 0$, we must have $q_1 - q_2 = 0 \Rightarrow q_1 = q_2$. □

Example 3.1. Prove that

1. $4 \mid 20$
2. $5 \nmid 23$
3. Every even integer n is divisible by 2
4. Every odd integer n is not divisible by 2 **H.W**

Sol. 1. By Division Algorithm, there exists integers q, r such that:

$$20 = 4q + r.$$

We check:

$$20 = 4 \times 5.$$

Since $q = 5$, and $r = 0$, then

$$4 \mid 20.$$

2. By Division Algorithm, there exists integers q, r such that:

$$23 = 5q + r.$$

We check:

$$23 = 5 \times 4 + 3.$$

Since $q = 5$, and $r = 3$, then

$$5 \nmid 23.$$

3. By Division Algorithm, there exists integers q, r such that:

$$n = 2q + r.$$

The only possible values for r are:

$$r = 0 \quad \text{or} \quad r = 1.$$

Case 1: If $r = 0$

Then

$$n = 2q \Rightarrow 2 \mid n.$$

Case 1: If $r = 1$

Then

$$n = 2q + 1 \Rightarrow n \text{ is odd integer } \textbf{C!}$$

$$\therefore 2 \mid n$$

□

3.2 Prime Numbers

Prime Number

Definition 3.2. A prime number is an integer $p > 1$ that has exactly two distinct positive divisors: 1 and itself.

Formally, p is prime if:

$$p > 1 \quad \text{and} \quad \forall d \mid p, \quad d = 1, \ or \ d = p.$$

Examples: $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$

Definition 3.3. A **composite number** is an integer greater than 1 that is **not prime**, meaning **it has at least one divisor** other than 1 and itself.

Examples: $4, 6, 8, 9, 10, 12, 14, 15, \ldots$

Lemma 3.1. If n is composite, then there exist integers a and b, such that:

$$n = ab, \quad 1 < a < n, \quad 1 < b < n.$$

Prime Numbers									
2, 3, 5,	151,	271,	409,	557,	683,	839,	997,	1151,	1301,
7, 11,	157,	277,	419,	563,	691,	853,	1009,	1153,	1303,
13, 17,	163,	281,	421,	569,	701,	857,	1013,	1163,	1307,
19, 23,	167,	283,	431,	571,	709,	859,	1019,	1171,	1319,
29, 31,	173,	293,	433,	577,	719,	863,	1021,	1181,	1321,
37, 41,	179,	307,	439,	587,	727,	877,	1031,	1187,	1327,
43, 47,	181,	311,	443,	593,	733,	881,	1033,	1193,	1361,
53, 59,	191,	313,	449,	599,	739,	883,	1039,	1201,	1367,
61, 67,	193,	317,	457,	601,	743,	887,	1049,	1213,	1373,
71, 73,	197,	331,	461,	607,	751,	907,	1051,	1217,	1381,
79, 83,	199,	337,	463,	613,	757,	911,	1061,	1223,	1399,
89, 97,	211,	347,	467,	617,	761,	919,	1063,	1229,	1409,
101,	223,	349,	479,	619,	769,	929,	1069,	1231,	1423,
103,	227,	353,	487,	631,	773,	937,	1087,	1237,	1427,
107,	229,	359,	491,	641,	787,	941,	1091,	1249,	1429,
109,	233,	367,	499,	643,	797,	947,	1093,	1259,	1433,
113,	239,	373,	503,	647,	809,	953,	1097,	1277,	1439,
127,	241,	379,	509,	653,	811,	967,	1103,	1279,	1447,
131,	251,	383,	521,	659,	821,	971,	1109,	1283,	1451,
137,	257,	389,	523,	661,	823,	977,	1117,	1289,	1453,
139,	263,	397,	541,	673,	827,	983,	1123,	1291,	1459,
149,	269,	401,	547,	677,	829,	991,	1129,	1297,	1471

3.3 Exercises of Divisibility and Prime Numbers

Exercises

1. Prove that if x is even, then $x^2 + 2x + 4$ is divisible by 4.

2. Suppose $a \mid b$ and $a \mid c$. Prove the following:

   (a) $a \mid b + c$.

   (b) $a \mid b - c$.

   (c) $a \mid mb$ for all $m \in \mathbb{Z}$.

3. Prove that if $a \mid b$ and $b \mid a$, then $a = b$ or $a = -b$.

4. Show that $5 \mid 25$, $-19 \mid 38$, $-5 \nmid 27$ and $2 \mid 98$.

5. List all prime numbers less than 30 and briefly justify why each is prime.

6. Find the prime factorization of 84.

4 Great Common Divisor and Euclidean Algorithm

4.1 Great Common Divisor

Greatest Common Divisor (GCD)

Definition 4.1. The **GCD** of two integers a and b, denoted as $\gcd(a, b)$, is the largest positive integer that divides both a and b without leaving a remainder.

$$\gcd(a, b) = \max\{d \in \mathbb{Z} : d \mid a \text{ and } d \mid b\}.$$

For example, $\gcd(1, 2) = 1$, $\gcd(6, 27) = 3$, and for any a, $\gcd(0, a) = \gcd(a, 0) = a$.

Remark 4.1. unless both a and b are 0 in which case $\gcd(0, 0) = 0$.

Definition 4.2 (Co-Prime Numbers)**.** Two integers a and b are **co-prime** (or relatively prime) if the only positive integer that divides both of them is 1; equivalently, their greatest common divisor is 1:

$$\gcd(a, b) = 1.$$

For examples: $(8, 15), (7, 9), (13, 27)$ are co-prime pairs.

Lemma 4.1. For any integers a,b and n, we have

$$\gcd(a, b) = \gcd(b, a) = \gcd(\pm a, \pm b) = \gcd(a, b - a) = \gcd(a, b + a) = \gcd(a, b - na).$$

Lemma 4.2. For any integers a, b, and n, we have

$$\gcd(an, bn) = |n| \cdot \gcd(a, b).$$

Lemma 4.3. Suppose a, b, and n are integers such that $n \mid a$ and $n \mid b$. Then

$$n \mid \gcd(a, b).$$

Theorem 4.1. *For any integers a and b, there exist integers x and y such that*

$$d = \gcd(a, b) = ax + by.$$

Theorem 4.2. *If* $\gcd(a, b) = d$, *then* $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Proof. (1). Assume that k is a positive common divisor such that $k \mid a/d$ and $k \mid b/d$.

$$\Rightarrow ad = km \quad \text{and} \quad bd = kn, \quad n, m \in \mathbb{Z}$$

$$\Rightarrow a = kmd \quad \text{and} \quad b = knd.$$

Hence, $kd \mid a$ and $kd \mid b$. Also, $kd \mid d$. However, d is the GCD of a and b, so $kd \leq d$.

Since $kd \mid d \Rightarrow kd = d \Rightarrow k = 1$.

Thus, the only common divisor of a/d and b/d is 1.

$$\therefore \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

□

Proof. (2). $d = ax + by \Rightarrow 1 = \frac{a}{d}x + \frac{b}{d}y \Rightarrow \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. □

4.2 Euclidean Algorithm

Lemma 4.4. Let $a, b \in \mathbb{Z}$, such that $a = bq + r$ for some integers q, r. Then

$$\gcd(a, b) = \gcd(b, r).$$

Proof. Let $d = \gcd(a, b) \Rightarrow d \mid a, d \mid b$. Since $a = bq + r$, we have $r = a - bq$.

$\Rightarrow d \mid a - bq$, which means $d \mid r$. Thus, d is a common divisor of b and r, so $d \leq \gcd(b, r)$.

Conversely, let $d' = \gcd(b, r)$. Since $d' \mid b, d' \mid r \Rightarrow d' \mid a = bq + r$

Thus, d' is a common divisor of a and b, so $d' \leq \gcd(a, b)$. We have $d' = d$ □

Euclidean algorithm

Theorem 4.3. *Let a, b be nonzero integers. Repeatedly apply the division algorithm as follows:*

$$a = bq_1 + r_1, \quad 0 \leq r_1 < |b|$$

$$b = r_1q_2 + r_2, \quad 0 \leq r_2 < r_1$$

$$r_1 = r_2q_3 + r_3, \quad 0 \leq r_3 < r_2$$

$$\vdots$$

Continue this process until some remainder $r_n = 0$, at which point the greatest common divisor is given by:

$$\gcd(a, b) = r_{n-1}.$$

Example 4.1. Let $a = 75$ and $b = 45$. We apply the Euclidean algorithm:

$$75 = 45 \times 1 + 30$$

$$45 = 30 \times 1 + 15$$

$$30 = 15 \times 2 + 0$$

Since the remainder is now 0, we conclude that:

$$\gcd(75, 45) = 15.$$

Example 4.2. Let $a = 517$ and $b = 89$. We apply the Euclidean algorithm:

$$517 = 89 \times 5 + 72$$

$$89 = 72 \times 1 + 17$$

$$72 = 17 \times 4 + 4$$

$$17 = 4 \times 4 + 1$$

$$4 = 1 \times 4 + 0$$

Since the remainder is now 0, we conclude that:

$$\gcd(517, 89) = 1.$$

Least Common Multiple (LCM)

Definition 4.3. The **Least Common Multiple (LCM)** of two integers a and b is the smallest positive integer that is divisible by both a and b.

$$\text{LCM}(a, b) = \frac{|a \times b|}{\gcd(a, b)}$$

Properties of LCM

- $\text{LCM}(a, b) \times \gcd(a, b) = |a \times b|$
- $\text{LCM}(a, b) \geq \max(a, b)$
- If a divides b, then $\text{LCM}(a, b) = b$.

Example

For $a = 12$ and $b = 18$:

$$\gcd(12, 18) = 6$$
$$\text{LCM}(12, 18) = \frac{12 \times 18}{6} = 36$$

Thus, $\text{LCM}(12, 18) = 36$.

4.3 Exercises of Great Common Divisor and Euclidean Algorithm

Exercises

1. Let a and b be two positive even integers. Prove that $\gcd(a, b) = 2\gcd(a/2, b/2)$.
2. By Euclidean Algorithm to find
   (a) $\gcd(12378, 3054)$.
   (b) $\gcd(51, 288)$.
   (c) $\gcd(7544, 115)$.
3. Show that if a and b are positive integers where a is even and b is odd, then $\gcd(a, b) = \gcd(a/2, b)$
4. Let $a, b, c \in \mathbb{Z}$ such that $a \mid bc$ and $\gcd(a, c) = 1$. Prove that $a \mid b$.
5. If $a \mid b$ and $a > 0$, prove that $\gcd(a, b) = a$.
6. If $n \in \mathbb{Z}$ prove that n and $n + 1$ co-prime i.e $\gcd(n, n + 1) = 1$.
7. Find $lcm(15, 20)$ and $lcm(51, 288)$
8. Let $a, b \in \mathbb{Z}$, if $lcm(a, b) = ab$, prove that $\gcd(a, b) = 1$.

5 Prime Numbers

We have previously been introduced to prime numbers. In this section, we will explore these numbers in greater depth and study their special Sequences.

Number of primes infinite

Theorem 5.1. *There are infinitely many prime numbers.*

Proof. Let the number of primes is finite

$$p_1, p_2, p_3, \ldots, p_n.$$

and let

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

There are two cases: either N is a prime number or a composite number.

Case 1: If N prime **C!** with (the number of primes is finite).

Case 2: If N composite, then $p \mid N$.

But $p_1, p_2, \ldots, p_n \nmid N$, because leaves a remainder of 1 **C!** with N composite.

$\Rightarrow N$ is prime **C!** with (the number of primes is finite).

Therefore, there are infinitely many prime numbers. □

Sequence of $N_n = (p_1 p_2 p_3 \ldots p_n) + 1$

$$\begin{aligned} 3 &= 2+1 \\ 7 &= 2 \cdot 3 + 1 \\ 31 &= 2 \cdot 3 \cdot 5 + 1 \\ 211 &= 2 \cdot 3 \cdot 5 \cdot 7 + 1 \\ 2311 &= 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 \end{aligned}$$

where p_i represents the first n prime numbers.

Example 5.1. From $N_n = (p_1p_2p_3 \dots p_n) + 1$, find N_4, N_7 and N_9.

Sol.

$$\begin{aligned} N_4 &= (2 \cdot 3 \cdot 5 \cdot 7) + 1 \\ &= 210 + 1 = 211 \end{aligned} \qquad \begin{aligned} N_7 &= (2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17) + 1 \\ &= 510510 + 1 = 510511 \end{aligned}$$

□

The Fundamental Theorem of Arithmetic

Theorem 5.2. *Every integer $n > 1$ can be written uniquely in the form*

$$n = p_1p_2 \cdots p_s$$

where $p_1, p_2, \dots, p_s$ are primes such that $p_1 \leq p_2 \leq \cdots \leq p_s$.

Remark 5.1. If $n = p_1p_2 \cdots p_s$ where each p_i is prime, we call this the prime **factorization** of n.

The number 1 is neither prime nor composite.

Ans. 1 is not composite because there are no integers $a, b > 1$ such that $1 = ab$.

Now, let 1 is prime number and n composite $\ni n = pq$, p, q primes. Then

$$n = p \times q$$

$$n = 1 \times p \times q$$

$$n = 1 \times 1 \times p \times q$$

$$n = 1 \times 1 \times 1 \times p \times q$$

$$\vdots$$

$$n = 1 \times 1 \times \cdots \times 1 \times p \times q \textbf{ C!} \text{ with unique product of primes}$$

$\therefore$ 1 is not prime number.

Theorem 5.3. *Let p be a prime and $a, b \in \mathbb{N}$. If $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Proof. If $p \mid a$ we are done.

If $p \nmid a \Rightarrow \gcd(p, a) = 1 \Rightarrow \gcd(bp, ab) = b$.

Since $p \mid pb,\ p \mid ab$, then $p \mid \gcd(bp, ab) \Rightarrow p \mid b \gcd(p, a) \Rightarrow p \mid b \cdot 1 \Rightarrow p \mid b$. □

Prime Divisor

Lemma 5.1. If $n > 1$ is composite, then n has a prime divisor $p \leq \sqrt{n}$.

Example 5.2. $n = 97$. Note that $\sqrt{97} < \sqrt{100} = 10$. The primes less than 10 are 2, 3, 5, and 7.

5.1 Lists of primes by type

Cousin Primes

Cousin Primes are pairs of prime numbers that differ by 4. In other words, two primes p and q are cousin primes if:

$$q = p + 4 \quad \text{and both } p \text{ and } q \text{ are primes.}$$

Examples:

1. For $p = 3$:

$$q = 3 + 4 = 7$$

Both 3 and 7 are prime numbers. So, (3, 7) is a pair of **Cousin Primes**.

2. For $p = 7$:

$$q = 7 + 4 = 11$$

Both 7 and 11 are prime numbers. So, (7, 11) is a pair of **Cousin Primes**.

3. For $p = 13$:

$$q = 13 + 4 = 17$$

Both 13 and 17 are prime numbers. So, (13, 17) is a pair of **Cousin Primes**.

Cullen Primes

A **Cullen Prime** is a prime number of the form:

$$C_n = n \cdot 2^n + 1$$

where n is a positive integer and C_n is prime.

Examples:

1. For $n = 1$:

$$C_1 = 1 \cdot 2^1 + 1 = 3$$

Since 3 is prime, $C_1 = 3$ is a **Cullen Prime**.

2. For $n = 2$:

$$C_2 = 2 \cdot 2^2 + 1 = 9$$

Since 9 is not prime, $C_2 = 9$ is not a Cullen prime.

3. For $n = 3$:

$$C_3 = 3 \cdot 2^3 + 1 = 25$$

Since 25 is not prime, $C_3 = 25$ is not a Cullen prime.

4. For $n = 5$:

$$C_5 = 5 \cdot 2^5 + 1 = 161$$

Since 161 is not prime, $C_5 = 161$ is not a Cullen prime.

5. A known large Cullen prime is:

$$C_{141} = 141 \cdot 2^{141} + 1$$

5.2 Exercises of Prime Numbers

Exercises

1. Let p and q be prime numbers. Suppose that the polynomial

$$x^2 - px + q = 0$$

has an integer root. Find all possible values of p and q.

2. From $N_n = (p_1 p_2 p_3 \dots p_n) + 1$, find

   (a) N_1 *to* N_3.

   (b) $N_1 * N_2 + 1$

3. Let p be a prime and a, k be positive integers. If $p \mid a^k$, then $p^k \mid a^k$.

4. Write prime between 72 and 111.

5. Let $q_1, q_2, \dots, q_m$ be prime numbers. If a prime p divides their product,

$$p \mid q_1 q_2 \cdots q_m,$$

Then p must be equal to one of $q_1, q_2, \dots, q_m$, i.e., $p = q_k$ for some k.

6 Mersenne Primes

Mersenne Primes

Definition 6.1. A number $M_p = 2^p - 1$ is called a Mersenne number. If M_p is prime, then it is called a Mersenne prime.

For example:

$M_2 = 2^2 - 1 = 3, \quad M_3 = 2^3 - 1 = 7, \quad M_5 = 2^5 - 1 = 31, \quad M_7 = 2^7 - 1 = 127$

Remark 6.1. **Necessary Condition:** If M_p is prime, then p must be prime. (However, the converse is not true; e.g., when $p = 11$, $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$ is composite.)

Example 6.1. – For $p = 2$:

$$M_2 = 2^2 - 1 = 3 \quad \text{(prime)}.$$

– For $p = 3$:

$$M_3 = 2^3 - 1 = 7 \quad \text{(prime)}.$$

– For $p = 5$:

$$M_5 = 2^5 - 1 = 31 \quad \text{(prime)}.$$

– For $p = 7$:

$$M_7 = 2^7 - 1 = 127 \quad \text{(prime)}.$$

– For $p = 11$:

$$M_{11} = 2^{11} - 1 = 2047 \quad \text{(composite, since } 2047 = 23 \times 89\text{)}.$$

Theorem 6.1. *If n is a positive composite number, then $2^n - 1$ is a composite number.*

Example 6.2. The numbers 4, 6, and 9 are composite. Accordingly, $2^4 - 1 = 15$, $2^6 - 1 = 63$, and $2^9 - 1 = 511 = 7 \times 73$ are composite.

Lemma 6.1. For any integer $n \geq 1$, we have the factorization

$$x^n - 1 = (x-1)\left(x^{n-1} + x^{n-2} + \cdots + x + 1\right).$$

Lemma 6.2. Let $a > 1$ and $n > 1$. If $a^n + 1$ is prime, then a is even and $n = 2^k$ for some $k \geq 1$.

Proof. We first prove that n must be even.

Step 1: Suppose n is odd.

Assume that n is odd:

Since

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1).$$

Now, we replace a with $-a$:

$$(-a)^n - 1 = (-a-1)((-a)^n + (-a)^{n-1} + (-a)^{n-2} + \cdots + (-a) + 1).$$

$$\Rightarrow (-a)^n = -a^n, (-a)^{n-1} = a^{n-1}, (-a)^{n-2} = -a^{n-2}, \ldots.$$

$$\Rightarrow -(a^n + 1) = -(a+1)(a^{n-1} - a^{n-2} + \cdots - a + 1).$$

$$\Rightarrow a^n + 1 = (a+1)(a^{n-1} - a^{n-2} + \cdots - a + 1).$$

For $n \geq 2$, we have: $1 < a + 1 < a^n + 1$.

Thus, if n is odd, the number $a^n + 1$ is divisible by $a + 1$, and it is not prime. Hence, n cannot be odd, then n even.

Now, since n even, let $n = 2^s \cdot t$, where t is odd. If $a^n + 1$ is prime, then:

$$a^n + 1 = a^{2^s \cdot t} + 1.$$

But $a^n + 1$ cannot be prime if $t \geq 2$ and t is odd. Therefore, $t = 1$, which gives $n = 2^s$.

Thus, $n = 2^k$ for some integer $k \geq 1$. □

7 The Group, Ring, and Field

7.1 Groups

Definition 7.1. Let G be a non-empty set. A function from $G \times G$ into G. That is, $* : G \times G \to G$ is a binary operation if and only if

$$a * b \in G, \quad \forall a, b \in G.$$

Example 7.1. The ordinary addition is a binary operation on $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$. This is because:

$$a + b \in \mathbb{Z}, \quad \forall a, b \in \mathbb{Z},$$

$$a + b \in \mathbb{Q}, \quad \forall a, b \in \mathbb{Q},$$

$$a + b \in \mathbb{R}, \quad \forall a, b \in \mathbb{R}.$$

The ordinary multiplication is also a binary operation on $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$.

Definition 7.2. A *semigroup* is a pair $(G, *)$ in which G is a non-empty set and $*$ is a binary operation on G that satisfies the associative law. i.e.
$(G, *)$ is a semigroup if and only if the following conditions hold:

- $G \neq \emptyset$,
- $*$ is a binary operation on G,
- For all $a, b, c \in G$, the operation satisfies the associative law:

$$(a * b) * c = a * (b * c).$$

Example 7.2. $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{R}, +)$,$(\mathbb{R}, \cdot)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}, \cdot)$ are semigroup.

Definition of Group

Definition 7.3. A pair $(G, *)$ is called a *group* if the following conditions are satisfied:

1. **Closure**: G is closed under the operation $*$, i.e., for all $a, b \in G$, we have $a * b \in G$.
2. **Associativity**: The operation $*$ is associative on G, i.e., for all $a, b, c \in G$, we have
$$(a * b) * c = a * (b * c).$$
3. **Identity element**: There exists an element $e \in G$ such that for all $a \in G$, we have
$$a * e = e * a = a.$$
4. **Inverse element**: For every element $a \in G$, there exists an element $a^{-1} \in G$ such that
$$a * a^{-1} = a^{-1} * a = e.$$

Remark 7.1.
1. The pair $(G, *)$ is a group if and only if $(G, *)$ is a semigroup with an identity element in which each element of G has an inverse.
2. Every group is a semigroup, but the converse is not true. For example, $(\mathbb{N}, +)$ is a semigroup but not a group because there does not exist an inverse element for every $a \in \mathbb{N}$, i.e., for some $a \in \mathbb{N}$, there is no element $a^{-1} \in \mathbb{N}$.

Definition 7.4. A group $(G, *)$ is called a *commutative group* (or *abelian group*) if and only if
$$a * b = b * a \quad \text{for all} \quad a, b \in G.$$

Example 7.3. The pairs $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, and $(\mathbb{R}, +)$ are commutative groups.

Example 7.4. Given: Let $G = \mathbb{Z}$ and define the operation $*$ on G by:

$$a * b = a + b + 2, \quad \forall a, b \in \mathbb{Z}.$$

We will show that $(G, *)$ satisfies the group axioms.

Step 1: Closure

By definition of $*$, for any $a, b \in \mathbb{Z}$,

$$a * b = a + b + 2 \in \mathbb{Z}.$$

Thus, G is closed under $*$.

Step 2: Associativity

To check associativity, we need to verify:

$$(a * b) * c = a * (b * c), \quad \forall a, b, c \in \mathbb{Z}.$$

Computing both sides:

Left-hand side:

$$(a * b) * c = (a + b + 2) * c = (a + b + 2) + c + 2 = a + b + c + 4.$$

Right-hand side:

$$a * (b * c) = a * (b + c + 2) = a + (b + c + 2) + 2 = a + b + c + 4.$$

Since both sides are equal, $*$ is associative.

Step 3: Identity Element

Let e be the identity element, meaning:

$$a * e = a, \quad \forall a \in \mathbb{Z}.$$

Using the operation definition:

$$a * e = a + e + 2 = a.$$

Solving for e,

$$a + e + 2 = a \Rightarrow e + 2 = 0 \Rightarrow e = -2.$$

Thus, the identity element is $e = -2$.

Step 4: Inverse Element

For each $a \in \mathbb{Z}$, we need an element $a' \in \mathbb{Z}$ such that:

$$a * a' = e.$$

That is,

$$a + a' + 2 = -2.$$

Solving for a',

$$a' = -a - 4.$$

Since $a' \in \mathbb{Z}$ for all $a \in \mathbb{Z}$, every element has an inverse.

Since closure, associativity, identity, and inverses are satisfied, $(G, *)$ is a group.

Theorem 7.1. *The identity element of a group $(G, *)$ is unique.*

Proof. Let has two identity elements, say e and e'.

By the definition of the identity element, we have:

$$a * e = e * a = a, \quad \forall a \in G.$$

$$a * e' = e' * a = a, \quad \forall a \in G.$$

Since e' is identity, then

$$e' * e = e * e' = e. \tag{6}$$

Also, e ,

$$e * e' = e' * e = e'. \tag{7}$$

From (1) and (2), we have

$$e' = e.$$

Thus, the identity element in G is unique. □

7.2 Rings

Definition Ring

Definition 7.5. A ring $(R, +, \cdot)$ is a non-empty set R with two operations $(+)$ and $(\cdot)$, such that:

1. $(R, +)$ is an Abelian Group.
2. $(R, \cdot)$ is a semigroup.
3. Left and Right Distributive Laws Hold
   - $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in R$.
   - $(a + b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in R$.

Example 7.5. The pairs $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, and $(\mathbb{R}, +, \cdot)$ are rings.

Commutative Ring

Definition 7.6. A ring $(R, \cdot)$ is said to be commutative ring if

$$a \cdot b = b \cdot a, \quad \forall a, b \in R.$$

Unity of Ring

Definition 7.7. A ring $(R, \cdot)$ is said to be ring with identity if there exists an element $e \in R$, such that

$$a \cdot e = e \cdot a = a, \forall a \in R.$$

e is called identity of R or unity of R

Example 7.6. The pairs $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, and $(\mathbb{R}, +, \cdot)$ are commutative rings with identity.

7.3 Field

Definition Field

Definition 7.8. A ring $(F, +, \cdot)$ is a non-empty set F with two operations $(+)$ and $(\cdot)$, such that:

1. $(F, +)$ is an Abelian Group.
2. $(F, \cdot)$ is an Abelian Group.
3. Left and Right Distributive Laws Hold
   - $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in F$.
   - $(a + b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in F$.

Example 7.7. The pair $(\mathbb{R}, +, \cdot)$ is Field.

7.4 Exercises of The Group, Ring, and Field

Exercises

1. Prove that in a group $(G, *)$, each element has exactly one inverse.

2. If $(G, *)$ is a group, then for all $a, b \in G$,

$$(a * b)^{-1} = b^{-1} * a^{-1}.$$

3. If $(G, *)$ is a commutative group, then for all $a, b \in G$,

$$(a * b)^{-1} = a^{-1} * b^{-1}.$$

4. Consider the set G of all diagonal matrices of the form

$$G = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{R}, a, b \neq 0 \right\}$$

Prove that $(G, \cdot)$ is abelian group.

5. Consider the set R of all diagonal matrices of the form

$$R = \left\{ \begin{pmatrix} 2^n & 0 \\ 0 & 2^m \end{pmatrix} : 2^n, 2^m \in \mathbb{R}, n, m \in \mathbb{Z} \right\}$$

Is $(R, +\cdot)$ a commutative ring.

6. If $\forall a, b \in G$, $a * b = a + b + ab$. Is $(G, *)$ a group?

7. If $\forall a, b \in G$, $a * b = a^2 + b^2$. Is $(G, *)$ a ring?

8. If $\forall a, b \in G$, $a \oplus b = a + b - 1$ and $a \otimes b = a + b - ab$. Is $(G, *, \circ)$ a ring?

8 Theory of Congruence's

Defintion of Congruent

Definition 8.1. Let m be a positive integer. We say that a is congruent to b modulo m denoted as $a \equiv b \pmod{m}$, if $m \mid (a-b)$, where a and b are integers.

Example 8.1. We want to check if $a \equiv b \pmod{m}$

1. $25 \equiv 1 \pmod{4}$ since $4 \mid 25-1$.
2. $25 \not\equiv 2 \pmod{4}$ since $4 \nmid 25-2$.
3. $1 \equiv -3 \pmod{4}$ since $4 \mid 1-(-3)$.
4. If n is even $n \equiv 0 \pmod{2}$.
5. If n is odd $n \equiv 1 \pmod{2}$.

Theorem 8.1. *If a and b are integers, then $a \equiv b \pmod{m}$ if and only if there is an integer k such that $a = b + km$.*

Proof. ($\Rightarrow$): Suppose $a \equiv b \pmod{m} \Rightarrow m \mid (a-b) \Rightarrow a - b = km \Rightarrow a = b + km$

($\Leftarrow$) suppose that there exists an integer k such that $a = b + km \Rightarrow a - b = km \Rightarrow m \mid (a-b)$. Then

$$a \equiv b \pmod{m}$$

□

Theorem 8.2. *For $m > 0$ and for all integers a and b:*

$$a \equiv b \,(\textit{mod}\ m) \iff a \,(\textit{mod}\ m) = b \mod m.$$

$a \pmod{m} = r$ where r is the remainder given by the Division Algorithm when m is divided by m.

Example 8.2. It is 11 PM, and you want to sleep for 8 hours. To determine when to set your alarm, you need to compute the time 8 hours after 11 PM.

First, we add 8 hours to 11 PM:

$$11 + 8 = 19$$

Since time is typically measured on a 12-hour clock, we need to take the result modulo 12:

$$19 \pmod{12} = 7$$

Thus, you should set your alarm for 7 AM.

Example 8.3. To what least residue (mod 11) is each of 23, 29, 31, 37, and 41 congruent?

Sol. We will compute the remainder when each number is divided by 11.

$$23 \div 11 = 2 \text{ remainder } 1 \quad \Rightarrow \quad 23 \equiv 1 \pmod{11}$$

$$29 \div 11 = 2 \text{ remainder } 7 \quad \Rightarrow \quad 29 \equiv 7 \pmod{11}$$

$$31 \div 11 = 2 \text{ remainder } 9 \quad \Rightarrow \quad 31 \equiv 9 \pmod{11}$$

$$37 \div 11 = 3 \text{ remainder } 4 \quad \Rightarrow \quad 37 \equiv 4 \pmod{11}$$

$$41 \div 11 = 3 \text{ remainder } 8 \quad \Rightarrow \quad 41 \equiv 8 \pmod{11}$$

Thus, the least residues modulo 11 are:

$$23 \equiv 1 \,(\mathrm{mod}\, 11), \quad 29 \equiv 7 \,(\mathrm{mod}\, 11), \quad 31 \equiv 9 \,(\mathrm{mod}\, 11), \quad 37 \equiv 4 \,(\mathrm{mod}\, 11), \quad 41 \equiv 8 \,(\mathrm{mod}\, 11).$$

□

Theorem 8.3. *Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then:*

$$a + c \equiv b + d \pmod{m}.$$

Proof.

$$a \equiv b \pmod{m} \iff m \mid (a-b) \iff (a-b) = k_1 \cdot m \quad \text{for some integer } k_1.$$

$$c \equiv d \pmod{m} \iff m \mid (c-d) \iff (c-d) = k_2 \cdot m \quad \text{for some integer } k_2.$$

Now, consider the expression $(a+c)-(b+d)$:

$$(a+c)-(b+d) = (a-b)+(c-d) = k_1 \cdot m + k_2 \cdot m = m \cdot (k_1+k_2).$$

Since $m \mid [(a+c)-(b+d)]$, by the equivalent definition of congruence, we conclude that:

$$a+c \equiv b+d \pmod{m}.$$

□

Example 8.4.

$$10001 + 20000005 + 3004 \equiv ? \pmod{10}$$

Sol. First, we calculate each number modulo 10:

$$10001 \equiv 1 \pmod{10}$$

$$20000005 \equiv 5 \pmod{10}$$

$$3004 \equiv 4 \pmod{10}$$

Now, add them together modulo 10:

$$10001 + 20000005 + 3004 \equiv 1 + 5 + 4 \pmod{10} \equiv 10 \pmod{10} \equiv 0 \pmod{10}$$

□

Theorem 8.4. *Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then:*

$$ac \equiv bd \pmod{m}.$$

Proof.

$$a \equiv b \pmod{m} \iff m \mid (a-b) \iff (a-b) = k_1 \cdot m \quad \text{for some integer } k_1.$$

$$c \equiv d \pmod{m} \iff m \mid (c-d) \iff (c-d) = k_2 \cdot m \quad \text{for some integer } k_2.$$

Now, consider the expression $ac - bd$:

$$ac - bd = ac - ad + ad - bd = a(c-d) + d(a-b).$$

We can factor out m from both terms:

$$ac - bd = a \cdot m \cdot k_2 + d \cdot m \cdot k_1 = m \cdot (a \cdot k_2 + d \cdot k_1).$$

Since $m \mid (ac - bd)$, by the equivalent definition of congruence, we conclude that:

$$ac \equiv bd \pmod{m}.$$

□

Example 8.5. Compute $10001 \times 20000005 \mod 13$.

Sol. First, compute each number modulo 13:

$$10001 \equiv 4 \pmod{13}$$

$$20000005 \equiv 12 \pmod{13}$$

Now, multiply these values:

$$10001 \times 20000005 \equiv 4 \times 12 \pmod{13}$$

$$\equiv 48 \pmod{13}.$$

Since $48 \div 13 = 3$ with a remainder of 9, we conclude:

$$48 \equiv 9 \pmod{13}.$$

Thus,

$$10001 \times 20000005 \equiv 9 \pmod{13}.$$

□

8.1 Exercises of Theory of Congruence's

Exercises

1. If $a \equiv b \pmod{m}$ and $n \mid m$, prove that $a \equiv b \pmod{n}$.
2. Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, prove that $a + c \equiv b + d \pmod{m}$.
3. Find $46, 59, 61, 77, \ and \ 58 \pmod{39}$.
4. Find the least nonnegative residue modulo 13
   (a) $22 \mod 13$
   (b) $-1 \mod 13$
   (c) $-100 \mod 13$
5. What time does a clock read: (1). 29 hours after it reads 11 o'clock? (2) 50 hours before it reads 6 o'clock?

9 Congruent Modulo

Properties of Congruence Modulo m

Theorem 9.1. *Let $m \in \mathbb{Z}$. For all $a, b, c \in \mathbb{Z}$, the following properties hold:*

1. ***Reflexivity:*** $a \equiv a \pmod{m}$.
2. ***Symmetry:*** *If* $a \equiv b \pmod{m}$, *then* $b \equiv a \pmod{m}$.
3. ***Transitivity:*** *If* $a \equiv b \pmod{m}$ *and* $b \equiv c \pmod{m}$, *then* $a \equiv c \pmod{m}$.

Proof. We prove each property separately.

1. Reflexivity: By definition, $a \equiv b \pmod{m} \Rightarrow m \mid a - b$. Setting $b = a$, we have $m \mid a - a = 0 \Rightarrow m \mid 0$. Therefore, $a \equiv a \pmod{m}$.

2. Symmetry: H.W

3. Transitivity: If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then we have:

$$m \mid (a - b) \quad \text{and} \quad m \mid (b - c).$$

This means there exist integers k_1 and k_2 such that:

$$a - b = k_1 m, \quad b - c = k_2 m.$$

Adding these two equations:

$$(a - b) + (b - c) = k_1 m + k_2 m.$$

Simplifying, we obtain:

$$a - c = (k_1 + k_2)m.$$

Since m divides $a - c$, it follows that $a \equiv c \pmod{m}$. □

Theorem 9.2. *If $a \equiv b \pmod{n}$, then for any positive integer $k \in \mathbb{Z}^+$,*

$$a^k \equiv b^k \pmod{n}.$$

Proof. We proceed by induction on k.

Base Case ($k = 1$): If $k = 1$, then $a^1 = a$ and $b^1 = b$, so $a \equiv b \pmod{n}$.

Inductive Step: Assume that for some $k = m$, the statement holds:

$$a^m \equiv b^m \pmod{n}.$$

We need to show that it holds for $k = m + 1$, i.e.,

$$a^{m+1} \equiv b^{m+1} \pmod{n}.$$

By the induction hypothesis,

$$a^m \equiv b^m \pmod{n}.$$

Multiplying both sides by a, we get:

$$a^m \cdot a \equiv b^m \cdot a \pmod{n}.$$

Since $a \equiv b \pmod{n}$, replacing a with b in the right-hand term gives:

$$b^m \cdot a \equiv b^m \cdot b \pmod{n}.$$

Thus,

$$a^{m+1} \equiv b^{m+1} \pmod{n}.$$

By induction, the theorem holds for all $k \in \mathbb{Z}^+$. □ □

Theorem 9.3. *Let m be a positive integer and a, b be integers. Then,*

$$(a+b) \mod m = ((a \mod m) + (b \mod m)) \mod m.$$

Proof. Clearly, we have:

$$a \equiv a \pmod{m}, \quad \text{and} \quad b \equiv b \pmod{m}.$$

Thus, adding both congruences,

$$a + b \equiv (a \mod m) + (b \mod m) \pmod{m}.$$

□

Theorem 9.4. *Let m be a positive integer and a, b be integers. Then,*

$$(a \cdot b) \mod m = ((a \mod m) \cdot (b \mod m)) \mod m.$$

Proof: *H.W*

Example 9.1. What is $2008^{2008} \mod 3$?

Sol.

$$2008^{2008} = \underbrace{(2008 \times 2008 \times \cdots \times 2008)}_{\text{(2008 times)}} \mod 3$$

Using the property of modular arithmetic:

$$= \underbrace{((2008 \mod 3) \times \cdots \times (2008 \mod 3))}_{\text{(2008 times)}} \mod 3$$

Since $2008 \mod 3 = 1$, we have:

$$= (1 \times 1 \times \cdots \times 1) \mod 3$$

Thus,

$$= 1^{2008} \mod 3 = 1 \mod 3 = 1.$$

So, $2008^{2008} \mod 3 = 1$. □

Example 9.2. Find the remainder when $1! + 2! + \cdots + 100!$ is divided by 15.

Sol. Notice that when $k \geq 5$, $k! \equiv 0 \pmod{15}$. Therefore,

$$1! + 2! + \cdots + 100! \equiv 1! + 2! + 3! + 4! + 0 + \cdots + 0 \pmod{15}.$$

Now, compute the factorials modulo 15 for $1!$, $2!$, $3!$, and $4!$:

$$1! = 1, \quad 2! = 2, \quad 3! = 6, \quad 4! = 24.$$

Thus, we have:

$$1! + 2! + 3! + 4! \equiv 1 + 2 + 6 + 24 \pmod{15}.$$

Simplifying the sum:

$$1 + 2 + 6 + 24 = 33.$$

Now, take modulo 15:

$$33 \mod 15 = 3.$$

Therefore, the remainder when the given sum is divided by 15 is 3. □

Example 9.3. Find the remainder when 16^{53} is divided by 7.

Sol. First, reduce the base to its least residue modulo 7:

$$16 \equiv 2 \pmod{7}.$$

So,

$$16^{53} \equiv 2^{53} \pmod{7}.$$

we can write 53 as $53 = 3 \times 17 + 2$, so:

$$2^{53} = 2^{3 \cdot 17 + 2} = (2^3)^{17} \cdot 2^2.$$

Since $2^3 \equiv 1 \pmod 7$, we have:

$$(2^3)^{17} \equiv 1^{17} \equiv 1 \pmod 7.$$

Therefore:

$$2^{53} \equiv 1 \cdot 2^2 \equiv 4 \pmod 7.$$

Thus, $16^{53} \equiv 4 \pmod 7$, by the transitive property.

Therefore, the remainder when 16^{53} is divided by 7 is 4. □

9.1 Exercises of Congruent modulo

Exercises

1. If $a \equiv b \pmod m$, prove that $b \equiv a \pmod m$.
2. Let m be a positive integer and a, b be integers. Prove that,

$$(a \cdot b) \mod m = ((a \mod m) \cdot (b \mod m)) \mod m.$$

3. Find the remainder when 3^247 is divided by 17.
4. Find the value of each of the following:
   (a) $2^{32} \mod 7$.
   (b) $10^{35} \mod 7$.
   (c) $3^{35} \mod 7$.
5. If $a \equiv 4 \pmod 7$ and $b \equiv 5 \pmod 7$, what is $a+b \mod 7$? What is $a \times b \mod 7$?

10 Divisibility Tests

Elementary school children know how to tell if a number is even, or divisible by 5, by looking at the least significant digit.

Theorem 10.1. *If a number a has the decimal representation*

$$a = a_{n-1}10^{n-1} + a_{n-2}10^{n-2} + \cdots + a_1 10 + a_0$$

then:

1. $a \mod 2 = a_0 \mod 2$
2. $a \mod 5 = a_0 \mod 5$

Proof. Consider the polynomial function:

$$f(x) = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

Note that $10 \equiv 0 \pmod 2$. So

$$a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0 \equiv a_{n-1}0^{n-1} + \cdots + a_1 0 + a_0 \pmod 2.$$

That is,

$$a \equiv a_0 \pmod 2.$$

This proves item (1).

Similarly, since $10 \equiv 0 \pmod 5$, the proof of item (2) follows in the same manner. □

Example 10.1. Thus, the number 1457 is odd because 7 is odd:

$$1457 \mod 2 = 7 \mod 2 = 1.$$

And on division by 5, it leaves a remainder of:

$$1457 \mod 5 = 7 \mod 5 = 2.$$

Theorem 10.2. *Let*

$$a = a_{n-1}10^{n-1} + a_{n-2}10^{n-2} + \cdots + a_1 10 + a_0$$

be the decimal representation of a*. Then:*

1. $a \mod 3 = (a_{n-1} + \cdots + a_0) \mod 3$.
2. $a \mod 9 = (a_{n-1} + \cdots + a_0) \mod 9$.
3. $a \mod 11 = (a_0 - a_1 + a_2 - a_3 + \dots) \mod 11$.

Proof. Note that $10 \equiv 1 \pmod 3$.

$$a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0 \equiv a_{n-1}1^{n-1} + \cdots + a_1 1 + a_0 \pmod 3.$$

Thus,

$$a \equiv a_{n-1} + \cdots + a_1 + a_0 \pmod 3.$$

This proves item (1). Similarly, since $10 \equiv 1 \pmod 9$, the proof of item (2) follows the same steps.

For item (3), note that $10 \equiv -1 \pmod{11}$, so:

$$a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0 \equiv a_{n-1}(-1)^{n-1} + \cdots + a_1(-1) + a_0 \pmod{11}.$$

That is,

$$a \equiv a_0 - a_1 + a_2 - a_3 + \dots \pmod{11}.$$

□

Example 10.2. Consider the number 1457. We calculate its remainder modulo 3, 9, and 11.

Modulo 3:

$$1457 \mod 3 = (1+4+5+7) \mod 3 = 17 \mod 3 = 8 \mod 3 = 2.$$

Modulo 9:

$$1457 \mod 9 = (1+4+5+7) \mod 9 = 17 \mod 9 = 8 \mod 9 = 8.$$

Modulo 11:

$$1457 \mod 11 = (7-5+4-1) \mod 11 = 5 \mod 11 = 5.$$

Thus, the least nonnegative residues are:

$$1457 \equiv 2 \pmod 3, \quad 1457 \equiv 8 \pmod 9, \quad 1457 \equiv 5 \pmod{11}.$$

Remark 10.1.

$$m \mid a \iff a \mod m = 0$$

Corollary 10.1. Let $a = a_{n-1}10^{n-1} + a_{n-2}10^{n-2} + \cdots + a_1 10 + a_0$. Then:

1. $2 \mid a \iff a_0 = 0, 2, 4, 6,$ or 8.
2. $5 \mid a \iff a_0 = 0$ or 5.
3. $3 \mid a \iff 3 \mid (a_0 + a_1 + \cdots + a_{n-1})$.
4. $9 \mid a \iff 9 \mid (a_0 + a_1 + \cdots + a_{n-1})$.
5. $11 \mid a \iff 11 \mid (a_0 - a_1 + a_2 - a_3 + \dots)$.

Theorem 10.3. *Let $a = a_r 10^r + \cdots + a_2 10^2 + a_1 10 + a_0$ be the decimal representation, so that we write a as the sequence $a_r a_{r-1} \ldots a_1 a_0$. Then:*

1. $7 \mid a \iff 7 \mid (a_r \ldots a_1 - 2a_0)$.
2. $13 \mid a \iff 13 \mid (a_r \ldots a_1 - 9a_0)$,

where $a_r \ldots a_1$ is the sequence representing $\frac{a-a_0}{10}$.

Example 10.3. We can test whether 7 divides 2481:

$$7 \mid 2481 \iff 7 \mid (248 - 2) \iff 7 \mid 246 \iff 7 \mid (24 - 12) \iff 7 \mid 12.$$

Since $7 \nmid 12$, we conclude that $7 \nmid 2481$.

Example 10.4. The number 12987 is divisible by 13 because:

$$13 \mid 12987 \iff 13 \mid (1298 - 63) \iff 13 \mid 1235 \iff 13 \mid (123 - 45) \iff 13 \mid 78.$$

And since $13 \times 6 = 78$, we conclude that 12987 is divisible by 13.

10.1 Exercises of Divisibility Tests

Exercises

1. Let $a = 18726132117057$. Find $a \mod m$ for $m = 2, 3, 5, 9$, and 11.
2. Determine which of the following are divisible by 7:
   (a) 6994 (b) 6993
3. Let $a = a_n a_{n-1} \cdots a_1 a_0$ be the decimal representation of a. Prove the following:
   (a) $a \mod 10 = a_0$.
   (b) $a \mod 100 = a_1 a_0$.
   (c) $a \mod 1000 = a_2 a_1 a_0$.

11 More Properties of Congruences

The Inverse of a Modulo m

Theorem 11.1. *Let $m \geq 2$. If a and m are relatively prime ($\gcd(a, m) = 1$), then there exists a unique integer a^{-1} such that*

$$aa^{-1} \equiv 1 \pmod{m} \quad \textit{and} \quad 0 < a^{-1} < m.$$

Proof. Since $\gcd(a, m) = 1$. Then there exist integers s and t such that

$$as + mt = 1. \Rightarrow as - 1 = m(-t),$$

$\Rightarrow m \mid (as - 1) \Rightarrow as \equiv 1 \pmod{m}$. Thus, $a^{-1} = s \mod m$ satisfies $0 < a^* < m$ and we have:

$$aa^{-1} \equiv 1 \pmod{m}.$$

To prove uniqueness, Let there exists an integer c such that $ac \equiv 1 \pmod{m}$ and $0 < c < m$. From this, we have:

$$ac \equiv aa^{-1} \pmod{m} \Rightarrow c \equiv a^{-1} \pmod{m}.$$

Proving the uniqueness. □

Example 11.1. Let $m = 15$ and $a = 2$. We find the integer a^{-1} such that $a \cdot a^{-1} \equiv 1 \pmod{15}$.

$$\begin{aligned}
&2 \cdot 0 \not\equiv 1 \pmod{15}, \quad 2 \cdot 1 \not\equiv 1 \pmod{15}, \quad 2 \cdot 2 \not\equiv 1 \pmod{15}, \\
&2 \cdot 3 \not\equiv 1 \pmod{15}, \quad 2 \cdot 4 \not\equiv 1 \pmod{15}, \quad 2 \cdot 5 \not\equiv 1 \pmod{15}, \\
&2 \cdot 6 \not\equiv 1 \pmod{15}, \quad 2 \cdot 7 \not\equiv 1 \pmod{15}, \quad 2 \cdot 8 \equiv 1 \pmod{15},
\end{aligned}$$

because $15 \mid (16 - 1)$. Thus, we can take $a^- = 8$.

Remark 11.1. We call a^{-1} the inverse of a modulo m.

Theorem 11.2. *Let $m > 0$. If $ab \equiv 1 \pmod{m}$, then both a and b are relatively prime to m, i.e., $\gcd(a, m) = 1$ and $\gcd(b, m) = 1$.*

Corollary 11.1. A number a has an inverse modulo m if and only if a and m are relatively prime, i.e., $\gcd(a, m) = 1$.

Theorem 11.3. *Let $m > 0$. If $\gcd(c, m) = 1$, then $ca \equiv cb \pmod{m}$ implies $a \equiv b \pmod{m}$.*

Theorem 11.4. *If $c > 0$ and $m > 0$, then*

$$a \equiv b \pmod{m} \iff ca \equiv cb \pmod{cm}.$$

Theorem 11.5. *If $m > 0$ and $a \equiv b \pmod{m}$, then*

$$\gcd(a, m) = \gcd(b, m).$$

11.1 Finding Modular Inverses Using the Extended Euclidean Algorithm

Given an integer a and a modulus m, the modular inverse of a modulo m is an integer x such that:

$$ax \equiv 1 \pmod{m} \tag{8}$$

The modular inverse exists if and only if $\gcd(a, m) = 1$. We use the **Extended Euclidean Algorithm** to compute it.

Example 11.2. Find the inverse of 7 modulo 20.

Sol. We apply the Euclidean algorithm:

$$20 = 2 \times 7 + 6$$

$$7 = 1 \times 6 + 1$$

$$6 = 6 \times 1 + 0$$

Since $\gcd(7, 20) = 1$, an inverse exists.

Now, we work backward:

$$\begin{aligned} 1 &= 7 - 1 \times 6 \\ &= 7 - 1(20 - 2 \times 7) \\ &= 7 - 20 + 2 \times 7 \\ &= 3 \times 7 - 1 \times 20 \end{aligned}$$

Thus, $7^{-1} \equiv 3 \pmod{20}$. □

Example 11.3. Find the inverse of 11 modulo 26.

Sol. Using the Euclidean algorithm:

$$\begin{aligned} 26 &= 2 \times 11 + 4 \\ 11 &= 2 \times 4 + 3 \\ 4 &= 1 \times 3 + 1 \\ 3 &= 3 \times 1 + 0 \end{aligned}$$

Since $\gcd(11, 26) = 1$, an inverse exists.

Working backward:

$$\begin{aligned} 1 &= 4 - 1 \times 3 \\ &= 4 - 1(11 - 2 \times 4) \\ &= 3 \times 4 - 1 \times 11 \\ &= 3(26 - 2 \times 11) - 1 \times 11 \\ &= 3 \times 26 - 7 \times 11 \end{aligned}$$

Thus, $11^{-1} \equiv -7 \equiv 19 \pmod{26}$. □

Example 11.4. Find the inverse of 17 modulo 43

Sol. Using the Euclidean algorithm:

$$43 = 2 \times 17 + 9$$
$$17 = 1 \times 9 + 8$$
$$9 = 1 \times 8 + 1$$
$$8 = 8 \times 1 + 0$$

Since $\gcd(17, 43) = 1$, an inverse exists.

Working backward:

$$\begin{aligned} 1 &= 9 - 1 \times 8 \\ &= 9 - 1(17 - 1 \times 9) \\ &= 2 \times 9 - 1 \times 17 \\ &= 2(43 - 2 \times 17) - 1 \times 17 \\ &= 2 \times 43 - 5 \times 17 \end{aligned}$$

Thus, $17^{-1} \equiv -5 \equiv 38 \pmod{43}$. □

11.2 Exercises of More Properties of Congruences

Exercises

1. Show that the inverse of 2 modulo 7 is not the inverse of 2 modulo 15.
2. Let $m > 0$. If $ab \equiv 1 \pmod{m}$, then both a and b are relatively prime to m.
3. If $c > 0$ and $m > 0$, then $a \equiv b \pmod{m} \iff ca \equiv cb \pmod{cm}$.
4. If there exists $a^{-}1$ find for each following

   (a) 11^{-1} mod 43, (b) 29^{-1} mod 78, (c) 6^{-1} mod 19.

12 Residue Classes

In *modular arithmetic*, a *residue class* is a set of integers that are congruent to each other modulo a given number. When working with congruences, these residue classes help us group numbers that share certain properties under a modulo operation.

Defintion Residue Class of a modulo m

Definition 12.1. Let $m > 0$ be given. For each integer a, we define

$$[a]_m = \bar{a} = \{x : x \equiv a \pmod{m}\}.$$

In other words, $[a]_m$ or $\bar{a}$ is the set of all integers that are congruent to a modulo m. We call $[a]_m$ the residue class of a modulo m. Some people also call $[a]_m$ the congruence class or equivalence class of a modulo m.

Example 12.1. Consider $m = 5$ and look at the residue class of $2 \mod 5$. We are looking for all integers that leave the same remainder as 2 when divided by 5. These integers are:

$$\{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\}$$

Thus, the residue class of 2 modulo 5 is:

$$\bar{2} = [2]_5 = \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\}$$

Similarly, the residue class of $3 \mod 5$ would be:

$$\bar{3} = [3]_5 = \{\ldots, -7, -2, 3, 8, 13, 18, \ldots\}$$

Theorem 12.1. *For $m > 0$, we have*

$$\bar{a} = [a]_m = \{mq + a \mid q \in \mathbb{Z}\}.$$

Proof.

$$x \in [a]_m \iff x \equiv a \pmod{m} \iff m \mid (x - a) \iff x - a = mq \text{ for some } q \in \mathbb{Z}$$

$$\iff x = mq + a \text{ for some } q \in \mathbb{Z}.$$

□

Theorem 12.2. *For a given modulus $m > 0$, we have:*

$$[a]_m = [b]_m \iff a \equiv b \pmod{m}.$$

Proof. "⇒" Assume $[a] = [b]$. Since $a \equiv a \pmod{m}$, we have $a \in [a]$. Since $[a] = [b]$, we have $a \in [b]$. By the definition of $[b]$, this gives $a \equiv b \pmod{m}$.

"⇐" Assume $a \equiv b \pmod{m}$. We must prove that the sets $[a]$ and $[b]$.

Let $x \in [a]$. Then $x \equiv a \pmod{m}$. Since $a \equiv b \pmod{m}$, by transitivity, $x \equiv b \pmod{m}$, so $x \in [b]$.

Conversely, if $x \in [b]$, then $x \equiv b \pmod{m}$. By symmetry, since $a \equiv b \pmod{m}$, we also have $b \equiv a \pmod{m}$. Thus, by transitivity, $x \equiv a \pmod{m}$, and so $x \in [a]$.

This proves that $[a] = [b]$. □

Distinct Residue Classes modulo m

Theorem 12.3. *Given $m > 0$, there are exactly m distinct residue classes modulo m, namely,*

$$[0], [1], [2], \ldots, [m - 1].$$

12.1 $\mathbb{Z}_m$ and Complete Residue Systems

Defintion Set of All Residue Classes

Definition 12.2. We define

$$\mathbb{Z}_m = \{[a] \mid a \in \mathbb{Z}\},$$

that is, $\mathbb{Z}_m$ is the set of all residue classes modulo m. We call $(\mathbb{Z}_m, +, \cdot)$ the **ring of integers modulo** m.

$$\mathbb{Z}_m = \{[0], [1], \ldots, [m-1]\}.$$

or

$$\mathbb{Z}_m = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}.$$

Example 12.2.

- For $m = 2$:

$$\mathbb{Z}_2 = \{[0], [1]\}$$

- For $m = 3$:

$$\mathbb{Z}_3 = \{[0], [1], [2]\}$$

- For $m = 4$:

$$\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$$

- For $m = 5$:

$$\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$$

Definition 12.3. A set of m integers

$$\{a_0, a_1, \ldots, a_{m-1}\}$$

is called a **complete residue system modulo** m if

$$\mathbb{Z}_m = \{[a_0], [a_1], \ldots, [a_{m-1}]\}.$$

12.2 Addition and Multiplication in $\mathbb{Z}_m$

Definition 12.4. For $[a], [b] \in \mathbb{Z}_m$, we define

$$[a] + [b] = [a + b]$$

and

$$[a] \cdot [b] = [ab].$$

Remark 12.1. For $m = 5$, we have

$$[2] + [3] = [5], \quad \text{and} \quad [2] \cdot [3] = [6].$$

Since $5 \equiv 0 \pmod 5$ and $6 \equiv 1 \pmod 5$, we obtain

$$[5] = [0] \quad \text{and} \quad [6] = [1],$$

so we can also write

$$[2] + [3] = [0], \quad [2] \cdot [3] = [1].$$

Theorem 12.4. *For any modulus $m > 0$, if $[a] = [b]$ and $[c] = [d]$, then*

$$[a] + [c] = [b] + [d]$$

and

$$[a] \cdot [c] = [b] \cdot [d].$$

Example 12.3. Take $m = 151$. Then $150 \equiv -1 \pmod{151}$ and $149 \equiv -2 \pmod{151}$, so

$$[150][149] = [-1][-2] = [2]$$

and

$$[150] + [149] = [-1] + [-2] = [-3] = [148]$$

since $148 \equiv -3 \pmod{151}$.

Example 12.4. Addition and Multiplication Tables for $\mathbb{Z}_4$

Addition Table

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Multiplication Table

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Theorem 12.5. *$\mathbb{Z}_n$ is a ring for any positive integer n.*

Proof. Let n be a positive integer. Define $\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$.

Step 1: Proving $\mathbb{Z}_n$ is a Commutative Group under Addition

1. **Closure under addition:** $\forall [a], [b] \in \mathbb{Z}_n$, we have

$$[a] + [b] = [a + b] \pmod{n}.$$

Since $a + b$ is an integer, $[a + b] \in \mathbb{Z}_n$, Therefore, $\mathbb{Z}_n$ is closed.

2. **Associativity of addition:** For $[a], [b], [c] \in \mathbb{Z}_n$, we have

$$([a] + [b]) + [c] = [a + b] + [c] = [a + b + c] = [a] + [b + c] = [a] + ([b] + [c]).$$

Therefore, addition is associative.

3. **Commutativity of addition:** For $[a], [b] \in \mathbb{Z}_n$, we have

$$[a] + [b] = [a + b] = [b + a] = [b] + [a].$$

Thus, addition is commutative.

4. **Identity:** The element $[0] \in \mathbb{Z}_n$ is identity because for any $[a] \in \mathbb{Z}_n$, we have

$$[a] + [0] = [a + 0] = [a].$$

5. **Inverse:** For each $[a] \in \mathbb{Z}_n$, there exists an element $[b] \in \mathbb{Z}_n$ such that

$$[a] + [b] = [0].$$

The additive inverse of $[a]$ is $[n - a]$, since

$$[a] + [n - a] = [a + (n - a)] = [n] = [0].$$

Therefore, every element has an additive inverse.

Thus, $\mathbb{Z}_n$ is a commutative group under addition.

Step 2: Proving $\mathbb{Z}_n$ is a Semigroup under Multiplication

1. **Closure under multiplication:** For any $[a], [b] \in \mathbb{Z}_n$, we have

$$[a] \cdot [b] = [a \cdot b] \pmod{n}.$$

   Since $a \cdot b$ is an integer, $[a \cdot b] \in \mathbb{Z}_n$. Therefore, $\mathbb{Z}_n$ is closed.

2. **Associativity of multiplication:** For $[a], [b], [c] \in \mathbb{Z}_n$, we have

$$([a] \cdot [b]) \cdot [c] = [a \cdot b] \cdot [c] = [a \cdot b \cdot c] = [a] \cdot [b \cdot c] = [a] \cdot ([b] \cdot [c]).$$

   Therefore, multiplication is associative.

Thus, $\mathbb{Z}_n$ is a semigroup under multiplication.

Step 3: Proving Distributivity of Multiplication over Addition

Finally, we show that multiplication distributes over addition in $\mathbb{Z}_n$. For $[a], [b], [c] \in \mathbb{Z}_n$, we need to prove that

$$[a] \cdot ([b] + [c]) = [a] \cdot [b] + [a] \cdot [c].$$

We have

$$[a] \cdot ([b] + [c]) = [a] \cdot [b + c] = [a(b + c)] = [a \cdot b + a \cdot c] = [a \cdot b] + [a \cdot c].$$

Thus, multiplication distributes over addition.

Since $\mathbb{Z}_n$ satisfies the properties of a commutative group under addition, a semigroup under multiplication, and distributivity of multiplication over addition, we conclude that $\mathbb{Z}_n$ is a ring.

□

13 Theorems of Euler, Fermat and Carmichael

Definition 13.1. A function f defined on the positive integers is said to be **multiplicative** if

$$f(m)f(n) = f(mn), \quad \forall m, n \in \mathbb{Z}^+, \tag{9}$$

where $\gcd(m, n) = 1$.

If

$$f(m)f(n) = f(mn), \quad \forall m, n \in \mathbb{Z}^+, \tag{10}$$

then f is **completely multiplicative**. Every completely multiplicative function is multiplicative.

Euler's φ-function

Definition 13.2. Let n be a positive integer. Euler's φ-function, $\varphi(n)$, is defined to be the number of positive integers k less than n which are relatively prime to n:

$$\varphi(n) = |\{k \mid 0 \leq k < n, \gcd(k, n) = 1\}|.$$

Example 13.1. By Definition 13.2, we have the following values of $\varphi(n)$:

n	1	2	3	4	5	6	7	8	9	10	100	101	102	103
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	40	100	32	102

Lemma 13.1. For any positive integer n,

$$\sum_{d|n} \varphi(d) = n.$$

Theorem 13.1. *Let n be a positive integer and $\gcd(m, n) = 1$. Then:*

1. *Euler's φ-function is multiplicative. That is,*

$$\varphi(mn) = \varphi(m)\varphi(n),$$

where $\gcd(m, n) = 1$.

2. *If* n *is a prime, say* p*, then*

$$\varphi(p) = p - 1.$$

(Conversely, if p *is a positive integer with* $\varphi(p) = p - 1$*, then* p *is prime.)*

3. *If* n *is a prime power* p^α *with* $\alpha > 1$*, then*

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

4. *If* n *is composite and has the standard prime factorization form, then*

$$\varphi(n) = p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) \cdots p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right).$$

Equivalently,

$$\varphi(n) = n \prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right).$$

Carmichael's λ-function

Definition 13.3. Carmichael's λ-function, $\lambda(n)$, is defined as follows:

$$\lambda(p) = \varphi(p) = p - 1 \quad \text{for prime } p,$$

$$\lambda(p^\alpha) = \varphi(p^\alpha) \quad \text{for } p = 2 \text{ and } \alpha \leq 2,$$

$$\lambda(p^\alpha) = \varphi(p^\alpha) \quad \text{for } p \geq 3,$$

$$\lambda(2^\alpha) = \frac{1}{2}\varphi(2^\alpha) \quad \text{for } \alpha \geq 3,$$

$$\lambda(n) = \operatorname{lcm}\left(\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), \ldots, \lambda(p_k^{\alpha_k})\right) \quad \text{if } n = \prod_{i=1}^{k} p_i^{\alpha_i}.$$

Example 13.2. By Definition 13.3, we have the following values for $\lambda(n)$:

n	1	2	3	4	5	6	7	8	9	10	100	101	102	103
$\lambda(n)$	1	1	2	2	4	2	6	2	6	4	20	100	16	102

Example 13.3. Let $n = 65520 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$, and $a = 11$. Then, $\gcd(65520, 11) = 1$ and we have

$$\varphi(65520) = 8 \cdot 6 \cdot 4 \cdot 6 \cdot 12 = 13824,$$

$$\lambda(65520) = \text{lcm}(4, 6, 4, 6, 12) = 12.$$

The number of multiplicative inverses

Theorem 13.2. *The number of multiplicative inverses b^{-1} modulo n is $\varphi(n)$, where $\varphi(n)$ is Euler's totient function. Specifically, the number of integers b such that $\gcd(b, n) = 1$ (i.e., the number of integers that have a multiplicative inverse modulo n) is given by $\varphi(n)$.*

Example 13.4. et $n = 21$. Since $\varphi(21) = 12$, there are twelve values of b for which the multiplicative inverse $b^{-1} \pmod{21}$ exists. In fact, the multiplicative inverse modulo 21 only exists for each of the following values of b:

$$b : 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20.$$

The corresponding values of $b^{-1} \pmod{21}$ are:

$$b^{-1} \pmod{21} : 1, 11, 16, 17, 8, 19, 2, 13, 4, 5, 10, 20.$$

Euler's Theorem

Theorem 13.3. *If $m > 0$ and a is relatively prime to m, then*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Fermat's Little Theorem

Theorem 13.4. *If p is prime and a is relatively prime to p, then*

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

Let's look at some examples. Take $m = 12$, then

$$\varphi(m) = \varphi(2^2 \cdot 3) = (2^2 - 2)(3 - 1) = 4.$$

The positive integers $a < m$ with $\gcd(a, m) = 1$ are $1, 5, 7$, and 11.

$$14 \equiv 1 \pmod{12} \quad \text{is clear.}$$

$$5^2 \equiv 1 \pmod{12} \quad \text{since} \quad 12 \mid 5^2 - 1.$$

Therefore,

$$5^4 \equiv 1 \pmod{12}.$$

Now, since $7 \equiv -5 \pmod{12}$ and 4 is even, we have:

$$7^4 \equiv (-5)^4 \equiv 5^4 \pmod{12}.$$

Thus,

$$7^4 \equiv 1 \pmod{12}.$$

Next, $11 \equiv -1 \pmod{12}$, and since 4 is even, we get:

$$11^4 \equiv (-1)^4 \equiv 1 \pmod{12}.$$

Corollary 13.1 (Converse of Fermat's Little Theorem)**.** Let n be an odd positive integer. If $\gcd(a, n) = 1$ and

$$a^{n-1} \equiv 1 \pmod{n},$$

then n is composite.

Carmichael's Theorem

Theorem 13.5. *Let a and n be positive integers with $\gcd(a, n) = 1$. Then,*

$$a^{\lambda(n)} \equiv 1 \pmod{n},$$

where $\lambda(n)$ is Carmichael's function.

The Order of an Element

The order of an element

Definition 13.4. For integers a, $m \neq 0$ with $\gcd(a, m) = 1$, the order of $a \mod m$ is its order in the multiplicative group $\mathbb{Z}_m$, that is,

$$\text{ord}_m(a) = \min\{\gamma \in \mathbb{N} \mid a^\gamma \equiv 1 \pmod{m}\}.$$

Example 13.5. The powers of 2 modulo 7 yield the following congruences:

$$2^1 \equiv 2 \pmod{7},$$

$$2^2 \equiv 4 \pmod{7},$$

$$2^3 \equiv 1 \pmod{7},$$

$$2^4 \equiv 2 \pmod 7,$$

$$2^5 \equiv 4 \pmod 7,$$

$$2^6 \equiv 1 \pmod 7.$$

This means that the integer 2 has order 3 modulo 7, as the smallest integer γ such that $2^\gamma \equiv 1 \pmod 7$ is $\gamma = 3$.

Remark 13.1. $\lambda(n)$ will never exceed $\varphi(n)$ and is often much smaller than $\varphi(n)$; it is the value of the largest order it is possible to have.

Example 13.6. Let $a = 11$ and $n = 24$. Then $\varphi(24) = 8$, $\lambda(24) = 2$. So,

$$11^{\varphi(24)} = 11^8 \equiv 1 \pmod{24},$$

$$11^{\lambda(24)} = 11^2 \equiv 1 \pmod{24}.$$

That is, $\text{ord}_{24}(11) = 2$.

Lemma 13.2. If $a^n \equiv 1 \pmod m$, then $\text{ord}_m(a) \mid n$. In particular, $\text{ord}_m(a) \mid \varphi(m)$.

Primitive Root

Theorem 13.6. *If $\text{ord}_m(a) = \varphi(m)$, then a is called a primitive root modulo m.*

The primitive root of 7 is 3 because the following holds: $\varphi(7) = 6$, and $3^1 \equiv 3$, $3^2 \equiv 2$, $3^3 \equiv 6$, $3^4 \equiv 4$, $3^5 \equiv 5$, $3^6 \equiv 1 \pmod 7$.

Exercises

1. Find $\varphi(8)$, $\varphi(19)$ and $\varphi(101)$.
2. Find $\lambda(8)$, $\lambda(19)$ and $\lambda(101)$.
3. Compute the order of 2 with respect to the prime modulo 3, 5, 7, 11, 13, 17, and 19.
4. Compute the order of -7 modulo 13

14 The Chinese Remainder Theorem

The Chinese Remainder Theorem is a structure theorem for the ring $\mathbb{Z}_n$. It is arguably the most important theorem in all of number theory!

The Chinese Remainder Theorem - CRT

Theorem 14.1. *Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime integers greater than 1, and let $a_1, a_2, \ldots, a_n$ be any integers. Then there is a solution x to the following system of simultaneous congruences:*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1}, \\ x &\equiv a_2 \pmod{n_2}, \\ &\vdots \\ x &\equiv a_n \pmod{n_n}. \end{aligned}$$

Furthermore, if x and x' are two solutions to the system, then

$$x \equiv x' \pmod{M},$$

where $M = n_1 n_2 \ldots n_n$ is the product of the modulo.

The **Chinese Remainder Theorem** states that if we have a system of congruences:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

where $n_1, n_2, \ldots, n_k$ are pairwise coprime, then there exists a unique solution modulo M,

Steps to Solve Using CRT

1. Compute $M = n_1 \times n_2 \times \cdots \times n_k$.
2. Compute $m_i = \frac{M}{n_i}$ for each i.
3. Find the modular x_i such that:

$$x_i \equiv m_i^{-1} \pmod{n_i}$$

4. Compute:

$$x = \sum_{i=1}^{k} x_i \cdot m_i \cdot a_i \pmod{M}$$

If $i = 2$, Then

$$x = x_1 m_1 a_1 + x_2 m_2 a_2 \pmod{M}$$

where

$x_1 \equiv m_1^{-1} \pmod{n_1}$, $m_1 = \frac{M}{n_1}$, $x_2 \equiv m_2^{-1} \pmod{n_2}$, $m_2 = \frac{M}{n_2}$, and $M = n_1 n_2$

Example 14.1. Solve the system:

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{4}$$

Step 1: Compute M

$$M = 3 \times 4 = 12$$

Step 2: Compute $m_i = \frac{M}{n_i}$

$$m_1 = \frac{12}{3} = 4, \quad m_2 = \frac{12}{4} = 3$$

Step 3: Compute the Modular Inverses

Find x_i such that $x_i \equiv m_i^{-1} \pmod{n_i}$:

$$x_1 \equiv 4^{-1} \pmod{3} \quad \Rightarrow \quad x_1 = 1$$

$$x_2 \equiv 3^{-1} \pmod{4} \quad \Rightarrow \quad x_2 = 3$$

Step 4: Compute x

$$x = x_1 m_1 a_1 + x_2 m_2 a_2 \pmod{M}$$

$$x = (1 \times 4 \times 2) + (3 \times 3 \times 3) \pmod{12}$$

$$x = (8) + (27) \pmod{12}$$

$$x = 35 \pmod{12}$$

$$x \equiv 11 \pmod{12}$$

Thus, the solution is:

$$x \equiv 11 \pmod{12}$$

Example 14.2. Solve the system:

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{4}$$

$$x \equiv 1 \pmod{5}$$

Step 1: Compute M

$$M = 3 \times 4 \times 5 = 60$$

Step 2: Compute $m_i = \frac{M}{n_i}$

$$m_1 = \frac{60}{3} = 20, \quad m_2 = \frac{60}{4} = 15, \quad M_3 = \frac{60}{5} = 12$$

Step 3: Compute the Modular Inverses

Find x_i such that $x_i \equiv m_i^{-1} \pmod{n_i}$:

$$x_1 \equiv 20^{-1} \pmod{3} \quad \Rightarrow \quad x_1 = 2$$

$$x_2 \equiv 15^{-1} \pmod{4} \quad \Rightarrow \quad x_2 = 3$$

$$x_3 \equiv 12^{-1} \pmod{5} \quad \Rightarrow \quad x_3 = 3$$

Step 4: Compute x

$$x = (2 \times 20 \times 2) + (3 \times 15 \times 3) + (1 \times 12 \times 3) \pmod{60}$$

$$x = (80) + (135) + (36) \pmod{60}$$

$$x = 251 \pmod{60}$$

$$x \equiv 11 \pmod{60}$$

Thus, the solution is:

$$x \equiv 11 \pmod{60}$$

Exercises

1. Find x satisfying:

$$x \equiv 3 \pmod 5$$

$$x \equiv 4 \pmod 7$$

2. Find x satisfying:

$$x \equiv 2 \pmod 3$$

$$x \equiv 3 \pmod 4$$

$$x \equiv 1 \pmod 5$$

3. Find x satisfying:

$$x \equiv 1 \pmod 6$$

$$x \equiv 3 \pmod 7$$

4. Find x satisfying:

$$x \equiv 2 \pmod 4$$

$$x \equiv 3 \pmod 5$$

$$x \equiv 4 \pmod 6$$

5. Solve the following system:

$$x \equiv 5 \pmod 9$$

$$x \equiv 7 \pmod{11}$$

$$x \equiv 3 \pmod{13}$$

$$x \equiv 1 \pmod{17}$$

15 Finite Galois Field

Finite Field

Definition 15.1. Galois field, is a field with a finite number of elements. A finite field with q elements is denoted as $\mathbb{F}_q$ (or $GF(q)$).

Prime Field

Theorem 15.1. *If p is prime number, Then $\mathbb{Z}_p$ prime field $\mathbb{F}_p$.*

For example $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7, \ldots, \mathbb{Z}_p = \mathbb{F}_p$ are field.

Remark 15.1. If the positive integer n is composite, $\mathbb{Z}_n$ is not a field.

For example $\mathbb{Z}_4, \mathbb{Z}_6, \mathbb{Z}_8, \mathbb{Z}_9, \ldots$ are not field.

Order of a Finite Field

Definition 15.2. The **order** of a finite field $\mathbb{F}_q$ is the number of distinct elements in $\mathbb{F}_q$ (denoted by $|\mathbb{F}_q|$).

For example $|\mathbb{F}_p| = p$, where $\mathbb{F}_p = \{0, 1, 2, \ldots p-1\}$.
If $p = 7$, $|\mathbb{F}_7| = 7$, where $\mathbb{F}_p = \{0, 1, 2, 3, 4, 5, 6\}$

Order of a Finite Field

Definition 15.3. The field $\mathbb{F}_{p^n}$, also denoted as $GF(p^n)$, is a **finite field** with p^n elements, where:

- p is a prime number (the **characteristic** of the field).
- n is a positive integer (the **degree** of the field extension).

It is an extension field of $\mathbb{F}_p$, meaning it contains $\mathbb{F}_p$ as a subfield.

Construction

The field $\mathbb{F}_{p^n}$ is constructed as follows:

1. Consider the prime field $\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$.

2. Choose an **irreducible polynomial** $f(x)$ of degree n over $\mathbb{F}_p$.

3. Define $\mathbb{F}_{p^n}$ as the set of all polynomials in x of degree less than n with coefficients in $\mathbb{F}_p$, where arithmetic is performed modulo $f(x)$.

Properties

- The multiplicative group $\mathbb{F}_{p^n}^{\times} = \mathbb{F}_{p^n} \setminus \{0\}$ of order $p^n - 1$, meaning there exists a **primitive element** g such that every nonzero element can be written as g^k for some k.

- Every element of $\mathbb{F}_{p^n}$ satisfies the equation:

$$x^{p^n} = x$$

  which characterizes the field.

Example: $\mathbb{F}_{2^3}$

Consider $p = 2$ and $n = 3$. The field $\mathbb{F}_{2^3}$ has $2^3 = 8$ elements.

To construct it:

- Start with $\mathbb{F}_2 = \{0, 1\}$.

- Choose an irreducible polynomial of degree 3 over $\mathbb{F}_2$, such as $f(x) = x^3 + x + 1$.

- The elements of $\mathbb{F}_{2^3}$ are represented as:

$$\{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$$

  where α is a root of $f(x)$ and a primitive element.

16 Discrete Logarithm Problem

The **Discrete Logarithm Problem** (DLP) is a fundamental mathematical problem in cryptography.

16.1 Definition of the Discrete Logarithm Problem

Let p be a large prime, there exists a **primitive root** g in the field $\mathbb{F}_p$. This means that every nonzero element of $\mathbb{F}_p$ can be written as some power of g.

In particular, by Fermat's Little Theorem:

$$g^{p-1} \equiv 1 \pmod{p}$$

and no smaller positive power of g is congruent to 1. Thus, the elements of the multiplicative group $\mathbb{F}_p$ are:

$$1, g, g^2, g^3, \ldots, g^{p-2}.$$

Definition of the Discrete Logarithm Problem (DLP)

Definition 16.1. Let g be a primitive root of $\mathbb{F}_p$, and let h be a nonzero element of $\mathbb{F}_p$. The **Discrete Logarithm Problem** is the problem of finding an exponent x such that:

$$g^x \equiv h \pmod{p}.$$

The number x is called the **discrete logarithm** of h to the base g and is denoted by:

$$\log_g(h).$$

16.2 Applications in Cryptography

The Discrete Logarithm Problem forms the basis for several cryptographic protocols, include **Diffie-Hellman Key Exchange**, **ElGamal Encryption** and **Digital Signature Algorithms**

17 Public-key cryptography

17.1 Introduction

Public-key cryptography, also known as **asymmetric cryptography**, is a cryptographic system that uses a pair of keys:

- A **public key**, which is shared openly.
- A **private key**, which is kept secret by the owner.

Unlike symmetric cryptography, where both the sender and receiver use the same key, public-key cryptography allows secure communication without prior key exchange.

17.2 Basic Concept

In a public-key cryptosystem, encryption and decryption are performed using different keys:

- The sender encrypts a message using the recipient's **public key**.
- The recipient decrypts the message using their **private key**.

The encryption function E and decryption function D satisfy:

$$D(K_{priv}, E(K_{pub}, M)) = M$$

where:

- M is the plaintext message.
- K_{pub} is the public key.
- K_{priv} is the private key.
- $E(K_{pub}, M)$ is the encrypted message (ciphertext).

17.3 Mathematical Foundation

Most public-key cryptosystems rely on mathematical problems that are computationally hard to solve. Commonly used problems include:

- **Integer Factorization Problem**: Used in RSA cryptosystem.
- **Discrete Logarithm Problem**: Used in Diffie-Hellman key exchange and ElGamal cryptosystem.
- **Elliptic Curve Discrete Logarithm Problem**: Used in elliptic curve cryptography (ECC).

17.4 Diffie-Hellman Key Exchange (DHKE)

Diffie-Hellman Key Exchange is an asymmetric cryptographic protocol for key exchange, and its security is based on the computational hardness of solving a discrete logarithm problem.

The Diffie–Hellman key exchange algorithm proceeds as follows:

- **Public Parameter Creation:** A trusted party chooses and publishes a large prime p and an integer g, where g has a large prime order in $\mathbb{F}_p$.
- **Private Computations:**
  - Alice chooses a secret integer a and computes $A \equiv g^a \pmod{p}$.
  - Bob chooses a secret integer b and computes $B \equiv g^b \pmod{p}$.
- **Public Exchange of Values:** Alice sends A to Bob, and Bob sends B to Alice.
- **Further Private Computations:**
  - Alice computes $S_A = B^a = (g^b)^a \pmod{p}$.
  - Bob computes $S_B = A^b = (g^a)^b \pmod{p}$.

  Both Alice and Bob will now have the same shared secret $S = S_A = S_B$, which can be used for further cryptographic operations.

17.4.1 Example of Diffie-Hellman Key Exchange

Let us consider an example where Alice and Bob agree on:

- A prime $p = 23$,
- A generator $g = 5$.

Step 1: Private Key Selection

- Alice chooses a secret integer $a = 6$.
- Bob chooses a secret integer $b = 15$.

Step 2: Compute Public Keys

$$A = g^a \mod p = 5^6 \mod 23 = 15625 \mod 23 = 8.$$

$$B = g^b \mod p = 5^{15} \mod 23 = 30517578125 \mod 23 = 19.$$

Step 3: Exchange Public Keys Alice sends $A = 8$ to Bob, and Bob sends $B = 19$ to Alice.

Step 4: Compute Shared Secret

$$S_A = B^a \mod p = 19^6 \mod 23 = 47045881 \mod 23 = 2.$$

$$S_B = A^b \mod p = 8^{15} \mod 23 = 35184372088832 \mod 23 = 2.$$

Since both Alice and Bob compute the same shared secret $S = 2$, they can now use it for encryption.

17.4.2 Diffie-Hellman Key Exchange Analysis

The security of the Diffie-Hellman key exchange is based on the fact that it is difficult to calculate discrete logarithms in a finite field. An attacker who intercepts the public values A and B would need to solve the discrete logarithm problem to calculate the shared secret key, which is computationally infeasible for large prime numbers.

17.5 ElGamal Cryptosystem

The ElGamal encryption algorithm is a public key cryptography algorithm that uses a key pair consisting of a private key and a public key. The algorithm involves three steps: key generation, encryption, and decryption.

The following are the steps involved in the ElGamal encryption algorithm:

1. **Key generation**:
   (a) Choose a large prime p and a generator g in the multiplicative $\mathbb{F}_p$.
   (b) Alice selects a secret key a such that $1 \leq a \leq p-1$.
   (c) Compute $h = g^a \pmod{p}$.
   (d) The public key is (p, g, h), and the private key is a.
2. **Encryption**:
   (a) Let m be the message to be encrypted, where $0 \leq m \leq p-1$.
   (b) Bob selects a random integer k such that $1 \leq k \leq p-1$.
   (c) Compute $c_1 = g^k \pmod{p}$ and $c_2 = m \cdot h^k \pmod{p}$.
   (d) Send (c_1, c_2) to Alice.
3. **Decryption**:
   (a) (c_1, c_2) the ciphertext.
   (b) Alice Computes $m = c_2 \cdot (c_1^a)^{-1} \pmod{p}$. This value is the same as plaintext m.

17.5.1 Example of ElGamal Cryptosystem

1. **Key generation**:
   (a) Choose a large prime $p = 467$ and a generator $g = 2$ in the multiplicative group $\mathbb{F}_p$.

(b) Alice selects a secret key $a = 153$ such that $1 \leq a \leq p - 1$.

(c) Compute $h = g^a \pmod{p} = 2^{153} \pmod{467} = 63$.

(d) The public key is $(p, g, h) = (467, 2, 63)$, and the private key is $a = 153$.

2. **Encryption**:

(a) Let $m = 123$ be the message to be encrypted, where $0 \leq m \leq p - 1$.

(b) Bob selects a random integer $k = 85$ such that $1 \leq k \leq p - 1$.

(c) Compute:

$$c_1 = g^k \pmod{p} = 2^{85} \pmod{467} = 61$$

$$c_2 = m \cdot h^k \pmod{p} = 123 \cdot 63^{85} \pmod{467} = 123 \cdot 217 \pmod{467} = 85$$

(d) Send $(c_1, c_2) = (61, 85)$ to Alice.

3. **Decryption**:

(a) Received $(c_1, c_2) = (61, 85)$ as the ciphertext.

(b) Alice computes:

$$s = c_1^a \pmod{p} = 61^{153} \pmod{467} = 217$$

(c) Find the inverse of $s \mod p$. Using Extended Euclidean Algorithm, we get:

$$s^{-1} = 217^{-1} \pmod{467} = 127$$

(d) Recover the message m:

$$m = c_2 \cdot s^{-1} \pmod{p} = 85 \cdot 127 \pmod{467} = 123$$

(e) Thus, the decrypted message is $m = 123$, which is the same as the original plaintext.

17.5.2 ElGamal Analysis

The security of the ElGamal encryption algorithm is based on the hardness of the discrete logarithm problem. Given a large prime p and a primitive root g modulo p, and given $h \equiv g^a \pmod{p}$ for some secret key a, it is computationally infeasible to find a from p, g, and h. This is known as the discrete logarithm problem, and it is to be a hard problem.

The security of the ElGamal encryption algorithm also depends on the randomness of the key used for encryption. If the same key k is used to encrypt multiple messages, an attacker can use the ciphertexts to find the secret key a. Therefore, it is important to choose a different key k for each message that is encrypted.

In addition, the security of the ElGamal encryption algorithm can be enhanced by using a large prime p and a large secret key a. The security of the algorithm also depends on the security of the random number generator used to generate the secret key a and the encryption key k. If the random number generator is predictable, an attacker may be able to predict the secret key a or the encryption key k and break the encryption.

In general, the security of the ElGamal encryption algorithm is considered to be strong, and it is widely used in practice. However, it is important to use appropriate key sizes and follow best practices for key management to maintain the security of the algorithm.

17.6 RSA Cryptosystem

Public and private keys are both used in RSA algorithm. The public key, which is used to convert communications from plaintext to ciphertext, can be known and released to anybody. However, only the accompanying private key may be used to decode communications that have been encrypted using this particular public key. The RSA algorithm's key generation procedure, which has a high level of complexity compared to other cryptosystem methods, is what makes it so safe and dependable today.

The following are the steps involved in the RSA algorithm:

Step 1: Key Generation

1. Alice selects two distinct large prime numbers p and q.
2. Compute $n = p \cdot q$.
3. Compute Euler's Totient function $\varphi(n) = (p-1)(q-1)$
4. Choose an encryption exponent e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$.
5. Compute the decryption exponent d such that:

$$d \cdot e \equiv 1 \mod \varphi(n)$$

6. Alice's public key: (e, n).
7. Alice's private key: (d, n).

Step 2: Encryption (Bob to Alice)

1. Bob obtains Alice's public key (e, n).
2. Represent the message M as an integer where $M < n$.
3. Compute the ciphertext C:

$$C = M^e \mod n$$

4. Bob sends C to Alice.

Step 3: Decryption (Alice's Side)

1. Upon receiving C, Alice uses her private key (d, n).
2. Recover the original message M:

$$M = C^d \mod n$$

17.6.1 Example of RSA Public Key Cryptosystem

Step 1: Key Generation

1. Choose two prime numbers: $p = 11, q = 13$.
2. Compute $n = p \cdot q = 11 \times 13 = 143$.
3. Compute Euler's Totient:

$$\varphi(n) = (p-1)(q-1) = 10 \times 12 = 120$$

4. Choose public exponent $e = 7$ such that $\gcd(7, 120) = 1$.
5. Compute the private key d such that:

$$d \cdot e \equiv 1 \mod 120$$

   The solution is $d = 103$.

6. Public key: $(e = 7, n = 143)$.
7. Private key: $(d = 103, n = 143)$.

Step 2: Encryption (Bob to Alice)

1. Message $M = 9$.
2. Compute ciphertext C:

$$C = M^e \mod n = 9^7 \mod 143 = 48$$

3. Bob sends $C = 48$ to Alice.

Step 3: Decryption (Alice's side)

1. Compute the original message M:

$$M = C^d \mod n = 48^{103} \mod 143 = 9$$

2. Alice recovers the message $M = 9$.

Result: The decrypted message is $M = 9$.

17.6.2 RSA Analysis

The security of the RSA cryptosystem is fundamentally based on the computational difficulty of factorizing the product $n = p \cdot q$, where p and q are large prime numbers. As of now, no efficient algorithm exists for factorizing large numbers in polynomial time, making RSA secure if appropriately large primes are used. The hardness of this factorization problem is what prevents adversaries from deriving the private key from the public key. The larger the primes, the more secure the system becomes, as the time required to factorize n grows exponentially with its size.

A crucial aspect of RSA security is the choice of key size. Commonly used key sizes are 2048 bits or greater, which are currently considered secure against brute-force attacks. Increasing the key size exponentially increases the difficulty of factorization and ensures that the encryption remains safe even with advances in computational power. However, larger key sizes also demand more processing power for encryption and decryption, creating a trade-off between security and performance.

Despite its robustness, RSA is vulnerable to several potential attacks. One of the primary threats is brute-force attacks, which involve attempting all possible keys until the correct one is found. This method, however, becomes infeasible with sufficiently large key sizes. Mathematical attacks focus on exploiting weaknesses in the number theory behind RSA, primarily through factorization techniques. Factoring attacks directly target the difficulty of breaking n into p and q. Another mathematical approach, discrete logarithm attacks, is impractical for RSA due to the nature of modular arithmetic.