Number theory

1 INTRODUCTION

This chapter investigates some basic properties of the *natural numbers* (or *positive integers*), that is, the set

$$\mathbf{N} = \{1, 2, 3, \ldots\}$$

and their "cousins," the integers, that is, the set

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

(The letter **Z** comes from the word "Zahlen" which means numbers in German.)

The following simple rules concerning the addition and multiplication of these numbers are assumed (where a, b, c are arbitrary integers):

(a) Associative law for multiplication and addition:

$$(a + b) + c = a + (b + c) \quad \text{and} \quad (ab)c = a(bc)$$

(b) Commutative law for multiplication and addition:

$$a + b = b + a \quad \text{and} \quad ab = ba$$

(c) Distributive law:

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

(d) Additive identity 0 and multiplicative identity 1:

$$a + 0 = 0 + a = a \quad \text{and} \quad a \cdot 1 = 1 \cdot a = a$$

(e) Additive inverse $-a$ for any integer a:

$$a + (-a) = (-a) + a = 0$$

2 ORDER AND INEQUALITIES, ABSOLUTE VALUE

This section discusses the elementary properties of order and absolute value.

Order

Observe that we define order in **Z** in terms of the positive integers **N**. All the usual properties of this order relation are a consequence of the following two properties of **N**:

[P_1] If a and b belong to **N**, then $a + b$ and ab belong to **N**.

[P_2] For any integer a, either $a \in \mathbf{N}$, $a = 0$, or $-a \in \mathbf{N}$.

The following notation is also used:

$a > b$ means $b < a$;	read: a is greater than b.
$a \leq b$ means $a < b$ or $a = b$;	read: a is less than or equal to b.
$a \geq b$ means $b \geq a$;	read: a is greater than or equal to b.

The relations $<$, $>$, $\leq$ and $\geq$ are called *inequalities* in order to distinguish them from the relation $=$ of equality. The reader is certainly familiar with the representation of the integers as points on a straight line, called the *number line* **R**, as shown in Fig. 1.

Fig. 1

We note that $a < b$ if and only if a lies to the left of b on the number line **R** in Fig. 1. For example,

$$2 < 5; \quad -6 < -3; \quad 4 \leq 4; \quad 5 > -8; \quad 6 \geq 0; \quad -7 \leq 0$$

We also note that a is positive iff $a > 0$, and a is negative iff $a < 0$. (Recall "iff" means "if and only if.") Basic properties of the inequality relations follow.

Proposition 1 : The relation $\leq$ in **Z** has the following properties:

(i) $a \leq a$, for any integer a.

(ii) If $a \leq b$ and $b \leq a$, then $a = b$.

(iii) If $a \leq b$ and $b \leq c$, then $a \leq c$.

Proposition 2 (Law of Trichotomy): For any integers a and b, exactly one of the following holds:

$$a < b, \quad a = b, \quad \text{or} \quad a > b$$

Proposition 3: Suppose $a \leq b$, and let c be any integer. Then:

(i) $a + c \leq b + c$.

(ii) $ac \leq bc$ when $c > 0$; but $ac \leq bc$ when $c < 0$.

Absolute Value

The *absolute value* of an integer a. written $|a|$, is formally defined by

$$|a| = \begin{cases} a & \text{if } a \geq 0 \\ -a & \text{if } a < 0 \end{cases}$$

Accordingly, $|a| > 0$ except when $a = 0$. Geometrically speaking, $|a|$ may be viewed as the distance between the points a and 0 on the number line **R**. Also, $|a - b| = |b - a|$ may be viewed as the distance between the points a and b. For example:

(a) $|-3| = 3$; $|7| = 7$; $|-13| = 13$; (b) $|2 - 7| = |-5| = 5$; $|7 - 2| = |5| = 5$

Proposition 4: Let a and b be any integers. Then:

(i) $|a| \geq 0$, and $|a| = 0$ iff $a = 0$
(ii) $-|a| \leq a \leq |a|$
(iii) $|ab| = |a||b|$
(iv) $|a \pm b| \leq |a| + |b|$
(v) $||a| - |b|| \leq |a \pm b|$

DIVISION ALGORITHM

The following fundamental property of arithmetic is essentially a restatement of the result of long division.

Theorem (**Division Algorithm**): Let a and b be integers with $b \neq 0$. Then there exists integers q and r such that

$$a = bq + r \quad \text{and} \quad 0 \leq r < |b|$$

Also, the integers q and r are unique.

The number q in the above theorem is called the *quotient*, and r is called the *remainder*. We stress the fact that r must be non-negative. The theorem also states that

$$r = a - bq$$

This equation will be used subsequently

If a and b are positive, then q is non negative. If b is positive, then Fig. 2 gives a geometrical interpretation of this theorem. That is, the positive and negative multiples of b will be evenly distributed throughout the number line **R**, and a will fall between some multiples qb and $(q + 1)b$. The distance between qb and a is then the remainder r.

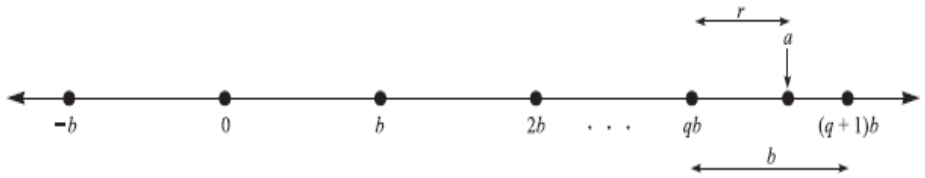

Fig. 2

EXAMPLE

(a) Let $a = 4461$ and $b = 16$. We can find that the quotient $q = 278$ and the remainder $r = 13$ by long division, Alternately, using a calculator, we obtain q and r as follows:

$$a/b = 278.8125\ldots, \quad q = 278, \qquad r = 4461 - 16(278) = 13$$

As expected, $a = bq + r$, namely:

$$4461 = 16(278) + 13$$

(b) Let $a = -262$ and $b = 3$. First we divide $|a| = 262$ by $b = 3$. This yields a quotient $q' = 87$ and a remainder $r' = 1$. Thus

$$262 = 3(87) + 1$$

We need $a = -262$, so we multiply by -1 obtaining

$$-262 = 3(-87) - 1$$

However, -1 is negative and hence cannot be r. We correct this by adding and subtracting the value of b (which is 3) as follows:

$$-262 = 3(-87) - 3 + 3 - 1 = 3(-88) + 2$$

Therefore, $q = -88$ and $r = 2$.

(c) Let $b = 2$. Then any integer a can be written in the form

$$a = 2q + r \quad \text{where} \quad 0 \leq r < 2$$

Thus r can only be 0 or 1. Thus every integer is of the form $2k$ or $2k + 1$. The integers of the form $2k$ are called *even* integers, while those of the form $2k + 1$ are called *odd* integers. (Usually, an even integer is defined as an integer divisible by 2, and all other integers are said to be odd. Thus the division algorithm proves that every odd integer has the form $2k + 1$.)

DIVISIBILITY, PRIMES

Let a and b be integers with $a \neq 0$. Suppose $ac = b$ for some integer c. We then say that a divides b or b is divisible by a, and we denote this by writing

$$a \mid b$$

We also say that b is a *multiple* of a or that a is a *factor* or *divisor* of b. If a does not divide b, we will write $a \nmid b$.

EXAMPLE

(a) Clearly, $3 \mid 6$ since $3 \cdot 2 = 6$, and $-4 \mid 28$ since $(-4)(-7) = 28$.

(b) The divisors of 4 are $\pm 1, \pm 2, \pm 4$ and the divisors of 9 are $\pm 1, \pm 3, \pm 9$.

(c) If $a \neq 0$, then $a \mid 0$ since $a \cdot 0 = 0$.

(d) Every integer a is divisible by ± 1 and $\pm a$. These are sometimes called the *trivial divisors* of a. The basic properties of divisibility is stated in the next theorem

Theorem : Suppose a, b, c are integers.

(i) If $a \mid b$ and $b \mid c$, then $a \mid c$.

(ii) If $a \mid b$ then, for any integer x, $a \mid bx$.

(iii) If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$ and $a \mid (b - c)$.

(iv) If $a \mid b$ and $b \neq 0$, then $a = \pm b$ or $|a| < |b|$.

(v) If $a \mid b$ and $b \mid a$, then $|a| = |b|$, i.e., $a = \pm b$.

(vi) If $a \mid 1$, then $a = \pm 1$

Putting (ii) and (iii) together, we obtain the following important result.

Corollary : Suppose $a \mid b$ and $a \mid c$. Then, for any integers x and y, $a \mid (bx + cy)$. The expression $bx + cy$ will be called a *linear combination* of b and c.