Chapter 2

Sets and Elementary Properties of the Real Numbers

2.1 INTRODUCTION

This chapter investigates some sets and basic properties of the real numbers **R** and the integers

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

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

The following simple rules concerning the addition and multiplication of these numbers are assumed:

(*a*) Associative law for multiplication and addition:

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

(*b*) Commutative law for multiplication and addition:

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

(*c*) Distributive law:

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

(*d*) Additive identity and multiplicative identity: There exists a zero element 0 and a unity element 1 such that, for any number a,

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

(*e*) Additive inverse (negative): For any number a, there exists its negative $-a$ such that

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

(*f*) Multiplicative inverse: For any number $a \neq 0$, there exists an inverse a^{-1} such that

$$a \cdot a^{-1} = a^{-1} \cdot a = 1$$

Subtraction and division (except by 0) are defined in **R** by

$$a - b \equiv a + (-b) \qquad \text{and} \qquad a \cdot b^{-1}$$

Observe that subtraction uses property (*e*) of negatives, and division uses property (*f*) of inverses.

Warning. The last property (*f*) holds for the real numbers **R** and the rational numbers **Q**, but does not hold for the integers **Z**. That is, one can add, subtract, multiply, and divide (except by 0) in **R** and **Q**, but only add, subtract, and multiply in **Z**.

2.2 REAL NUMBER SYSTEM R

The notation **R** will be used to denote the real numbers. These are the numbers one uses in basic arithmetic and algebra. **R** together with its properties is called the *real number system.*

The set **R** of real numbers includes the following sets of numbers:

$$\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} = \text{ set of } \textit{integers} \text{ (signed whole numbers)}$$
$$\mathbf{P} = \{1, 2, 3, \ldots\} = \text{ set of positive integers (counting numbers)}$$
$$\mathbf{N} = \{0, 1, 2, \ldots\} = \text{ set of nonnegative integers (natural numbers)}$$
$$\mathbf{Q} = \text{ set of } \textit{rational numbers}, \text{ i.e. numbers which are ratios of integers}$$

Examples of rational numbers are $2/3$ and $-3/4$. Those real numbers that are not rational, such as π and $\sqrt{2}$, i.e., real numbers which cannot be represented as the ratio of integers, are called *irrational numbers*. The integer 0 is also a real number. Furthermore, for each positive real number, there is a corresponding negative real number.

Real Line R, Decimal Expansion

One of the most important properties of the real numbers is that they can be represented graphically by points on a straight line. Specifically, as pictured in Fig. 2-1, a point, called the *origin*, is chosen to represent 0, and another point, usually to the right of 0, is chosen to represent 1. The direction from 0 to 1 is the *positive direction* and is sometimes indicated by an arrowhead at the end of the line. The distance between 0 and 1 is the *unit length*. Now there is a natural way to pair off the points on the line and the real numbers, that is, where each point on the line corresponds to a unique real number and vice versa. The positive real numbers are those to the right of 0 (on the same side as 1) and the negative numbers are those to the left of 0. The points representing the rational numbers $5/4$ and $-3/2$ are indicated in Fig. 2-1. We refer to such a line as the *real line* or the *real line* **R**.

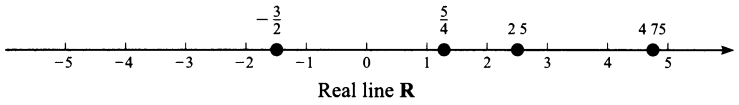

Fig. 2-1

Real numbers can also be represented by decimals. The decimal expansion of a rational number will either stop as in $\frac{3}{4} = 0.75$ or will have a pattern that repeats indefinitely, such as $\frac{17}{11} = 1.545454\ldots$. Even when the decimal expansion stops, it can be rewritten using repeated 9's, for example, $\frac{3}{4} = 0.74999\ldots$. The decimal expansion of an irrational number never stops nor does it have a repeating pattern. The points representing the decimal 2.5 and 4.75 are indicated in Fig. 2-1.

2.3 ORDER AND INEQUALITIES

Let a and b be real numbers. We say a is *less* than b, written

$$a < b$$

if the difference $b - a$ is positive. Geometrically, $a < b$ if and only if the point a lies to the left of the point b on the real line **R**.

Observe that we define order in **R** in terms of the positive real numbers denoted by $\mathbf{R}^+$. All the usual properties of this order relation are a consequence of the following two properties of the positive real numbers $\mathbf{R}^+$:

$[\mathbf{P}_1]$ If a and b are positive, then $a + b$ and ab are positive.
$[\mathbf{P}_2]$ For any real number a, either a is positive, $a = 0$, or $-a$ is positive.

The following additional notation and terminology are 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 $b \leq a$;	read: *a is greater than or equal to b*

Any statement of the form $a < b$, $a \leq b$, $a > b$, or $a \geq b$ is called an *inequality*; and any statement of the form $a < b$ or $a > b$ is sometimes called a *strict inequality*.

EXAMPLE 2.1

(*a*) $2 < 5$; $-6 < -3$; $4 \leq 4$; $5 > -8$; $6 \geq 0$; $-7 \leq 0$.

(*b*) Sorting the numbers 4, −7, 9, −2, 6, 0, −11, 13, −1, −5 in increasing order we obtain:

$$-11, -7, -5, -2, -1, 0, 3, 4, 6, 9, 13$$

(*c*) A real number a is positive iff $a > 0$, and a is negative iff $a < 0$. (Recall that "iff" is short for "if and only if.")

(*d*) The statement $2 < x < 7$ means $2 < x$ and $x < 7$; hence x will lie between 2 and 7 on the real line $\mathbf{R}$.

Basic properties of the inequality relations follow.

Proposition 2.1: Let a, b, c be real numbers. Then:

(i) $a \leq a$.
(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 2.2 (Law of Trichotomy): For any real numbers a and b, exactly one of the following holds:

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

Proposition 2.3: Let a, b, c be real numbers such that $a \leq b$. Then:

(i) $a + c \leq b + c$.
(ii) $ac \leq bc$ when $c > 0$; but $ac \geq bc$ when $c < 0$.

Remark: Observe that the above two properties $[\mathbf{P}_1]$ and $[\mathbf{P}_2]$ of the positive real numbers $\mathbf{R}^+$ are also true for the positive rational numbers $\mathbf{Q}^+$ viewed as a subset of the rational numbers $\mathbf{Q}$, and the positive integers $\mathbf{P} = \mathbf{Z}^+$ viewed as a subset of the integers $\mathbf{Z}$. Accordingly, Propositions 2.1, 2.2, and 2.3 also hold for the rational numbers $\mathbf{Q}$ and the integers $\mathbf{Z}$.

2.4 ABSOLUTE VALUE, DISTANCE

The *absolute value* of a real number a, denoted by $|a|$, may be viewed as the distance between a and the origin 0 on the real line $\mathbf{R}$. Formally, $|a| = a$ or $-a$ according as a is positive or negative, and $|0| = 0$. That is:

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

Accordingly, $|a|$ is always positive when $a \neq 0$. Intuitively, $|a|$ may be viewed as the magnitude of a without regard to sign.

The distance d between two points (real numbers) a and b is denoted by $d(a, b)$ and is obtained from the formula

$$d = d(a, b) = |a - b| = |b - a|$$

Alternatively:

$$d = \begin{cases} |a| + |b|, & \text{if } a \text{ and } b \text{ have different signs} \\ |a| - |b|, & \text{if } a \text{ and } b \text{ have the same sign and } |a| \geq |b| \end{cases}$$

These two cases are pictured in Fig. 2-2.

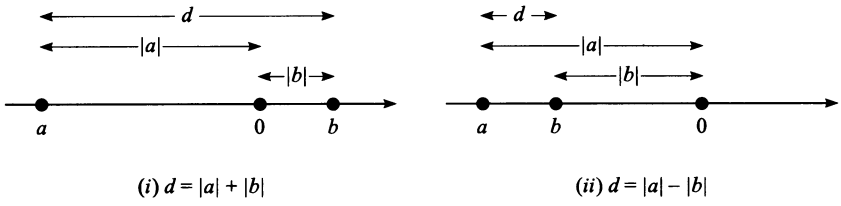

Fig. 2-2

EXAMPLE 2.2

(*a*) $|-3| = 3$, $|7| = 7$, $|-13| = 13$, $|4.25| = 4.25$, $|-0.75| = 0.75$.

(*b*) $|2-7| = |-5| = 5$, $|7-2| = |5| = 5$, $|-3-8| = |-11| = 11$.

(*c*) Using Fig. 2-2,

$$d(-2,9) = 2+9 = 11, \qquad d(5,8) = 8-5 = 3, \qquad d(-4,-11) = 11-4 = 7$$

The following proposition gives some properties of the absolute value function. [Problems 2.14 and 2.15 prove (iii) and (iv).]

Proposition 2.4: Let a and b be any real numbers.

(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) $||a| - |b|| \leq |a \pm b|$.

2.5 INTERVALS

Let a and b be distinct real numbers with, say, $a < b$. The *intervals* with *endpoints* a to b are denoted and defined as follows:

$$(a,b) = \{x : a \leq x \leq b\}, \quad \text{open interval from } a \text{ to } b$$
$$[a,b] = \{x : a \leq x \leq b\}, \quad \text{closed interval from } a \text{ to } b$$
$$(a,b] = \{x : a < x \leq b\}, \quad \text{open-closed interval from } a \text{ to } b$$
$$[a,b) = \{x : a \leq x < b\}, \quad \text{closed-open interval from } a \text{ to } b$$

Observe that an interval is open if it does not include its endpoints and is closed if it does include its endpoints. Also, a parenthesis "(" or ")" is used to indicate that an endpoint does not belong to the interval, and a bracket "[" or "]" is used to indicate that an endpoint does belong to the interval.

Figure 2-3 shows how we picture each of the above four intervals on the real line **R**. Notice that in each case the endpoints a and b are circled, the line segment between a and b is thickened, and the circle about the endpoint is filled if the endpoint belongs to the interval.

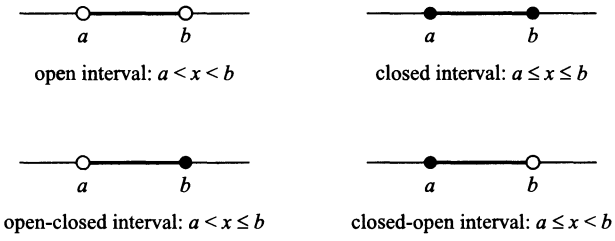

Fig. 2-3

EXAMPLE 2.3

(*a*) Find the interval satisfying each inequality, i.e., rewrite the inequality in terms of x alone:

$$(1)\ 2 \le x - 5 \le 8, \quad (2)\ -1 \le x + 3 \le 4, \quad (3)\ -6 \le 3x \le 12, \quad (4)\ -6 \le -2x \le 4$$

(1) Add 5 to each side to obtain $7 \le x \le 13$.

(2) Add -3 to each side to obtain $-4 \le x \le 1$.

(3) Divide each side by 3 (or: multiply by $\frac{1}{3}$) to obtain $-2 \le x \le 4$.

(4) Divide each side by -2 (or: multiply by $-\frac{1}{2}$) and reverse inequalities to obtain $-6 \le x \le 3$.

(*b*) The inequality $|x| < 5$ may be interpreted to mean that the distance between x and the origin 0 is less than 5; hence x must lie between -5 and 5 on the real line **R**. In other words,

$$|x| < 5 \quad \text{and} \quad -5 < x < 5,$$

have the same meaning and, similarly,

$$|x| \le 5 \quad \text{and} \quad -5 \le x \le 5$$

have the same meaning.

Definition: A set A of real numbers is said to be *dense* in **R** if every open interval contains a point of A or, equivalently, if there is a point of A between any two points in **R**.

The following theorem applies.

Theorem 2.5: The rational numbers **Q** are dense in **R**.

The proof of the above theorem lies beyond the scope of this text. It is closely related to the fact that every real number may be expressed as an infinite decimal or, equivalently, that every real number is the limit of a sequence of rational numbers.

Infinite Intervals

Let a be any real number. Then the set of real numbers x satisfying $x < a$, $x \le a$, $x > a$, or $x \ge a$, is called an *infinite* interval with endpoint a. The interval is said to be *closed* or *open* according as the endpoint a does or does not belong to the interval. The four infinite intervals may also be denoted and defined as follows:

$$(-\infty, a) = \{x : x < a\} \qquad (a, \infty) = \{x : x > a\}$$
$$(-\infty, a] = \{x : x \le a\} \qquad [a, \infty) = \{x : x \ge a\}$$

Note that the infinity symbol ∞ means all the numbers in the positive direction of a, whereas the minus infinity symbol $-\infty$ means all the numbers in the negative direction of a. A parenthesis is used with ∞ and $-\infty$ since they do not represent numbers in the interval. These infinite intervals are pictured in Fig. 2-4.

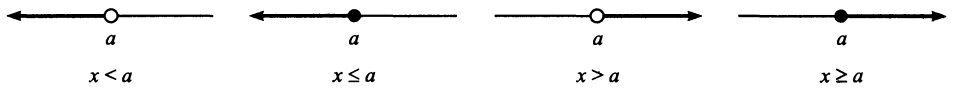

Fig. 2-4

2.6 BOUNDED SETS, COMPLETION PROPERTY

Let A be a set of real numbers. Then A is said to be:

(i) bounded, (ii) bounded from above, (iii) bounded from below

according as there exists a real number M such that, for every $x \in A$:

$$\text{(i) } |x| \leq M, \quad \text{(ii) } x \leq M, \quad \text{(iii) } M \leq x$$

The number M is called a *bound* in (i), an *upper bound* in (ii), and a *lower bound* in (iii). Note that A is bounded if and only if A is a subset of some finite interval. Specifically, M is a bound of A if and only if A is a subset of $[-M, M]$.

If A is finite then A is necessarily bounded. If A is infinite, then A may be bounded, bounded from above (below), or unbounded.

EXAMPLE 2.4

(*a*) $A = \{1, 1/2, 1/3, \ldots, 1/n, \ldots\}$ is bounded since A is certainly a subset of the closed *unit* interval $I = [0, 1]$.

(*b*) $B = \{2, 4, 6, \ldots\}$ is unbounded, but it is bounded from below.

(*c*) $C = \{\ldots, -5, -3, -1\}$ is unbounded, but it is bounded from above.

(*d*) $\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ is unbounded. It has neither an upper bound nor a lower bound.

Definition: Let A be a set of real numbers. A number M is called the *least upper bound* or *supremum* of A, written

$$M = \sup(A)$$

if M is an upper bound of A but any number less than M is not an upper bound of A, that is, for any positive number ϵ, there exist $a \in A$ such that, $M - \epsilon < a$.

The following statement applies.

Completion Property of R: If a set A of real numbers is bounded from above, then $\sup(A)$ exists.

The real numbers **R** are said to be *complete* since it satisfies the above property. We note that the rational numbers **Q** is not complete as seen by the following example.

EXAMPLE 2.5 Let A be the following subset of the rational numbers **Q**:

$$A = \{x \in \mathbf{Q} : x > 0, x^2 < 3\}$$

Observe that A is bounded. However $\sup(A)$ does not exist. We cannot let $\sup(A) = \sqrt{3}$ since $\sqrt{3}$ is not a rational number.

The next two theorems (see Problems 6.17 and 6.49) follow from the completion property of **R**.

Nested Interval Theorem: The intersection $S = \cap_n I_n$ of a nested sequence of closed intervals is not empty. [A sequence $\{I_n\}$ of intervals is nested if $I_1 \supseteq I_2, \ldots$.]

Heine-Borel Theorem: Let $\mathscr{C}$ be a collection of open intervals which contain a closed interval $A = [a, b]$. Then a finite subcollection of $\mathscr{C}$ contains A.

2.7 INTEGERS Z (OPTIONAL MATERIAL)

The notation **Z** is used to denote the integers, the "signed whole numbers"; that is,

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

As noted above, **Z** satisfies all the properties in Section 2.1 except (f). Accordingly, one can always add, subtract, and multiply integers obtaining integers. However, the quotient of two integers need not be an integer, hence the question of divisibility plays an important role in **Z**.

One fundamental property of the integers **Z** is mathematical induction, which was discussed in Section 1.11. We give an equivalent statement below.

Well-Ordering Principle

A property of the positive integers **P** which is equivalent to the principle of induction, although apparently very dissimilar, is the well-ordering principle (proved in Problem 2.32). Namely:

Theorem 2.6 (Well-Ordering Principle): Let S be a nonempty set of positive integers. Then S contains a *least element*; that is, S contains an element a such that $a \leq s$ for every s in S.

Generally speaking, an ordered set S is said to be *well-ordered* if every subset of S contains a first element. Thus Theorem 2.6 states that **P** is well-ordered.

A set S of integers is said to be *bounded from below* if every element of S is greater than some integer m (which may be negative). (The number m is called a *lower bound* of S.) A simple corollary of the above theorem follows:

Corollary 2.7: Let S be a nonempty set of integers which is bounded from below. Then S contains a least element.

Division Algorithm

The following fundamental property of arithmetic (proved in Problems 2.36 and 2.37) is essentially a restatement of the result of long division.

Theorem 2.8 (Division Algorithm): Let a and b be integers with $b \neq 0$. Then there exists integers q and r such that

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

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 nonnegative. The theorem also states that

$$a - bq = r$$

This equation will be used subsequently.

EXAMPLE 2.6

(a) Let $a = 4461$ and $b = 16$. Dividing $a = 4461$ by $b = 16$ yields a quotient $q = 278$ and remainder $r = 13$. As expected, $a = bq + r$, that is,

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

(b) Let $a = -262$ and $b = 3$. Here a is negative. First divide $|a| = 262$ by $b = 3$ to obtain a quotient $q' = 87$ and a remainder $r' = 1$; hence

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

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 $b = 3$ as follows:

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

Therefore, $q = -(q' + 1) = -88$ and $r = b - r' = 2$.

Remark: The result in Example 2.6(b) is true in general. That is, suppose a is negative and suppose we want to find the quotient q and remainder r when a is divided by b. First divide $|a|$ by b to obtain a positive quotient q' and remainder r'. If $r' \neq 0$, then set

$$q = -(q' + 1) \qquad \text{and} \qquad r = b - r'$$

but if $r' = 0$, then set $q = -q'$ and $r = r' = 0$.

Divisibility

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 write

$$a|b$$

We may 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 2.7

(a) $3|6$ since $3 \cdot 2 = 6$; and $-4|28$ since $(-4)(-7) = 28$.

(b) The divisors:

(i) of 1 are ± 1 (iii) of 4 are $\pm 1, \pm 2, \pm 4$ (v) of 7 are $\pm 1, \pm 7$,

(ii) of 2 are $\pm 1, \pm 2$ (iv) of 5 are $\pm 1, \pm 5$ (vi) of 9 are $\pm 1, \pm 3, \pm 9$

(c) If $a \neq 0$, then $a|0$ 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.

Simple properties of divisibility follow.

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

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

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

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

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

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

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

Proposition 2.9: Suppose $a|b$ and $a|c$. Then, for any integers x and y, $a|(bx + cy)$.

The expression $bx + cy$ will be called a *linear combination* of b and c.

Primes

A positive integer $p > 1$ is called a *prime number* or a *prime* if its only divisors are ± 1 and $\pm p$, that is, if p only has trivial divisors. If $n > 1$ is not prime, then n is said to be *composite*. We note (Problem 2.31) that if $n > 1$ is composite then $n = ab$ where $1 < a, b < n$.

EXAMPLE 2.8

(*a*) The integers 2 and 7 are primes, whereas $6 = 2 \cdot 3$ and $15 = 3 \cdot 5$ are composite.

(*b*) The primes less than 50 follow:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47$$

(*c*) Although 21, 24, and 1729 are not primes, each can be written as a product of primes:

$$21 = 3 \cdot 7, \qquad 24 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3, \qquad 1729 = 7 \cdot 13 \cdot 19$$

The Fundamental Theorem of Arithmetic states that every integer $n > 1$ can be written as a product of primes in essentially one way; it is a deep and somewhat difficult theorem to prove. However, using induction, it is easy at this point to prove that such a product exists. Namely:

Theorem 2.10: Every integer $n > 1$ can be written as a product of primes.

Note that a product may consist of a single factor so that a prime p is itself a product of primes.

We prove Theorem 2.10 here, since its proof is relatively simple.

Proof: The proof is by induction. Let $n = 2$. Since 2 is prime, n is a product of primes. Suppose $n > 2$, and the theorem holds for positive integers less than n. If n is prime, then n is a product of primes. If n is composite, then $n = ab$ where $a, b < n$. By induction, a and b are products of primes; hence $n = ab$ is also a product of primes.

Euclid, who proved the Fundamental Theorem of Arithmetic, also asked whether or not there was a largest prime. He answered the question thus:

Theorem 2.11: There is no largest prime, that is, there exists an infinite number of primes.

Proof: Suppose there is a finite number of primes, say $p_1, p_2, \ldots, p_m$. Consider the integer

$$n = p_1 p_2 \cdots p_m + 1$$

Since n is a product of primes (Theorem 2.10), it is divisible by one of the primes, say p_k. Note that p_k also divides the product $p_1 p_2 \cdots p_m$. Therefore p_k divides

$$n - p_1 p_2 \cdots p_m = 1$$

This is impossible, and so n is divisible by some other prime. This contradicts the assumption that $p_1, p_2, \ldots, p_m$ are the only primes. Thus the number of primes is infinite, and the theorem is proved.

2.8 GREATEST COMMON DIVISOR, EUCLIDEAN ALGORITHM

Suppose a and b are integers, not both 0. An integer d is called a *common divisor* of a and b if d divides both a and b, that is, if $d|a$ and $d|b$. Note that 1 is always a positive common divisor of a and b, and that any common divisor of a and b cannot be greater than $|a|$ or $|b|$. Thus there exists a largest common divisor of a and b; it is denoted by

$$\gcd(a, b)$$

and it is called the *greatest common divisor* of a and b.

EXAMPLE 2.9

(*a*) The common divisors of 12 and 18 are $\pm 1, \pm 2, \pm 3, \pm 6$. Thus $\gcd(12, 18) = 6$. Similarly,

$$\gcd(12, -18) = 6, \qquad \gcd(12, -16) = 4, \qquad \gcd(29, 15) = 1, \qquad \gcd(14, 49) = 7$$

(*b*) For any integer a, we have gcd $(1, a) = 1$.

(*c*) For any prime p, we have gcd $(p, a) = p$ or gcd $(p, a) = 1$ according as $p|a$ or $p \nmid a$.

(*d*) Suppose a is positive. Then $a|b$ if and only if gcd $(a, b) = a$.

The following theorem (proved in Problem 2.43) gives an alternative characterization of the greatest common divisor.

Theorem 2.12: Let d be the smallest positive integer of the form $ax + by$. Then $d = \gcd(a, b)$.

Corollary 2.13: Suppose $d = \gcd(a, b)$. Then there exists integers x and y such that $d = ax + by$.

Another way to characterize the greatest common divisor, without using the inequality relation, follows:

Theorem 2.14: A positive integer $d = \gcd(a, b)$ if and only if d has the following properties:
(1) d divides both a and b;
(2) if c divides both a and b, then $c|d$.

Simple properties of the greatest common divisor follow.

(*a*) gcd $(a, b) = \gcd(b, a)$.
(*b*) If $x > 0$, then gcd $(ax, bx) = x \cdot \gcd(a, b)$.
(*c*) If $d = \gcd(a, b)$, then gcd $(a/d,\ b/d) = 1$.
(*d*) For any integer x, gcd $(a, b) = \gcd(a, b + ax)$.

Euclidean Algorithm

Let a and b be integers, and let $d = \gcd(a, b)$. One can always find d by listing all the divisors of a and then all the divisors of b and then choosing the largest common divisor. This procedure does not find the integers x and y such that

$$d = ax + by$$

This subsection gives a very efficient algorithm for finding both $d = \gcd(a, b)$ and the above integers x and y.

This algorithm, called the Euclidean algorithm, consists of repeatedly applying the division algorithm (long division). We illustrate the algorithm with an example.

EXAMPLE 2.10 Let $a = 540$ and $b = 168$. We find $d = \gcd(a, b)$ by dividing a by b and then repeatedly dividing each remainder into the divisor until obtaining a zero remainder. These steps are pictured in Fig. 2-5. The last nonzero remainder is 12. Thus

$$12 = \gcd(540, 168)$$

This follows from the fact that

$$\gcd(540, 168) = \gcd(168, 36) = \gcd(36, 24) = \gcd(24, 12) = 12$$

$$\begin{array}{r} 3 \\ 168\overline{)540} \\ \underline{504} \\ 36 \end{array} \qquad \begin{array}{r} 4 \\ 36\overline{)168} \\ \underline{144} \\ 24 \end{array} \qquad \begin{array}{r} 1 \\ 24\overline{)36} \\ \underline{24} \\ 12 \end{array} \qquad \begin{array}{r} 2 \\ 12\overline{)24} \\ \underline{24} \\ 0 \end{array}$$

Fig. 2-5

Next we find x and y such that

$$12 = 540x + 168y$$

The first three quotients in Fig. 2-5 yield the equations:

$$\begin{array}{lll} (1) & 540 = 3(168) + 36 & \text{or} \quad 36 = 540 - 3(168) \\ (2) & 168 = 4(36) + 24 & \text{or} \quad 24 = 168 - 4(36) \\ (3) & 36 = 1(24) + 12 & \text{or} \quad 12 = 36 - 1(24) \end{array}$$

Equation (*3*) tells us that 12 is a linear combination of 36 and 24. We use (*2*) to replace 24 in (*3*) so we can write 12 as a linear combination of 168 and 36 as follows:

$$\begin{aligned} (4) \quad 12 &= 36 - 1[168 - 4(36)] = 36 - (168) + 4(36) \\ &= 5(36) - 1(168) \end{aligned}$$

We now use (*1*) in (*4*) so we can write 12 as a linear combination of 168 and 540 as follows:

$$\begin{aligned} 12 &= 5[540 - 3(168)] - 1(168) \\ &= 5(540) - 15(168) - 1(168) \\ &= 5(540) - 16(168) \end{aligned}$$

This is our desired linear combination. Thus $x = 5$ and $y = -16$.

Least Common Multiple

Suppose a and b are nonzero integers. Note that $|ab|$ is a positive common multiple of a and b. Thus there exists a smallest positive common multiple of a and b; it is denoted by

$$\text{lcm } (a, b)$$

and it is called the *least common multiple* of a and b.

EXAMPLE 2.11

(*a*) lcm $(2, 3) = 6$, lcm $(4, 6) = 12$, lcm $(9, 10) = 90$.

(*b*) For any positive integer a, we have lcm $(1, a) = a$.

(*c*) For any prime p and any positive integer a, lcm $(p, a) = a$ or lcm $(p, a) = ap$ according as $p|a$ or $p \nmid a$.

(*d*) Suppose a and b are positive integers. Then $a|b$ if and only if lcm $(a, b) = b$.

The next theorem gives an important relationship between the greatest common divisor and the least common multiple.

Theorem 2.15: Suppose a and b are nonzero integers. Then

$$\text{lcm } (a, b) = \frac{|ab|}{\text{gcd } (a, b)}$$

2.9 FUNDAMENTAL THEOREM OF ARITHMETIC

This section discusses the Fundamental Theorem of Arithmetic. First we need the notion of relatively prime integers.

Two integers a and b are said to be *relatively prime*, or *coprime*, if

$$\text{gcd } (a, b) = 1$$

Accordingly, if a and b are relatively prime, then there exist integers x and y such that

$$ax + by = 1$$

Conversely, if $ax + by = 1$, then a and b are relatively prime.

EXAMPLE 2.12

(*a*) Observe that gcd $(12, 35) = 1$, gcd $(49, 18) = 1$, gcd $(21, 64) = 1$, gcd $(-28, 45) = 1$

(*b*) If p and q are distinct primes, then gcd $(p, q) = 1$.

(*c*) For any integer a, we have gcd $(a, a + 1) = 1$. This follows from the fact that any common divisor of a and $a + 1$ must divide their difference $(a + 1) - a = 1$.

The relation of being relatively prime is particularly important because of the following results. We will prove the second theorem here.

Theorem 2.16: Suppose gcd $(a, b) = 1$, and a and b both divide c. Then ab divides c.

Theorem 2.17: Suppose $a|bc$, and gcd $(a, b) = 1$. Then $a|c$.

Proof: Since gcd $(a, b) = 1$, there exist x and y such that $ax + by = 1$. Multiplying by c yields

$$acx + bcy = c$$

We have $a|acx$. Also, $a|bcy$ since, by hypothesis, $a|bc$. Hence a divides the sum $acx + bcy = c$.

Corollary 2.18: Suppose a prime p divides a product ab. Then

$$p|a \text{ or } p|b$$

This corollary dates back to Euclid. In fact, it is the basis of his proof of the fundamental theorem of arithmetic.

Fundamental Theorem of Arithmetic

Theorem 2.10 asserts that every positive integer is a product of primes. Can different products of primes yield the same number? Clearly, we can rearrange the order of the prime factors, e.g.

$$30 = 2 \cdot 3 \cdot 5 = 5 \cdot 2 \cdot 3 = 3 \cdot 2 \cdot 5$$

The fundamental theorem of arithmetic (proved in Problem 2.49) says that this is the only way that two "different" products can give the same number. Namely:

Theorem 2.19 (Fundamental Theorem of Arithmetic): Every integer $n > 1$ can be expressed uniquely (except for order) as a product of primes.

The primes in the factorization of n need not be distinct. Frequently, it is useful to collect together all equal primes. Then n can be expressed uniquely in the form

$$n = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$$

where the m_i are positive and $p_1 < p_2 < \cdots < p_r$. This is called the *canonical factorization* of n.

EXAMPLE 2.13 Let $a = 2^4 \cdot 3^3 \cdot 7 \cdot 11 \cdot 13$ and $b = 2^3 \cdot 3^2 \cdot 5^2 \cdot 11 \cdot 17$. Find $d = \gcd(a, b)$ and $m = \text{lcm}(a, b)$.

(*a*) First we find $d = \gcd(a, b)$. Those primes p_i which appear in both a and b, i.e., 2, 3, and 11, will also appear in d, and the exponent of p_i in d will be the smaller of its exponents in a and b. Thus

$$d = \gcd(a, b) = 2^3 \cdot 3^2 \cdot 11 = 792$$

(*b*) Next we find $m = \text{lcm}(a, b)$. Those primes p_i which appear in either a and b, i.e., 2, 3, 5, 7, 11, 13 and 17 will also appear in m, and the exponent of p_i in m will be the larger of its exponents in a and b. Thus

$$m = \text{lcm}(a, b) = 2^4 \cdot 3^3 \cdot 5^2 \cdot 11 \cdot 13 \cdot 17$$