



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



1st class

2024-2025

Number Theory

Lecture 2

Asst. Lect. Mohammed Jabbar

mohammed.jabbar.obaid@uomus.edu.iq

الرياضيات :المرحلة الاولى **نظرية الاعداد** المحاضرة الثانية

استاذ المادة: م.م محمد جبار



Cybersecurity Department قسم الأمن السيبراني

Contents

1	Algebra Preliminaries			1
	1.1	Sets .		1
1.2 Integer and Natural Numbers		and Natural Numbers	1	
		1.2.1	Basic Properties of Natural Numbers	2
		1.2.2	Basic Properties of Integer Numbers	3
		1.2.3	Laws of Exponents	4
		1.2.4	Properties of Inequalities	5
	1.3	Even a	nd Odd Numbers	5

1 Algebra Preliminaries

1.1 Sets

Definition 1.1. A set is a well-defined collection of distinct objects, called **elements**, enclosed in curly brackets {}.

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

Examples of Sets

- Finite Set: $A = \{1, 2, 3, 4, 5\}$
- Infinite Set: $B = \{1, 2, 3, ...\}$
- 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)

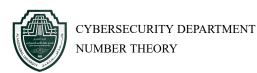
1.2 Integer and Natural Numbers

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

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



1.2.1 Basic Properties of Natural Numbers

Addition in $\ensuremath{\mathbb{N}}$

- 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.

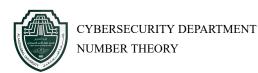
Multiplication in \mathbb{N}

- 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 $\ensuremath{\mathbb{N}}$

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



1.2.2 Basic Properties of Integer Numbers

Addition in $\ensuremath{\mathbb{Z}}$

- 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.

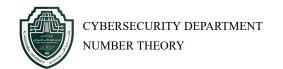
Subtraction in $\ensuremath{\mathbb{Z}}$

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}

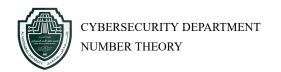
Division is not a closed operation in \mathbb{Z} . For example, $3 \div 2$ is not an integer.

Important Theorem Theorem 1.1. Let $a, b \in Z$, Then: *1.* $a \cdot 0 = 0 \cdot a = 0$ 2. (-a)b = a(-b) = -ab3. (-a)(-b) = ab1. 0 + 0 = 0 (Identity element in \mathbb{Z}) Proof. $\Rightarrow (0+0)a = 0a \Rightarrow 0a + 0a = 0a$ $\Rightarrow 0a + 0a + (-0a) = 0a + (-0a)$ (inverse in \mathbb{Z}) $\Rightarrow 0a = 0$ Similarly a0 = 02. b + (-b) = 0 (inverse in \mathbb{Z}) $\Rightarrow a(b + (-b)) = a0 = 0 \text{ (From (1))}$ $\Rightarrow ab + a(-b) = ab + (-ab) \Rightarrow a(-b) = -ab$ 3. (-a)(-b) = abIn (2), replace a by $(-a) \Rightarrow (-a)(-b) = -((-a)b) = -(-ab) = ab$

1.2.3 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: $\frac{a^m}{a^n} = a^{m-n}$, for $m \ge n$, $a \ne 0$
- 3. Power of a Power: $(a^m)^n = a^{m \cdot n}$
- 4. Power of a Product: $(ab)^n = a^n \cdot b^n$



1.2.4 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.
- Multiplication by a Negative Number: If a < b and c < 0, then ac > bc (the inequality sign reverses).

1.3 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