2.1. Introduction

Number theory is that branch of mathematics that deals with the properties of integers, more specifically, the properties of positive integers or natural numbers. The first scientific approach to the study of integers (i.e, true origin of the theory of numbers) is attributed to the Greeks. Around 600 BC, Pythagoras and his disciples made thorough study of integers. Euclid, Diophantus, Fermat, Euler, Gauss, Goldbach, Dirichlet and Ramanujan were among the main contributors of the theory of numbers.

Number theory has enormous application in diverse field of study. Though it was viewed as a subject of pure mathematics, number theory now has been applied to the problems asociated with transmission, coding and manipulation of numeric data and also in digital domain. Number system has major contribution in complexity analysis of algorithms, generating random numbers in simulation, developing hash functions in memory addressing, generation of highly secured codes for ATM and others, determination of check digits in ATM, UPC and ISBN codes, in the study of cryptography - specially in the study of authorization and authentication verification with digital signature, and many more.

In this chapter we introduce some basic properties of integers and congruence relation and their applications.

2.2. Positive Integers

Positive integers or natural numbers evolve from the concept of counting. While counting, we make a one-to-one correspondence between the set of real objects in hand and a set of abstract objects. This second set of abstract objects is embodied into the set of positive integers (or natural numbers) which is an abstract notion manifested through our perception. However, G. Peano axiomatized the set of natural numbers (or positive integers) as follows.

Peano's Axioms

A set $\mathbb{N}$ of objects is called the set of natural numbers if it satisfies the following axioms called ***Peano's axioms :***

Axiom **1.** $1 \in \mathbb{N}$.

Axiom **2.** To each element $n \in \mathbb{N}$, there corresponds a unique element $n' \in \mathbb{N}$, called the successor of n.

Axiom **3.** For each $n \in \mathbb{N}$, we have $n' \neq 1$.

Axiom **4.** If $m, n \in \mathbb{N}$ such that $m' = n' \Rightarrow m = n$

or, $m \neq n \Rightarrow m' \neq n'$.

Axiom **5.** If M be a set of elements of $\mathbb{N}$ i.e, $M \subseteq \mathbb{N}$ then $M = \mathbb{N}$ provided the following two conditions are satisfied

(i) $1 \in M$.

(ii) If $k \in M$ then $k' \in M$, k' being the successor of k.

We observe the following :

- $\mathbb{N}$ is nonempty (Axiom 1).
- $1' \in \mathbb{N}$ (Axiom 2) and $2' \neq 1$ (Axiom 3) and $2' \neq 2$ (Axiom 4) since $2' \neq 1$. We call $2'$ as 3. Thus $1, 2, 3 \in \mathbb{N}$. Proceeding in this way we generate the successive natural numbers calling them as $3' = 4$, $4' = 5$ and so on.
- Axiom 5 is known as the "*Principle of Mathematical Induction*" which is restated as follows :

Principle of Mathematical Induction

Let for each $n \in \mathbb{N}$, $P(n)$ be a proposition or statement.

Let $P(1)$ be true.

If $P(n')$ be true whenever $P(n)$ is true, then $P(n)$ is true for all $n \in \mathbb{N}$, n' being the successor of n.

Well-ordering Principle

Every nonempty subset A of the set $\mathbb{N}$ of natural numbers has a least element.

Remark. By the "*least element of a set A*" it is meant that there exists an element $x \in A$ such that $x \leq y$, $\forall y \in A$.

Theorem 2.1. The Well-ordering Principle is equivalent to the Principle of Mathematical Induction.

***Proof*.** Let the Well-ordering Principle hold. Let M be the set of natural numbers with the property that

- $1 \in M$,
- Whenever $n \in M$, $n+1 \in M$.

The above two properties of M are the two conditions of the Principle of Mathematical Induction. Hence to establish this principle it is required to prove that $M = \mathbb{N}$.

Let F be the set of natural numbers with the property that $x \in F \Leftrightarrow x \notin M$.

Then $M \cup F = \mathbb{N}$ and $M \cap F = \phi$.

If we can prove that $F = \phi$, then it will immediately follow that $M = \mathbb{N}$.

Let, if possible, $F \neq \phi$. Then by the Well-ordering Principle, there exists a least element m of F, i.e., $\exists\, m \in F$ such that $m \leq n$, $\forall n \in F$.

We note that $1 \neq m$, since $1 \in M$. $\therefore\ 1 \notin F$.

Since m is the least element of F, $m-1 \notin F$ and so $m-1 \in M$.

Since $m - 1 \in M$, then by our construction of M, $(m-1)+1 \in M$, i.e., $m \in M$ which is a contradiction as $m \in F$ and $M \cap F = \phi$.

Hence $F = \phi$. Thus $M = \mathbb{N}$ and the Principle of Mathematical Induction is established.

Conversely, let Principle of Mathematical Induction holds.

Let $A \subseteq \mathbb{N}$ and $A \neq \phi$. Also let A has no least element.

We construct a set M of natural numbers as follows :

$M = \{ x : x \in \mathbb{N}$ and $x < a$ for every $a \in A \}$.

Thus $x \in M$ and $a \in A \Leftrightarrow a > x$.

This is true for all $x \in M$ and for all $a \in A$.

Hence $M \cap A = \phi$. It also imply that $M \cup A = \mathbb{N}$.

Now $1 \notin A$; for, otherwise, 1 would become the least element of A and we have assumed that A has no least element.

$\therefore 1 \in M$. Then $1 < a, \forall a \in A$.

Let us assume that $p \in M$. Then $p < a$ for $\forall a \in A$.

We assert that $p+1 \notin A$; for if $p+1 \in A$, then $p+1$, being the next natural number larger than p, would become the least element of A, but A has no least element (by our assumption).

Hence $p+1 \in M$.

Thus $1 \in M$ and $p \in M \Rightarrow p+1 \in M$.

Hence by the Principle of Mathematical Induction $M = \mathbb{N}$.

But $M \cap A = \phi \Rightarrow N \cap A = \phi \Rightarrow A = \phi$ which contradicts our assumption that A is a nonempty subset of $\mathbb{N}$. Hence A must have a least element.

Thus Well-ordering Principle is established.

It implies that each of the two principles, namely, Well ordering Principle and Principle of Mathematical Induction, is deducible from the other. Hence they are equivalent.

Note 1. *Negative Integers :* We introduce the symbols $-1, -2, -3, \ldots$ and call them negative integers corresponding to the positive integers 1, 2, 3, ...respectively.

Zero : We define 0 (zero) with the following properties :

(i) $0 + a = a + 0 = a, \forall a \in \mathbb{N}$ (ii) $0.a = a.0 = 0, \forall a \in \mathbb{N}$.

We then introduce the set $\mathbb{Z}$ of all integers as

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

2.3. Divisibility Theory

An integer a is said to be divisible by an integer $b(\neq 0)$ if there exists an integer q such that $a = bq$.

The statement "*a is divisible by b*" or "*b divides a*" is denoted by $b \mid a$.

If $b \mid a$ we can say "*a is a multiple of b*".

If $b \mid a$ then $-b \mid a$, because $b \mid a \Rightarrow \exists q$ such that $a = bq$ $\Rightarrow a = (-b)(-q) \Rightarrow -b \mid a$ since $-q$ is an integer.

Thus divisors of an integer occur in pairs.

Theorem 2.2. For any integers a, b, c and d the following statements hold :

(i) $a \mid 0$, $1 \mid a$ and $a \mid a$.

(ii) $x \mid y \Rightarrow ax \mid ay$, $\forall a \in \mathbb{Z}$.

(iii) $a \mid b$ and $c \mid d \Rightarrow ac \mid bd$.

(iv) $a \mid b$ and $b \mid c \Rightarrow a \mid c$. (Transitivity)

(v) $a \mid b$ and $b \mid a \Rightarrow a = \pm b$.

(vi) $a \mid b$ and $a \mid c \Rightarrow a \mid (bx+cy)$, for arbitrary integers x, y.

Proof. (i) and (ii) are obvious.

(iii) $a \mid b \Rightarrow b = ap$ for some integer p. $c \mid d \Rightarrow d = cq$ for some integer q.

$\therefore bd = ac(pq) \Rightarrow ac \mid bd$ as pq is an integer.

(iv) $a \mid b \Rightarrow b = ap$ for some integer p.

Also $b \mid c \Rightarrow c = bq$ for some integer q.

$\therefore \quad c = a(pq) \Rightarrow a \mid c$ as pq is an integer.

(v) Left to the reader.

(vi) $a \mid b \Rightarrow b = ap$ for some integer p.

$a \mid c \Rightarrow c = aq$ for some integer q.

$\therefore$ for arbitrary integers x and y, we have

$bx + cy = apx + aqy = a(px + qy)$

$\Rightarrow a \mid (bx+cy)$ since $px+qy$ is an integer as p, q, x, y are integers.

Remark. We use the symbol ' $\nmid$ ' to mean '*does not divide*'. Thus $b \nmid a$ means '*b does not divide a*' or '*a is not divisible by b*'.