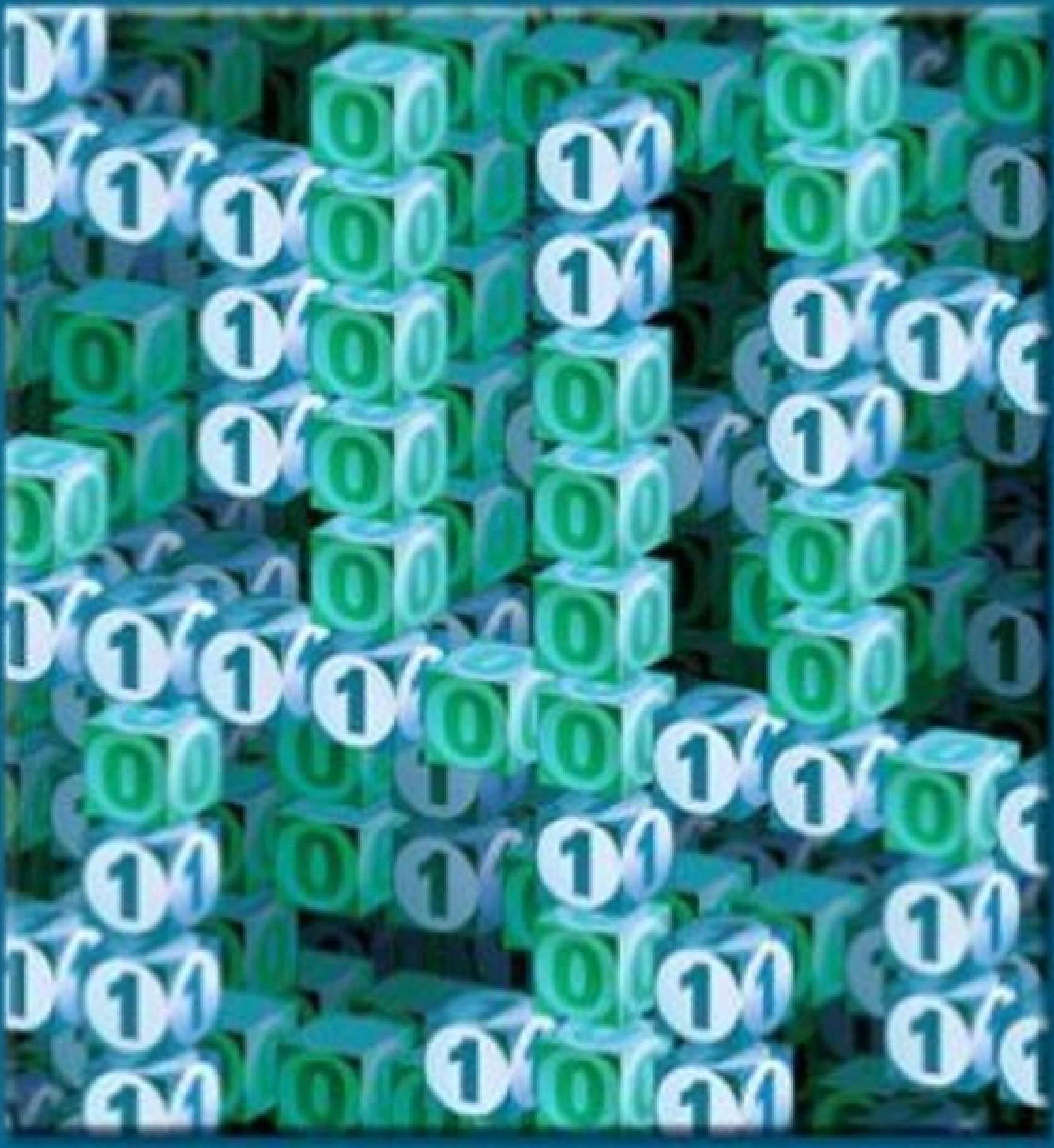
DISCRETE and COMBINATORIAL MATHEMATICS

An Applied Introduction



Ralph P. Grimaldi

Fifth Edition

DISCRETE AND COMBINATORIAL MATHEMATICS

An Applied Introduction

FIFTH EDITION

RALPH P. GRIMALDI
Rose-Hulman Institute of Technology

PEARSON
Addison
Wesley

Boston San Francisco New York
London Toronto Sydney Tokyo Singapore Madrid
Mexico City Munich Paris Cape Town Hong Kong Montreal

NOTATION

LOGIC	p, q	statements (or propositions)
	$\neg p$	the negation of (statement) p: *not* p
	$p \wedge q$	the conjunction of p, q: p *and* q
	$p \vee q$	the disjunction of p, q: p *or* q
	$p \rightarrow q$	the implication of q by p: p *implies* q
	$p \leftrightarrow q$	the biconditional of p and q: p *if and only if* q
	iff	if and only if
	$p \Rightarrow q$	logical implication: p *logically implies* q
	$p \Longleftrightarrow q$	logical equivalence: p is *logically equivalent* to q
	T_0	tautology
	F_0	contradiction
	$\forall x$	For *all* x (the universal quantifier)
	$\exists x$	For *some* x (the existential quantifier)
SET THEORY	$x \in A$	element x is a member of set A
	$x \notin A$	element x is not a member of set A
	$\mathcal{U}$	the universal set
	$A \subseteq B$, $B \supseteq A$	A is a subset of B
	$A \subset B$, $B \supset A$	A is a proper subset of B
	$A \nsubseteq B$	A is not a subset of B
	$A \not\subset B$	A is not a proper subset of B
	$\lvert A \rvert$	the cardinality, or size, of set A — that is, the number of elements in A
	$\emptyset = \{\ \}$	the empty, or null, set
	$\mathcal{P}(A)$	the power set of A — that is, the collection of all subsets of A
	$A \cap B$	the intersection of sets A, B: $\{x \mid x \in A$ and $x \in B\}$
	$A \cup B$	the union of sets A, B: $\{x \mid x \in A$ or $x \in B\}$
	$A \triangle B$	the symmetric difference of sets A, B: $\{x \mid x \in A$ or $x \in B$, but $x \notin A \cap B\}$
	$\overline{A}$	the complement of set A: $\{x \mid x \in \mathcal{U}$ and $x \notin A\}$
	$A - B$	the (relative) complement of set B in set A: $\{x \mid x \in A$ and $x \notin B\}$
	$\bigcup_{i \in I} A_i$	$\{x \mid x \in A_i$, for at least one $i \in I\}$, where I is an index set
	$\bigcap_{i \in I} A_i$	$\{x \mid x \in A_i$, for every $i \in I\}$, where I is an index set
PROBABILITY	S	the sample space for an experiment $\mathcal{E}$
	$A \subseteq S$	A is an event
	$Pr(A)$	the probability of event A
	$Pr(A \mid B)$	the probability of A given B; conditional probability
	X	random variable
	$E(X)$	the expected value of X, a random variable
	$\mathrm{Var}(X) = \sigma_X^2$	the variance of X, a random variable
	σ_X	the standard deviation of X, a random variable
NUMBERS	$a \mid b$	a divides b, for a, $b \in \mathbf{Z}$, $a \neq 0$
	$a \nmid b$	a does not divide b, for a, $b \in \mathbf{Z}$, $a \neq 0$
	$\gcd(a, b)$	the greatest common divisor of the integers a, b
	$\mathrm{lcm}(a, b)$	the least common multiple of the integers a, b
	$\phi(n)$	Euler's phi function for $n \in \mathbf{Z}^+$
	$\lfloor x \rfloor$	the greatest integer less than or equal to the real number x: the greatest integer in x: the *floor* of x

NOTATION

	$\lceil x \rceil$	the smallest integer greater than or equal to the real number x: the *ceiling* of x
	$a \equiv b \pmod{n}$	a is congruent to b modulo n
RELATIONS	$A \times B$	the Cartesian, or cross, product of sets A, B: $\{(a, b) \mid a \in A, b \in B\}$
	$\mathcal{R} \subseteq A \times B$	$\mathcal{R}$ is a relation from A to B
	$a \mathcal{R} b$; $(a, b) \in \mathcal{R}$	a is related to b
	$a \not{\mathcal{R}} b$; $(a, b) \notin \mathcal{R}$	a is not related to b
	$\mathcal{R}^c$	the converse of relation $\mathcal{R}$: $(a, b) \in \mathcal{R}$ iff $(b, a) \in \mathcal{R}^c$
	$\mathcal{R} \circ \mathcal{S}$	the composite relation for $\mathcal{R} \subseteq A \times B$, $\mathcal{S} \subseteq B \times C$: $(a, c) \in \mathcal{R} \circ \mathcal{S}$ if $(a, b) \in \mathcal{R}$, $(b, c) \in \mathcal{S}$ for some $b \in B$
	$\text{lub}\{a, b\}$	the least upper bound of a and b
	$\text{glb}\{a, b\}$	the greatest lower bound of a and b
	$[a]$	the equivalence class of element a (relative to an equivalence relation $\mathcal{R}$ on a set A): $\{x \in A \mid x \mathcal{R} a\}$
FUNCTIONS	$f: A \to B$	f is a function from A to B
	$f(A_1)$	for $f: A \to B$ and $A_1 \subseteq A$, $f(A_1)$ is the image of A_1 under f — that is, $\{f(a) \mid a \in A_1\}$
	$f(A)$	for $f: A \to B$, $f(A)$ is the range of f
	$f: A \times A \to B$	f is a binary operation on A
	$f: A \times A \to B \ (\subseteq A)$	f is a closed binary operation on A
	$1_A: A \to A$	the identity function on A: $1_A(a) = a$ for each $a \in A$
	$f\vert_{A_1}$	the restriction of $f: A \to B$ to $A_1 \subseteq A$
	$g \circ f$	the composite function for $f: A \to B$, $g: B \to C$: $(g \circ f)a = g(f(a))$, for $a \in A$
	f^{-1}	the inverse of function f
	$f^{-1}(B_1)$	the preimage of $B_1 \subseteq B$ for $f: A \to B$
	$f \in O(g)$	f is "big Oh" of g; f is of order g
THE ALGEBRA OF STRINGS	$\mathbf{\Sigma}$	a finite set of symbols called an alphabet
	λ	the empty string
	$\Vert x \Vert$	the length of string x
	$\mathbf{\Sigma}^n$	$\{x_1 x_2 \cdots x_n \mid x_i \in \mathbf{\Sigma}\}$, $n \in \mathbf{Z}^+$
	$\mathbf{\Sigma}^0$	$\{\lambda\}$
	$\mathbf{\Sigma}^+$	$\bigcup_{n \in \mathbf{Z}^+} \mathbf{\Sigma}^n$: the set of all strings of positive length
	$\mathbf{\Sigma}^*$	$\bigcup_{n \geq 0} \mathbf{\Sigma}^n$: the set of all finite strings
	$A \subseteq \mathbf{\Sigma}^*$	A is a language
	AB	the concatenation of languages $A, B \subseteq \mathbf{\Sigma}^*$: $\{ab \mid a \in A, b \in B\}$
	A^n	$\{a_1 a_2 \cdots a_n \mid a_i \in A \subseteq \mathbf{\Sigma}^*\}$, $n \in \mathbf{Z}^+$
	A^0	$\{\lambda\}$
	A^+	$\bigcup_{n \in \mathbf{Z}^+} A^n$
	A^*	$\bigcup_{n \geq 0} A^n$: the Kleene closure of language A
	$M = (S, \mathcal{S}, \mathcal{O}, \nu, \omega)$	a finite state machine M with internal states S, input alphabet $\mathcal{S}$, output alphabet $\mathcal{O}$, next state function $\nu: S \times \mathcal{S} \to S$ and output function $\omega: S \times \mathcal{S} \to \mathcal{O}$

Contents

PART 1
Fundamentals of Discrete Mathematics 1

1

Fundamental Principles of Counting

Enumeration, or counting, may strike one as an obvious process that a student learns when first studying arithmetic. But then, it seems, very little attention is paid to further development in counting as the student turns to "more difficult" areas in mathematics, such as algebra, geometry, trigonometry, and calculus. Consequently, this first chapter should provide some warning about the seriousness and difficulty of "mere" counting.

Enumeration does not end with arithmetic. It also has applications in such areas as coding theory, probability and statistics, and in the analysis of algorithms. Later chapters will offer some specific examples of these applications.

As we enter this fascinating field of mathematics, we shall come upon many problems that are very simple to state but somewhat "sticky" to solve. Thus, be sure to learn and understand the basic formulas — but do *not* rely on them too heavily. For without an analysis of each problem, a mere knowledge of formulas is next to useless. Instead, welcome the challenge to solve unusual problems or those that are different from problems you have encountered in the past. Seek solutions based on your own scrutiny, regardless of whether it reproduces what the author provides. There are often several ways to solve a given problem.

1.1 The Rules of Sum and Product

Our study of discrete and combinatorial mathematics begins with two basic principles of counting: the rules of sum and product. The statements and initial applications of these rules appear quite simple. In analyzing more complicated problems, one is often able to break down such problems into parts that can be solved using these basic principles. We want to develop the ability to "decompose" such problems and piece together our partial solutions in order to arrive at the final answer. A good way to do this is to analyze and solve many diverse enumeration problems, taking note of the principles being used. This is the approach we shall follow here.

Our first principle of counting can be stated as follows:

The Rule of Sum: If a first task can be performed in m ways, while a second task can be performed in n ways, and the two tasks cannot be performed simultaneously, then performing either task can be accomplished in any one of $m + n$ ways.

Note that when we say that a particular occurrence, such as a first task, can come about in m ways, these m ways are assumed to be distinct, unless a statement is made to the contrary. This will be true throughout the entire text.

EXAMPLE 1.1

A college library has 40 textbooks on sociology and 50 textbooks dealing with anthropology. By the rule of sum, a student at this college can select among $40 + 50 = 90$ textbooks in order to learn more about one or the other of these two subjects.

EXAMPLE 1.2

The rule can be extended beyond two tasks as long as no pair of tasks can occur simultaneously. For instance, a computer science instructor who has, say, seven different introductory books each on C++, Java, and Perl can recommend any one of these 21 books to a student who is interested in learning a first programming language.

EXAMPLE 1.3

The computer science instructor of Example 1.2 has two colleagues. One of these colleagues has three textbooks on the analysis of algorithms, and the other has five such textbooks. If n denotes the maximum number of different books on this topic that this instructor can borrow from them, then $5 \leq n \leq 8$, for here both colleagues *may* own copies of the same textbook(s).

The following example introduces our second principle of counting.

EXAMPLE 1.4

In trying to reach a decision on plant expansion, an administrator assigns 12 of her employees to two committees. Committee A consists of five members and is to investigate possible favorable results from such an expansion. The other seven employees, committee B, will scrutinize possible unfavorable repercussions. Should the administrator decide to speak to just one committee member before making her decision, then by the rule of sum there are 12 employees she can call upon for input. However, to be a bit more unbiased, she decides to speak with a member of committee A on Monday, and then with a member of committee B on Tuesday, before reaching a decision. Using the following principle, we find that she can select two such employees to speak with in $5 \times 7 = 35$ ways.

The Rule of Product: **If a procedure can be broken down into first and second stages, and if there are m possible outcomes for the first stage and if, for each of these outcomes, there are n possible outcomes for the second stage, then the total procedure can be carried out, in the designated order, in mn ways.**

EXAMPLE 1.5

The drama club of Central University is holding tryouts for a spring play. With six men and eight women auditioning for the leading male and female roles, by the rule of product the director can cast his leading couple in $6 \times 8 = 48$ ways.

EXAMPLE 1.6

Here various extensions of the rule are illustrated by considering the manufacture of license plates consisting of two letters followed by four digits.

a) If no letter or digit can be repeated, there are $26 \times 25 \times 10 \times 9 \times 8 \times 7 = 3{,}276{,}000$ different possible plates.

b) With repetitions of letters and digits allowed, $26 \times 26 \times 10 \times 10 \times 10 \times 10 = 6{,}760{,}000$ different license plates are possible.

c) If repetitions are allowed, as in part (b), how many of the plates have only vowels (A, E, I, O, U) and even digits? (0 is an even integer.)

EXAMPLE 1.7

In order to store data, a computer's main memory contains a large collection of circuits, each of which is capable of storing a *bit* — that is, one of the *bi*nary digi*ts* 0 or 1. These storage circuits are arranged in units called (memory) cells. To identify the cells in a computer's main memory, each is assigned a unique name called its *address*. For some computers, such as embedded microcontrollers (as found in the ignition system for an automobile), an address is represented by an ordered list of eight bits, collectively referred to as a *byte*. Using the rule of product, there are $2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 = 2^8 = 256$ such bytes. So we have 256 addresses that may be used for cells where certain information may be stored.

A kitchen appliance, such as a microwave oven, incorporates an embedded microcontroller. These "small computers" (such as the PICmicro microcontroller) contain thousands of memory cells and use two-byte addresses to identify these cells in their main memory. Such addresses are made up of two consecutive bytes, or 16 consecutive bits. Thus there are $256 \times 256 = 2^8 \times 2^8 = 2^{16} = 65{,}536$ available addresses that could be used to identify cells in the main memory. Other computers use addressing systems of four bytes. This 32-bit architecture is presently used in the Pentium[†] processor, where there are as many as $2^8 \times 2^8 \times 2^8 \times 2^8 = 2^{32} = 4{,}294{,}967{,}296$ addresses for use in identifying the cells in main memory. When a programmer deals with the UltraSPARC[‡] or Itanium[§] processors, he or she considers memory cells with eight-byte addresses. Each of these addresses comprises $8 \times 8 = 64$ bits, and there are $2^{64} = 18{,}446{,}744{,}073{,}709{,}551{,}616$ possible addresses for this architecture. (Of course, not all of these possibilities are actually used.)

EXAMPLE 1.8

At times it is necessary to combine several different counting principles in the solution of one problem. Here we find that the rules of both sum and product are needed to attain the answer.

At the AWL corporation Mrs. Foster operates the Quick Snack Coffee Shop. The menu at her shop is limited: six kinds of muffins, eight kinds of sandwiches, and five beverages (hot coffee, hot tea, iced tea, cola, and orange juice). Ms. Dodd, an editor at AWL, sends her assistant Carl to the shop to get her lunch — either a muffin and a hot beverage or a sandwich and a cold beverage.

By the rule of product, there are $6 \times 2 = 12$ ways in which Carl can purchase a muffin and hot beverage. A second application of this rule shows that there are $8 \times 3 = 24$ possibilities for a sandwich and cold beverage. So by the rule of sum, there are $12 + 24 = 36$ ways in which Carl can purchase Ms. Dodd's lunch.

[†] Pentium (R) is a registered trademark of the Intel Corporation.

[‡] The UltraSPARC processor is manufactured by Sun (R) Microsystems, Inc.

[§] Itanium (TM) is a trademark of the Intel Corporation.

1.2 Permutations

Continuing to examine applications of the rule of product, we turn now to counting linear arrangements of objects. These arrangements are often called *permutations* when the objects are distinct. We shall develop some systematic methods for dealing with linear arrangements, starting with a typical example.

EXAMPLE 1.9

In a class of 10 students, five are to be chosen and seated in a row for a picture. How many such linear arrangements are possible?

The key word here is *arrangement*, which designates the importance of *order*. If A, B, C, . . . , I, J denote the 10 students, then BCEFI, CEFIB, and ABCFG are three such different arrangements, even though the first two involve the same five students.

To answer this question, we consider the positions and possible numbers of students we can choose from in order to fill each position. The filling of a position is a stage of our procedure.

$$\underset{\textbf{1st position}}{10} \times \underset{\textbf{2nd position}}{9} \times \underset{\textbf{3rd position}}{8} \times \underset{\textbf{4th position}}{7} \times \underset{\textbf{5th position}}{6}$$

Each of the 10 students can occupy the 1st position in the row. Because repetitions are not possible here, we can select only one of the nine remaining students to fill the 2nd position. Continuing in this way, we find only six students to select from in order to fill the 5th and final position. This yields a total of 30,240 possible arrangements of five students selected from the class of 10.

Exactly the same answer is obtained if the positions are filled from right to left—namely, $6 \times 7 \times 8 \times 9 \times 10$. If the 3rd position is filled first, the 1st position second, the 4th position third, the 5th position fourth, and the 2nd position fifth, then the answer is $9 \times 6 \times 10 \times 8 \times 7$, still the same value, 30,240.

As in Example 1.9, the product of certain consecutive positive integers often comes into play in enumeration problems. Consequently, the following notation proves to be quite useful when we are dealing with such counting problems. It will frequently allow us to express our answers in a more convenient form.

Definition 1.1

For an integer $n \geq 0$, *n factorial* (denoted $n!$) is defined by

$$0! = 1,$$
$$n! = (n)(n-1)(n-2)\cdots(3)(2)(1), \quad \text{for} \quad n \geq 1.$$

One finds that $1! = 1$, $2! = 2$, $3! = 6$, $4! = 24$, and $5! = 120$. In addition, for each $n \geq 0$, $(n+1)! = (n+1)(n!)$.

Before we proceed any further, let us try to get a somewhat better appreciation for how fast $n!$ grows. We can calculate that $10! = 3{,}628{,}800$, and it just so happens that this is exactly the number of *seconds* in six *weeks*. Consequently, 11! exceeds the number of seconds in one *year*, 12! exceeds the number in 12 years, and 13! surpasses the number of seconds in a *century*.

If we make use of the factorial notation, the answer in Example 1.9 can be expressed in the following more compact form:

$$10 \times 9 \times 8 \times 7 \times 6 = 10 \times 9 \times 8 \times 7 \times 6 \times \frac{5 \times 4 \times 3 \times 2 \times 1}{5 \times 4 \times 3 \times 2 \times 1} = \frac{10!}{5!}.$$

Definition 1.2 Given a collection of n distinct objects, any (linear) arrangement of these objects is called a *permutation* of the collection.

Starting with the letters a, b, c, there are six ways to arrange, or permute, all of the letters: abc, acb, bac, bca, cab, cba. If we are interested in arranging only two of the letters at a time, there are six such size-2 permutations: ab, ba, ac, ca, bc, cb.

If there are n distinct objects and r is an integer, with $1 \leq r \leq n$, then by the rule of product, the number of permutations of size r for the n objects is

$$\begin{aligned} P(n,r) &= \underbrace{n}_{\text{1st position}} \times \underbrace{(n-1)}_{\text{2nd position}} \times \underbrace{(n-2)}_{\text{3rd position}} \times \cdots \times \underbrace{(n-r+1)}_{r\text{th position}} \\ &= (n)(n-1)(n-2)\cdots(n-r+1) \times \frac{(n-r)(n-r-1)\cdots(3)(2)(1)}{(n-r)(n-r-1)\cdots(3)(2)(1)} \\ &= \frac{n!}{(n-r)!}. \end{aligned}$$

For $r = 0$, $P(n, 0) = 1 = n!/(n-0)!$, so $P(n, r) = n!/(n-r)!$ holds for all $0 \leq r \leq n$. A special case of this result is Example 1.9, where $n = 10$, $r = 5$, and $P(10, 5) = 30{,}240$. When permuting all of the n objects in the collection, we have $r = n$ and find that $P(n, n) = n!/0! = n!$.

Note, for example, that if $n \geq 2$, then $P(n, 2) = n!/(n-2)! = n(n-1)$. When $n > 3$ one finds that $P(n, n-3) = n!/[n-(n-3)]! = n!/3! = (n)(n-1)(n-2)\cdots(5)(4)$.

The number of permutations of size r, where $0 \leq r \leq n$, from a collection of n objects, is $P(n, r) = n!/(n-r)!$. (Remember that $P(n, r)$ counts (linear) arrangements in which the objects can*not* be repeated.) However, if repetitions are allowed, then by the rule of product there are n^r possible arrangements, with $r \geq 0$.

EXAMPLE 1.10 The number of permutations of the letters in the word COMPUTER is 8!. If only five of the letters are used, the number of permutations (of size 5) is $P(8, 5) = 8!/(8-5)! = 8!/3! = 6720$. If repetitions of letters are allowed, the number of possible 12-letter sequences is $8^{12} \doteq 6.872 \times 10^{10}$.[†]

EXAMPLE 1.11 Unlike Example 1.10, the number of (linear) arrangements of the four letters in BALL is 12, not 4! (= 24). The reason is that we do not have four distinct letters to arrange. To get the 12 arrangements, we can list them as in Table 1.1(a).

[†] The symbol "$\doteq$" is read "is approximately equal to."

Table 1.1

A	B	L	L	A	B	L_1	L_2	A	B	L_2	L_1
A	L	B	L	A	L_1	B	L_2	A	L_2	B	L_1
A	L	L	B	A	L_1	L_2	B	A	L_2	L_1	B
B	A	L	L	B	A	L_1	L_2	B	A	L_2	L_1
B	L	A	L	B	L_1	A	L_2	B	L_2	A	L_1
B	L	L	A	B	L_1	L_2	A	B	L_2	L_1	A
L	A	B	L	L_1	A	B	L_2	L_2	A	B	L_1
L	A	L	B	L_1	A	L_2	B	L_2	A	L_1	B
L	B	A	L	L_1	B	A	L_2	L_2	B	A	L_1
L	B	L	A	L_1	B	L_2	A	L_2	B	L_1	A
L	L	A	B	L_1	L_2	A	B	L_2	L_1	A	B
L	L	B	A	L_1	L_2	B	A	L_2	L_1	B	A
(a)				(b)							

If the two L's are distinguished as L_1, L_2, then we can use our previous ideas on permutations of distinct objects; with the four distinct symbols B, A, L_1, L_2, we have $4! = 24$ permutations. These are listed in Table 1.1(b). Table 1.1 reveals that for each arrangement in which the L's are indistinguishable there corresponds a *pair* of permutations with distinct L's. Consequently,

$$2 \times (\text{Number of arrangements of the letters B, A, L, L})$$
$$= (\text{Number of permutations of the symbols B, A, } L_1, L_2),$$

and the answer to the original problem of finding all the arrangements of the four letters in BALL is $4!/2 = 12$.

EXAMPLE 1.12

Using the idea developed in Example 1.11, we now consider the arrangements of all nine letters in DATABASES.

There are $3! = 6$ arrangements with the A's distinguished for each arrangement in which the A's are not distinguished. For example, $DA_1TA_2BA_3SES$, $DA_1TA_3BA_2SES$, $DA_2TA_1BA_3SES$, $DA_2TA_3BA_1SES$, $DA_3TA_1BA_2SES$, and $DA_3TA_2BA_1SES$ all correspond to DATABASES, when we remove the subscripts on the A's. In addition, to the arrangement $DA_1TA_2BA_3SES$ there corresponds the pair of permutations $DA_1TA_2BA_3S_1ES_2$ and $DA_1TA_2BA_3S_2ES_1$, when the S's are distinguished. Consequently,

$$(2!)(3!)(\text{Number of arrangements of the letters in DATABASES})$$
$$= (\text{Number of permutations of the symbols D, } A_1, \text{T}, A_2, \text{B}, A_3, S_1, \text{E}, S_2),$$

so the number of arrangements of the nine letters in DATABASES is $9!/(2!\,3!) = 30{,}240$.

Before stating a general principle for arrangements with repeated symbols, note that in our prior two examples we solved a new type of problem by relating it to previous enumeration principles. This practice is common in mathematics in general, and often occurs in the derivations of discrete and combinatorial formulas.

If there are n objects with n_1 indistinguishable objects of a first type, n_2 indistinguishable objects of a second type, ..., and n_r indistinguishable objects of an rth type, where $n_1 + n_2 + \cdots + n_r = n$, then there are $\dfrac{n!}{n_1!\,n_2!\cdots n_r!}$ (linear) arrangements of the given n objects.

EXAMPLE 1.13

The MASSASAUGA is a brown and white venomous snake indigenous to North America. Arranging all of the letters in MASSASAUGA, we find that there are

$$\frac{10!}{4!\,3!\,1!\,1!\,1!} = 25{,}200$$

possible arrangements. Among these are

$$\frac{7!}{3!\,1!\,1!\,1!\,1!} = 840$$

in which all four A's are together. To get this last result, we considered all arrangements of the seven symbols AAAA (one symbol), S, S, S, M, U, G.

EXAMPLE 1.14

Determine the number of (staircase) paths in the xy-plane from (2, 1) to (7, 4), where each such path is made up of individual steps going one unit to the right (R) or one unit upward (U). The blue lines in Fig. 1.1 show two of these paths.

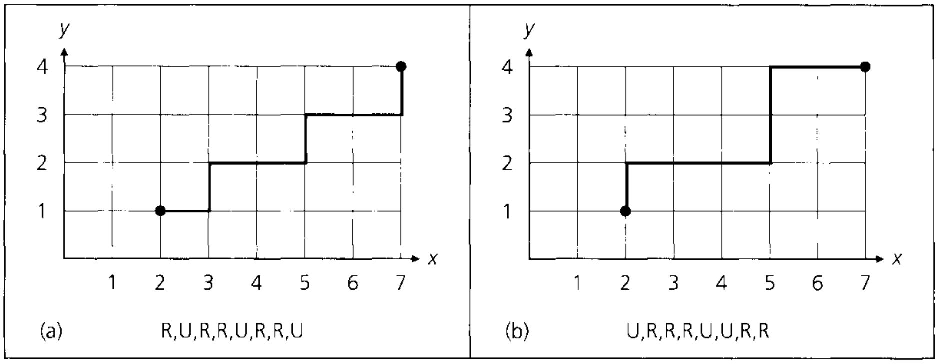


Figure 1.1

Beneath each path in Fig. 1.1 we have listed the individual steps. For example, in part (a) the list R, U, R, R, U, R, R, U indicates that starting at the point (2, 1), we first move one unit to the right [to (3, 1)], then one unit upward [to (3, 2)], followed by two units to the right [to (5, 2)], and so on, until we reach the point (7, 4). The path consists of five R's for moves to the right and three U's for moves upward.

The path in part (b) of the figure is also made up of five R's and three U's. In general, the overall trip from (2, 1) to (7, 4) requires $7 - 2 = 5$ horizontal moves to the right and $4 - 1 = 3$ vertical moves upward. Consequently, each path corresponds to a list of five R's and three U's, and the solution for the number of paths emerges as the number of arrangements of the five R's and three U's, which is $8!/(5!\,3!) = 56$.

EXAMPLE 1.15

We now do something a bit more abstract and prove that if n and k are positive integers with $n = 2k$, then $n!/2^k$ is an integer. Because our argument relies on counting, it is an example of a *combinatorial proof.*

Consider the n symbols $x_1, x_1, x_2, x_2, \ldots, x_k, x_k$. The number of ways in which we can arrange all of these $n = 2k$ symbols is an integer that equals

$$\frac{n!}{\underbrace{2!\,2!\cdots 2!}_{k\text{ factors of }2!}} = \frac{n!}{2^k}.$$

Finally, we will apply what has been developed so far to a situation in which the arrangements are no longer linear.

EXAMPLE 1.16

If six people, designated as A, B, . . . , F, are seated about a round table, how many different circular arrangements are possible, if arrangements are considered the same when one can be obtained from the other by rotation? [In Fig. 1.2, arrangements (a) and (b) are considered identical, whereas (b), (c), and (d) are three distinct arrangements.]

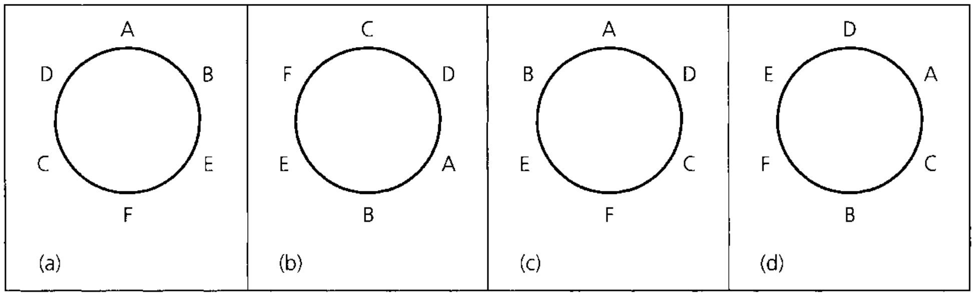


Figure 1.2

We shall try to relate this problem to previous ones we have already encountered. Consider Figs. 1.2(a) and (b). Starting at the top of the circle and moving clockwise, we list the distinct linear arrangements ABEFCD and CDABEF, which correspond to the same circular arrangement. In addition to these two, four other linear arrangements — BEFCDA, DABEFC, EFCDAB, and FCDABE — are found to correspond to the same circular arrangement as in (a) or (b). So inasmuch as each circular arrangement corresponds to six linear arrangements, we have 6 × (Number of circular arrangements of A, B, . . . , F) = (Number of linear arrangements of A, B, . . . , F) = 6!.

Consequently, there are $6!/6 = 5! = 120$ arrangements of A, B, . . . , F around the circular table.

EXAMPLE 1.17

Suppose now that the six people of Example 1.16 are three married couples and that A, B, and C are the females. We want to arrange the six people around the table so that the sexes alternate. (Once again, arrangements are considered identical if one can be obtained from the other by rotation.)

Before we solve this problem, let us solve Example 1.16 by an alternative method, which will assist us in solving our present problem. If we place A at the table as shown in Fig. 1.3(a), five locations (clockwise from A) remain to be filled. Using B, C, . . . , F to fill

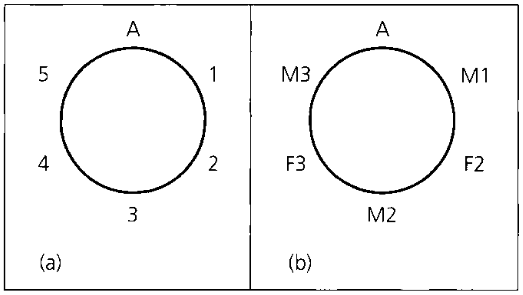


Figure 1.3

these five positions is the problem of permuting B, C, . . . , F in a linear manner, and this can be done in $5! = 120$ ways.

To solve the new problem of alternating the sexes, consider the method shown in Fig. 1.3(b). A (a female) is placed as before. The next position, clockwise from A, is marked M1 (Male 1) and can be filled in three ways. Continuing clockwise from A, position F2 (Female 2) can be filled in two ways. Proceeding in this manner, by the rule of product, there are $3 \times 2 \times 2 \times 1 \times 1 = 12$ ways in which these six people can be arranged with no two men or women seated next to each other.

EXERCISES 1.1 AND 1.2

1. During a local campaign, eight Republican and five Democratic candidates are nominated for president of the school board.

a) If the president is to be one of these candidates, how many possibilities are there for the eventual winner?

b) How many possibilities exist for a pair of candidates (one from each party) to oppose each other for the eventual election?

c) Which counting principle is used in part (a)? in part (b)?

2. Answer part (c) of Example 1.6.

3. Buick automobiles come in four models, 12 colors, three engine sizes, and two transmission types. (a) How many distinct Buicks can be manufactured? (b) If one of the available colors is blue, how many different blue Buicks can be manufactured?

4. The board of directors of a pharmaceutical corporation has 10 members. An upcoming stockholders' meeting is scheduled to approve a new slate of company officers (chosen from the 10 board members).

a) How many different slates consisting of a president, vice president, secretary, and treasurer can the board present to the stockholders for their approval?

b) Three members of the board of directors are physicians. How many slates from part (a) have (i) a physician nominated for the presidency? (ii) exactly one physician appearing on the slate? (iii) at least one physician appearing on the slate?

5. While on a Saturday shopping spree Jennifer and Tiffany witnessed two men driving away from the front of a jewelry shop, just before a burglar alarm started to sound. Although everything happened rather quickly, when the two young ladies were questioned they were able to give the police the following information about the license plate (which consisted of two letters followed by four digits) on the get-away car. Tiffany was sure that the second letter on the plate was either an O or a Q and the last digit was either a 3 or an 8. Jennifer told the investigator that the first letter on the plate was either a C or a G and that the first digit was definitely a 7. How many different license plates will the police have to check out?

6. To raise money for a new municipal pool, the chamber of commerce in a certain city sponsors a race. Each participant pays a \$5 entrance fee and has a chance to win one of the different-sized trophies that are to be awarded to the first eight runners who finish.

a) If 30 people enter the race, in how many ways will it be possible to award the trophies?

b) If Roberta and Candice are two participants in the race, in how many ways can the trophies be awarded with these two runners among the top three?

7. A certain "Burger Joint" advertises that a customer can have his or her hamburger with or without any or all of the following: catsup, mustard, mayonnaise, lettuce, tomato, onion, pickle, cheese, or mushrooms. How many different kinds of hamburger orders are possible?

8. Matthew works as a computer operator at a small university. One evening he finds that 12 computer programs have been submitted earlier that day for batch processing. In how many ways can Matthew order the processing of these programs if (a) there are no restrictions? (b) he considers four of the programs higher in priority than the other eight and wants to process those four first? (c) he first separates the programs into four of top priority, five of lesser priority, and three of least priority, and he wishes to process the 12 programs in such a way that the top-priority programs are processed first and the three programs of least priority are processed last?

9. Patter's Pastry Parlor offers eight different kinds of pastry and six different kinds of muffins. In addition to bakery items one can purchase small, medium, or large containers of the following beverages: coffee (black, with cream, with sugar, or with cream and sugar), tea (plain, with cream, with sugar, with cream and sugar, with lemon, or with lemon and sugar), hot cocoa, and orange juice. When Carol comes to Patter's, in how many ways can she order

a) one bakery item and one medium-sized beverage for herself?

b) one bakery item and one container of coffee for herself and one muffin and one container of tea for her boss, Ms. Didio?

c) one piece of pastry and one container of tea for herself, one muffin and a container of orange juice for Ms. Didio, and one bakery item and one container of coffee for each of her two assistants, Mr. Talbot and Mrs. Gillis?

10. Pamela has 15 different books. In how many ways can she place her books on two shelves so that there is at least one book on each shelf? (Consider the books in each arrangement to be stacked one next to the other, with the first book on each shelf at the left of the shelf.)

11. Three small towns, designated by A, B, and C, are interconnected by a system of two-way roads, as shown in Fig. 1.4.

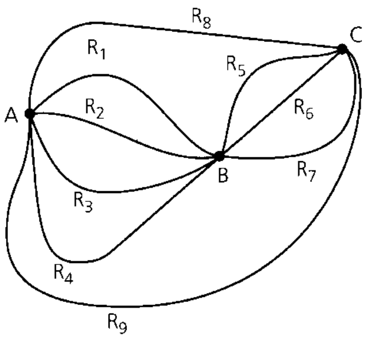


Figure 1.4

a) In how many ways can Linda travel from town A to town C?

b) How many different round trips can Linda travel from town A to town C and back to town A?

c) How many of the round trips in part (b) are such that the return trip (from town C to town A) is at least partially different from the route Linda takes from town A to town C? (For example, if Linda travels from town A to town C along roads R_1 and R_6, then on her return she might take roads R_6 and R_3, or roads R_7 and R_2, or road R_9, among other possibilities, but she does *not* travel on roads R_6 *and* R_1.)

12. List all the permutations for the letters a, c, t.

13. a) How many permutations are there for the eight letters a, c, f, g, i, t, w, x?

b) Consider the permutations in part (a). How many start with the letter t? How many start with the letter t and end with the letter c?

14. Evaluate each of the following.

a) $P(7, 2)$ **b)** $P(8, 4)$ **c)** $P(10, 7)$ **d)** $P(12, 3)$

15. In how many ways can the symbols a, b, c, d, e, e, e, e, e be arranged so that no e is adjacent to another e?

16. An alphabet of 40 symbols is used for transmitting messages in a communication system. How many distinct messages (lists of symbols) of 25 symbols can the transmitter generate if symbols can be repeated in the message? How many if 10 of the 40 symbols can appear only as the first and/or last symbols of the message, the other 30 symbols can appear anywhere, and repetitions of all symbols are allowed?

17. In the Internet each network interface of a computer is assigned one, or more, Internet addresses. The nature of these Internet addresses is dependent on network size. For the Internet Standard regarding reserved network numbers (STD 2), each address is a 32-bit string which falls into one of the following three classes: (1) A class A address, used for the largest networks, begins with a 0 which is then followed by a seven-bit *network number*, and then a 24-bit *local address*. However, one is restricted from using the network numbers of all 0's or all 1's and the local addresses of all 0's or all 1's. (2) The class B address is meant for an intermediate-sized network. This address starts with the two-bit string 10, which is followed by a 14-bit network number and then a 16-bit local address. But the local addresses of all 0's or all 1's are not permitted. (3) Class C addresses are used for the smallest networks. These addresses consist of the three-bit string 110, followed by a 21-bit network number, and then an eight-bit local address. Once again the local addresses of all 0's or all 1's are excluded. How many different addresses of each class are available on the Internet, for this Internet Standard?

18. Morgan is considering the purchase of a low-end computer system. After some careful investigating, she finds that there are seven basic systems (each consisting of a monitor, CPU, keyboard, and mouse) that meet her requirements. Furthermore, she also plans to buy one of four modems, one of three CD ROM drives, and one of six printers. (Here each peripheral device of a given type, such as the modem, is compatible with all seven basic systems.) In how many ways can Morgan configure her low-end computer system?

19. A computer science professor has seven different programming books on a bookshelf. Three of the books deal with C++, the other four with Java. In how many ways can the professor arrange these books on the shelf (a) if there are no restrictions? (b) if the languages should alternate? (c) if all the C++ books must be next to each other? (d) if all the C++ books must be next to each other and all the Java books must be next to each other?

20. Over the Internet, data are transmitted in structured blocks of bits called *datagrams*.

a) In how many ways can the letters in DATAGRAM be arranged?

b) For the arrangements of part (a), how many have all three A's together?

21. **a)** How many arrangements are there of all the letters in SOCIOLOGICAL?

b) In how many of the arrangements in part (a) are A and G adjacent?

c) In how many of the arrangements in part (a) are all the vowels adjacent?

22. How many positive integers n can we form using the digits 3, 4, 4, 5, 5, 6, 7 if we want n to exceed 5,000,000?

23. Twelve clay targets (identical in shape) are arranged in four hanging columns, as shown in Fig. 1.5. There are four red targets in the first column, three white ones in the second column, two green targets in the third column, and three blue ones in the fourth column. To join her college drill team, Deborah must break all 12 of these targets (using her pistol and only 12 bullets) and in so doing must always break the existing target at the bottom of a column. Under these conditions, in how many different orders can Deborah shoot down (and break) the 12 targets?

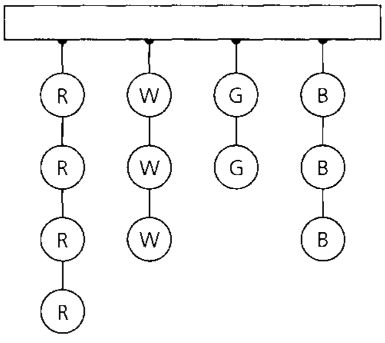


Figure 1.5

24. Show that for all integers $n, r \geq 0$, if $n + 1 > r$, then

$$P(n+1, r) = \left(\frac{n+1}{n+1-r}\right) P(n, r).$$

25. Find the value(s) of n in each of the following:
(a) $P(n, 2) = 90$, (b) $P(n, 3) = 3P(n, 2)$, and
(c) $2P(n, 2) + 50 = P(2n, 2)$.

26. How many different paths in the xy-plane are there from (0, 0) to (7, 7) if a path proceeds one step at a time by going either one space to the right (R) or one space upward (U)? How many such paths are there from (2, 7) to (9, 14)? Can any general statement be made that incorporates these two results?

27. **a)** How many distinct paths are there from $(-1, 2, 0)$ to $(1, 3, 7)$ in Euclidean three-space if each move is one of the following types?

$$(H)\colon (x, y, z) \to (x+1, y, z);$$
$$(V)\colon (x, y, z) \to (x, y+1, z);$$
$$(A)\colon (x, y, z) \to (x, y, z+1)$$

b) How many such paths are there from (1, 0, 5) to (8, 1, 7)?

c) Generalize the results in parts (a) and (b).

28. **a)** Determine the value of the integer variable *counter* after execution of the following program segment. (Here i, j, and k are integer variables.)

```
counter := 0
for i := 1 to 12 do
  counter := counter + 1
for j := 5 to 10 do
  counter := counter + 2
for k := 15 downto 8 do
  counter := counter + 3
```

b) Which counting principle is at play in part (a)?

29. Consider the following program segment where i, j, and k are integer variables.

```
for i := 1 to 12 do
  for j := 5 to 10 do
    for k := 15 downto 8 do
      print (i - j)*k
```

a) How many times is the **print** statement executed?

b) Which counting principle is used in part (a)?

30. A sequence of letters of the form abcba, where the expression is unchanged upon reversing order, is an example of a *palindrome* (of five letters). (a) If a letter may appear more than twice, how many palindromes of five letters are there? of six letters? (b) Repeat part (a) under the condition that no letter appears more than twice.

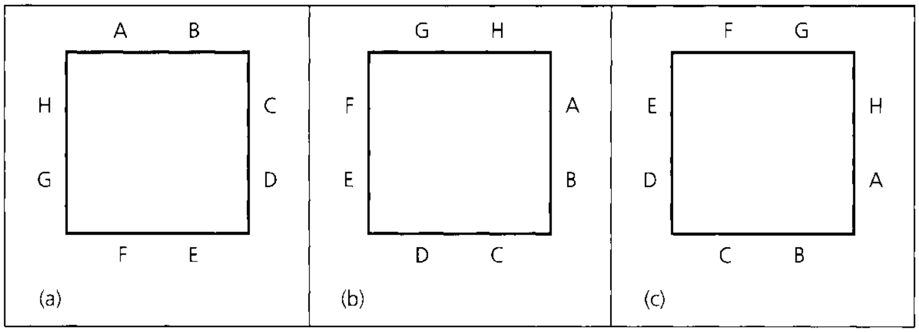


Figure 1.6

31. Determine the number of six-digit integers (no leading zeros) in which (a) no digit may be repeated; (b) digits may be repeated. Answer parts (a) and (b) with the extra condition that the six-digit integer is (i) even; (ii) divisible by 5; (iii) divisible by 4.

32. **a)** Provide a combinatorial argument to show that if n and k are positive integers with $n = 3k$, then $n!/(3!)^k$ is an integer.

b) Generalize the result of part (a).

33. **a)** In how many possible ways could a student answer a 10-question true-false test?

b) In how many ways can the student answer the test in part (a) if it is possible to leave a question unanswered in order to avoid an extra penalty for a wrong answer?

34. How many distinct four-digit integers can one make from the digits 1, 3, 3, 7, 7, and 8?

35. **a)** In how many ways can seven people be arranged about a circular table?

b) If two of the people insist on sitting next to each other, how many arrangements are possible?

36. **a)** In how many ways can eight people, denoted A, B, . . . , H be seated about the square table shown in Fig. 1.6, where Figs. 1.6(a) and 1.6(b) are considered the same but are distinct from Fig. 1.6(c)?

b) If two of the eight people, say A and B, do not get along well, how many different seatings are possible with A and B not sitting next to each other?

37. Sixteen people are to be seated at two circular tables, one of which seats 10 while the other seats six. How many different seating arrangements are possible?

38. A committee of 15 — nine women and six men — is to be seated at a circular table (with 15 seats). In how many ways can the seats be assigned so that no two men are seated next to each other?

39. Write a computer program (or develop an algorithm) to determine whether there is a three-digit integer abc ($= 100a + 10b + c$) where $abc = a! + b! + c!$.

1.3 Combinations: The Binomial Theorem

The standard deck of playing cards consists of 52 cards comprising four suits: clubs, diamonds, hearts, and spades. Each suit has 13 cards: ace, 2, 3, . . . , 9, 10, jack, queen, king. If we are asked to draw three cards from a standard deck, in succession and without replacement, then by the rule of product there are

$$52 \times 51 \times 50 = \frac{52!}{49!} = P(52, 3)$$

possibilities, one of which is AH (ace of hearts), 9C (nine of clubs), KD (king of diamonds). If instead we simply select three cards at one time from the deck so that the order of selection of the cards is no longer important, then the six permutations AH–9C–KD, AH–KD–9C, 9C–AH–KD, 9C–KD–AH, KD–9C–AH, and KD–AH–9C all correspond to just one (unordered) selection. Consequently, each selection, or combination, of three cards, *with no reference to order*, corresponds to 3! permutations of three cards. In equation form this translates into

$$\begin{aligned}(3!) \times (\text{Number of selections of size 3 from a deck of 52})\\ &= \text{Number of permutations of size 3 for the 52 cards}\\ &= P(52, 3) = \frac{52!}{49!}.\end{aligned}$$

Consequently, three cards can be drawn, without replacement, from a standard deck in $52!/(3!\,49!) = 22{,}100$ ways.

If we start with n distinct objects, each *selection*, or *combination*, of r of these objects, with no reference to order, corresponds to $r!$ permutations of size r from the n objects. Thus the number of combinations of size r from a collection of size n is

$$C(n, r) = \frac{P(n, r)}{r!} = \frac{n!}{r!(n-r)!}, \qquad 0 \leq r \leq n.$$

In addition to $C(n, r)$ the symbol $\binom{n}{r}$ is also frequently used. Both $C(n, r)$ and $\binom{n}{r}$ are sometimes read "n choose r." Note that for all $n \geq 0$, $C(n, 0) = C(n, n) = 1$. Further, for all $n \geq 1$, $C(n, 1) = C(n, n-1) = n$. When $0 \leq n < r$, then $C(n, r) = \binom{n}{r} = 0$.

A word to the wise! When dealing with any counting problem, we should ask ourselves about the importance of order in the problem. When order is relevant, we think in terms of permutations and arrangements and the rule of product. When order is not relevant, combinations could play a key role in solving the problem.

EXAMPLE 1.18

A hostess is having a dinner party for some members of her charity committee. Because of the size of her home, she can invite only 11 of the 20 committee members. Order is not important, so she can invite "the lucky 11" in $C(20, 11) = \binom{20}{11} = 20!/(11!\,9!) = 167{,}960$ ways. However, once the 11 arrive, how she arranges them around her rectangular dining table is an arrangement problem. Unfortunately, no part of the theory of combinations and permutations can help our hostess deal with "the offended nine" who were not invited.

EXAMPLE 1.19

Lynn and Patti decide to buy a PowerBall ticket. To win the grand prize for PowerBall one must match five numbers selected from 1 to 49 inclusive and then must also match the powerball, an integer from 1 to 42 inclusive. Lynn selects the five numbers (between 1 and 49 inclusive). This she can do in $\binom{49}{5}$ ways (since matching does *not* involve order). Meanwhile Patti selects the powerball — here there are $\binom{42}{1}$ possibilities. Consequently, by the rule of product, Lynn and Patti can select the six numbers for their PowerBall ticket in $\binom{49}{5}\binom{42}{1} = 80{,}089{,}128$ ways.

EXAMPLE 1.20

a) A student taking a history examination is directed to answer any seven of 10 essay questions. There is no concern about order here, so the student can answer the examination in

$$\binom{10}{7} = \frac{10!}{7!\,3!} = \frac{10 \times 9 \times 8}{3 \times 2 \times 1} = 120 \text{ ways.}$$

b) If the student must answer three questions from the first five and four questions from the last five, three questions can be selected from the first five in $\binom{5}{3} = 10$ ways, and the other four questions can be selected in $\binom{5}{4} = 5$ ways. Hence, by the rule of product, the student can complete the examination in $\binom{5}{3}\binom{5}{4} = 10 \times 5 = 50$ ways.

c) Finally, should the directions on this examination indicate that the student must answer seven of the 10 questions where at least three are selected from the first five, then there are three cases to consider:

i) The student answers three of the first five questions and four of the last five: By the rule of product this can happen in $\binom{5}{3}\binom{5}{4} = 10 \times 5 = 50$ ways, as in part (b).

ii) Four of the first five questions and three of the last five questions are selected by the student: This can come about in $\binom{5}{4}\binom{5}{3} = 5 \times 10 = 50$ ways — again by the rule of product.

iii) The student decides to answer all five of the first five questions and two of the last five: The rule of product tells us that this last case can occur in $\binom{5}{5}\binom{5}{2} = 1 \times 10 = 10$ ways.

Combining the results for cases (i), (ii), and (iii), by the rule of sum we find that the student can make $\binom{5}{3}\binom{5}{4} + \binom{5}{4}\binom{5}{3} + \binom{5}{5}\binom{5}{2} = 50 + 50 + 10 = 110$ selections of seven (out of 10) questions where each selection includes at least three of the first five questions.

EXAMPLE 1.21

a) At Rydell High School, the gym teacher must select nine girls from the junior and senior classes for a volleyball team. If there are 28 juniors and 25 seniors, she can make the selection in $\binom{53}{9} = 4{,}431{,}613{,}550$ ways.

b) If two juniors and one senior are the best spikers and must be on the team, then the rest of the team can be chosen in $\binom{50}{6} = 15{,}890{,}700$ ways.

c) For a certain tournament the team must comprise four juniors and five seniors. The teacher can select the four juniors in $\binom{28}{4}$ ways. For each of these selections she has $\binom{25}{5}$ ways to choose the five seniors. Consequently, by the rule of product, she can select her team in $\binom{28}{4}\binom{25}{5} = 1{,}087{,}836{,}750$ ways for this particular tournament.

Some problems can be treated from the viewpoint of either arrangements or combinations, depending on how one analyzes the situation. The following example demonstrates this.

EXAMPLE 1.22

The gym teacher of Example 1.21 must make up four volleyball teams of nine girls each from the 36 freshman girls in her P.E. class. In how many ways can she select these four teams? Call the teams A, B, C, and D.

a) To form team A, she can select any nine girls from the 36 enrolled in $\binom{36}{9}$ ways. For team B the selection process yields $\binom{27}{9}$ possibilities. This leaves $\binom{18}{9}$ and $\binom{9}{9}$ possible ways to select teams C and D, respectively. So by the rule of product, the four teams can be chosen in

$$\binom{36}{9}\binom{27}{9}\binom{18}{9}\binom{9}{9} = \left(\frac{36!}{9!\,27!}\right)\left(\frac{27!}{9!\,18!}\right)\left(\frac{18!}{9!\,9!}\right)\left(\frac{9!}{9!\,0!}\right)$$
$$= \frac{36!}{9!\,9!\,9!\,9!} \doteq 2.145 \times 10^{19} \text{ ways.}$$

b) For an alternative solution, consider the 36 students lined up as follows:

1st	2nd	3rd		35th	36th
student	student	student	. . .	student	student

To select the four teams, we must distribute nine A's, nine B's, nine C's, and nine D's in the 36 spaces. The number of ways in which this can be done is the number of arrangements of 36 letters comprising nine each of A, B, C, and D. This is now the familiar problem of arrangements of nondistinct objects, and the answer is

$$\frac{36!}{9!\,9!\,9!\,9!}, \quad \text{as in part (a).}$$

Our next example points out how some problems require the concepts of both arrangements and combinations for their solutions.

EXAMPLE 1.23

The number of arrangements of the letters in TALLAHASSEE is

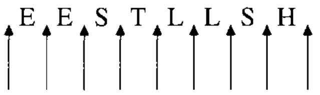
$$\frac{11!}{3!\,2!\,2!\,2!\,1!\,1!} = 831{,}600.$$

How many of these arrangements have no adjacent A's?

When we disregard the A's, there are

$$\frac{8!}{2!\,2!\,2!\,1!\,1!} = 5040$$

ways to arrange the remaining letters. One of these 5040 ways is shown in the following figure, where the arrows indicate nine possible locations for the three A's.



Three of these locations can be selected in $\binom{9}{3} = 84$ ways, and because this is also possible for all the other 5039 arrangements of E, E, S, T, L, L, S, H, by the rule of product there are 5040 × 84 = 423,360 arrangements of the letters in TALLAHASSEE with no consecutive A's.

Before proceeding we need to introduce a concise way of writing the sum of a list of $n+1$ terms like $a_m, a_{m+1}, a_{m+2}, \ldots, a_{m+n}$, where m and n are integers and $n \geq 0$. This notation is called the *Sigma notation* because it involves the capital Greek letter Σ; we use it to represent a summation by writing

$$a_m + a_{m+1} + a_{m+2} + \cdots + a_{m+n} = \sum_{i=m}^{m+n} a_i.$$

Here, the letter i is called the *index* of the summation, and this index accounts for all integers starting with the *lower limit* m and continuing on up to (and including) the *upper limit* $m+n$.

We may use this notation as follows.

1) $\sum_{i=3}^{7} a_i = a_3 + a_4 + a_5 + a_6 + a_7 = \sum_{j=3}^{7} a_j$, for there is nothing special about the letter i.

2) $\sum_{i=1}^{4} i^2 = 1^2 + 2^2 + 3^2 + 4^2 = 30 = \sum_{k=0}^{4} k^2$, because $0^2 = 0$.

3) $\sum_{i=11}^{100} i^3 = 11^3 + 12^3 + 13^3 + \cdots + 100^3 = \sum_{j=12}^{101} (j-1)^3 = \sum_{k=10}^{99} (k+1)^3$.

4) $\sum_{i=7}^{10} 2i = 2(7) + 2(8) + 2(9) + 2(10) = 68 = 2(34) = 2(7+8+9+10) = 2\sum_{i=7}^{10} i$.

5) $\sum_{i=3}^{3} a_i = a_3 = \sum_{i=4}^{4} a_{i-1} = \sum_{i=2}^{2} a_{i+1}$.

6) $\sum_{i=1}^{5} a = a + a + a + a + a = 5a$.

Furthermore, using this summation notation, we see that one can express the answer to part (c) of Example 1.20 as

$$\binom{5}{3}\binom{5}{4} + \binom{5}{4}\binom{5}{3} + \binom{5}{5}\binom{5}{2} = \sum_{i=3}^{5}\binom{5}{i}\binom{5}{7-i} = \sum_{j=2}^{4}\binom{5}{7-j}\binom{5}{j}.$$

We shall find use for this new notation in the following example and in many other places throughout the remainder of this book.

EXAMPLE 1.24

In the studies of algebraic coding theory and the theory of computer languages, we consider certain arrangements, called *strings*, made up from a prescribed *alphabet* of symbols. If the prescribed alphabet consists of the symbols 0, 1, and 2, for example, then 01, 11, 21, 12, and 20 are five of the nine strings of *length* 2. Among the 27 strings of length 3 are 000, 012, 202, and 110.

In general, if n is any positive integer, then by the rule of product there are 3^n strings of length n for the alphabet 0, 1, and 2. If $x = x_1x_2x_3 \cdots x_n$ is one of these strings, we define the *weight* of x, denoted wt(x), by wt(x) $= x_1 + x_2 + x_3 + \cdots + x_n$. For example, wt(12) = 3 and wt(22) = 4 for the case where $n = 2$; wt(101) = 2, wt(210) = 3, and wt(222) = 6 for $n = 3$.

Among the 3^{10} strings of length 10, we wish to determine how many have even weight. Such a string has even weight precisely when the number of 1's in the string is even.

There are six different cases to consider. If the string x contains no 1's, then each of the 10 locations in x can be filled with either 0 or 2, and by the rule of product there are 2^{10} such strings. When the string contains two 1's, the locations for these two 1's can be selected in $\binom{10}{2}$ ways. Once these two locations have been specified, there are 2^8 ways to place either 0 or 2 in the other eight positions. Hence there are $\binom{10}{2}2^8$ strings of even weight that contain two 1's. The numbers of strings for the other four cases are given in Table 1.2.

Table 1.2

Number of 1's	Number of Strings	Number of 1's	Number of Strings
4	$\binom{10}{4}2^6$	8	$\binom{10}{8}2^2$
6	$\binom{10}{6}2^4$	10	$\binom{10}{10}$

Consequently, by the rule of sum, the number of strings of length 10 that have even weight is $2^{10} + \binom{10}{2}2^8 + \binom{10}{4}2^6 + \binom{10}{6}2^4 + \binom{10}{8}2^2 + \binom{10}{10} = \sum_{n=0}^{5} \binom{10}{2n}2^{10-2n}$.

Often we must be careful of *overcounting* — a situation that seems to arise in what may appear to be rather easy enumeration problems. The next example demonstrates how overcounting may come about.

EXAMPLE 1.25

a) Suppose that Ellen draws five cards from a standard deck of 52 cards. In how many ways can her selection result in a hand with no clubs? Here we are interested in counting all five-card selections such as

   i) ace of hearts, three of spades, four of spades, six of diamonds, and the jack of diamonds.

   ii) five of spades, seven of spades, ten of spades, seven of diamonds, and the king of diamonds.

   iii) two of diamonds, three of diamonds, six of diamonds, ten of diamonds, and the jack of diamonds.

   If we examine this more closely we see that Ellen is restricted to selecting her five cards from the 39 cards in the deck that are not clubs. Consequently, she can make her selection in $\binom{39}{5}$ ways.

b) Now suppose we want to count the number of Ellen's five-card selections that contain at least one club. These are precisely the selections that were *not* counted in part (a). And since there are $\binom{52}{5}$ possible five-card hands in total, we find that

$$\binom{52}{5} - \binom{39}{5} = 2{,}598{,}960 - 575{,}757 = 2{,}023{,}203$$

   of all five-card hands contain at least one club.

c) Can we obtain the result in part (b) in another way? For example, since Ellen wants to have at least one club in the five-card hand, let her first select a club. This she can do in $\binom{13}{1}$ ways. And now she doesn't care what comes up for the other four cards. So after she eliminates the one club chosen from her standard deck, she can then select the other four cards in $\binom{51}{4}$ ways. Therefore, by the rule of product, we count the number of selections here as

$$\binom{13}{1}\binom{51}{4} = 13 \times 249{,}900 = 3{,}248{,}700.$$

   Something here is definitely *wrong*! This answer is larger than that in part (b) by more than one million hands. Did we make a mistake in part (b)? Or is something wrong with our present reasoning?

   For example, suppose that Ellen first selects

   the three of clubs

   and then selects

   the five of clubs,
   king of clubs,
   seven of hearts, and
   jack of spades.

If, however, she first selects

the five of clubs

and then selects

the three of clubs,
king of clubs,
seven of hearts, and
jack of spades,

is her selection here really different from the prior selection we mentioned? Unfortunately, no! And the case where she first selects

the king of clubs

and then follows this by selecting

the three of clubs,
five of clubs,
seven of hearts, and
jack of spades

is not different from the other two selections mentioned earlier.

Consequently, this approach is *wrong* because we are overcounting — by considering like selections as if they were distinct.

d) But is there any other way to arrive at the answer in part (b)? Yes! Since the five-card hands must each contain at least one club, there are five cases to consider. These are given in Table 1.3. From the results in Table 1.3 we see, for example, that there are $\binom{13}{2}\binom{39}{3}$ five-card hands that contain exactly two clubs. If we are interested in having exactly three clubs in the hand, then the results in the table indicate that there are $\binom{13}{3}\binom{39}{2}$ such hands.

Table 1.3

Number of Clubs	Number of Ways to Select This Number of Clubs	Number of Cards That Are Not Clubs	Number of Ways to Select This Number of Nonclubs
1	$\binom{13}{1}$	4	$\binom{39}{4}$
2	$\binom{13}{2}$	3	$\binom{39}{3}$
3	$\binom{13}{3}$	2	$\binom{39}{2}$
4	$\binom{13}{4}$	1	$\binom{39}{1}$
5	$\binom{13}{5}$	0	$\binom{39}{0}$

Since no two of the cases in Table 1.3 have any five-card hand in common, the number of hands that Ellen can select with at least one club is

$$\binom{13}{1}\binom{39}{4}+\binom{13}{2}\binom{39}{3}+\binom{13}{3}\binom{39}{2}+\binom{13}{4}\binom{39}{1}+\binom{13}{5}\binom{39}{0}$$

$$=\sum_{i=1}^{5}\binom{13}{i}\binom{39}{5-i}$$

$$= (13)(82{,}251) + (78)(9139) + (286)(741) + (715)(39) + (1287)(1)$$

$$= 2{,}023{,}203.$$

We shall close this section with three results related to the concept of combinations.

First we note that for integers n, r, with $n \geq r \geq 0$, $\binom{n}{r} = \binom{n}{n-r}$. This can be established algebraically from the formula for $\binom{n}{r}$, but we prefer to observe that when dealing with a selection of size r from a collection of n distinct objects, the selection process leaves behind $n - r$ objects. Consequently, $\binom{n}{r} = \binom{n}{n-r}$ affirms the existence of a correspondence between the selections of size r (objects chosen) and the selections of size $n - r$ (objects left behind). An example of this correspondence is shown in Table 1.4, where $n = 5$, $r = 2$, and the distinct objects are 1, 2, 3, 4, and 5. This type of correspondence will be more formally defined in Chapter 5 and used in other counting situations.

Table 1.4

Selections of Size $r = 2$ (Objects Chosen)		Selections of Size $n - r = 3$ (Objects Left Behind)	
1. 1, 2	6. 2, 4	1. 3, 4, 5	6. 1, 3, 5
2. 1, 3	7. 2, 5	2. 2, 4, 5	7. 1, 3, 4
3. 1, 4	8. 3, 4	3. 2, 3, 5	8. 1, 2, 5
4. 1, 5	9. 3, 5	4. 2, 3, 4	9. 1, 2, 4
5. 2, 3	10. 4, 5	5. 1, 4, 5	10. 1, 2, 3

Our second result is a theorem from our past experience in algebra.

THEOREM 1.1 *The Binomial Theorem.* If x and y are variables and n is a positive integer, then

$$(x+y)^n = \binom{n}{0}x^0y^n + \binom{n}{1}x^1y^{n-1} + \binom{n}{2}x^2y^{n-2} + \cdots$$

$$+ \binom{n}{n-1}x^{n-1}y^1 + \binom{n}{n}x^ny^0 = \sum_{k=0}^{n}\binom{n}{k}x^ky^{n-k}.$$

Before considering the general proof, we examine a special case. If $n = 4$, the coefficient of x^2y^2 in the expansion of the product

$$\underset{\textbf{1st factor}}{(x+y)}\ \underset{\textbf{2nd factor}}{(x+y)}\ \underset{\textbf{3rd factor}}{(x+y)}\ \underset{\textbf{4th factor}}{(x+y)}$$

is the number of ways in which we can select two x's from the four x's, one of which is available in each factor. (Although the x's are the same in appearance, we distinguish them as the x in the first factor, the x in the second factor, . . . , and the x in the fourth factor. Also, we note that when we select two x's, we use two factors, leaving us with two other factors from which we can select the two y's that are needed.) For example, among the possibilities, we can select (1) x from the first two factors and y from the last two or (2) x from the first and third factors and y from the second and fourth. Table 1.5 summarizes the six possible selections.

Table 1.5

Factors Selected for x		Factors Selected for y	
(1)	1, 2	(1)	3, 4
(2)	1, 3	(2)	2, 4
(3)	1, 4	(3)	2, 3
(4)	2, 3	(4)	1, 4
(5)	2, 4	(5)	1, 3
(6)	3, 4	(6)	1, 2

Consequently, the coefficient of x^2y^2 in the expansion of $(x+y)^4$ is $\binom{4}{2} = 6$, the number of ways to select two distinct objects from a collection of four distinct objects.

Now we turn to the proof of the general case.

Proof: In the expansion of the product

$$\underset{\textbf{1st factor}}{(x+y)}\ \underset{\textbf{2nd factor}}{(x+y)}\ \underset{\textbf{3rd factor}}{(x+y)} \cdots \underset{\textbf{\textit{n}th factor}}{(x+y)}$$

the coefficient of $x^k y^{n-k}$, where $0 \le k \le n$, is the number of different ways in which we can select k x's [and consequently $(n-k)$ y's] from the n available factors. (One way, for example, is to choose x from the first k factors and y from the last $n-k$ factors.) The total number of such selections of size k from a collection of size n is $C(n, k) = \binom{n}{k}$, and from this the binomial theorem follows.

In view of this theorem, $\binom{n}{k}$ is often referred to as a *binomial coefficient*. Notice that it is also possible to express the result of Theorem 1.1 as

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{n-k} x^k y^{n-k}.$$

EXAMPLE 1.26

a) From the binomial theorem it follows that the coefficient of x^5y^2 in the expansion of $(x+y)^7$ is $\binom{7}{5} = \binom{7}{2} = 21$.

b) To obtain the coefficient of a^5b^2 in the expansion of $(2a-3b)^7$, replace $2a$ by x and $-3b$ by y. From the binomial theorem the coefficient of x^5y^2 in $(x+y)^7$ is $\binom{7}{5}$, and $\binom{7}{5}x^5y^2 = \binom{7}{5}(2a)^5(-3b)^2 = \binom{7}{5}(2)^5(-3)^2a^5b^2 = 6048a^5b^2$.

COROLLARY 1.1 For each integer $n > 0$,

a) $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$, and

b) $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n\binom{n}{n} = 0$.

Proof: Part (a) follows from the binomial theorem when we set $x = y = 1$. When $x = -1$ and $y = 1$, part (b) results.

Our third and final result generalizes the binomial theorem and is called the *multinomial theorem.*

THEOREM 1.2 For positive integers n, t, the coefficient of $x_1^{n_1}x_2^{n_2}x_3^{n_3}\cdots x_t^{n_t}$ in the expansion of $(x_1 + x_2 + x_3 + \cdots + x_t)^n$ is

$$\frac{n!}{n_1!\,n_2!\,n_3!\cdots n_t!},$$

where each n_i is an integer with $0 \le n_i \le n$, for all $1 \le i \le t$, and $n_1 + n_2 + n_3 + \cdots + n_t = n$.

Proof: As in the proof of the binomial theorem, the coefficient of $x_1^{n_1}x_2^{n_2}x_3^{n_3}\cdots x_t^{n_t}$ is the number of ways we can select x_1 from n_1 of the n factors, x_2 from n_2 of the $n - n_1$ remaining factors, x_3 from n_3 of the $n - n_1 - n_2$ now remaining factors, ..., and x_t from n_t of the last $n - n_1 - n_2 - n_3 - \cdots - n_{t-1} = n_t$ remaining factors. This can be carried out, as in part (a) of Example 1.22, in

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots\binom{n-n_1-n_2-n_3-\cdots-n_{t-1}}{n_t}$$

ways. We leave to the reader the details of showing that this product is equal to

$$\frac{n!}{n_1!\,n_2!\,n_3!\cdots n_t!},$$

which is also written as

$$\binom{n}{n_1, n_2, n_3, \ldots, n_t}$$

and is called a *multinomial coefficient.* (When $t = 2$ this reduces to a binomial coefficient.)

EXAMPLE 1.27

a) In the expansion of $(x + y + z)^7$ it follows from the multinomial theorem that the coefficient of $x^2y^2z^3$ is $\binom{7}{2,2,3} = \frac{7!}{2!\,2!\,3!} = 210$, while the coefficient of xyz^5 is $\binom{7}{1,1,5} = 42$ and that of x^3z^4 is $\binom{7}{3,0,4} = \frac{7!}{3!\,0!\,4!} = 35$.

b) Suppose we need to know the coefficient of $a^2b^3c^2d^5$ in the expansion of $(a + 2b - 3c + 2d + 5)^{16}$. If we replace a by v, $2b$ by w, $-3c$ by x, $2d$ by y, and 5 by z, then we can apply the multinomial theorem to $(v + w + x + y + z)^{16}$ and determine the coefficient of $v^2w^3x^2y^5z^4$ as $\binom{16}{2,3,2,5,4} = 302{,}702{,}400$. But $\binom{16}{2,3,2,5,4}(a)^2(2b)^3(-3c)^2(2d)^5(5)^4 = \binom{16}{2,3,2,5,4}(1)^2(2)^3(-3)^2(2)^5(5)^4(a^2b^3c^2d^5) = 435{,}891{,}456{,}000{,}000\,a^2b^3c^2d^5$.

EXERCISES 1.3

1. Calculate $\binom{6}{2}$ and check your answer by listing all the selections of size 2 that can be made from the letters a, b, c, d, e, and f.

2. Facing a four-hour bus trip back to college, Diane decides to take along five magazines from the 12 that her sister Ann Marie has recently acquired. In how many ways can Diane make her selection?

3. Evaluate each of the following.

a) $C(10, 4)$ **b)** $\binom{12}{7}$ **c)** $C(14, 12)$ **d)** $\binom{15}{10}$

4. In the Braille system a symbol, such as a lowercase letter, punctuation mark, suffix, and so on, is given by raising at least one of the dots in the six-dot arrangement shown in part (a) of Fig. 1.7. (The six Braille positions are labeled in this part of the figure.) For example, in part (b) of the figure the dots in positions 1 and 4 are raised and this six-dot arrangement represents the letter c. In parts (c) and (d) of the figure we have the representations for the letters m and t, respectively. The definite article "the" is shown in part (e) of the figure, while part (f) contains the form for the suffix "ow." Finally, the semicolon, ; , is given by the six-dot arrangement in part (g), where the dots at positions 2 and 3 are raised.

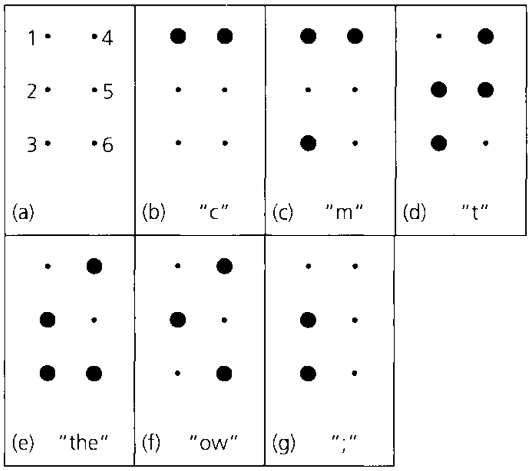


Figure 1.7

a) How many different symbols can we represent in the Braille system?

b) How many symbols have exactly three raised dots?

c) How many symbols have an even number of raised dots?

5. a) How many *permutations* of size 3 can one produce with the letters m, r, a, f, and t?

b) List all the *combinations* of size 3 that result for the letters m, r, a, f, and t.

6. If n is a positive integer and $n > 1$, prove that $\binom{n}{2} + \binom{n-1}{2}$ is a perfect square.

7. A committee of 12 is to be selected from 10 men and 10 women. In how many ways can the selection be carried out if (a) there are no restrictions? (b) there must be six men and six women? (c) there must be an even number of women? (d) there must be more women than men? (e) there must be at least eight men?

8. In how many ways can a gambler draw five cards from a standard deck and get (a) a flush (five cards of the same suit)? (b) four aces? (c) four of a kind? (d) three aces and two jacks? (e) three aces and a pair? (f) a full house (three of a kind and a pair)? (g) three of a kind? (h) two pairs?

9. How many bytes contain (a) exactly two 1's; (b) exactly four 1's; (c) exactly six 1's; (d) at least six 1's?

10. How many ways are there to pick a five-person basketball team from 12 possible players? How many selections include the weakest and the strongest players?

11. A student is to answer seven out of 10 questions on an examination. In how many ways can he make his selection if (a) there are no restrictions? (b) he must answer the first two questions? (c) he must answer at least four of the first six questions?

12. In how many ways can 12 different books be distributed among four children so that (a) each child gets three books? (b) the two oldest children get four books each and the two youngest get two books each?

13. How many arrangements of the letters in MISSISSIPPI have no consecutive S's?

14. A gym coach must select 11 seniors to play on a football team. If he can make his selection in 12,376 ways, how many seniors are eligible to play?

15. a) Fifteen points, no three of which are collinear, are given on a plane. How many lines do they determine?

b) Twenty-five points, no four of which are coplanar, are given in space. How many triangles do they determine? How many planes? How many tetrahedra (pyramidlike solids with four triangular faces)?

16. Determine the value of each of the following summations.

a) $\sum_{i=1}^{6}(i^2+1)$ **b)** $\sum_{j=-2}^{2}(j^3-1)$ **c)** $\sum_{i=0}^{10}[1+(-1)^i]$

d) $\sum_{k=n}^{2n}(-1)^k$, where n is an odd positive integer

e) $\sum_{i=1}^{6} i(-1)^i$

17. Express each of the following using the summation (or Sigma) notation. In parts (a), (d), and (e), n denotes a positive integer.

a) $\frac{1}{2!}+\frac{1}{3!}+\frac{1}{4!}+\cdots+\frac{1}{n!}$, $n \geq 2$

b) $1 + 4 + 9 + 16 + 25 + 36 + 49$

c) $1^3 - 2^3 + 3^3 - 4^3 + 5^3 - 6^3 + 7^3$

d) $\frac{1}{n} + \frac{2}{n+1} + \frac{3}{n+2} + \cdots + \frac{n+1}{2n}$

e) $n - \left(\frac{n+1}{2!}\right) + \left(\frac{n+2}{4!}\right) - \left(\frac{n+3}{6!}\right) + \cdots + (-1)^n \left(\frac{2n}{(2n)!}\right)$

18. For the strings of length 10 in Example 1.24, how many have (a) four 0's, three 1's, and three 2's; (b) at least eight 1's; (c) weight 4?

19. Consider the collection of all strings of length 10 made up from the alphabet 0, 1, 2, and 3. How many of these strings have weight 3? How many have weight 4? How many have even weight?

20. In the three parts of Fig. 1.8, eight points are equally spaced and marked on the circumference of a given circle.

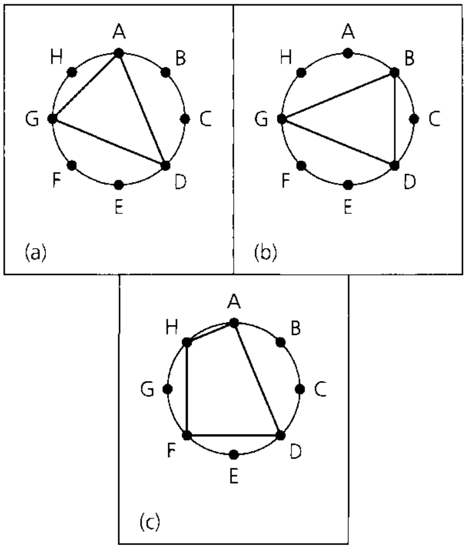


Figure 1.8

a) For parts (a) and (b) of Fig. 1.8 we have two different (though congruent) triangles. These two triangles (distinguished by their vertices) result from two selections of size 3 from the vertices A, B, C, D, E, F, G, H. How many different (whether congruent or not) triangles can we inscribe in the circle in this way?

b) How many different quadrilaterals can we inscribe in the circle, using the marked vertices? [One such quadrilateral appears in part (c) of Fig. 1.8.]

c) How many different polygons of three or more sides can we inscribe in the given circle by using three or more of the marked vertices?

21. How many triangles are determined by the vertices of a regular polygon of n sides? How many if no side of the polygon is to be a side of any triangle?

22. a) In the complete expansion of $(a + b + c + d) \cdot (e + f + g + h)(u + v + w + x + y + z)$ one obtains the sum of terms such as agw, cfx, and dgv. How many such terms appear in this complete expansion?

b) Which of the following terms do *not* appear in the complete expansion from part (a)?

i) afx	ii) bvx	iii) chz
iv) cgw	v) egu	vi) dfz

23. Determine the coefficient of x^9y^3 in the expansions of (a) $(x + y)^{12}$, (b) $(x + 2y)^{12}$, and (c) $(2x - 3y)^{12}$.

24. Complete the details in the proof of the multinomial theorem.

25. Determine the coefficient of

a) xyz^2 in $(x + y + z)^4$

b) xyz^2 in $(w + x + y + z)^4$

c) xyz^2 in $(2x - y - z)^4$

d) xyz^{-2} in $(x - 2y + 3z^{-1})^4$

e) $w^3x^2yz^2$ in $(2w - x + 3y - 2z)^8$

26. Find the coefficient of $w^2x^2y^2z^2$ in the expansion of (a) $(w + x + y + z + 1)^{10}$, (b) $(2w - x + 3y + z - 2)^{12}$, and (c) $(v + w - 2x + y + 5z + 3)^{12}$.

27. Determine the sum of all the coefficients in the expansions of

a) $(x + y)^3$ b) $(x + y)^{10}$ c) $(x + y + z)^{10}$

d) $(w + x + y + z)^5$

e) $(2s - 3t + 5u + 6v - 11w + 3x + 2y)^{10}$

28. For any positive integer n determine

a) $\sum_{i=0}^{n} \frac{1}{i!(n-i)!}$ b) $\sum_{i=0}^{n} \frac{(-1)^i}{i!(n-i)!}$

29. Show that for all positive integers m and n,

$$n\binom{m+n}{m} = (m+1)\binom{m+n}{m+1}.$$

30. With n a positive integer, evaluate the sum

$$\binom{n}{0} + 2\binom{n}{1} + 2^2\binom{n}{2} + \cdots + 2^k\binom{n}{k} + \cdots + 2^n\binom{n}{n}.$$

31. For x a real number and n a positive integer, show that

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

b) $1 = (2 + x)^n - \binom{n}{1}(x + 1)(2 + x)^{n-1} + \binom{n}{2}(x + 1)^2(2 + x)^{n-2} - \cdots + (-1)^n\binom{n}{n}(x + 1)^n$

c) $2^n = (2+x)^n - \binom{n}{1}x^1(2+x)^{n-1} + \binom{n}{2}x^2(2+x)^{n-2} - \cdots + (-1)^n\binom{n}{n}x^n$

32. Determine x if $\sum_{i=0}^{50}\binom{50}{i}8^i = x^{100}$.

33. **a)** If a_0, a_1, a_2, a_3 is a list of four real numbers, what is $\sum_{i=1}^{3}(a_i - a_{i-1})$?

b) Given a list—$a_0, a_1, a_2, \ldots, a_n$—of $n+1$ real numbers, where n is a positive integer, determine $\sum_{i=1}^{n}(a_i - a_{i-1})$.

c) Determine the value of $\sum_{i=1}^{100}\left(\frac{1}{i+2} - \frac{1}{i+1}\right)$.

34. **a)** Write a computer program (or develop an algorithm) that lists all selections of size 2 from the objects 1, 2, 3, 4, 5, 6.

b) Repeat part (a) for selections of size 3.

1.4 Combinations with Repetition

When repetitions are allowed, we have seen that for n distinct objects an arrangement of size r of these objects can be obtained in n^r ways, for an integer $r \geq 0$. We now turn to the comparable problem for combinations and once again obtain a related problem whose solution follows from our previous enumeration principles.

EXAMPLE 1.28

On their way home from track practice, seven high school freshmen stop at a restaurant, where each of them has one of the following: a cheeseburger, a hot dog, a taco, or a fish sandwich. How many different purchases are possible (from the viewpoint of the restaurant)?

Let c, h, t, and f represent cheeseburger, hot dog, taco, and fish sandwich, respectively. Here we are concerned with how many of each item are purchased, not with the order in which they are purchased, so the problem is one of selections, or combinations, with repetition.

In Table 1.6 we list some possible purchases in column (a) and another means of representing each purchase in column (b).

Table 1.6

<table>
<tr><td>1. c, c, h, h, t, t, f</td><td>1. x x | x x | x x | x</td></tr>
<tr><td>2. c, c, c, c, h, t, f</td><td>2. x x x x | x | x | x</td></tr>
<tr><td>3. c, c, c, c, c, c, f</td><td>3. x x x x x x | | | x</td></tr>
<tr><td>4. h, t, t, f, f, f, f</td><td>4. | x | x x | x x x x</td></tr>
<tr><td>5. t, t, t, t, t, f, f</td><td>5. | | x x x x x | x x</td></tr>
<tr><td>6. t, t, t, t, t, t, t</td><td>6. | | x x x x x x x |</td></tr>
<tr><td>7. f, f, f, f, f, f, f</td><td>7. | | | x x x x x x x</td></tr>
<tr><td>(a)</td><td>(b)</td></tr>
</table>

For a purchase in column (b) of Table 1.6 we realize that each x to the left of the first bar (|) represents a c, each x between the first and second bars represents an h, the x's between the second and third bars stand for t's, and each x to the right of the third bar stands for an f. The third purchase, for example, has three consecutive bars because no one bought a hot dog or taco; the bar at the start of the fourth purchase indicates that there were no cheeseburgers in that purchase.

Once again a correspondence has been established between two collections of objects, where we know how to count the number in one collection. For the representations in column (b) of Table 1.6, we are enumerating all arrangements of 10 symbols consisting of seven x's and three |'s, so by our correspondence the number of different purchases for column (a) is

$$\frac{10!}{7!\,3!} = \binom{10}{7}.$$

In this example we note that the seven x's (one for each freshman) correspond to the size of the selection and that the three bars are needed to separate the $3 + 1 = 4$ possible food items that can be chosen.

When we wish to select, *with repetition*, r of n distinct objects, we find (as in Table 1.6) that we are considering all arrangements of r x's and $n - 1$ |'s and that their number is

$$\frac{(n+r-1)!}{r!(n-1)!} = \binom{n+r-1}{r}.$$

Consequently, the number of combinations of n objects taken r at a time, *with repetition*, is $C(n+r-1, r)$.

(In Example 1.28, $n = 4$, $r = 7$, so it is possible for r to exceed n when repetitions are allowed.)

EXAMPLE 1.29

A donut shop offers 20 kinds of donuts. Assuming that there are at least a dozen of each kind when we enter the shop, we can select a dozen donuts in $C(20 + 12 - 1, 12) = C(31, 12) = 141{,}120{,}525$ ways. (Here $n = 20$, $r = 12$.)

EXAMPLE 1.30

President Helen has four vice presidents: (1) Betty, (2) Goldie, (3) Mary Lou, and (4) Mona. She wishes to distribute among them \$1000 in Christmas bonus checks, where each check will be written for a multiple of \$100.

a) Allowing the situation in which one or more of the vice presidents get nothing, President Helen is making a selection of size 10 (one for each unit of \$100) from a collection of size 4 (four vice presidents), with repetition. This can be done in $C(4 + 10 - 1, 10) = C(13, 10) = 286$ ways.

b) If there are to be no hard feelings, each vice president should receive at least \$100. With this restriction, President Helen is now faced with making a selection of size 6 (the remaining six units of \$100) from the same collection of size 4, and the choices now number $C(4 + 6 - 1, 6) = C(9, 6) = 84$. [For example, here the selection 2, 3, 3, 4, 4, 4 is interpreted as follows: Betty does not get anything extra—for there is no 1 in the selection. The one 2 in the selection indicates that Goldie gets an additional \$100. Mary Lou receives an additional \$200 (\$100 for each of the two 3's in the selection). Due to the three 4's, Mona's bonus check will total \$100 + 3(\$100) = \$400.]

c) If each vice president must get at least \$100 and Mona, as executive vice president, gets at least \$500, then the number of ways President Helen can distribute the bonus checks is

$$\underbrace{C(3+2-1,2)}_{\substack{\textbf{Mona gets}\\ \textbf{exactly \$500}}}+\underbrace{C(3+1-1,1)}_{\substack{\textbf{Mona gets}\\ \textbf{exactly \$600}}}+\underbrace{C(3+0-1,0)}_{\substack{\textbf{Mona gets}\\ \textbf{exactly \$700}}}=10=\underbrace{C(4+2-1,2)}_{\substack{\textbf{Using the}\\ \textbf{technique in part (b)}}}$$

Having worked examples utilizing combinations with repetition, we now consider two examples involving other counting principles as well.

EXAMPLE 1.31

In how many ways can we distribute seven bananas and six oranges among four children so that each child receives at least one banana?

After giving each child one banana, consider the number of ways the remaining three bananas can be distributed among these four children. Table 1.7 shows four of the distributions we are considering here. For example, the second distribution in part (a) of Table 1.7 — namely, 1, 3, 3 — indicates that we have given the first child (designated by 1) one additional banana and the third child (designated by 3) two additional bananas. The corresponding arrangement in part (b) of Table 1.7 represents this distribution in terms of three *b*'s and three bars. These six symbols — three of one type (the *b*'s) and three others of a second type (the bars) — can be arranged in $6!/(3!\,3!) = C(6, 3) = C(4 + 3 - 1, 3) = 20$ ways. [Here $n = 4$, $r = 3$.] Consequently, there are 20 ways in which we can distribute the three additional bananas among these four children. Table 1.8 provides the comparable situation for distributing the six oranges. In this case we are arranging nine symbols — six of one type (the *o*'s) and three of a second type (the bars). So now we learn that the number of ways we can distribute the six oranges among these four children is $9!/(6!\,3!) = C(9, 6) = C(4 + 6 - 1, 6) = 84$ ways. [Here $n = 4$, $r = 6$.] Therefore, by the rule of product, there are $20 \times 84 = 1680$ ways to distribute the fruit under the stated conditions.

Table 1.7

1) 1, 2, 3	1) $b \mid b \mid b \mid$
2) 1, 3, 3	2) $b \mid \; \mid b\, b \mid$
3) 3, 4, 4	3) $\mid \mid b \mid b\, b$
4) 4, 4, 4	4) $\mid \mid \mid b\, b\, b$
(a)	**(b)**

Table 1.8

1) 1, 2, 2, 3, 3, 4	1) $o \mid o\, o \mid o\, o \mid o$
2) 1, 2, 2, 4, 4, 4	2) $o \mid o\, o \mid \mid o\, o\, o$
3) 2, 2, 2, 3, 3, 3	3) $\mid o\, o\, o \mid o\, o\, o \mid$
4) 4, 4, 4, 4, 4, 4	4) $\mid \mid \mid o\, o\, o\, o\, o\, o$
(a)	**(b)**

EXAMPLE 1.32

A message is made up of 12 different symbols and is to be transmitted through a communication channel. In addition to the 12 symbols, the transmitter will also send a total of 45 (blank) spaces between the symbols, with at least three spaces between each pair of consecutive symbols. In how many ways can the transmitter send such a message?

There are 12! ways to arrange the 12 different symbols, and for each of these arrangements there are 11 positions between the 12 symbols. Because there must be at least three spaces between successive symbols, we use up 33 of the 45 spaces and must now locate the remaining 12 spaces. This is now a selection, with repetition, of size 12 (the spaces) from a collection of size 11 (the locations), and this can be accomplished in $C(11 + 12 - 1, 12) = 646{,}646$ ways.

Consequently, by the rule of product the transmitter can send such messages with the required spacing in $(12!)\binom{22}{12} \doteq 3.097 \times 10^{14}$ ways.

In the next example an idea is introduced that appears to have more to do with number theory than with combinations or arrangements. Nonetheless, the solution of this example will turn out to be equivalent to counting combinations with repetitions.

EXAMPLE 1.33

Determine all integer solutions to the equation

$$x_1 + x_2 + x_3 + x_4 = 7, \qquad \text{where } x_i \geq 0 \quad \text{for all } 1 \leq i \leq 4.$$

One solution of the equation is $x_1 = 3, x_2 = 3, x_3 = 0, x_4 = 1$. (This is different from a solution such as $x_1 = 1, x_2 = 0, x_3 = 3, x_4 = 3$, even though the same four integers are being used.) A possible interpretation for the solution $x_1 = 3, x_2 = 3, x_3 = 0, x_4 = 1$ is that we are distributing seven pennies (identical objects) among four children (distinct containers), and here we have given three pennies to each of the first two children, nothing to the third child, and the last penny to the fourth child. Continuing with this interpretation, we see that each nonnegative integer solution of the equation corresponds to a selection, with repetition, of size 7 (the *identical* pennies) from a collection of size 4 (the *distinct* children), so there are $C(4 + 7 - 1, 7) = 120$ solutions.

At this point it is crucial that we recognize the equivalence of the following:

a) The number of integer solutions of the equation

$$x_1 + x_2 + \cdots + x_n = r, \qquad x_i \geq 0, \qquad 1 \leq i \leq n.$$

b) The number of selections, with repetition, of size r from a collection of size n.

c) The number of ways r identical objects can be distributed among n distinct containers.

In terms of distributions, part (c) is valid only when the r objects being distributed are identical and the n containers are distinct. When both the r objects and the n containers are distinct, we can select any of the n containers for each one of the objects and get n^r distributions by the rule of product.

When the objects are distinct but the containers are identical, we shall solve the problem using the Stirling numbers of the second kind (Chapter 5). For the final case, in which both objects and containers are identical, the theory of partitions of integers (Chapter 9) will provide some necessary results.

EXAMPLE 1.34

In how many ways can one distribute 10 (identical) white marbles among six distinct containers?

Solving this problem is equivalent to finding the number of nonnegative integer solutions to the equation $x_1 + x_2 + \cdots + x_6 = 10$. That number is the number of selections of size 10, with repetition, from a collection of size 6. Hence the answer is $C(6 + 10 - 1, 10) = 3003$.

We now examine two other examples related to the theme of this section.

EXAMPLE 1.35

From Example 1.34 we know that there are 3003 nonnegative integer solutions to the equation $x_1 + x_2 + \cdots + x_6 = 10$. How many such solutions are there to the inequality $x_1 + x_2 + \cdots + x_6 < 10$?

One approach that may seem feasible in dealing with this inequality is to determine the number of such solutions to $x_1 + x_2 + \cdots + x_6 = k$, where k is an integer and $0 \leq k \leq 9$. Although feasible now, the technique becomes unrealistic if 10 is replaced by a somewhat larger number, say 100. In Example 3.12 of Chapter 3, however, we shall establish a combinatorial identity that will help us obtain an alternative solution to the problem by using this approach.

For the present we transform the problem by noting the correspondence between the nonnegative integer solutions of

$$x_1 + x_2 + \cdots + x_6 < 10 \qquad (1)$$

and the integer solutions of

$$x_1 + x_2 + \cdots + x_6 + x_7 = 10, \qquad 0 \leq x_i, \qquad 1 \leq i \leq 6, \qquad 0 < x_7. \qquad (2)$$

The number of solutions of Eq. (2) is the same as the number of nonnegative integer solutions of $y_1 + y_2 + \cdots + y_6 + y_7 = 9$, where $y_i = x_i$ for $1 \leq i \leq 6$, and $y_7 = x_7 - 1$. This is $C(7 + 9 - 1, 9) = 5005$.

Our next result takes us back to the binomial and multinomial expansions.

EXAMPLE 1.36

In the binomial expansion for $(x + y)^n$, each term is of the form $\binom{n}{k}x^k y^{n-k}$, so the total number of terms in the expansion is the number of nonnegative integer solutions of $n_1 + n_2 = n$ (n_1 is the exponent for x, n_2 the exponent for y). This number is $C(2 + n - 1, n) = n + 1$.

Perhaps it seems that we have used a rather long-winded argument to get this result. Many of us would probably be willing to believe the result on the basis of our experiences in expanding $(x + y)^n$ for various small values of n.

Although experience is worthwhile in pattern recognition, it is not always enough to find a general principle. Here it would prove of little value if we wanted to know how many terms there are in the expansion of $(w + x + y + z)^{10}$.

Each distinct term here is of the form $\binom{10}{n_1, n_2, n_3, n_4} w^{n_1} x^{n_2} y^{n_3} z^{n_4}$, where $0 \leq n_i$ for $1 \leq i \leq 4$, and $n_1 + n_2 + n_3 + n_4 = 10$. This last equation can be solved in $C(4 + 10 - 1, 10) = 286$ ways, so there are 286 terms in the expansion of $(w + x + y + z)^{10}$.

And now once again the binomial expansion will come into play, as we find ourselves using part (a) of Corollary 1.1

EXAMPLE 1.37

a) Let us determine all the different ways in which we can write the number 4 as a sum of positive integers, where the order of the summands is considered relevant. These representations are called the *compositions* of 4 and may be listed as follows:

1) 4
2) $3 + 1$
3) $1 + 3$
4) $2 + 2$
5) $2 + 1 + 1$
6) $1 + 2 + 1$
7) $1 + 1 + 2$
8) $1 + 1 + 1 + 1$

Here we include the sum consisting of only one summand — namely, 4. We find that for the number 4 there are eight compositions in total. (If we do *not* care about the order of the summands, then the representations in (2) and (3) are no longer considered to be different — nor are the representations in (5), (6), and (7). Under these circumstances we find that there are five *partitions* for the number 4 — namely, 4; $3 + 1$; $2 + 2$; $2 + 1 + 1$; and $1 + 1 + 1 + 1$. We shall learn more about partitions of positive integers in Section 9.3.)

b) Now suppose that we wish to *count* the number of compositions for the number 7. Here we do *not* want to list all of the possibilities — which include 7; $6 + 1$; $1 + 6$; $5 + 2$; $1 + 2 + 4$; $2 + 4 + 1$; and $3 + 1 + 2 + 1$. To count all of these compositions, let us consider the number of possible summands.

i) For one summand there is only one composition — namely, 7.

ii) If there are two (positive) summands, we want to count the number of integer solutions for

$$w_1 + w_2 = 7, \qquad \text{where } w_1, w_2 > 0.$$

This is equal to the number of integer solutions for

$$x_1 + x_2 = 5, \qquad \text{where } x_1, x_2 \geq 0.$$

The number of such solutions is $\binom{2+5-1}{5} = \binom{6}{5}$.

iii) Continuing with our next case, we examine the compositions with three (positive) summands. So now we want to count the number of *positive* integer solutions for

$$y_1 + y_2 + y_3 = 7.$$

This is equal to the number of *nonnegative* integer solutions for

$$z_1 + z_2 + z_3 = 4,$$

and that number is $\binom{3+4-1}{4} = \binom{6}{4}$.

We summarize cases (i), (ii), and (iii), and the other four cases in Table 1.9, where we recall for case (i) that $1 = \binom{6}{6}$.

Table 1.9

n = The Number of Summands in a Composition of 7		The Number of Compositions of 7 with n Summands	
(i)	$n = 1$	(i)	$\binom{6}{6}$
(ii)	$n = 2$	(ii)	$\binom{6}{5}$
(iii)	$n = 3$	(iii)	$\binom{6}{4}$
(iv)	$n = 4$	(iv)	$\binom{6}{3}$
(v)	$n = 5$	(v)	$\binom{6}{2}$
(vi)	$n = 6$	(vi)	$\binom{6}{1}$
(vii)	$n = 7$	(vii)	$\binom{6}{0}$

Consequently, the results from the right-hand side of our table tell us that the (total) number of compositions of 7 is

$$\binom{6}{6}+\binom{6}{5}+\binom{6}{4}+\binom{6}{3}+\binom{6}{2}+\binom{6}{1}+\binom{6}{0}=\sum_{k=0}^{6}\binom{6}{k}.$$

From part (a) of Corollary 1.1 this reduces to 2^6.

In general, one finds that for each positive integer m, there are $\sum_{k=0}^{m-1}\binom{m-1}{k}=2^{m-1}$ compositions.

EXAMPLE 1.38

From Example 1.37 we know that there are $2^{12-1}=2^{11}=2048$ compositions of 12. If our interest is in those compositions where each summand is even, then we consider, for instance, compositions such as

$$\begin{array}{ll} 2+4+6=2(1+2+3) & 2+8+2=2(1+4+1) \\ 8+2+2=2(4+1+1) & 6+6=2(3+3). \end{array}$$

In each of these four examples, the parenthesized expression is a composition of 6. This observation indicates that the number of compositions of 12, where each summand is even, equals the number of (all) compositions of 6, which is $2^{6-1}=2^5=32$.

Our next two examples provide applications from the area of computer science. Furthermore, the second example will lead to an important summation formula that we shall use in many later chapters.

EXAMPLE 1.39

Consider the following program segment, where i, j, and k are integer variables.

```
for i := 1 to 20 do
  for j := 1 to i do
    for k := 1 to j do
      print (i * j + k)
```

How many times is the **print** statement executed in this program segment?

Among the possible choices for i, j, and k (in the order i–first, j–second, k–third) that will lead to execution of the **print** statement, we list (1) 1, 1, 1; (2) 2, 1, 1; (3) 15, 10, 1; and (4) 15, 10, 7. We note that $i=10$, $j=12$, $k=5$ is not one of the selections to be considered, because $j=12>10=i$; this violates the condition set forth in the second **for** loop. Each of the above four selections where the **print** statement is executed satisfies the condition $1\le k\le j\le i\le 20$. In fact, any selection a, b, c ($a\le b\le c$) of size 3, with repetitions allowed, from the list 1, 2, 3, . . . , 20 results in one of the correct selections: here, $k=a$, $j=b$, $i=c$. Consequently the **print** statement is executed

$$\binom{20+3-1}{3}=\binom{22}{3}=1540 \text{ times.}$$

If there had been r (≥ 1) **for** loops instead of three, the **print** statement would have been executed $\binom{20+r-1}{r}$ times.

EXAMPLE 1.40

Here we use a program segment to derive a summation formula. In this program segment, the variables i, j, n, and *counter* are integer variables. Furthermore, we assume that the value of n has been set prior to this segment.

```
counter := 0
for i := 1 to n do
  for j := 1 to i do
    counter := counter + 1
```

From the results in Example 1.39, after this segment is executed the value of (the variable) *counter* will be $\binom{n+2-1}{2} = \binom{n+1}{2}$. (This is also the number of times that the statement

(*) `counter := counter + 1`

is executed.)

This result can also be obtained as follows: When $i := 1$, then j varies from 1 to 1 and (*) is executed once; when i is assigned the value 2, then j varies from 1 to 2 and (*) is executed twice; j varies from 1 to 3 when i is assigned the value 3, and (*) is executed three times; in general, for $1 \leq k \leq n$, when $i := k$, then j varies from 1 to k and (*) is executed k times. In total, the variable *counter* is incremented [and the statement (*) is executed] $1 + 2 + 3 + \cdots + n$ times.

Consequently,

$$\sum_{i=1}^{n} i = 1 + 2 + 3 + \cdots + n = \binom{n+1}{2} = \frac{n(n+1)}{2}.$$

The derivation of this summation formula, obtained by counting the same result in two different ways, constitutes a combinatorial proof.

Our last example for this section introduces the idea of a run, a notion that arises in statistics — in particular, in the detecting of trends in a statistical process.

EXAMPLE 1.41

The counter at Patti and Terri's Bar has 15 bar stools. Upon entering the bar Darrell finds the stools occupied as follows:

O O E O O O O E E E O O O E O,

where O indicates an occupied stool and E an empty one. (Here we are not concerned with the occupants of the stools, just whether or not a stool is occupied.) In this case we say that the occupancy of the 15 stools determines seven runs, as shown:

$$\underbrace{\text{OO}}_{\textbf{Run}}\ \underbrace{\text{E}}_{\textbf{Run}}\ \underbrace{\text{OOOO}}_{\textbf{Run}}\ \underbrace{\text{EEE}}_{\textbf{Run}}\ \underbrace{\text{OOO}}_{\textbf{Run}}\ \underbrace{\text{E}}_{\textbf{Run}}\ \underbrace{\text{O}}_{\textbf{Run}}\ .$$

In general, a *run* is a consecutive list of identical entries that are preceded and followed by different entries or no entries at all.

A second way in which five E's and 10 O's can be arranged to provide seven runs is

E O O O E E O O E O O O O O E.

We want to find the total number of ways five E's and 10 O's can determine seven runs. If the first run starts with an E, then there must be four runs of E's and three runs of O's. Consequently, the last run must end with an E.

Let x_1 count the number of E's in the first run, x_2 the number of O's in the second run, x_3 the number of E's in the third run, . . . , and x_7 the number of E's in the seventh run. We want to find the number of integer solutions for

$$x_1 + x_3 + x_5 + x_7 = 5, \qquad x_1, x_3, x_5, x_7 > 0 \tag{3}$$

and

$$x_2 + x_4 + x_6 = 10, \qquad x_2, x_4, x_6 > 0. \tag{4}$$

The number of integer solutions for Eq. (3) equals the number of integer solutions for

$$y_1 + y_3 + y_5 + y_7 = 1, \qquad y_1, y_3, y_5, y_7 \geq 0.$$

This number is $\binom{4+1-1}{1} = \binom{4}{1} = 4$. Similarly, for Eq. (4), the number of solutions is $\binom{3+7-1}{7} = \binom{9}{7} = 36$. Consequently, by the rule of product there are $4 \cdot 36 = 144$ arrangements of five E's and 10 O's that determine seven runs, the first run starting with E.

The seven runs may also have the first run starting with an O and the last run ending with an O. So now let w_1 count the number of O's in the first run, w_2 the number of E's in the second run, w_3 the number of O's in the third run, . . . , and w_7 the number of O's in the seventh run. Here we want the number of integer solutions for

$$w_1 + w_3 + w_5 + w_7 = 10, \qquad w_1, w_3, w_5, w_7 > 0$$

and

$$w_2 + w_4 + w_6 = 5, \qquad w_2, w_4, w_6 > 0.$$

Arguing as above, we find that the number of ways to arrange five E's and 10 O's, resulting in seven runs where the first run starts with an O, is $\binom{4+6-1}{6}\binom{3+2-1}{2} = \binom{9}{6}\binom{4}{2} = 504$.

Consequently, by the rule of sum, the five E's and 10 O's can be arranged in $144 + 504 = 648$ ways to produce seven runs.

EXERCISES 1.4

1. In how many ways can 10 (identical) dimes be distributed among five children if (a) there are no restrictions? (b) each child gets at least one dime? (c) the oldest child gets at least two dimes?

2. In how many ways can 15 (identical) candy bars be distributed among five children so that the youngest gets only one or two of them?

3. Determine how many ways 20 coins can be selected from four large containers filled with pennies, nickels, dimes, and quarters. (Each container is filled with only one type of coin.)

4. A certain ice cream store has 31 flavors of ice cream available. In how many ways can we order a dozen ice cream cones if (a) we do not want the same flavor more than once? (b) a flavor may be ordered as many as 12 times? (c) a flavor may be ordered no more than 11 times?

5. a) In how many ways can we select five coins from a collection of 10 consisting of one penny, one nickel, one dime, one quarter, one half-dollar, and five (identical) Susan B. Anthony dollars?

b) In how many ways can we select n objects from a collection of size $2n$ that consists of n distinct and n identical objects?

6. Answer Example 1.32, where the 12 symbols being transmitted are four A's, four B's, and four C's.

7. Determine the number of integer solutions of

$$x_1 + x_2 + x_3 + x_4 = 32,$$

where

a) $x_i \geq 0, \quad 1 \leq i \leq 4$ **b)** $x_i > 0, \quad 1 \leq i \leq 4$

c) $x_1, x_2 \geq 5, \quad x_3, x_4 \geq 7$

d) $x_i \geq 8, \quad 1 \leq i \leq 4$ **e)** $x_i \geq -2, \quad 1 \leq i \leq 4$

f) $x_1, x_2, x_3 > 0, \quad 0 < x_4 \leq 25$

8. In how many ways can a teacher distribute eight chocolate donuts and seven jelly donuts among three student helpers if each helper wants at least one donut of each kind?

9. Columba has two dozen each of n different colored beads. If she can select 20 beads (with repetitions of colors allowed) in 230,230 ways, what is the value of n?

10. In how many ways can Lisa toss 100 (identical) dice so that at least three of each type of face will be showing?

11. Two n-digit integers (leading zeros allowed) are considered equivalent if one is a rearrangement of the other. (For example, 12033, 20331, and 01332 are considered equivalent five-digit integers.) (a) How many five-digit integers are not equivalent? (b) If the digits 1, 3, and 7 can appear at most once, how many nonequivalent five-digit integers are there?

12. Determine the number of integer solutions for

$$x_1 + x_2 + x_3 + x_4 + x_5 < 40,$$

where

a) $x_i \geq 0, \quad 1 \leq i \leq 5$

b) $x_i \geq -3, \quad 1 \leq i \leq 5$

13. In how many ways can we distribute eight identical white balls into four distinct containers so that (a) no container is left empty? (b) the fourth container has an odd number of balls in it?

14. a) Find the coefficient of v^2w^4xz in the expansion of $(3v + 2w + x + y + z)^8$.

b) How many distinct terms arise in the expansion in part (a)?

15. In how many ways can Beth place 24 different books on four shelves so that there is at least one book on each shelf? (For any of these arrangements consider the books on each shelf to be placed one next to the other, with the first book at the left of the shelf.)

16. For which positive integer n will the equations

$$(1)\ x_1 + x_2 + x_3 + \cdots + x_{19} = n, \quad \text{and}$$

$$(2)\ y_1 + y_2 + y_3 + \cdots + y_{64} = n$$

have the same number of positive integer solutions?

17. How many ways are there to place 12 marbles of the same size in five distinct jars if (a) the marbles are all black? (b) each marble is a different color?

18. a) How many nonnegative integer solutions are there to the pair of equations $x_1 + x_2 + x_3 + \cdots + x_7 = 37$, $x_1 + x_2 + x_3 = 6$?

b) How many solutions in part (a) have $x_1, x_2, x_3 > 0$?

19. How many times is the **print** statement executed for the following program segment? (Here, i, j, k, and m are integer variables.)

```
for i := 1 to 20 do
  for j := 1 to i do
    for k := 1 to j do
      for m := 1 to k do
        print (i * j) + (k * m)
```

20. In the following program segment, i, j, k, and *counter* are integer variables. Determine the value that the variable *counter* will have after the segment is executed.

```
counter := 10
for i := 1 to 15 do
  for j := i to 15 do
    for k := j to 15 do
      counter := counter + 1
```

21. Find the value of *sum* after the given program segment is executed. (Here i, j, k, *increment*, and *sum* are integer variables.)

```
increment := 0
sum := 0
for i := 1 to 10 do
  for j := 1 to i do
    for k := 1 to j do
      begin
        increment := increment + 1
        sum := sum + increment
      end
```

22. Consider the following program segment, where i, j, k, n, and *counter* are integer variables and the value of n (a positive integer) is set prior to this segment.

```
counter := 0
for i := 1 to n do
  for j := 1 to i do
    for k := 1 to j do
      counter := counter + 1
```

We shall determine, in two different ways, the number of times the statement

```
counter := counter + 1
```

is executed. (This is also the value of *counter* after execution of the program segment.) From the result in Example 1.39, we know that the statement is executed $\binom{n+3-1}{3} = \binom{n+2}{3}$ times. For a fixed value of i, the **for** loops involving j and k result in $\binom{i+1}{2}$ executions of the counter increment statement. Consequently, $\binom{n+2}{3} = \sum_{i=1}^{n} \binom{i+1}{2}$. Use this result to obtain a summation formula for

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \sum_{i=1}^{n} i^2.$$

23. a) Given positive integers m, n with $m \geq n$, show that the number of ways to distribute m identical objects into n distinct containers with no container left empty is

$$C(m - 1, m - n) = C(m - 1, n - 1).$$

b) Show that the number of distributions in part (a) where each container holds at least r objects ($m \geq nr$) is

$$C(m - 1 + (1 - r)n, n - 1).$$

24. Write a computer program (or develop an algorithm) to list the integer solutions for

a) $x_1 + x_2 + x_3 = 10, \quad 0 \leq x_i, \quad 1 \leq i \leq 3$

b) $x_1 + x_2 + x_3 + x_4 = 4, \quad -2 \leq x_i, \quad 1 \leq i \leq 4$

25. Consider the 2^{19} compositions of 20. (a) How many have each summand even? (b) How many have each summand a multiple of 4?

26. Let n, m, k be positive integers with $n = mk$. How many compositions of n have each summand a multiple of k?

27. Frannie tosses a coin 12 times and gets five heads and seven tails. In how many ways can these tosses result in (a) two runs of heads and one run of tails; (b) three runs; (c) four runs;

(d) five runs; (e) six runs; and (f) equal numbers of runs of heads and runs of tails?

28. a) For $n \geq 4$, consider the strings made up of n bits — that is, a total of n 0's and 1's. In particular, consider those strings where there are (exactly) two occurrences of 01. For example, if $n = 6$ we want to include strings such as 010010 and 100101, but not 101111 or 010101. How many such strings are there?

b) For $n \geq 6$, how many strings of n 0's and 1's contain (exactly) three occurrences of 01?

c) Provide a combinatorial proof for the following: For $n \geq 1$,

$$2^n = \binom{n+1}{1} + \binom{n+1}{3} + \cdots + \begin{cases} \binom{n+1}{n}, & n \text{ odd} \\ \binom{n+1}{n+1}, & n \text{ even.} \end{cases}$$

1.5 The Catalan Numbers (Optional)

In this section a very prominent sequence of numbers is introduced. This sequence arises in a wide variety of combinatorial situations. We'll begin by examining one specific instance where it is found.

EXAMPLE 1.42

Let us start at the point (0, 0) in the xy-plane and consider two kinds of moves:

$$\text{R: } (x, y) \to (x + 1, y) \qquad \text{U: } (x, y) \to (x, y + 1).$$

We want to know how we can move from (0, 0) to (5, 5) using such moves — one unit to the right or one unit up. So we'll need five R's and five U's. At this point we have a situation like that in Example 1.14, so we know there are $10!/(5!\,5!) = \binom{10}{5}$ such paths. But now we'll add a twist! In going from (0, 0) to (5, 5) one may touch but *never* rise above the line $y = x$. Consequently, we want to include paths such as those shown in parts (a) and (b) of Fig. 1.9 but not the path shown in part (c).

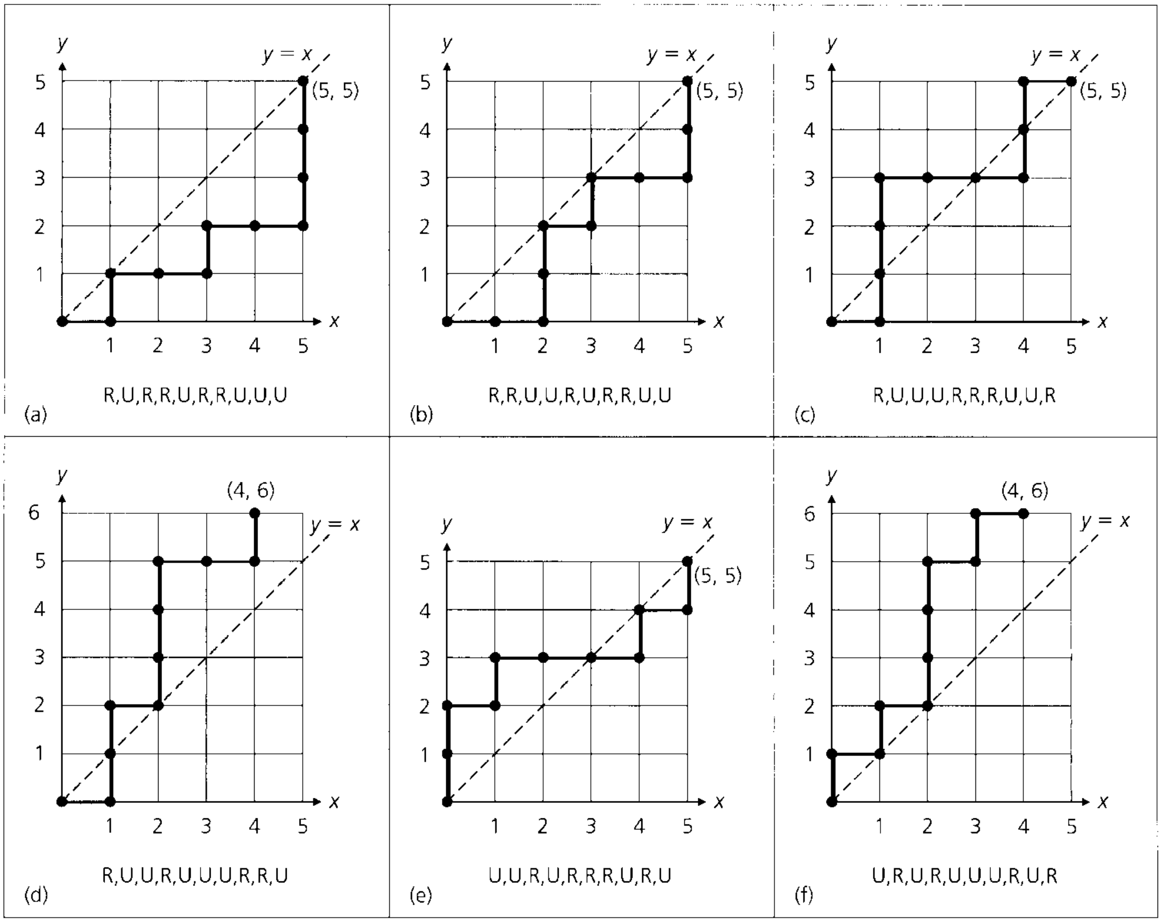
The first thing that is evident is that each such arrangement of five R's and five U's must start with an R (and end with a U). Then as we move across this type of arrangement — going from left to right — the number of R's at any point must equal or exceed the number of U's. Note how this happens in parts (a) and (b) of Fig. 1.9 but not in part (c). Now we can solve the problem at hand if we can count the paths [like the one in part (c)] that go from (0, 0) to (5, 5) but rise above the line $y = x$. Look again at the path in part (c) of Fig. 1.9. Where does the situation there break down for the first time? After all, we start with the requisite R — then follow it by a U. So far, so good! But then there is a second U and, at this (first) time, the number of U's exceeds the number of R's.

Now let us consider the following transformation:

$$\text{R, U, U, } \vdots \text{ U, R, R, R, U, U, R} \leftrightarrow \text{R, U, U, } \vdots \text{ R, U, U, U, R, R, U.}$$

What have we done here? For the path on the left-hand side of the transformation, we located the first move (the second U) where the path rose above the line $y = x$. The moves up to and including this move (the second U) remain as is, but the moves that follow are interchanged — each U is replaced by an R and each R by a U. The result is the path on the right-hand side of the transformation — an arrangement of four R's and six U's, as seen in part (d) of Fig. 1.9. Part (e) of that figure provides another path to be avoided; part (f) shows what happens when this path is transformed by the method described above. Now suppose we start with an arrangement of six U's and four R's, say

$$\text{R, U, R, R, U, U, U, } \vdots \text{ U, U, R.}$$



(a) R,U,R,R,U,R,R,U,U,U

(b) R,R,U,U,R,U,R,R,U,U

(c) R,U,U,U,R,R,R,U,U,R

(d) R,U,U,R,U,U,U,R,R,U

(e) U,U,R,U,R,R,R,U,R,U

(f) U,R,U,R,U,U,U,R,U,R

Figure 1.9

Focus on the first place where the number of U's exceeds the number of R's. Here it is in the seventh position, the location of the fourth U. This arrangement is now transformed as follows: The moves up to and including the fourth U remain as they are; the last three moves are interchanged — each U is replaced by an R, each R by a U. This results in the arrangement

R, U, R, R, U, U, U, ¦ R, R, U.

— one of the *bad* arrangements (of five R's and five U's) we wish to avoid as we go from (0, 0) to (5, 5). The correspondence established by these transformations gives us a way to count the number of bad arrangements. We alternatively count the number of ways to arrange four R's and six U's — this is $10!/(4!\,6!) = \binom{10}{4}$. Consequently, the number of ways to go from (0, 0) to (5, 5) without rising above the line $y = x$ is

$$\binom{10}{5}-\binom{10}{4}=\frac{10!}{5!\,5!}-\frac{10!}{4!\,6!}=\frac{6(10)!-5(10)!}{6!\,5!}$$

$$=\left(\frac{1}{6}\right)\left(\frac{10!}{5!\,5!}\right)=\frac{1}{(5+1)}\binom{10}{5}=\frac{1}{(5+1)}\binom{2\cdot 5}{5}=42.$$

The above result generalizes as follows. For any integer $n \geq 0$, the number of paths (made up of n R's and n U's) going from $(0, 0)$ to (n, n), without rising above the line $y = x$, is

$$b_n = \binom{2n}{n} - \binom{2n}{n-1} = \frac{1}{n+1}\binom{2n}{n}, \qquad n \geq 1, \qquad b_0 = 1.$$

The numbers $b_0, b_1, b_2, \ldots$ are called the *Catalan numbers*, after the Belgian mathematician Eugène Charles Catalan (1814–1894), who used them in determining the number of ways to parenthesize the product $x_1x_2x_3x_4 \cdots x_n$. For instance, the five ($= b_3$) ways to parenthesize $x_1x_2x_3x_4$ are:

$$(((x_1x_2)x_3)x_4) \quad ((x_1(x_2x_3))x_4) \quad ((x_1x_2)(x_3x_4)) \quad (x_1((x_2x_3)x_4)) \quad (x_1(x_2(x_3x_4))).$$

The first seven Catalan numbers are $b_0 = 1$, $b_1 = 1$, $b_2 = 2$, $b_3 = 5$, $b_4 = 14$, $b_5 = 42$, and $b_6 = 132$.

EXAMPLE 1.43

Here are some other situations where the Catalan numbers arise. Some of these examples are very much like the result in Example 1.42. A change in vocabulary is often the only difference.

a) In how many ways can one arrange three 1's and three -1's so that all six partial sums (starting with the first summand) are nonnegative? There are five ($= b_3$) such arrangements:

$1, 1, 1, -1, -1, -1$

$1, 1, -1, -1, 1, -1$

$1, 1, -1, 1, -1, -1$

$1, -1, 1, 1, -1, -1$

$1, -1, 1, -1, 1, -1$

In general, for $n \geq 0$, one can arrange n 1's and n -1's, with all $2n$ partial sums nonnegative, in b_n ways.

b) Given four 1's and four 0's, there are 14 ($= b_4$) ways to list these eight symbols so that in each list the number of 0's never exceeds the number of 1's (as a list is read from left to right). The following shows these 14 lists:

10101010
10101100
10110010
10110100
10111000

11001010
11001100
11010010
11010100
11011000

11100010
11100100
11101000

11110000

For $n \geq 0$, there are b_n such lists of n 1's and n 0's.

c) **Table 1.10**

$(((ab)c)d)$	$(((abc$	111000
$((a(bc))d)$	$((a(bc$	110100
$((ab)(cd))$	$((ab(c$	110010
$(a((bc)d))$	$(a((bc$	101100
$(a(b(cd)))$	$(a(b(c$	101010

Consider the first column in Table 1.10. Here we find five ways to parenthesize the product $abcd$. The first of these is $(((ab)c)d)$. Reading left to right, we list the three occurrences of the left parenthesis "(" and the letters a, b, c — maintaining the order in which these six symbols occur. This results in $(((abc$, the first expression in column 2 of Table 1.10. Likewise, $((a(bc))d)$ in column 1 corresponds to $((a(bc$ in column 2 — and so on, for the other three entries in each of columns 1 and 2. Now one can also go backward, from column 2 to column 1. Take an expression in column 2 and append "d)" to the right end. For instance, $((ab(c$ becomes $((ab(cd)$. Reading this new expression from left to right, we now insert a right parenthesis ")" whenever a product of two results arises. So, for example, $((ab(cd)$ becomes

$$((ab\underset{\uparrow}{)}(cd)\underset{\uparrow}{)})$$

For the product of *a* and *b*

For the product of (*ab*) and (*cd*)

The correspondence between the entries in columns 2 and 3 is more immediate. For an entry in column 2 replace each "(" by a "1" and each letter by a "0". Reversing this process, we replace each "1" by a "(", the first 0 by a, the second by b, and the third by c. This takes us from the entries in column 3 to those in column 2.

Now consider the correspondence between columns 1 and 3. (This correspondence arises from the correspondence between columns 1 and 2 and the one between columns 2 and 3.) It shows us that the number of ways to parenthesize the product $abcd$ equals the number of ways to list three 1's and three 0's so that, as such a list is read from left to right, the number of 1's always equals or exceeds the number of 0's. The number of ways here is 5 $(= b_3)$.

In general, one can parenthesize the product $x_1x_2x_3 \cdots x_n$ in b_{n-1} ways.

d) Let us arrange the integers 1, 2, 3, 4, 5, 6 in two rows of three so that (1) the integers increase in value as each row is read, from left to right, and (2) in any column the smaller integer is on top. For example, one way to do this is

$$\begin{matrix} 1 & 2 & 4 \\ 3 & 5 & 6 \end{matrix}$$

Now consider three 1's and three 0's. Arrange these six symbols in a list so that the 1's are in positions 1, 2, 4 (the top row) and the 0's are in positions 3, 5, 6 (the bottom row). The result is 110100. Reversing the process, start with another list, say 101100 (where the number of 0's never exceeds the number of 1's, as the list is read from left to right). The 1's are in positions 1, 3, 4 and the 0's are in positions 2, 5, 6. This corresponds to the arrangement

$$\begin{matrix} 1 & 3 & 4 \\ 2 & 5 & 6 \end{matrix}$$

which satisfies conditions (1) and (2), as stated above. From this correspondence we learn that the number of ways to arrange 1, 2, 3, 4, 5, 6, so that conditions (1) and (2) are satisfied, is the number of ways to arrange three 1's and three 0's in a list so that as the six symbols are read, from left to right, the number of 0's never exceeds the number of 1's. Consequently, one can arrange 1, 2, 3, 4, 5, 6 and satisfy conditions (1) and (2) in b_3 $(= 5)$ ways.

In closing let us mention that the Catalan numbers will come up in other sections — in particular, Section 5 of Chapter 10. Further examples can be found in reference [3] by M. Gardner. For even more results about these numbers one should consult the references for Chapter 10.

EXERCISES 1.5

1. Verify that for each integer $n \geq 1$,

$$\binom{2n}{n} - \binom{2n}{n-1} = \frac{1}{n+1}\binom{2n}{n}.$$

2. Determine the value of b_7, b_8, b_9, and b_{10}.

3. **a)** In how many ways can one travel in the xy-plane from $(0, 0)$ to $(3, 3)$ using the moves R: $(x, y) \rightarrow (x + 1, y)$ and U: $(x, y) \rightarrow (x, y + 1)$, if the path taken may touch but *never* fall below the line $y = x$? In how many ways from $(0, 0)$ to $(4, 4)$?

b) Generalize the results in part (a).

c) What can one say about the first and last moves of the paths in parts (a) and (b)?

4. Consider the moves

$$\text{R: } (x, y) \rightarrow (x + 1, y) \quad \text{and} \quad \text{U: } (x, y) \rightarrow (x, y + 1),$$

as in Example 1.42. In how many ways can one go

a) from $(0, 0)$ to $(6, 6)$ and not rise above the line $y = x$?

b) from $(2, 1)$ to $(7, 6)$ and not rise above the line $y = x - 1$?

c) from $(3, 8)$ to $(10, 15)$ and not rise above the line $y = x + 5$?

5. Find the other three ways to arrange 1, 2, 3, 4, 5, 6 in two rows of three so that the conditions in part (d) of Example 1.43 are satisfied.

6. There are b_4 (= 14) ways to arrange 1, 2, 3, . . . , 8 in two rows of four so that (1) the integers increase in value as each row is read, from left to right, and (2) in any column the smaller integer is on top. Find, as in part (d) of Example 1.43,

a) the arrangements that correspond to each of the following.

i) 10110010 **ii)** 11001010 **iii)** 11101000

b) the lists of four 1's and four 0's that correspond to each of these arrangements of 1, 2, 3, . . . , 8.

i) $\begin{matrix}1 & 3 & 4 & 5\\ 2 & 6 & 7 & 8\end{matrix}$ **ii)** $\begin{matrix}1 & 2 & 3 & 7\\ 4 & 5 & 6 & 8\end{matrix}$ **iii)** $\begin{matrix}1 & 2 & 4 & 5\\ 3 & 6 & 7 & 8\end{matrix}$

7. In how many ways can one parenthesize the product $abcdef$?

8. There are 132 ways in which one can parenthesize the product $abcdefg$.

a) Determine, as in part (c) of Example 1.43, the list of five 1's and five 0's that corresponds to each of the following.

i) $(((ab)c)(d(ef)))$
ii) $(a(b(c(d(ef)))))$
iii) $((((ab)(cd))e)f)$

b) Find, as in Example 1.43, the way to parenthesize $abcdef$ that corresponds to each given list of five 1's and five 0's.

i) 1110010100
ii) 1100110010
iii) 1011100100

9. Consider drawing n semicircles on and above a horizontal line, with no two semicircles intersecting. In parts (a) and (b) of Fig. 1.10 we find the two ways this can be done for $n = 2$; the results for $n = 3$ are shown in parts (c)–(g).

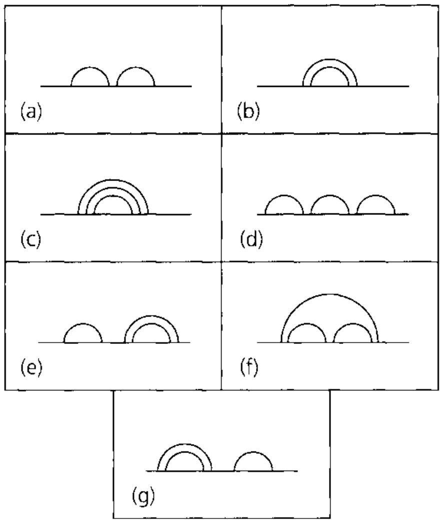


Figure 1.10

i) How many different drawings are there for four semicircles?

ii) How many for any $n \geq 0$? Explain why.

10. **a)** In how many ways can one go from $(0, 0)$ to $(7, 3)$ if the only moves permitted are R: $(x, y) \rightarrow (x + 1, y)$ and U: $(x, y) \rightarrow (x, y + 1)$, and the number of U's may never exceed the number of R's along the path taken?

b) Let m, n be positive integers with $m > n$. Answer the question posed in part (a), upon replacing 7 by m and 3 by n.

11. Twelve patrons, six each with a \$5 bill and the other six each with a \$10 bill, are the first to arrive at a movie theater, where the price of admission is five dollars. In how many ways can these 12 individuals (all loners) line up so that the number with a \$5 bill is never exceeded by the number with a \$10 bill (and, as a result, the ticket seller is always able to make any necessary change from the bills taken in from the first 11 of these 12 patrons)?

1.6 Summary and Historical Review

In this first chapter we introduced the fundamentals for counting combinations, permutations, and arrangements in a large variety of problems. The breakdown of problems into components requiring the same or different formulas for their solutions provided a key insight into the areas of discrete and combinatorial mathematics. This is somewhat similar to the *top-down approach* for developing algorithms in a structured programming language. Here one develops the algorithm for the solution of a difficult problem by first considering major subproblems that need to be solved. These subproblems are then further *refined* — subdivided into more easily workable programming tasks. Each level of refinement improves on the clarity, precision, and thoroughness of the algorithm until it is readily translatable into the code of the programming language.

Table 1.11 summarizes the major counting formulas we have developed so far. Here we are dealing with a collection of n distinct objects. The formulas count the number of ways to select, or order, with or without repetitions, r of these n objects. The summaries of Chapters 5 and 9 include other such charts that evolve as we extend our investigations into other counting methods.

Table 1.11

Order Is Relevant	Repetitions Are Allowed	Type of Result	Formula	Location in Text
Yes	No	Permutation	$P(n, r) = n!/(n-r)!$, $0 \leq r \leq n$	Page 7
Yes	Yes	Arrangement	n^r, $n, r \geq 0$	Page 7
No	No	Combination	$C(n, r) = n!/[r!(n-r)!] = \binom{n}{r}$, $0 \leq r \leq n$	Page 15
No	Yes	Combination with repetition	$\binom{n+r-1}{r}$, $n, r \geq 0$	Page 27

As we continue to investigate further principles of enumeration, as well as discrete mathematical structures for applications in coding theory, enumeration, optimization, and sorting schemes in computer science, we shall rely on the fundamental ideas introduced in this chapter.

The notion of permutation can be found in the Hebrew work *Sefer Yetzirah* (*The Book of Creation*), a manuscript written by a mystic sometime between 200 and 600. However, even earlier, it is of interest to note that a result of Xenocrates of Chalcedon (396–314 B.C.) may possibly contain "the first attempt on record to solve a difficult problem in permutations and combinations." For further details consult page 319 of the text by T. L. Heath [4], as well as page 113 of the article by N. L. Biggs [1], a valuable source on the history of enumeration. The first textbook dealing with some of the material we discussed in this chapter was *Ars Conjectandi* by the Swiss mathematician Jakob Bernoulli (1654–1705). The text was published posthumously in 1713 and contained a reprint of the first formal treatise on probability. This treatise had been written in 1657 by Christiaan Huygens (1629–1695), the Dutch physicist, mathematician, and astronomer who discovered the rings of Saturn.

The binomial theorem for $n = 2$ appears in the work of Euclid (300 B.C.), but it was not until the sixteenth century that the term "binomial coefficient" was actually introduced by Michel Stifel (1486–1567). In his *Arithmetica Integra* (1544) he gives the binomial coefficients up to the order of $n = 17$. Blaise Pascal (1623–1662), in his research on probability, published in the 1650s a treatise dealing with the relationships among binomial coefficients, combinations, and polynomials. These results were used by Jakob Bernoulli in proving the general form of the binomial theorem in a manner analogous to that presented in this chapter. Actual use of the symbol $\binom{n}{r}$ did not begin until the nineteenth century, when it was used by Andreas von Ettinghausen (1796–1878).

Blaise Pascal (1623–1662)

It was not until the twentieth century, however, that the advent of the computer made possible the systematic analysis of processes and algorithms used to generate permutations and combinations. We shall examine one such algorithm in Section 10.1.

The first comprehensive textbook dealing with topics in combinations and permutations was written by W. A. Whitworth [10]. Also dealing with the material of this chapter are Chapter 2 of D. I. Cohen [2], Chapter 1 of C. L. Liu [5], Chapter 2 of F. S. Roberts [6], Chapter 4 of K. H. Rosen [7], Chapter 1 of H. J. Ryser [8], and Chapter 5 of A. Tucker [9].

REFERENCES

1. Biggs, Norman L. "The Roots of Combinatorics." *Historia Mathematica* 6 (1979): pp. 109–136.
2. Cohen, Daniel I. A. *Basic Techniques of Combinatorial Theory*. New York: Wiley, 1978.
3. Gardner, Martin. "Mathematical Games, Catalan Numbers: An Integer Sequence that Materializes in Unexpected Places." *Scientific American* 234, no. 6 (June 1976): pp. 120–125.
4. Heath, Thomas Little. *A History of Greek Mathematics*, vol. 1. Reprint of the 1921 edition. New York: Dover Publications, 1981.
5. Liu, C. L. *Introduction to Combinatorial Mathematics*. New York: McGraw-Hill, 1968.
6. Roberts, Fred S. *Applied Combinatorics*. Englewood Cliffs, N.J.: Prentice-Hall, 1984.
7. Rosen, Kenneth H. *Discrete Mathematics and Its Applications*, 5th ed. New York: McGraw-Hill, 2003.
8. Ryser, H. J. *Combinatorial Mathematics*. Published by the Mathematical Association of America. New York: Wiley, 1963.

9. Tucker, Alan. *Applied Combinatorics*, 4th ed. New York: Wiley, 2002.
10. Whitworth, W. A. *Choice and Chance*. Reprint of the 1901 edition. New York: Hafner, 1965.

SUPPLEMENTARY EXERCISES

1. In the manufacture of a certain type of automobile, four kinds of major defects and seven kinds of minor defects can occur. For those situations in which defects do occur, in how many ways can there be twice as many minor defects as there are major ones?

2. A machine has nine different dials, each with five settings labeled 0, 1, 2, 3, and 4.

a) In how many ways can all the dials on the machine be set?

b) If the nine dials are arranged in a line at the top of the machine, how many of the machine settings have no two adjacent dials with the same setting?

3. Twelve points are placed on the circumference of a circle and all the chords connecting these points are drawn. What is the largest number of points of intersection for these chords?

4. A choir director must select six hymns for a Sunday church service. She has three hymn books, each containing 25 hymns (there are 75 different hymns in all). In how many ways can she select the hymns if she wishes to select (a) two hymns from each book? (b) at least one hymn from each book?

5. How many ways are there to place 25 different flags on 10 numbered flagpoles if the order of the flags on a flagpole is (a) not relevant? (b) relevant? (c) relevant and every flagpole flies at least one flag?

6. A penny is tossed 60 times yielding 45 heads and 15 tails. In how many ways could this have happened so that there were no consecutive tails?

7. There are 12 men at a dance. (a) In how many ways can eight of them be selected to form a cleanup crew? (b) How many ways are there to pair off eight women at the dance with eight of these 12 men?

8. In how many ways can the letters in WONDERING be arranged with exactly two consecutive vowels?

9. Dustin has a set of 180 distinct blocks. Each of these blocks is made of either wood or plastic and comes in one of three sizes (small, medium, large), five colors (red, white, blue, yellow, green), and six shapes (triangular, square, rectangular, hexagonal, octagonal, circular). How many of the blocks in this set differ from

a) the *small red wooden square* block in exactly one way? (For example, the *small red plastic square* block is one such block.)

b) the *large blue plastic hexagonal* block in exactly two ways? (For example, the *small red plastic hexagonal* block is one such block.)

10. Mr. and Mrs. Richardson want to name their new daughter so that her initials (first, middle, and last) will be in alphabetical order with no repeated initial. How many such triples of initials can occur under these circumstances?

11. In how many ways can the 11 identical horses on a carousel be painted so that three are brown, three are white, and five are black?

12. In how many ways can a teacher distribute 12 different science books among 16 students if (a) no student gets more than one book? (b) the oldest student gets two books but no other student gets more than one book?

13. Four numbers are selected from the following list of numbers: $-5, -4, -3, -2, -1, 1, 2, 3, 4$. (a) In how many ways can the selections be made so that the product of the four numbers is positive and (i) the numbers are distinct? (ii) each number may be selected as many as four times? (iii) each number may be selected at most three times? (b) Answer part (a) with the product of the four numbers negative.

14. Waterbury Hall, a university residence hall for men, is operated under the supervision of Mr. Kelly. The residence has three floors, each of which is divided into four sections. This coming fall Mr. Kelly will have 12 resident assistants (one for each of the 12 sections). Among these 12 assistants are the four senior assistants — Mr. DiRocco, Mr. Fairbanks, Mr. Hyland, and Mr. Thornhill. (The other eight assistants will be new this fall and are designated as junior assistants.) In how many ways can Mr. Kelly assign his 12 assistants if

a) there are no restrictions?

b) Mr. DiRocco and Mr. Fairbanks must both be assigned to the first floor?

c) Mr. Hyland and Mr. Thornhill must be assigned to different floors?

15. a) How many of the 9000 four-digit integers 1000, 1001, 1002, . . . , 9998, 9999 have four distinct digits that are either increasing (as in 1347 and 6789) or decreasing (as in 6421 and 8653)?

b) How many of the 9000 four-digit integers 1000, 1001, 1002, . . . , 9998, 9999 have four digits that are either nondecreasing (as in 1347, 1226, and 7778) or nonincreasing (as in 6421, 6622, and 9888)?

16. a) Find the coefficient of x^2yz^2 in the expansion of $[(x/2) + y - 3z]^5$.

b) How many distinct terms are there in the complete expansion of

$$\left(\frac{x}{2}+y-3z\right)^5 ?$$

c) What is the sum of all coefficients in the complete expansion?

17. a) In how many ways can 10 people, denoted A, B, . . . , I, J, be seated about the rectangular table shown in Fig. 1.11, where Figs. 1.11(a) and 1.11(b) are considered the same but are considered different from Fig. 1.11(c)?

b) In how many of the arrangements of part (a) are A and B seated on longer sides of the table across from each other?

18. a) Determine the number of nonnegative integer solutions to the pair of equations

$$x_1+x_2+x_3=6, \qquad x_1+x_2+\cdots+x_5=15,$$
$$x_i \geq 0, \quad 1 \leq i \leq 5.$$

b) Answer part (a) with the pair of equations replaced by the pair of inequalities

$$x_1+x_2+x_3 \leq 6, \qquad x_1+x_2+\cdots+x_5 \leq 15,$$
$$x_i \geq 0, \quad 1 \leq i \leq 5.$$

19. For any given set in a tennis tournament, opponent A can beat opponent B in seven different ways. (At 6–6 they play a tie breaker.) The first opponent to win three sets wins the tournament. (a) In how many ways can scores be recorded with A winning in five sets? (b) In how many ways can scores be recorded with the tournament requiring at least four sets?

20. Given n distinct objects, determine in how many ways r of these objects can be arranged in a circle, where arrangements are considered the same if one can be obtained from the other by rotation.

21. For every positive integer n, show that

$$\binom{n}{0}+\binom{n}{2}+\binom{n}{4}+\cdots=\binom{n}{1}+\binom{n}{3}+\binom{n}{5}+\cdots$$

22. a) In how many ways can the letters in UNUSUAL be arranged?

b) For the arrangements in part (a), how many have all three U's together?

c) How many of the arrangements in part (a) have no consecutive U's?

23. Francesca has 20 different books but the shelf in her dormitory residence will hold only 12 of them.

a) In how many ways can Francesca line up 12 of these books on her bookshelf?

b) How many of the arrangements in part (a) include Francesca's three books on tennis?

24. Determine the value of the integer variable *counter* after execution of the following program segment. (Here i, j, k, l, m, and n are integer variables. The variables r, s, and t are also integer variables; their values—where $r \geq 1$, $s \geq 5$, and $t \geq 7$—have been set prior to this segment.)

```
counter := 10
for i := 1 to 12 do
  for j := 1 to r do
    counter := counter + 2
for k := 5 to s do
  for l := 3 to k do
    counter := counter + 4
for m := 3 to 12 do
  counter := counter + 6
for n := t downto 7 do
  counter := counter + 8
```

25. a) Find the number of ways to write 17 as a sum of 1's and 2's if order is relevant.

b) Answer part (a) for 18 in place of 17.

c) Generalize the results in parts (a) and (b) for n odd and for n even.

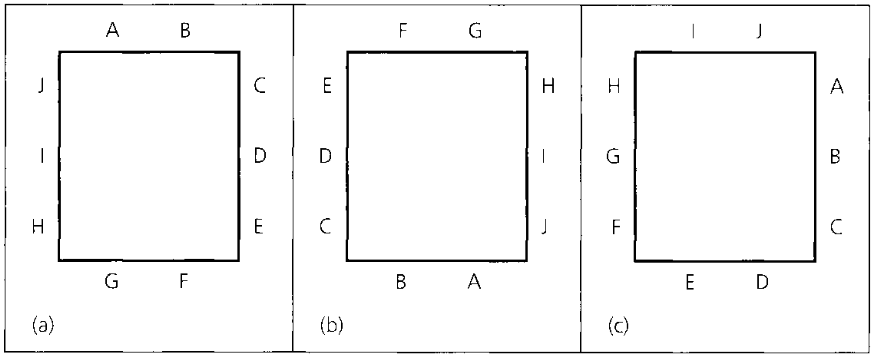


Figure 1.11

26. **a)** In how many ways can 17 be written as a sum of 2's and 3's if the order of the summands is (i) not relevant? (ii) relevant?

b) Answer part (a) for 18 in place of 17.

27. **a)** If n and r are positive integers with $n \geq r$, how many solutions are there to

$$x_1 + x_2 + \cdots + x_r = n,$$

where each x_i is a positive integer, for $1 \leq i \leq r$?

b) In how many ways can a positive integer n be written as a sum of r positive integer summands ($1 \leq r \leq n$) if the order of the summands is relevant?

28. **a)** In how many ways can one travel in the xy-plane from $(1, 2)$ to $(5, 9)$ if each move is one of the following types:

$$\text{(R): } (x, y) \rightarrow (x + 1, y); \quad \text{(U): } (x, y) \rightarrow (x, y + 1)?$$

b) Answer part (a) if a third (diagonal) move

$$\text{(D): } (x, y) \rightarrow (x + 1, y + 1)$$

is also possible.

29. **a)** In how many ways can a particle move in the xy-plane from the origin to the point $(7, 4)$ if the moves that are allowed are of the form:

$$\text{(R): } (x, y) \rightarrow (x + 1, y); \quad \text{(U): } (x, y) \rightarrow (x, y + 1)?$$

b) How many of the paths in part (a) do not use the path from $(2, 2)$ to $(3, 2)$ to $(4, 2)$ to $(4, 3)$ shown in Fig. 1.12?

c) Answer parts (a) and (b) if a third type of move

$$\text{(D): } (x, y) \rightarrow (x + 1, y + 1)$$

is also allowed.

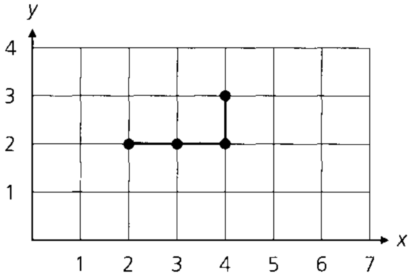


Figure 1.12

30. Due to their outstanding academic records, Donna and Katalin are the finalists for the outstanding physics student (in their college graduating class). A committee of 14 faculty members will each select one of the candidates to be the winner and place his or her choice (checked off on a ballot) into the ballot box. Suppose that Katalin receives nine votes and Donna receives five. In how many ways can the ballots be selected, one at a time, from the ballot box so that there are always more votes in favor of Katalin? [This is a special case of a general problem called, appropriately, *the ballot problem*. This problem was solved by Joseph Louis François Bertrand (1822–1900).]

31. Consider the 8×5 grid shown in Fig. 1.13. How many different rectangles (with integer-coordinate corners) does this grid contain? [For example, there is a rectangle (square) with corners $(1, 1), (2, 1), (2, 2), (1, 2)$, a second rectangle with corners $(3, 2), (4, 2), (4, 4), (3, 4)$, and a third with corners $(5, 0)$, $(7, 0)$, $(7, 3)$ $(5, 3)$.]

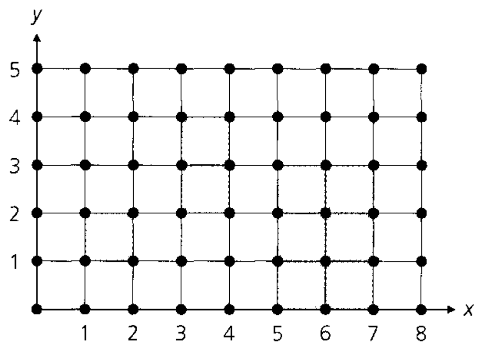


Figure 1.13

32. As head of quality control, Silvia examined 15 motors, one at a time, and found six defective (D) motors and nine in good (G) working condition. If she listed each finding (of D or G) after examining each individual motor, in how many ways could Silvia's list start with a run of three G's and have six runs in total?

33. In order to graduate on schedule, Hunter must take (and pass) four mathematics electives during his final six quarters. If he may select these electives from a list of 12 (that are offered every quarter) and he does not want to take more than one of these electives in any given quarter, in how many ways can he select and schedule these four electives?

34. In how many ways can a family of four (mother, father, and two children) be seated at a round table, with eight other people, so that the parents are seated next to each other and there is one child on a side of each parent? (Two seatings are considered the same if one can be rotated to look like the other.)

4

Properties of the Integers: Mathematical Induction

Having known about the integers since our first encounters with arithmetic, in this chapter we examine a special property exhibited by the subset of positive integers. This property will enable us to establish certain mathematical formulas and theorems by using a technique called *mathematical induction*. This method of proof will play a key role in many of the results we shall obtain in the later chapters of this text. Furthermore, this chapter will provide us with an introduction to five sets of numbers that are very important in the study of discrete mathematics and combinatorics — namely, the triangular numbers, the harmonic numbers, the Fibonacci numbers, the Lucas numbers, and the Eulerian numbers.

When $x, y \in \mathbf{Z}$, we know that $x + y, xy, x - y \in \mathbf{Z}$. Thus we say that the set $\mathbf{Z}$ is *closed* under (the binary operations of) addition, multiplication, and subtraction. Turning to division, however, we find, for example, that $2, 3 \in \mathbf{Z}$ but that the rational number $\frac{2}{3}$ is *not* a member of $\mathbf{Z}$. So the set $\mathbf{Z}$ of all integers is *not closed* under the binary operation of *nonzero* division. To cope with this situation, we shall introduce a somewhat restricted form of division for $\mathbf{Z}$ and shall concentrate on special elements of $\mathbf{Z}^+$ called *primes*. These primes turn out to be the "building blocks" of the integers, and they provide our first example of a representation theorem — in this case the Fundamental Theorem of Arithmetic.

4.1 The Well-Ordering Principle: Mathematical Induction

Given any two distinct integers x, y, we know that we must have either $x < y$ or $y < x$. However, this is also true if, instead of being integers, x and y are rational numbers or real numbers. What makes $\mathbf{Z}$ special in this situation?

Suppose we try to express the subset $\mathbf{Z}^+$ of $\mathbf{Z}$, using the inequality symbols $>$ and $\geq$. We find that we can define the set of positive elements of $\mathbf{Z}$ as

$$\mathbf{Z}^+ = \{x \in \mathbf{Z} | x > 0\} = \{x \in \mathbf{Z} | x \geq 1\}.$$

When we try to do likewise for the rational and real numbers, however, we find that

$$\mathbf{Q}^+ = \{x \in \mathbf{Q} | x > 0\} \qquad \text{and} \qquad \mathbf{R}^+ = \{x \in \mathbf{R} | x > 0\},$$

but we cannot represent $\mathbf{Q}^+$ or $\mathbf{R}^+$ using $\geq$ as we did for $\mathbf{Z}^+$.

The set $\mathbf{Z}^+$ is different from the sets $\mathbf{Q}^+$ and $\mathbf{R}^+$ in that *every* nonempty subset X of $\mathbf{Z}^+$ contains an integer a such that $a \leq x$, for all $x \in X$—that is, X contains a *least* (or *smallest*) element. This is not so for either $\mathbf{Q}^+$ or $\mathbf{R}^+$. The sets themselves do not contain least elements. There is no smallest positive rational number or smallest positive real number. If q is a positive rational number, then since $0 < q/2 < q$, we would have the smaller positive rational number $q/2$.

These observations lead us to the following property of the set $\mathbf{Z}^+ \subset \mathbf{Z}$.

The Well-Ordering Principle: **Every *nonempty* subset of $\mathbf{Z}^+$ contains a smallest element. (We often express this by saying that $\mathbf{Z}^+$ is *well ordered*.)**

This principle serves to distinguish $\mathbf{Z}^+$ from $\mathbf{Q}^+$ and $\mathbf{R}^+$. But does it lead anywhere that is mathematically interesting or useful? The answer is a resounding "Yes!" It is the basis of a proof technique known as mathematical induction. This technique will often help us to prove a general mathematical statement involving positive integers when certain instances of that statement suggest a general pattern.

We now establish the basis for this induction technique.

THEOREM 4.1

The Principle of Mathematical Induction. Let $S(n)$ denote an open mathematical statement (or set of such open statements) that involves one or more occurrences of the variable n, which represents a positive integer.

a) If $S(1)$ is true; and

b) If whenever $S(k)$ is true (for some particular, but arbitrarily chosen, $k \in \mathbf{Z}^+$), then $S(k+1)$ is true;

then $S(n)$ is true for all $n \in \mathbf{Z}^+$.

Proof: Let $S(n)$ be such an open statement satisfying conditions (a) and (b), and let $F = \{t \in \mathbf{Z}^+ | S(t) \text{ is false}\}$. We wish to prove that $F = \emptyset$, so to obtain a contradiction we assume that $F \neq \emptyset$. Then by the Well-Ordering Principle, F has a least element m. Since $S(1)$ is true, it follows that $m \neq 1$, so $m > 1$, and consequently $m - 1 \in \mathbf{Z}^+$. With $m - 1 \notin F$, we have $S(m-1)$ true. So by condition (b) it follows that $S((m-1)+1) = S(m)$ is true, contradicting $m \in F$. This contradiction arose from the assumption that $F \neq \emptyset$. Consequently, $F = \emptyset$.

We have now seen how the Well-Ordering Principle is used in the proof of the Principle of Mathematical Induction. It is also true that the Principle of Mathematical Induction is useful if one wants to prove the Well-Ordering Principle. However, we shall not concern ourselves with that fact right now. In this section our major goal will center on understanding and using the Principle of Mathematical Induction. (But in the exercises for Section 4.2 we shall examine how the Principle of Mathematical Induction is used to prove the Well-Ordering Principle.)

In the statement of Theorem 4.1 the condition in part (a) is referred to as the *basis step*, while that in part (b) is called the *inductive step*.

The choice of 1 in the first condition of Theorem 4.1 is not mandatory. All that is needed is for the open statement $S(n)$ to be true for some *first* element $n_0 \in \mathbf{Z}$ so that the induction process has a starting place. We need the truth of $S(n_0)$ for our basis step. The integer n_0 could be 5 just as well as 1. It could even be zero or negative because the set $\mathbf{Z}^+$ in union with $\{0\}$ or any *finite* set of negative integers is well ordered. (When we do an induction proof and start with $n_0 < 0$, we are considering the set of all *consecutive* negative integers $\geq n_0$ in union with $\{0\}$ and $\mathbf{Z}^+$.)

Under these circumstances, we may express the Principle of Mathematical Induction, using quantifiers, as

$$[S(n_0) \wedge [\forall k \geq n_0 \; [S(k) \Rightarrow S(k+1)]]] \Rightarrow \forall n \geq n_0 \; S(n).$$

We may get a somewhat better understanding of why this method of proof is valid by using our intuition in conjunction with the situation presented in Fig. 4.1.

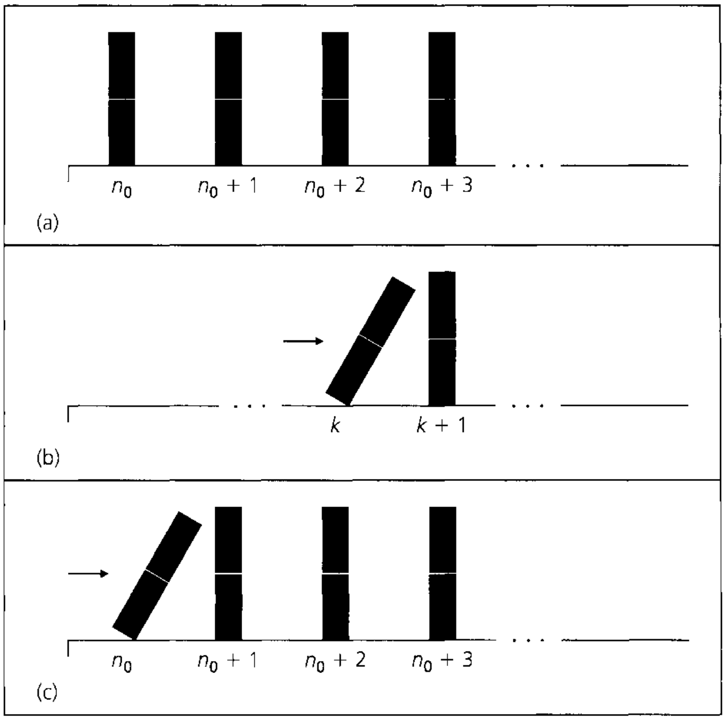


Figure 4.1

In part (a) of the figure we see the first four of an infinite (ordered) arrangement of dominos, each standing on end. The spacing between any two consecutive dominos is always the same, and it is such that if any one domino (say the kth) is pushed over to the right, then it will knock over the next ($(k + 1)$st) domino. This process is suggested in Fig. 4.1(b). Our intuition leads us to feel that this process will continue, the $(k + 1)$st domino toppling and knocking over (to the right) the $(k + 2)$nd domino, and so on. Part (c) of the figure indicates how the truth of $S(n_0)$ provides the push (to the right) to the first domino (at n_0). This provides the basis step and sets the process in motion. The truth of $S(k)$

forcing the truth of $S(k+1)$ gives us the inductive step and continues the toppling process. We then infer the fact that $S(n)$ is true for all $n \geq n_0$ as we imagine *all* the successive dominos toppling (to the right.)

We shall now demonstrate several results that call for the use of Theorem 4.1.

EXAMPLE 4.1

For all $n \in \mathbf{Z}^+$, $\sum_{i=1}^{n} i = 1+2+3+\cdots+n = \frac{n(n+1)}{2}$.

Proof: For $n = 1$ the open statement

$$S(n)\colon \quad \sum_{i=1}^{n} i = 1+2+3+\cdots+n = \frac{n(n+1)}{2}$$

becomes $S(1)$: $\sum_{i=1}^{1} i = 1 = (1)(1+1)/2$. So $S(1)$ is true and we have our *basis step*—and a starting point from which to begin the induction. Assuming the result true for $n = k$ (for some $k \in \mathbf{Z}^+$), we want to establish our *inductive step* by showing how the truth of $S(k)$ "forces" us to accept the truth of $S(k+1)$. [The assumption of the truth of $S(k)$ is our *induction hypothesis*.] To establish the truth of $S(k+1)$, we need to show that

$$\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}.$$

We proceed as follows.

$$\sum_{i=1}^{k+1} i = 1+2+\cdots+k+(k+1) = \left(\sum_{i=1}^{k} i\right) + (k+1) = \frac{k(k+1)}{2} + (k+1),$$

for we are assuming the truth of $S(k)$. But

$$\frac{k(k+1)}{2} + (k+1) = \frac{k(k+1)}{2} + \frac{2(k+1)}{2} = \frac{(k+1)(k+2)}{2},$$

establishing the inductive step [condition (b)] of the theorem.

Consequently, by the Principle of Mathematical Induction, $S(n)$ is true for all $n \in \mathbf{Z}^+$.

Now that we have obtained the summation formula for $\sum_{i=1}^{n} i$ in two ways (see Example 1.40), we shall digress from our main topic and consider two examples that use this summation formula.

EXAMPLE 4.2

A wheel of fortune has the numbers from 1 to 36 painted on it in a random manner. Show that regardless of how the numbers are situated, there are three consecutive (on the wheel) numbers whose total is 55 or more.

Let x_1 be any number on the wheel. Counting clockwise from x_1, label the other numbers $x_2, x_3, \ldots, x_{36}$. For the result to be false, we must have $x_1 + x_2 + x_3 < 55$, $x_2 + x_3 + x_4 < 55, \ldots, x_{34} + x_{35} + x_{36} < 55$, $x_{35} + x_{36} + x_1 < 55$, and $x_{36} + x_1 + x_2 < 55$. In these 36 inequalities, each of the terms $x_1, x_2, \ldots, x_{36}$ appears (exactly) three times, so each of the integers $1, 2, \ldots, 36$ appears (exactly) three times. Adding all 36 inequalities, we find that $3\sum_{i=1}^{36} x_i = 3\sum_{i=1}^{36} i < 36(55) = 1980$. But $\sum_{i=1}^{36} i = (36)(37)/2 = 666$, and this gives us the contradiction that $1998 = 3(666) < 1980$.

EXAMPLE 4.3

Among the 900 three-digit integers (from 100 to 999) those such as 131, 222, 303, 717, 848, and 969, where the integer is the same whether it is read from left to right or from right to left, are called *palindromes*. Without actually determining all of these three-digit palindromes, we would like to determine their sum.

The typical palindrome under study here has the form $aba = 100a + 10b + a = 101a + 10b$, where $1 \leq a \leq 9$ and $0 \leq b \leq 9$. With nine choices for a and ten for b, it follows from the rule of product that there are 90 such three-digit palindromes. Their sum is

$$\begin{aligned}
\sum_{a=1}^{9}\left(\sum_{b=0}^{9} aba\right) &= \sum_{a=1}^{9}\sum_{b=0}^{9} aba = \sum_{a=1}^{9}\sum_{b=0}^{9}(101a + 10b) \\
&= \sum_{a=1}^{9}\left[10(101a) + 10\sum_{b=0}^{9} b\right] = \sum_{a=1}^{9}\left[10(101a) + 10\sum_{b=1}^{9} b\right] \\
&= \sum_{a=1}^{9}\left[1010a + \frac{10(9 \cdot 10)}{2}\right] = \sum_{a=1}^{9}(1010a + 450) \\
&= 1010\sum_{a=1}^{9} a + 9(450) \\
&= \frac{1010(9 \cdot 10)}{2} + 4050 = 49{,}500.
\end{aligned}$$

The next summation formula takes us from first powers to squares.

EXAMPLE 4.4

Prove that for each $n \in \mathbf{Z}^+$,

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}.$$

Proof: Here we are dealing with the open statement

$$S(n): \quad \sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}.$$

Basis Step: We start with the statement $S(1)$ and find that

$$\sum_{i=1}^{1} i^2 = 1^2 = \frac{1(1+1)(2(1)+1)}{6}.$$

so $S(1)$ is true.

Inductive Step: Now we assume the truth of $S(k)$, for some (particular) $k \in \mathbf{Z}^+$ —that is, we assume that

$$\sum_{i=1}^{k} i^2 = \frac{k(k+1)(2k+1)}{6}$$

is a true statement (when n is replaced by k). From this assumption we want to deduce the truth of

$$\begin{aligned}
S(k+1): \quad \sum_{i=1}^{k+1} i^2 &= \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6} \\
&= \frac{(k+1)(k+2)(2k+3)}{6}.
\end{aligned}$$

Using the induction hypothesis $S(k)$, we find that

$$\begin{aligned}\sum_{i=1}^{k+1} i^2 &= 1^2+2^2+\cdots+k^2+(k+1)^2 = \sum_{i=1}^{k} i^2+(k+1)^2\\ &= \left[\frac{k(k+1)(2k+1)}{6}\right]+(k+1)^2\\ &= (k+1)\left[\frac{k(2k+1)}{6}+(k+1)\right] = (k+1)\left[\frac{2k^2+7k+6}{6}\right]\\ &= \frac{(k+1)(k+2)(2k+3)}{6},\end{aligned}$$

and the general result follows by the Principle of Mathematical Induction.

The formulas from Examples 4.1 and 4.4 prove handy in deriving our next result.

EXAMPLE 4.5

Figure 4.2 provides the first four entries of the sequence of *triangular* numbers. We see that $t_1 = 1$, $t_2 = 3$, $t_3 = 6$, $t_4 = 10$, and, in general, $t_i = 1+2+\cdots+i = i(i+1)/2$, for each $i \in \mathbf{Z}^+$. For a fixed $n \in \mathbf{Z}^+$ we want a formula for the sum of the first n triangular numbers—that is, $t_1+t_2+\cdots+t_n = \sum_{i=1}^{n} t_i$. When $n = 2$ we have $t_1+t_2 = 4$. For $n = 3$ the sum is 10. Considering n fixed (but arbitrary) we find that

$$\begin{aligned}\sum_{i=1}^{n} t_i &= \sum_{i=1}^{n}\frac{i(i+1)}{2} = \frac{1}{2}\sum_{i=1}^{n}(i^2+i) = \frac{1}{2}\sum_{i=1}^{n} i^2+\frac{1}{2}\sum_{i=1}^{n} i\\ &= \frac{1}{2}\left[\frac{n(n+1)(2n+1)}{6}\right]+\frac{1}{2}\left[\frac{n(n+1)}{2}\right] = n(n+1)\left[\frac{2n+1}{12}+\frac{1}{4}\right]\\ &= \frac{n(n+1)(n+2)}{6}.\end{aligned}$$

Consequently, if we wish to know the sum of the first 100 triangular numbers, we have

$$t_1+t_2+\cdots+t_{100} = \frac{100(101)(102)}{6} = 171{,}700.$$

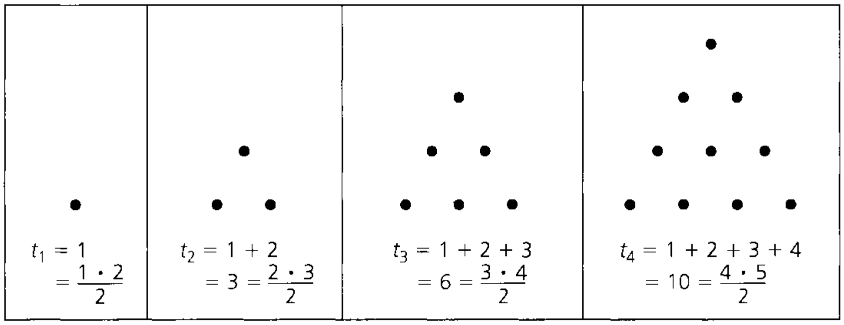

$t_1 = 1 = \frac{1 \cdot 2}{2}$
$t_2 = 1+2 = 3 = \frac{2 \cdot 3}{2}$
$t_3 = 1+2+3 = 6 = \frac{3 \cdot 4}{2}$
$t_4 = 1+2+3+4 = 10 = \frac{4 \cdot 5}{2}$

Figure 4.2

Before we present any more results, let us note how we started the proofs in Examples 4.1 and 4.4. In both cases we simply replaced the variable n by 1 and verified the truth of some rather easy equalities. Considering how the inductive step in each of these proofs was definitely more complicated to establish, we might question the need for bothering with these basis steps. So let us examine the following example.

EXAMPLE 4.6

If $n \in \mathbf{Z}^+$, establish the validity of the open statement

$$S(n):\quad \sum_{i=1}^{n} i = 1 + 2 + 3 + \cdots + n = \frac{n^2 + n + 2}{2}.$$

This time we shall go directly to the inductive step. Assuming the truth of the statement

$$S(k):\quad \sum_{i=1}^{k} i = 1 + 2 + 3 + \cdots + k = \frac{k^2 + k + 2}{2}$$

for some (particular) $k \in \mathbf{Z}^+$, we want to infer the truth of the statement

$$\begin{aligned} S(k+1):\quad \sum_{i=1}^{k+1} i &= 1 + 2 + 3 + \cdots + k + (k+1) = \frac{(k+1)^2 + (k+1) + 2}{2} \\ &= \frac{k^2 + 3k + 4}{2}. \end{aligned}$$

As we did previously, we use the induction hypothesis and calculate as follows:

$$\begin{aligned} \sum_{i=1}^{k+1} i &= 1 + 2 + 3 + \cdots + k + (k+1) = \left(\sum_{i=1}^{k} i\right) + (k+1) \\ &= \frac{k^2 + k + 2}{2} + (k+1) \\ &= \frac{k^2 + k + 2}{2} + \frac{2k + 2}{2} = \frac{k^2 + 3k + 4}{2}. \end{aligned}$$

Hence, for each $k \in \mathbf{Z}^+$, it follows that $S(k) \Rightarrow S(k+1)$. But before we decide to accept the statement $\forall n\ S(n)$ as a true statement, let us reconsider Example 4.1. From that example we learned that $\sum_{i=1}^{n} i = n(n+1)/2$, for all $n \in \mathbf{Z}^+$. Therefore, we can use these two results (from Example 4.1 and the one already "established" here) to conclude that for all $n \in \mathbf{Z}^+$,

$$\frac{n(n+1)}{2} = \sum_{i=1}^{n} i = \frac{n^2 + n + 2}{2},$$

which implies that $n(n+1) = n^2 + n + 2$ and $0 = 2$. (Something is wrong somewhere!)

If $n = 1$, then $\sum_{i=1}^{1} 1 = 1$, but $(n^2 + n + 2)/2 = (1 + 1 + 2)/2 = 2$. So $S(1)$ is not true. But we may feel that this result just indicates that we have the wrong starting point. Perhaps $S(n)$ is true for all $n \geq 7$, or all $n \geq 137$. Using the preceding argument, however, we know that for any starting point $n_0 \in \mathbf{Z}^+$, if $S(n_0)$ were true, then

$$\frac{n_0^2 + n_0 + 2}{2} = \sum_{i=1}^{n_0} i = 1 + 2 + 3 + \cdots + n_0.$$

From the result in Example 4.1 we have $\sum_{i=1}^{n_0} i = n_0(n_0 + 1)/2$, so it follows once again that $0 = 2$, and we have no possible starting point.

This example should indicate to the reader the need to establish the basis step — no matter how easy it may be to verify it.

Now consider the following pseudocode procedures. The procedure in Fig. 4.3 uses a **for** loop to accumulate the sum of the squares. The second procedure (Fig. 4.4) demonstrates how the result of Example 4.4 can be used in place of such a loop. In both procedures the input is a positive integer n and the output is $\sum_{i=1}^{n} i^2$. However, whereas the pseudocode within the **for** loop of the procedure in Fig. 4.3 entails a total of n additions and n multiplications (not to mention the $n - 1$ additions for incrementing the counter variable i), the procedure in Fig. 4.4 requires only two additions, three multiplications, and one (integer) division. And this total number of additions, multiplications, and (integer) divisions is still 6 as the value of n increases. Consequently, the procedure in Fig. 4.4 is considered more efficient. (This idea of a *more efficient* procedure will be examined further in Sections 5.7 and 5.8.)

```
procedure SumOfSquares1 (n: positive integer)
begin
  sum := 0
  for i := 1 to n do
    sum := sum + i^2
end
```

Figure 4.3

```
procedure SumOfSquares2 (n: positive integer)
begin
  sum := n * (n + 1) * (2 * n + 1)/6
end
```

Figure 4.4

Looking back at our first two applications of mathematical induction (in Examples 4.1 and 4.4), we might wonder whether this principle applies only to the verification of *known* summation formulas. The next seven examples show that mathematical induction is a vital tool in many other circumstances as well.

EXAMPLE 4.7

Let us consider the sums of consecutive odd positive integers.

1) 1	$= 1$	$(= 1^2)$
2) $1 + 3$	$= 4$	$(= 2^2)$
3) $1 + 3 + 5$	$= 9$	$(= 3^2)$
4) $1 + 3 + 5 + 7$	$= 16$	$(= 4^2)$

From these first four cases we *conjecture* the following result: The sum of the first n consecutive odd positive integers is n^2; that is, for all $n \in \mathbf{Z}^+$,

$$S(n): \quad \sum_{i=1}^{n} (2i - 1) = n^2.$$

Now that we have developed what we feel is a true summation formula, we use the Principle of Mathematical Induction to verify its truth for *all* $n \geq 1$.

From the preceding calculations, we see that $S(1)$ is true [as are $S(2)$, $S(3)$, and $S(4)$], and so we have our basis step. For the inductive step we assume the truth of $S(k)$ for some k (≥ 1) and have

$$\sum_{i=1}^{k}(2i-1)=k^2.$$

We now deduce the truth of $S(k+1)$: $\sum_{i=1}^{k+1}(2i-1)=(k+1)^2$. Since we have assumed the truth of $S(k)$, our induction hypothesis, we may now write

$$\begin{aligned}\sum_{i=1}^{k+1}(2i-1)&=\sum_{i=1}^{k}(2i-1)+[2(k+1)-1]=k^2+[2(k+1)-1]\\&=k^2+2k+1=(k+1)^2.\end{aligned}$$

Consequently, the result $S(n)$ is true for all $n \geq 1$, by the Principle of Mathematical Induction.

Now it is time to investigate some results that are not summation formulas.

EXAMPLE 4.8

In Table 4.1, we have listed in adjacent columns the values of $4n$ and n^2-7 for the positive integers n, where $1 \leq n \leq 8$. From the table, we see that $(n^2-7) < 4n$ for $n = 1, 2, 3, 4, 5$; but when $n = 6, 7, 8$, we have $4n < (n^2-7)$. These last three observations lead us to conjecture: For all $n \geq 6$, $4n < (n^2-7)$.

Table 4.1

n	$4n$	n^2-7	n	$4n$	n^2-7
1	4	−6	5	20	18
2	8	−3	6	24	29
3	12	2	7	28	42
4	16	9	8	32	57

Once again, the Principle of Mathematical Induction is the proof technique we need to verify our conjecture. Let $S(n)$ denote the open statement: $4n < (n^2-7)$. Then Table 4.1 confirms that $S(6)$ is true [as are $S(7)$ and $S(8)$], and we have our basis step. (At last we have an example wherein the starting point is an integer $n_0 \neq 1$.)

In this example, the induction hypothesis is $S(k)$: $4k < (k^2-7)$, where $k \in \mathbf{Z}^+$ and $k \geq 6$. In order to establish the inductive step, we need to obtain the truth of $S(k+1)$ from that of $S(k)$. That is, from $4k < (k^2-7)$ we must conclude that $4(k+1) < [(k+1)^2-7]$. Here are the necessary steps:

$$4k < (k^2-7) \Rightarrow 4k+4 < (k^2-7)+4 < (k^2-7)+(2k+1)$$

(because for $k \geq 6$, we find $2k+1 \geq 13 > 4$), and

$$4k+4 < (k^2-7)+(2k+1) \Rightarrow 4(k+1) < (k^2+2k+1)-7=(k+1)^2-7.$$

Therefore, by the Principle of Mathematical Induction, $S(n)$ is true for all $n \geq 6$.

EXAMPLE 4.9

Among the many interesting sequences of numbers encountered in discrete mathematics and combinatorics, one finds the *harmonic numbers* $H_1, H_2, H_3, \ldots,$ where

$$\begin{aligned} H_1 &= 1 \\ H_2 &= 1 + \frac{1}{2} \\ H_3 &= 1 + \frac{1}{2} + \frac{1}{3}, \\ &\ldots, \end{aligned}$$

and, in general, $H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$, for each $n \in \mathbf{Z}^+$.

The following property of the harmonic numbers provides one more opportunity for us to apply the Principle of Mathematical Induction.

$$\text{For all } n \in \mathbf{Z}^+, \sum_{j=1}^{n} H_j = (n+1)H_n - n.$$

Proof: As we have done in the earlier examples (that is, Examples 4.1, 4.4, and 4.7), we verify the basis step at $n = 1$ for the open statement $S(n)$: $\sum_{j=1}^{n} H_j = (n+1)H_n - n$. This result follows readily from

$$\sum_{j=1}^{1} H_j = H_1 = 1 = 2 \cdot 1 - 1 = (1+1)H_1 - 1.$$

To verify the inductive step, we assume the truth of $S(k)$, that is,

$$\sum_{j=1}^{k} H_j = (k+1)H_k - k.$$

This assumption then leads us to the following:

$$\begin{aligned} \sum_{j=1}^{k+1} H_j = \sum_{j=1}^{k} H_j + H_{k+1} &= [(k+1)H_k - k] + H_{k+1} \\ &= (k+1)H_k - k + H_{k+1} \\ &= (k+1)[H_{k+1} - (1/(k+1))] - k + H_{k+1} \\ &= (k+2)H_{k+1} - 1 - k \\ &= (k+2)H_{k+1} - (k+1). \end{aligned}$$

Consequently, we now know from the Principle of Mathematical Induction that $S(n)$ is true for all positive integers n.

EXAMPLE 4.10

For all $n \geq 0$ let $A_n \subset \mathbf{R}$, where $|A_n| = 2^n$ and the elements of A_n are listed in ascending order. If $r \in \mathbf{R}$, prove that in order to determine whether $r \in A_n$ (by the procedure developed below), we must compare r with no more than $n + 1$ elements in A_n.

When $n = 0$, $A_0 = \{a\}$ and only one comparison is needed. So the result is true for $n = 0$ (and we have our basis step). For $n = 1$, $A_1 = \{a_1, a_2\}$ with $a_1 < a_2$. In order to determine whether $r \in A_1$, at most two comparisons must be made. Hence the result follows when $n = 1$. Now if $n = 2$, we write $A_2 = \{b_1, b_2, c_1, c_2\} = B_1 \cup C_1$, where $b_1 < b_2 < c_1 < c_2$, $B_1 = \{b_1, b_2\}$, and $C_1 = \{c_1, c_2\}$. Comparing r with b_2, we determine which of the two possibilities — (i) $r \in B_1$; or (ii) $r \in C_1$ — can occur. Since $|B_1| = |C_1| = 2$, either one of the two possibilities requires at most two more comparisons (from the prior case where $n = 1$). Consequently, we can determine whether $r \in A_2$ by making no more than $2 + 1 = n + 1$ comparisons.

We now argue in general. Assume the result true for some $k \geq 0$ and consider the case for A_{k+1}, where $|A_{k+1}| = 2^{k+1}$. In order to establish our inductive step, let $A_{k+1} = B_k \cup C_k$, where $|B_k| = |C_k| = 2^k$, and the elements of B_k, C_k are in ascending order with the largest element x in B_k smaller than the least element in C_k. Let $r \in \mathbf{R}$. To determine whether $r \in A_{k+1}$, we consider whether $r \in B_k$ or $r \in C_k$.

a) First we compare r and x. (One comparison)

b) If $r \leq x$, then because $|B_k| = 2^k$, it follows by the induction hypothesis that we can determine whether $r \in B_k$ by making no more than $k + 1$ additional comparisons.

c) If $r > x$, we do likewise with the elements in C_k. We make at most $k + 1$ additional comparisons to see whether $r \in C_k$.

In any event, at most $(k + 1) + 1$ comparisons are made.

The general result now follows by the Principle of Mathematical Induction.

EXAMPLE 4.11

One of our first concerns when we evaluate the quality of a computer program is whether the program does what it is supposed to do. Just as we cannot prove a theorem by checking specific cases, so we cannot establish the correctness of a program simply by testing various sets of data. (Furthermore, doing this would be quite difficult if our program were to become a part of a larger software package wherein, perhaps, a data set is internally generated.) Since software development places a great deal of emphasis on structured programming, this has brought about the need for *program verification*. Here the programmer or the programming team must prove that the program being developed is correct *regardless* of the data set supplied. The effort invested at this stage considerably reduces the time that must be spent in debugging the program (or software package). One of the methods that can play a major role in such program verification is mathematical induction. Let us see how.

The pseudocode program segment shown in Fig. 4.5 is supposed to produce the answer $x(y^n)$ for real variables x, y with n a nonnegative integer. (The values for these three variables are assigned earlier in the program.) We shall verify the correctness of this program segment by mathematical induction for the open statement.

$S(n)$: For *all* x, $y \in \mathbf{R}$, if the program reaches the top of the **while** loop with $n \in \mathbf{N}$, after the loop is bypassed (for $n = 0$) or the two loop instructions are executed n (> 0) times, then the value of the real variable *answer* is $x(y^n)$.

```
while $n \neq 0$ do
  begin
    $x := x * y$
    $n := n - 1$
  end
answer := $x$
```

Figure 4.5

The flowchart for this program segment is shown in Fig. 4.6. Referring to it will help us as we develop our proof.

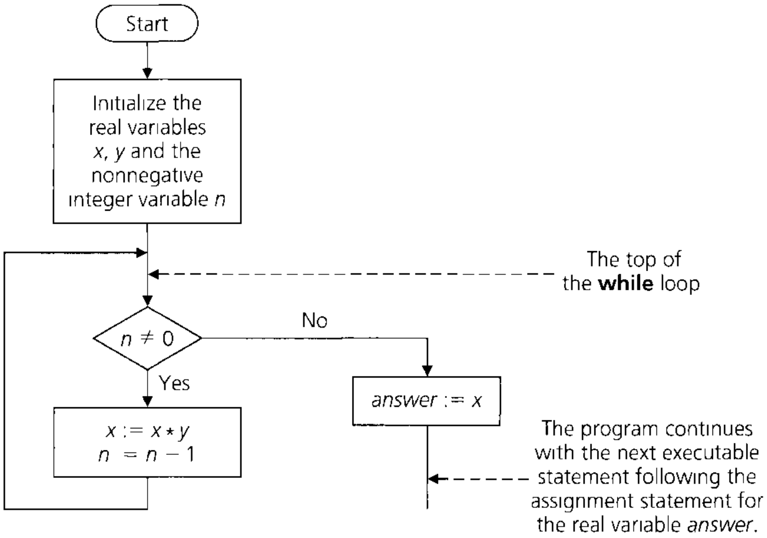

Start
Initialize the real variables x, y and the nonnegative integer variable n
The top of the **while** loop
n ≠ 0
No
Yes
answer := x
x := x * y
n = n − 1
The program continues with the next executable statement following the assignment statement for the real variable *answer*.

Figure 4.6

First consider $S(0)$, the statement for the case where $n = 0$. Here the program reaches the top of the **while** loop, but since $n = 0$, it follows the No branch in the flowchart and assigns the value $x = x(1) = x(y^0)$ to the real variable *answer*. Consequently, the statement $S(0)$ is true and the basis step of our induction argument is established.

Now we assume the truth of $S(k)$, for some nonnegative integer k. This provides us with the induction hypothesis.

$S(k)$: For *all* $x, y \in \mathbf{R}$, if the program reaches the top of the **while** loop with $k \in \mathbf{N}$, after the loop is bypassed (for $k = 0$) or the two loop instructions are executed k (> 0) times, then the value of the real variable *answer* is $x(y^k)$.

Continuing with the inductive step of the proof, when dealing with the statement $S(k+1)$, we note that because $k + 1 \geq 1$, the program will not simply follow the No branch and bypass the instructions in the **while** loop. Those two instructions (in the **while** loop) will be executed at least once. When the program reaches the top of the **while** loop for the first time, $n = k + 1 > 0$, so the loop instructions are executed and the program returns to the top of the **while** loop where now we find that

- The value of y is unchanged.
- The value of x is $x_1 = x(y^1) = xy$.
- The value of n is $(k + 1) - 1 = k$.

But now, by our induction hypothesis (applied to the real numbers x_1, y), we know that after the **while** loop for x_1, y and $n = k$ is bypassed (for $k = 0$) or the two loop instructions are executed k (> 0) times, then the value assigned to the real variable *answer* is

$$x_1(y^k) = (xy)(y^k) = x(y^{k+1}).$$

So by the Principle of Mathematical Induction, $S(n)$ is true for all $n \geq 0$ and the correctness of the program segment is established.

EXAMPLE 4.12

Recall (from Examples 1.37 and 3.11) that for a given $n \in \mathbf{Z}^+$, a *composition* of n is an *ordered* sum of positive-integer summands summing to n. In Fig. 4.7 we find the compositions of 1, 2, 3, and 4. We see that

a) 1 has $1 = 2^0 = 2^{1-1}$ composition, 2 has $2 = 2^1 = 2^{2-1}$ compositions, 3 has $4 = 2^2 = 2^{3-1}$ compositions, and 4 has $8 = 2^3 = 2^{4-1}$ compositions; and

b) the eight compositions of 4 arise from the four compositions of 3 in two ways: (i) Compositions (1′)–(4′) result by increasing the last summand (in each corresponding composition of 3) by 1; (ii) Each of compositions (1″)–(4″) is obtained by appending "+1" to the corresponding composition of 3.

$(n = 1)$	1		$(n = 4)$	$(1')$	4
				$(2')$	$1 + 3$
$(n = 2)$	2			$(3')$	$2 + 2$
	$1 + 1$			$(4')$	$1 + 1 + 2$
$(n = 3)$	(1)	3		$(1'')$	$3 + 1$
	(2)	$1 + 2$		$(2'')$	$1 + 2 + 1$
	(3)	$2 + 1$		$(3'')$	$2 + 1 + 1$
	(4)	$1 + 1 + 1$		$(4'')$	$1 + 1 + 1 + 1$

Figure 4.7

The observations in part (a) suggest that for all $n \in \mathbf{Z}^+$, $S(n)$: n has 2^{n-1} compositions. The result [in part (a)] for $n = 1$ provides our basis step, $S(1)$. So now let us assume the result true for some (fixed) $k \in \mathbf{Z}^+$ —namely, $S(k)$: k has 2^{k-1} compositions. At this point consider $S(k + 1)$. One can develop the compositions of $k + 1$ from those of k as in part (b) above (where $k = 3$). For $k \geq 1$, we find that the compositions of $k + 1$ fall into two distinct cases:

1) The compositions of $k + 1$, where the last summand is an integer $t > 1$: Here this last summand t is replaced by $t - 1$, and this type of replacement provides a correspondence between all of the compositions of k and all those compositions of $k + 1$, where the last summand exceeds 1.

2) The compositions of $k + 1$, where the last summand is 1: In this case we delete "+1" from the right side of this type of composition of $k + 1$. Once again we get a correspondence between all the compositions of k and all those compositions of $k + 1$, where the last summand is 1.

Therefore, the number of compositions of $k + 1$ is twice the number for k. Consequently, it follows from the induction hypothesis that the number of compositions of $k + 1$ is $2(2^{k-1}) = 2^k$. The Principle of Mathematical Induction now tells us that for all $n \in \mathbf{Z}^+$, $S(n)$: n has 2^{n-1} compositions (as we learned earlier in Examples 1.37 and 3.11).

EXAMPLE 4.13

We learn from the equation $14 = 3 + 3 + 8$ that we can express 14 using only 3's and 8's as summands. But what may prove to be surprising is that for all $n \geq 14$,

$S(n)$: n can be written as a sum of 3's and/or 8's (with no regard to order).

As we start to verify $S(n)$ for all $n \geq 14$, we realize that the given introductory sentence shows us that the basis step $S(14)$ is true. For the inductive step we assume the truth of $S(k)$ for some $k \in \mathbf{Z}^+$, where $k \geq 14$, and then consider what can happen for $S(k+1)$. If there is at least one 8 in the sum (of 3's and/or 8's) that equals k, then we can replace this 8 by three 3's and obtain $k+1$ as a sum of 3's and/or 8's. But suppose that no 8 appears as a summand of k. Then the only summand used is a 3, and, since $k \geq 14$, we must have at least five 3's as summands. And now if we replace five of these 3's by two 8's, we obtain the sum $k+1$, where the only summands are 3's and/or 8's. Consequently, we have shown how $S(k) \Rightarrow S(k+1)$ and so the result follows for all $n \geq 14$ by the Principle of Mathematical Induction.

Now that we have seen several applications of the Principle of Mathematical Induction, we shall close this section by introducing another form of mathematical induction. This second form is sometimes referred to as the *Alternative Form of the Principle of Mathematical Induction* or the *Principle of Strong Mathematical Induction.*

Once again we shall consider a statement of the form $\forall n \geq n_0\; S(n)$, where $n_0 \in \mathbf{Z}^+$, and we shall establish both a basis step and an inductive step. However, this time the basis step may require proving more than just the first case — where $n = n_0$. And in the inductive step we shall assume the truth of all the statements $S(n_0)$, $S(n_0+1)$, $\ldots$, $S(k-1)$, and $S(k)$, in order to establish the truth of the statement $S(k+1)$. We formally present this second Principle of Mathematical Induction in the following theorem.

THEOREM 4.2 *The Principle of Mathematical Induction—Alternative Form.* Let $S(n)$ denote an open mathematical statement (or set of such open statements) that involves one or more occurrences of the variable n, which represents a positive integer. Also let $n_0, n_1 \in \mathbf{Z}^+$ with $n_0 \leq n_1$.

a) If $S(n_0)$, $S(n_0+1)$, $S(n_0+2)$, $\ldots$, $S(n_1-1)$, and $S(n_1)$ are true; and

b) If whenever $S(n_0)$, $S(n_0+1)$, $\ldots$, $S(k-1)$, and $S(k)$ are true for some (particular but arbitrarily chosen) $k \in \mathbf{Z}^+$, where $k \geq n_1$, then the statement $S(k+1)$ is also true;

then $S(n)$ is true for all $n \geq n_0$.

As in Theorem 4.1, condition (a) is called the *basis step* and condition (b) is called the *inductive step.*

The proof of Theorem 4.2 is similar to that of Theorem 4.1 and will be requested in the Section Exercises. We shall also learn in the exercises for Section 4.2 that the two forms of mathematical induction (given in Theorems 4.1 and 4.2) are equivalent, for each can be shown to be a valid proof technique when we assume the truth of the other.

Before we give any examples where Theorem 4.2 is applied, let us mention, as we did for Theorem 4.1, that n_0 need not actually be a positive integer — it may, in reality, be 0 or even possibly a negative integer. And now that we have taken care of that point once again, let us see how we might apply this new proof technique.

Our first example should be familiar. We shall simply apply Theorem 4.2 in order to obtain the result in Example 4.13 in a second way.

EXAMPLE 4.14

The following calculations indicate that it is possible to write (without regard to order) the integers 14, 15, 16 using only 3's and/or 8's as summands:

$$14 = 3 + 3 + 8 \qquad 15 = 3 + 3 + 3 + 3 + 3 \qquad 16 = 8 + 8$$

On the basis of these three results, we make the conjecture

For every $n \in \mathbf{Z}^+$ where $n \geq 14$,

$$S(n): \quad n \text{ can be written as a sum of 3's and/or 8's.}$$

Proof: It is apparent that the statements $S(14)$, $S(15)$, and $S(16)$ are true — and this establishes our basis step. (Here $n_0 = 14$ and $n_1 = 16$.)

For the inductive step we assume the truth of the statements

$$S(14), S(15), \ldots, S(k-2), S(k-1), \text{ and } S(k)$$

for some $k \in \mathbf{Z}^+$, where $k \geq 16$. [The assumption of the truth of these $(k - 14) + 1$ statements constitutes our induction hypothesis.] And now if $n = k + 1$, then $n \geq 17$ and $k + 1 = (k-2) + 3$. But since $14 \leq k - 2 \leq k$, from the truth of $S(k-2)$ we know that $(k-2)$ can be written as a sum of 3's and/or 8's; so $(k+1) = (k-2) + 3$ can also be written in this form. Consequently, $S(n)$ is true for all $n \geq 14$ by the alternative form of the Principle of Mathematical Induction.

In Example 4.14 we saw how the truth of $S(k+1)$ was deduced by using the truth of the one prior result $S(k-2)$. Our last example presents a situation wherein the truth of more than one prior result is needed.

EXAMPLE 4.15

Let us consider the integer sequence $a_0, a_1, a_2, a_3, \ldots,$ where

$$a_0 = 1,\ a_1 = 2,\ a_2 = 3, \qquad \text{and}$$
$$a_n = a_{n-1} + a_{n-2} + a_{n-3}, \qquad \text{for all } n \in \mathbf{Z}^+ \text{ where } n \geq 3.$$

(Then, for instance, we find that $a_3 = a_2 + a_1 + a_0 = 3 + 2 + 1 = 6$; $a_4 = a_3 + a_2 + a_1 = 6 + 3 + 2 = 11$; and $a_5 = a_4 + a_3 + a_2 = 11 + 6 + 3 = 20$.)

We claim that the entries in this sequence are such that $a_n \leq 3^n$ for all $n \in \mathbf{N}$ — that is, $\forall n \in \mathbf{N}\ S'(n)$, where $S'(n)$ is the open statement: $a_n \leq 3^n$.

For the basis step, we observe that

i) $a_0 = 1 = 3^0 \leq 3^0$;

ii) $a_1 = 2 \leq 3 = 3^1$; and

iii) $a_2 = 3 \leq 9 = 3^2$.

Consequently, we know that $S'(0)$, $S'(1)$, and $S'(2)$ are true statements.

So now we turn our attention to the inductive step where we assume the truth of the statements $S'(0), S'(1), S'(2), \ldots, S'(k-1), S'(k)$, for some $k \in \mathbf{Z}^+$ where $k \geq 2$. For the case where $n = k + 1 \geq 3$ we see that

$$\begin{aligned} a_{k+1} &= a_k + a_{k-1} + a_{k-2} \\ &\leq 3^k + 3^{k-1} + 3^{k-2} \\ &\leq 3^k + 3^k + 3^k = 3(3^k) = 3^{k+1}, \end{aligned}$$

so $[S'(k-2) \wedge S'(k-1) \wedge S'(k)] \Rightarrow S'(k+1)$.

Therefore it follows from the alternative form of the Principle of Mathematical Induction that $a_n \leq 3^n$ for all $n \in \mathbf{N}$.

Before we close this section, let us take a second look at the preceding two results. In both Example 4.14 and Example 4.15 we established the basis step by verifying the truth of three statements: $S(14)$, $S(15)$, and $S(16)$ in Example 4.14; and, $S'(0)$, $S'(1)$, and $S'(2)$ in Example 4.15. However, to obtain the truth of $S(k+1)$ in Example 4.14, we actually used only one of the $(k-14)+1$ statements in the induction hypothesis — namely, the statement $S(k-2)$. For Example 4.15 we used three of the $k+1$ statements in the induction hypothesis — in this case, the statements $S'(k-2)$, $S'(k-1)$, and $S'(k)$.

EXERCISES 4.1

1. Prove each of the following for all $n \geq 1$ by the Principle of Mathematical Induction.

a) $1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2 = \dfrac{n(2n-1)(2n+1)}{3}$

b) $1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + \cdots + n(n+2) = \dfrac{n(n+1)(2n+7)}{6}$

c) $\displaystyle\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$

d) $\displaystyle\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4} = \left(\sum_{i=1}^{n} i\right)^2$

2. Establish each of the following for all $n \geq 1$ by the Principle of Mathematical Induction.

a) $\displaystyle\sum_{i=1}^{n} 2^{i-1} = \sum_{i=0}^{n-1} 2^i = 2^n - 1$

b) $\displaystyle\sum_{i=1}^{n} i(2^i) = 2 + (n-1)2^{n+1}$

c) $\displaystyle\sum_{i=1}^{n} (i)(i!) = (n+1)! - 1$

3. a) Note how $\sum_{i=1}^{n} i^3 + (n+1)^3 = \sum_{i=0}^{n} (i+1)^3 = \sum_{i=0}^{n} (i^3 + 3i^2 + 3i + 1)$. Use this result to obtain a formula for $\sum_{i=1}^{n} i^2$. (Compare with the formula given in Example 4.4.)

b) Use the idea presented in part (a) to find a formula for $\sum_{i=1}^{n} i^3$ and one for $\sum_{i=1}^{n} i^4$. [Compare the result for $\sum_{i=1}^{n} i^3$ with the formula in part (d) of Exercise 1 for this section.]

4. A wheel of fortune has the integers from 1 to 25 placed on it in a random manner. Show that regardless of how the numbers are positioned on the wheel, there are three adjacent numbers whose sum is at least 39.

5. Consider the following program segment (written in pseudocode):

```
for i := 1 to 123 do
  for j := 1 to i do
    print i * j
```

a) How many times is the print statement of the third line executed?

b) Replace i in the second line by i^2, and answer the question in part (a).

6. a) For the four-digit integers (from 1000 to 9999) how many are palindromes and what is their sum?

b) Write a computer program to check the answer for the sum in part (a).

7. A lumberjack has $4n + 110$ logs in a pile consisting of n layers. Each layer has two more logs than the layer directly above it. If the top layer has six logs, how many layers are there?

8. Determine the positive integer n for which

$$\sum_{i=1}^{2n} i = \sum_{i=1}^{n} i^2.$$

9. Evaluate each of the following:

a) $\sum_{i=11}^{33} i$ **b)** $\sum_{i=11}^{33} i^2$.

10. Determine $\sum_{i=51}^{100} t_i$, where t_i denotes the ith triangular number, for $51 \leq i \leq 100$.

11. a) Derive a formula for $\sum_{i=1}^{n} t_{2i}$, where t_{2i} denotes the $2i$th triangular number for $1 \leq i \leq n$.

b) Determine $\sum_{i=1}^{100} t_{2i}$.

c) Write a computer program to check the result in part (b).

12. a) Prove that $(\cos\theta + i \sin\theta)^2 = \cos 2\theta + i \sin 2\theta$, where $i \in \mathbf{C}$ and $i^2 = -1$.

b) Using induction, prove that for all $n \in \mathbf{Z}^+$,

$$(\cos\theta + i \sin\theta)^n = \cos n\theta + i \sin n\theta.$$

(This result is known as *DeMoivre's Theorem.*)

c) Verify that $1 + i = \sqrt{2}(\cos 45° + i \sin 45°)$, and compute $(1+i)^{100}$.

13. a) Consider an 8×8 chessboard. It contains sixty-four 1×1 squares and one 8×8 square. How many 2×2

squares does it contain? How many 3×3 squares? How many squares in total?

b) Now consider an $n \times n$ chessboard for some fixed $n \in \mathbf{Z}^+$. For $1 \leq k \leq n$, how many $k \times k$ squares are contained in this chessboard? How many squares in total?

14. Prove that for all $n \in \mathbf{Z}^+$, $n > 3 \Rightarrow 2^n < n!$

15. Prove that for all $n \in \mathbf{Z}^+$, $n > 4 \Rightarrow n^2 < 2^n$.

16. a) For $n = 3$ let $X_3 = \{1, 2, 3\}$. Now consider the sum

$$s_3 = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{1\cdot 2} + \frac{1}{1\cdot 3} + \frac{1}{2\cdot 3} + \frac{1}{1\cdot 2\cdot 3}$$
$$= \sum_{\emptyset \neq A \subseteq X_3} \frac{1}{p_A},$$

where p_A denotes the product of all elements in a nonempty subset A of X_3. Note that the sum is taken over all the nonempty subsets of X_3. Evaluate this sum.

b) Repeat the calculation in part (a) for s_2 (where $n = 2$ and $X_2 = \{1, 2\}$) and s_4 (where $n = 4$ and $X_4 = \{1, 2, 3, 4\}$).

c) Conjecture the general result suggested by the calculations from parts (a) and (b). Prove your conjecture using the Principle of Mathematical Induction.

17. For $n \in \mathbf{Z}^+$, let H_n denote the nth harmonic number (as defined in Example 4.9).

a) For all $n \in \mathbf{N}$ prove that $1 + \left(\frac{n}{2}\right) \leq H_{2^n}$.

b) Prove that for all $n \in \mathbf{Z}^+$,

$$\sum_{j=1}^{n} jH_j = \left[\frac{n(n+1)}{2}\right] H_{n+1} - \left[\frac{n(n+1)}{4}\right].$$

18. Consider the following four equations:

1) $1 = 1$

2) $2 + 3 + 4 = 1 + 8$

3) $5 + 6 + 7 + 8 + 9 = 8 + 27$

4) $10 + 11 + 12 + 13 + 14 + 15 + 16 = 27 + 64$

Conjecture the general formula suggested by these four equations, and prove your conjecture.

19. For $n \in \mathbf{Z}^+$, let $S(n)$ be the open statement

$$\sum_{i=1}^{n} i = \frac{(n + (1/2))^2}{2}.$$

Show that the truth of $S(k)$ implies the truth of $S(k+1)$ for all $k \in \mathbf{Z}^+$. Is $S(n)$ true for all $n \in \mathbf{Z}^+$?

20. Let S_1 and S_2 be two sets where $|S_1| = m$, $|S_2| = r$, for $m, r \in \mathbf{Z}^+$, and the elements in each of S_1, S_2 are in ascending order. It can be shown that the elements in S_1 and S_2 can be merged into ascending order by making no more than $m + r - 1$ comparisons. (See Lemma 12.1.) Use this result to establish the following.

For $n \geq 0$, let S be a set with $|S| = 2^n$. Prove that the number of comparisons needed to place the elements of S in ascending order is bounded above by $n \cdot 2^n$.

21. During the execution of a certain program segment (written in pseudocode), the user assigns to the integer variables x and n any (possibly different) positive integers. The segment shown in Fig. 4.8 immediately follows these assignments. If the program reaches the top of the **while** loop, state and prove (by mathematical induction) what the value assigned to *answer* will be after the two loop instructions are executed n (> 0) times.

```
while n ≠ 0 do
  begin
    x := x * n
    n := n - 1
  end
answer := x
```

Figure 4.8

22. In the program segment shown in Fig. 4.9, x, y, and *answer* are real variables, and n is an integer variable. Prior to execution of this **while** loop, the user supplies real values for x and y and a nonnegative integer value for n. Prove (by mathematical induction) that for all $x, y \in \mathbf{R}$, if the program reaches the top of the **while** loop with $n \in \mathbf{N}$, after the loop is bypassed (for $n = 0$) or the two loop instructions are executed n (> 0) times, then the value assigned to *answer* is $x + ny$.

```
while n ≠ 0 do
  begin
    x := x + y
    n := n - 1
  end
answer := x
```

Figure 4.9

23. a) Let $n \in \mathbf{Z}^+$, where $n \neq 1, 3$. Prove that n can be expressed as a sum of 2's and/or 5's.

b) For all $n \in \mathbf{Z}^+$ show that if $n \geq 24$, then n can be written as a sum of 5's and/or 7's.

24. A sequence of numbers $a_1, a_2, a_3, \ldots$ is defined by

$$a_1 = 1 \qquad a_2 = 2 \qquad a_n = a_{n-1} + a_{n-2},\ n \geq 3.$$

a) Determine the values of a_3, a_4, a_5, a_6, and a_7.

b) Prove that for all $n \geq 1$, $a_n < (7/4)^n$.

25. For a fixed $n \in \mathbf{Z}^+$, let X be the random variable where $Pr(X = x) = \frac{1}{n}$, $x = 1, 2, 3, \ldots, n$. (Here X is called a *uniform discrete* random variable.) Determine $E(X)$ and $\mathrm{Var}(X)$.

26. Let a_0 be a fixed constant and, for $n \geq 1$, let $a_n = \sum_{i=0}^{n-1} \binom{n-1}{i} a_i a_{(n-1)-i}$.

a) Show that $a_1 = a_0^2$ and that $a_2 = 2a_0^3$.

b) Determine a_3 and a_4 in terms of a_0.

c) Conjecture a formula for a_n in terms of a_0 when $n \geq 0$. Prove your conjecture using the Principle of Mathematical Induction.

27. Verify Theorem 4.2.

28. a) Of the $2^{5-1} = 2^4 = 16$ compositions of 5, determine how many start with (i) 1; (ii) 2; (iii) 3; (iv) 4; and (v) 5.

b) Provide a combinatorial proof for the result in part (a) of Exercise 2.

4.2 Recursive Definitions

Let us start this section by considering the integer sequence $b_0, b_1, b_2, b_3, \ldots,$ where $b_n = 2n$ for all $n \in \mathbf{N}$. Here we find that $b_0 = 2 \cdot 0 = 0$, $b_1 = 2 \cdot 1 = 2$, $b_2 = 2 \cdot 2 = 4$, and $b_3 = 2 \cdot 3 = 6$. If, for instance, we need to determine b_6, we simply calculate $b_6 = 2 \cdot 6 = 12$—without the need to calculate the value of b_n for any other $n \in \mathbf{N}$. We can perform such calculations because we have an *explicit* formula—namely, $b_n = 2n$—that tells us how b_n is determined from n (alone).

In Example 4.15 of the preceding section, however, we considered the integer sequence $a_0, a_1, a_2, a_3, \ldots,$ where

$$a_0 = 1, a_1 = 2, a_2 = 3, \qquad \text{and}$$
$$a_n = a_{n-1} + a_{n-2} + a_{n-3}, \quad \text{for all } n \in \mathbf{Z}^+ \text{ where } n \geq 3.$$

Here we do *not* have an *explicit* formula that defines each a_n in terms of n for all $n \in \mathbf{N}$. If we want the value of a_6, for example, we need to know the values of a_5, a_4, and a_3. And these values (of a_5, a_4, and a_3) require that we also know the values of a_2, a_1, and a_0. Unlike the rather easy situation where we determined $b_6 = 2 \cdot 6 = 12$, in order to calculate a_6, here we might find ourselves writing

$$\begin{aligned}
a_6 &= a_5 + a_4 + a_3 \\
&= (a_4 + a_3 + a_2) + (a_3 + a_2 + a_1) + (a_2 + a_1 + a_0) \\
&= [(a_3 + a_2 + a_1) + (a_2 + a_1 + a_0) + a_2] \\
&\quad + [(a_2 + a_1 + a_0) + a_2 + a_1] + (a_2 + a_1 + a_0) \\
&= [[(a_2 + a_1 + a_0) + a_2 + a_1] + (a_2 + a_1 + a_0) + a_2] \\
&\quad + [(a_2 + a_1 + a_0) + a_2 + a_1] + (a_2 + a_1 + a_0) \\
&= [[(3 + 2 + 1) + 3 + 2] + (3 + 2 + 1) + 3] \\
&\quad + [(3 + 2 + 1) + 3 + 2] + (3 + 2 + 1) \\
&= 37.
\end{aligned}$$

Or, in a somewhat easier manner, we could have gone in the opposite direction with these considerations:

$$\begin{aligned}
a_3 &= a_2 + a_1 + a_0 = 3 + 2 + 1 = 6 \\
a_4 &= a_3 + a_2 + a_1 = 6 + 3 + 2 = 11 \\
a_5 &= a_4 + a_3 + a_2 = 11 + 6 + 3 = 20 \\
a_6 &= a_5 + a_4 + a_3 = 20 + 11 + 6 = 37.
\end{aligned}$$

No matter how we arrive at a_6, we realize that the two integer sequences—$b_0, b_1, b_2, b_3, \ldots,$ and $a_0, a_1, a_2, a_3, \ldots$—are more than just numerically different. The integers $b_0, b_1, b_2, b_3, \ldots,$ can be very readily listed as $0, 2, 4, 6, \ldots,$ and for any $n \in \mathbf{N}$ we have the *explicit* formula $b_n = 2n$. On the other hand, we might find it rather difficult (if not impossible) to determine such an explicit formula for the integers $a_0, a_1, a_2, a_3, \ldots$.

What is happening here for a sequence of integers can also occur for other mathematical concepts — such as sets and binary operations [as well as functions (in Chapter 5), languages (in Chapter 6), and relations (in Chapter 7)]. Sometimes it is difficult to define a mathematical concept in an explicit manner. But, as for the sequence $a_0, a_1, a_2, a_3, \ldots$, we may be able to define what we need in terms of similar prior results. (We shall examine what we mean by this in several examples in this section.) When we do so we say that the concept is defined *recursively*, using the method, or process, of *recursion*. In this way we obtain the concept we are interested in studying — by means of a *recursive definition*. Hence, although we do not have an explicit formula here for the sequence $a_0, a_1, a_2, a_3, \ldots$, we do have a way of defining the integers a_n, for $n \in \mathbf{N}$, by recursion. The assignments

$$a_0 = 1, \qquad a_1 = 2, \qquad a_2 = 3$$

provide a base for the recursion.

The equation

$$a_n = a_{n-1} + a_{n-2} + a_{n-3}, \qquad \text{for } n \in \mathbf{Z}^+ \text{ where } n \geq 3, \qquad (*)$$

provides the recursive process; it indicates how to obtain new entries in the sequence from those prior results we already know (or can calculate). [*Note*: The integers computed from Eq. (*) may also be computed from the equation $a_{n+3} = a_{n+2} + a_{n+1} + a_n$, for $n \in \mathbf{N}$.]

We now use the concept of the *recursive definition* to settle something that was mentioned in three footnotes in Sections 2.1 and 2.3. After studying Section 2.2 we knew (from the laws of logic) that for any statements p_1, p_2, and p_3, we had

$$p_1 \wedge (p_2 \wedge p_3) \Longleftrightarrow (p_1 \wedge p_2) \wedge p_3,$$

and, consequently, we could write $p_1 \wedge p_2 \wedge p_3$ without any chance of ambiguity. This is because the truth value for the conjunction of three statements does not depend on the way parentheses might be introduced to direct the order of forming the conjunctions of pairs of (given or resultant) statements. But we were concerned about what meaning we should attach to an expression such as $p_1 \wedge p_2 \wedge p_3 \wedge p_4$. The following example now settles that issue.

EXAMPLE 4.16

The logical connective $\wedge$ was defined (in Section 2.1) for only two statements at a time. How, then, does one deal with an expression such as $p_1 \wedge p_2 \wedge p_3 \wedge p_4$, where p_1, p_2, p_3, and p_4 are statements? In order to answer this question we introduce the following recursive definition, wherein the concept at a certain [$(n + 1)$st] stage is developed from the comparable concept at an earlier [nth] stage.

Given any statements $p_1, p_2, \ldots, p_n, p_{n+1}$, we define

1) the conjunction of p_1, p_2 by $p_1 \wedge p_2$ (as we did in Section 2.1), and
2) the conjunction of $p_1, p_2, \ldots, p_n, p_{n+1}$, for $n \geq 2$, by

$$p_1 \wedge p_2 \wedge \cdots \wedge p_n \wedge p_{n+1} \Longleftrightarrow (p_1 \wedge p_2 \wedge \cdots \wedge p_n) \wedge p_{n+1}.$$

[The result in (1) establishes the base for the recursion, while the logical equivalence in (2) is used to provide the recursive process. Note that the statement on the right-hand side of the logical equivalence in (2) is the conjunction of *two* statements: p_{n+1} and the previously determined statement $(p_1 \wedge p_2 \wedge \cdots \wedge p_n)$.]

Therefore, we define the conjunction of p_1, p_2, p_3, p_4 by

$$p_1 \wedge p_2 \wedge p_3 \wedge p_4 \Longleftrightarrow (p_1 \wedge p_2 \wedge p_3) \wedge p_4.$$

Then, by the associative law of $\wedge$, we find that

$$\begin{aligned}(p_1 \wedge p_2 \wedge p_3) \wedge p_4 &\Longleftrightarrow [(p_1 \wedge p_2) \wedge p_3] \wedge p_4\\ &\Longleftrightarrow (p_1 \wedge p_2) \wedge (p_3 \wedge p_4)\\ &\Longleftrightarrow p_1 \wedge [p_2 \wedge (p_3 \wedge p_4)]\\ &\Longleftrightarrow p_1 \wedge [(p_2 \wedge p_3) \wedge p_4]\\ &\Longleftrightarrow p_1 \wedge (p_2 \wedge p_3 \wedge p_4).\end{aligned}$$

These logical equivalences show that the truth value for the conjunction of four statements is also independent of the way parentheses might be introduced to indicate how to associate the given statements.

Using the above definition, we now extend our results to the following "Generalized Associative Law for $\wedge$."

Let $n \in \mathbf{Z}^+$ where $n \geq 3$, and let $r \in \mathbf{Z}^+$ with $1 \leq r < n$. Then

$$S(n):\quad \text{For any statements } p_1, p_2, \ldots, p_r, p_{r+1}, \ldots, p_n,$$
$$(p_1 \wedge p_2 \wedge \cdots \wedge p_r) \wedge (p_{r+1} \wedge \cdots \wedge p_n) \Longleftrightarrow p_1 \wedge p_2 \wedge \cdots \wedge p_r \wedge p_{r+1} \wedge \cdots \wedge p_n.$$

Proof: The truth of the statement $S(3)$ follows from the associative law for $\wedge$ — and this establishes the basis step for our inductive proof. For the inductive step we assume that $S(k)$ is true for some $k \geq 3$ and all $1 \leq r < k$. That is, we assume the truth of

$$\begin{aligned}S(k):\quad &(p_1 \wedge p_2 \wedge \cdots \wedge p_r) \wedge (p_{r+1} \wedge \cdots \wedge p_k)\\ &\Longleftrightarrow p_1 \wedge p_2 \wedge \cdots \wedge p_r \wedge p_{r+1} \wedge \cdots \wedge p_k.\end{aligned}$$

Then we show that $S(k) \Rightarrow S(k+1)$. When we consider $k+1$ statements, then we must account for all $1 \leq r < k+1$.

1) If $r = k$, then

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_k) \wedge p_{k+1} \Longleftrightarrow p_1 \wedge p_2 \wedge \cdots \wedge p_k \wedge p_{k+1},$$

from our recursive definition.

2) For $1 \leq r < k$, we have

$$\begin{aligned}&(p_1 \wedge p_2 \wedge \cdots \wedge p_r) \wedge (p_{r+1} \wedge \cdots \wedge p_k \wedge p_{k+1})\\ &\quad\Longleftrightarrow (p_1 \wedge p_2 \wedge \cdots \wedge p_r) \wedge [(p_{r+1} \wedge \cdots \wedge p_k) \wedge p_{k+1}]\\ &\quad\Longleftrightarrow [(p_1 \wedge p_2 \wedge \cdots \wedge p_r) \wedge (p_{r+1} \wedge \cdots \wedge p_k)] \wedge p_{k+1}\\ &\quad\Longleftrightarrow (p_1 \wedge p_2 \wedge \cdots \wedge p_r \wedge p_{r+1} \wedge \cdots \wedge p_k) \wedge p_{k+1}\\ &\quad\Longleftrightarrow p_1 \wedge p_2 \wedge \cdots \wedge p_r \wedge p_{r+1} \wedge \cdots \wedge p_k \wedge p_{k+1}.\end{aligned}$$

So it follows by the Principle of Mathematical Induction (Theorem 4.1) that the open statement $S(n)$ is true for all $n \in \mathbf{Z}^+$ where $n \geq 3$.

Our next example provides us with a second opportunity to generalize an associative law—but this time we shall deal with sets instead of statements.

EXAMPLE 4.17

In Definition 3.10 we extended the binary operations of $\cup$ and $\cap$ to an arbitrary (finite or infinite) number of subsets from a given universe $\mathcal{U}$. However, these definitions do not rely on the binary nature of the operations involved, and they do not provide a *systematic* way of determining the union or intersection of any finite number of sets.

To overcome this difficulty, we consider the sets $A_1, A_2, \ldots, A_n, A_{n+1}$, where $A_i \subseteq \mathcal{U}$ for all $1 \leq i \leq n+1$, and we define their union *recursively* as follows:

1) The union of A_1, A_2 is $A_1 \cup A_2$. (This is the base for our recursive definition.)
2) The union of $A_1, A_2, \ldots, A_n, A_{n+1}$, for $n \geq 2$, is given by

$$A_1 \cup A_2 \cup \cdots \cup A_n \cup A_{n+1} = (A_1 \cup A_2 \cup \cdots \cup A_n) \cup A_{n+1},$$

where the set on the right-hand side of the set equality is the union of *two* sets, namely, $A_1 \cup A_2 \cup \cdots \cup A_n$ and A_{n+1}. (Here we have the recursive process needed to complete our recursive definition.)

From this definition we obtain the following "Generalized Associative Law for $\cup$." If $n, r \in \mathbf{Z}^+$ with $n \geq 3$ and $1 \leq r < n$, then

$$S(n): \quad (A_1 \cup A_2 \cup \cdots \cup A_r) \cup (A_{r+1} \cup \cdots \cup A_n) = A_1 \cup A_2 \cup \cdots \cup A_r \cup A_{r+1} \cup \cdots \cup A_n,$$

where $A_i \subseteq \mathcal{U}$ for all $1 \leq i \leq n$.

Proof: The truth of $S(n)$ for $n = 3$ follows from the associative law of $\cup$, thereby providing the basis step needed for this inductive proof. Assuming the truth of $S(k)$ for some $k \in \mathbf{Z}^+$, where $k \geq 3$ and $1 \leq r < k$, we shall now establish our inductive step by showing that $S(k) \Rightarrow S(k+1)$. When dealing with $k+1$ (≥ 4) sets we need to consider all $1 \leq r < k+1$. We find that

1) For $r = k$ we have

$$(A_1 \cup A_2 \cup \cdots \cup A_k) \cup A_{k+1} = A_1 \cup A_2 \cup \cdots \cup A_k \cup A_{k+1}.$$

This follows from the given recursive definition.

2) If $1 \leq r < k$, then

$$\begin{aligned}(A_1 \cup A_2 \cup \cdots \cup A_r) \cup (A_{r+1} \cup \cdots \cup A_k \cup A_{k+1}) \\ &= (A_1 \cup A_2 \cup \cdots \cup A_r) \cup [(A_{r+1} \cup \cdots \cup A_k) \cup A_{k+1}] \\ &= [(A_1 \cup A_2 \cup \cdots \cup A_r) \cup (A_{r+1} \cup \cdots \cup A_k)] \cup A_{k+1} \\ &= (A_1 \cup A_2 \cup \cdots \cup A_r \cup A_{r+1} \cup \cdots \cup A_k) \cup A_{k+1} \\ &= A_1 \cup A_2 \cup \cdots \cup A_r \cup A_{r+1} \cup \cdots \cup A_k \cup A_{k+1}.\end{aligned}$$

So it follows by the Principle of Mathematical Induction that $S(n)$ is true for all integers $n \geq 3$.

Similar to the result in Example 4.17, the intersection of the $n + 1$ sets $A_1, A_2, \ldots, A_n, A_{n+1}$ (each taken from the same universe $\mathcal{U}$) is defined recursively by:

1) The intersection of A_1, A_2 is $A_1 \cap A_2$.
2) For $n \geq 2$, the intersection of $A_1, A_2, \ldots, A_n, A_{n+1}$ is given by

$$A_1 \cap A_2 \cap \cdots \cap A_n \cap A_{n+1} = (A_1 \cap A_2 \cap \cdots \cap A_n) \cap A_{n+1},$$

the intersection of the *two* sets $A_1 \cap A_2 \cap \cdots \cap A_n$ and A_{n+1}.

We find that the recursive definitions for the union and intersection of any finite number of sets provide the means by which we can extend the DeMorgan Laws of Set Theory. We shall establish (by using mathematical induction) one of these extensions in the next example and request a proof of the other extension in the Section Exercises.

EXAMPLE 4.18

Let $n \in \mathbf{Z}^+$ where $n \geq 2$, and let $A_1, A_2, \ldots, A_n \subseteq \mathcal{U}$ for each $1 \leq i \leq n$. Then

$$\overline{A_1 \cap A_2 \cap \cdots \cap A_n} = \overline{A}_1 \cup \overline{A}_2 \cup \cdots \cup \overline{A}_n.$$

Proof: The basis step of this proof is given for $n = 2$. It follows from the fact that $\overline{A_1 \cap A_2} = \overline{A}_1 \cup \overline{A}_2$—by the second of DeMorgan's Laws (listed in the Laws of Set Theory in Section 3.2).

Assuming the truth of the result for some k, where $k \geq 2$, we have

$$\overline{A_1 \cap A_2 \cap \cdots \cap A_k} = \overline{A}_1 \cup \overline{A}_2 \cup \cdots \cup \overline{A}_k.$$

And when we consider $k + 1$ (≥ 3) sets, the induction hypothesis is used to obtain the third set equality in the following:

$$\overline{A_1 \cap A_2 \cap \cdots \cap A_k \cap A_{k+1}} = \overline{(A_1 \cap A_2 \cap \cdots \cap A_k) \cap A_{k+1}}$$
$$= \overline{(A_1 \cap A_2 \cap \cdots \cap A_k)} \cup \overline{A}_{k+1} = (\overline{A}_1 \cup \overline{A}_2 \cup \cdots \cup \overline{A}_k) \cup \overline{A}_{k+1}$$
$$= \overline{A}_1 \cup \overline{A}_2 \cup \cdots \cup \overline{A}_k \cup \overline{A}_{k+1}.$$

This then establishes the inductive step in our proof and so we obtain this generalized DeMorgan Law for all $n \geq 2$ by the Principle of Mathematical Induction.

Now that we have seen the two recursive definitions (in Examples 4.16 and 4.17), as we continue to investigate situations where this type of definition arises, we shall generally refrain from labeling the base and recursive parts. Likewise, we may not always designate the basis and inductive steps in a proof by mathematical induction.

As we look back at Examples 4.16 and 4.17, the recursive definitions in these two examples should seem similar to us. For if we interchange the statement p_i with the set A_i, for all $1 \leq i \leq n + 1$, and if we interchange each occurrence of $\wedge$ with $\cup$ and replace $\Longleftrightarrow$ with $=$, then we can obtain the recursive definition in Example 4.17 from the one given in Example 4.16.

In a similar way one can recursively define the sum and product of n real numbers, where $n \in \mathbf{Z}^+$ and $n \geq 2$. Then we can obtain (by the Principle of Mathematical Induction) generalized associative laws for the addition and multiplication of real numbers. (In the

Section Exercises the reader will be requested to do this.) We want to be aware of such generalized associative laws because we have been using them and will continue to use them. The reader may be surprised to learn that we have already used the generalized associative law of addition. In each of Examples 4.1 and 4.4, for instance, the generalized associative law of addition was used to establish the inductive step (in the proof by mathematical induction). Furthermore, now that we are more aware of it, the generalized associative law of addition can be used (usually, in an implicit manner) in recursive definitions — for now there will be no chance for ambiguity if one wants to add four or more summands. For example, we could define the sequence of harmonic numbers $H_1, H_2, H_3, \dots$, by

1) $H_1 = 1$; and
2) For $n \geq 1$, $H_{n+1} = H_n + \left(\frac{1}{n+1}\right)$.

Turning from addition to multiplication, we may use the generalized associative law of multiplication to provide a recursive definition of $n!$. In this case we write

1) $0! = 1$; and
2) For $n \geq 0$, $(n+1)! = (n+1)(n!)$.

(This was suggested in the paragraph following Definition 1.1 in Section 1.2.) Also, the integer sequence $b_0, b_1, b_2, b_3, \dots$, given explicitly (at the start of this section) by the formula $b_n = 2n$, $n \in \mathbf{N}$, can now be defined recursively by

1) $b_0 = 0$; and
2) For $n \geq 0$, $b_{n+1} = b_n + 2$.

When we investigate the sequences in our next two examples, we shall once again find recursive definitions. In addition we shall establish results where the generalized associative law of addition will be used — although in an implicit manner.

EXAMPLE 4.19

In Section 4.1 we introduced the sequence of rational numbers called the harmonic numbers. Now we introduce an integer sequence that is prominent in combinatorics and graph theory (and that we shall study further in Chapters 10, 11, and 12). The *Fibonacci numbers* may be defined recursively by

1) $F_0 = 0$, $F_1 = 1$; and
2) $F_n = F_{n-1} + F_{n-2}$, for $n \in \mathbf{Z}^+$ with $n \geq 2$.

Hence, from the recursive part of this definition, it follows that

$$F_2 = F_1 + F_0 = 1 + 0 = 1 \qquad F_4 = F_3 + F_2 = 2 + 1 = 3$$
$$F_3 = F_2 + F_1 = 1 + 1 = 2 \qquad F_5 = F_4 + F_3 = 3 + 2 = 5.$$

We also find that $F_6 = 8$, $F_7 = 13$, $F_8 = 21$, $F_9 = 34$, $F_{10} = 55$, $F_{11} = 89$, and $F_{12} = 144$.

The recursive definition of the Fibonacci numbers can be used (in conjunction with the Principle of Mathematical Induction) to establish many of the interesting properties that these numbers exhibit. We investigate one of these properties now.

Let us consider the following five results that deal with sums of squares of the Fibonacci numbers.

1) $F_0^2 + F_1^2 = 0^2 + 1^2 = 1 = 1 \times 1$
2) $F_0^2 + F_1^2 + F_2^2 = 0^2 + 1^2 + 1^2 = 2 = 1 \times 2$
3) $F_0^2 + F_1^2 + F_2^2 + F_3^2 = 0^2 + 1^2 + 1^2 + 2^2 = 6 = 2 \times 3$

4) $F_0^2 + F_1^2 + F_2^2 + F_3^2 + F_4^2 = 0^2 + 1^2 + 1^2 + 2^2 + 3^2 = 15 = 3 \times 5$

5) $F_0^2 + F_1^2 + F_2^2 + F_3^2 + F_4^2 + F_5^2 = 0^2 + 1^2 + 1^2 + 2^2 + 3^2 + 5^2 = 40 = 5 \times 8$

From what is suggested in these calculations, we conjecture that

$$\forall n \in \mathbf{Z}^+ \sum_{i=0}^{n} F_i^2 = F_n \times F_{n+1}.$$

Proof: For $n = 1$, the result in Eq. (1)—namely, $F_0^2 + F_1^2 = 1 \times 1$—shows us that the conjecture is true in this first case.

Assuming the truth of the conjecture for some $k \geq 1$, we obtain the induction hypothesis:

$$\sum_{i=0}^{k} F_i^2 = F_k \times F_{k+1}.$$

Turning now to the case where $n = k + 1$ (≥ 2) we find that

$$\sum_{i=0}^{k+1} F_i^2 = \sum_{i=0}^{k} F_i^2 + F_{k+1}^2 = (F_k \times F_{k+1}) + F_{k+1}^2 = F_{k+1} \times (F_k + F_{k+1}) = F_{k+1} \times F_{k+2}.$$

Hence the truth of the case for $n = k + 1$ follows from the case for $n = k$. So the given conjecture is true for all $n \in \mathbf{Z}^+$ by the Principle of Mathematical Induction. (The reader may wish to note that the prior calculation uses the generalized associative law of addition. Furthermore we employ the recursive definition of the Fibonacci numbers; it allows us to replace $F_k + F_{k+1}$ by F_{k+2}.)

EXAMPLE 4.20

Closely related to the Fibonacci numbers is the sequence known as the *Lucas numbers*. This sequence is defined recursively by

1) $L_0 = 2$, $L_1 = 1$; and

2) $L_n = L_{n-1} + L_{n-2}$, for $n \in \mathbf{Z}^+$ with $n \geq 2$.

The first eight Lucas numbers are given in Table 4.2

Table 4.2

n	0	1	2	3	4	5	6	7
L_n	2	1	3	4	7	11	18	29

Although they are not as prominent as the Fibonacci numbers, the Lucas numbers also possess many interesting properties. One of the interrelations between the Fibonacci and Lucas numbers is illustrated in the fact that

$$\forall n \in \mathbf{Z}^+ \; L_n = F_{n-1} + F_{n+1}.$$

Proof: Here we need to consider what happens when $n = 1$ and $n = 2$. We find that

$$L_1 = 1 = 0 + 1 = F_0 + F_2 = F_{1-1} + F_{1+1}, \quad \text{and}$$
$$L_2 = 3 = 1 + 2 = F_1 + F_3 = F_{2-1} + F_{2+1},$$

so the result is true in these first two cases.

Next we assume that $L_n = F_{n-1} + F_{n+1}$ for the integers $n = 1, 2, 3, \ldots, k-1, k$, where $k \geq 2$, and then we consider the Lucas number L_{k+1}. It turns out that

$$\begin{aligned} L_{k+1} &= L_k + L_{k-1} = (F_{k-1} + F_{k+1}) + (F_{k-2} + F_k) \qquad (*) \\ &= (F_{k-1} + F_{k-2}) + (F_{k+1} + F_k) = F_k + F_{k+2} = F_{(k+1)-1} + F_{(k+1)+1}. \end{aligned}$$

Therefore, it follows from the alternative form of the Principle of Mathematical Induction that $L_n = F_{n-1} + F_{n+1}$ for all $n \in \mathbf{Z}^+$. [The reader should observe how we used the recursive definitions for both the Fibonacci numbers and the Lucas numbers in the calculations at (*).]

EXAMPLE 4.21

In Section 1.3 we introduced the binomial coefficients $\binom{n}{r}$ for $n, r \in \mathbf{N}$, where $n \geq r \geq 0$. Corollary 1.1 in that section revealed that $\sum_{r=0}^{n} \binom{n}{r} = \sum_{r=0}^{n} C(n, r) = 2^n$, the total number of subsets for a set of size n. With the help of the result in Example 3.12 we can now define these binomial coefficients recursively by

$$\binom{n+1}{r} = \binom{n}{r} + \binom{n}{r-1}, \quad n \geq r \geq 0,$$

$$\binom{0}{0} = 1, \qquad \binom{n}{r} = 0, \quad r > n, \qquad \binom{n}{r} = 0, \quad r < 0.$$

At this time we present a second set of numbers, each of which is also dependent on two integers. For $m, k \in \mathbf{N}$, the *Eulerian numbers* $a_{m,k}$ are defined recursively by

$$\begin{aligned} &a_{m,k} = (m-k)a_{m-1,k-1} + (k+1)a_{m-1,k}, \quad 0 \leq k \leq m-1, \qquad (*) \\ &a_{0,0} = 1, \qquad a_{m,k} = 0, \quad k \geq m, \qquad a_{m,k} = 0, \quad k < 0. \end{aligned}$$

(In Exercise 18 of the Section Exercises we shall examine a situation that shows how this recursive definition may arise.) The values for $a_{m,k}$, where $1 \leq m \leq 5$ and $0 \leq k \leq m-1$, are given as follows:

										Row Sum
$(m = 1)$					1					$1 = 1!$
$(m = 2)$				1		1				$2 = 2!$
$(m = 3)$			1		4		1			$6 = 3!$
$(m = 4)$		1		11		11		1		$24 = 4!$
$(m = 5)$	1		26		66		26		1	$120 = 5!$

These results suggest that for a fixed $m \in \mathbf{Z}^+$, $\sum_{k=0}^{m-1} a_{m,k} = m!$, the number of permutations of m objects taken m at a time. We see that the result is true for $1 \leq m \leq 5$. Assuming the result true for some fixed m (≥ 1), upon using the recursive definition at (*), we find that

$$\begin{aligned} \sum_{k=0}^{m} a_{m+1,k} &= \sum_{k=0}^{m} [(m+1-k)a_{m,k-1} + (k+1)a_{m,k}] \\ &= [(m+1)a_{m,-1} + a_{m,0}] + [ma_{m,0} + 2a_{m,1}] + [(m-1)a_{m,1} + 3a_{m,2}] + \cdots \\ &\quad + [3a_{m,m-3} + (m-1)a_{m,m-2}] + [2a_{m,m-2} + ma_{m,m-1}] \\ &\quad + [a_{m,m-1} + (m+1)a_{m,m}]. \end{aligned}$$

Since $a_{m,-1} = 0 = a_{m,m}$ we can write

$$\begin{aligned}\sum_{k=0}^{m} a_{m+1,k} &= [a_{m,0} + ma_{m,0}] + [2a_{m,1} + (m-1)a_{m,1}] + \cdots \\ &\quad + [(m-1)a_{m,m-2} + 2a_{m,m-2}] + [ma_{m,m-1} + a_{m,m-1}] \\ &= (m+1)\sum_{k=0}^{m-1} a_{m,k} = (m+1)m! = (m+1)!\end{aligned}$$

Consequently, the result is true for all $m \geq 1$ — by the Principle of Mathematical Induction. (We'll see the Eulerian numbers again in Section 9.2.)

In closing this section we shall introduce the idea of a *recursively defined set* X. Here we start with an initial collection of elements that are in X — and this provides the base of the recursion. Then we provide a rule or list of rules that tell us how to find new elements in X from other elements already known to be in X. This rule (or list of rules) constitutes the recursive process. But now (and this part is new) we are also given an *implicit* restriction — that is, a statement to the effect that no element can be found in the set X except for those that were given in the initial collection or those that were formed using the prescribed rule(s) provided in the recursive process.

We demonstrate the ideas given here in the following example.

EXAMPLE 4.22

Define the set X recursively by

1) $1 \in X$; and

2) For each $a \in X$, $a + 2 \in X$.

Then we claim that X consists (precisely) of all positive odd integers.

Proof: If we let Y denote the set of all positive odd integers — that is, $Y = \{2n + 1 | n \in \mathbf{N}\}$ — then we want to show that $Y = X$. This means, as we learned in Section 3.1, that we must verify both $Y \subseteq X$ and $X \subseteq Y$.

In order to establish that $Y \subseteq X$, we must prove that every positive odd integer is in X. This will be accomplished through the Principle of Mathematical Induction. We start by considering the open statement

$$S(n): \quad 2n + 1 \in X,$$

which is defined for the universe $\mathbf{N}$. The basis step — that is, $S(0)$ — is true here because $1 = 2(0) + 1 \in X$ by part (1) of the recursive definition of X. For the inductive step we assume the truth of $S(k)$ for some $k \geq 0$; this tells us $2k + 1$ is an element in X. With $2k + 1 \in X$ it then follows by part (2) of the recursive definition of X that $(2k + 1) + 2 = (2k + 2) + 1 = 2(k + 1) + 1 \in X$, so $S(k + 1)$ is also true. Consequently, $S(n)$ is true (by the Principle of Mathematical Induction) for all $n \in \mathbf{N}$ and we have $Y \subseteq X$.

For the proof of the opposite inclusion (namely, $X \subseteq Y$) we use the recursive definition of X. First we consider part (1) of the definition. Since $1\ (= 2 \cdot 0 + 1)$ is a positive odd integer, we have $1 \in Y$. To complete the proof, we must verify that any integer in X that results from part (2) of the recursive definition is also in Y. This is done by showing that $a + 2 \in Y$ whenever the element a in X is also an element in Y. For if $a \in Y$, then $a = 2r + 1$, where $r \in \mathbf{N}$ — this by the definition of a positive odd integer. Thus

$a + 2 = (2r + 1) + 2 = (2r + 2) + 1 = 2(r + 1) + 1$, where $r + 1 \in \mathbf{N}$ (actually, $\mathbf{Z}^+$), and so $a + 2$ is a positive odd integer. This places $a + 2$ in Y and now shows that $X \subseteq Y$.

From the preceding two inclusions — that is, $Y \subseteq X$ and $X \subseteq Y$ — it follows that $X = Y$.

EXERCISES 4.2

1. The integer sequence $a_1, a_2, a_3, \ldots$, defined explicitly by the formula $a_n = 5n$ for $n \in \mathbf{Z}^+$, can also be defined recursively by

1) $a_1 = 5$; and

2) $a_{n+1} = a_n + 5$, for $n \geq 1$.

For the integer sequence $b_1, b_2, b_3, \ldots$, where $b_n = n(n + 2)$ for all $n \in \mathbf{Z}^+$, we can also provide the recursive definition:

1)′ $b_1 = 3$; and

2)′ $b_{n+1} = b_n + 2n + 3$, for $n \geq 1$.

Give a recursive definition for each of the following integer sequences $c_1, c_2, c_3, \ldots$, where for all $n \in \mathbf{Z}^+$ we have

a) $c_n = 7n$ **b)** $c_n = 7^n$

c) $c_n = 3n + 7$ **d)** $c_n = 7$

e) $c_n = n^2$ **f)** $c_n = 2 - (-1)^n$

2. a) Give a recursive definition for the disjunction of statements $p_1, p_2, \ldots, p_n, p_{n+1}, n \geq 1$.

b) Show that if $n, r \in \mathbf{Z}^+$, with $n \geq 3$ and $1 \leq r < n$, then

$$(p_1 \vee p_2 \vee \cdots \vee p_r) \vee (p_{r+1} \vee \cdots \vee p_n) \iff p_1 \vee p_2 \vee \cdots \vee p_r \vee p_{r+1} \vee \cdots \vee p_n.$$

3. Use the result of Example 4.16 to prove that if $p, q_1, q_2, \ldots, q_n$ are statements and $n \geq 2$, then

$$p \vee (q_1 \wedge q_2 \wedge \cdots \wedge q_n) \iff (p \vee q_1) \wedge (p \vee q_2) \wedge \cdots \wedge (p \vee q_n).$$

4. For $n \in \mathbf{Z}^+$, $n \geq 2$, prove that for any statements $p_1, p_2, \ldots, p_n$,

a) $\neg(p_1 \vee p_2 \vee \cdots \vee p_n) \iff \neg p_1 \wedge \neg p_2 \wedge \cdots \wedge \neg p_n$.

b) $\neg(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \iff \neg p_1 \vee \neg p_2 \vee \cdots \vee \neg p_n$.

5. a) Give a recursive definition for the intersection of the sets $A_1, A_2, \ldots, A_n, A_{n+1} \subseteq \mathcal{U}$, $n \geq 1$.

b) Use the result in part (a) to show that for all $n, r \in \mathbf{Z}^+$ with $n \geq 3$ and $1 \leq r < n$,

$$(A_1 \cap A_2 \cap \cdots \cap A_r) \cap (A_{r+1} \cap \cdots \cap A_n) = A_1 \cap A_2 \cap \cdots \cap A_r \cap A_{r+1} \cap \cdots \cap A_n.$$

6. For $n \geq 2$ and any sets $A_1, A_2, \ldots, A_n \subseteq \mathcal{U}$, prove that

$$\overline{A_1 \cup A_2 \cup \cdots \cup A_n} = \overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n}.$$

7. Use the result of Example 4.17 to show that if sets $A, B_1, B_2, \ldots, B_n \subseteq \mathcal{U}$ and $n \geq 2$, then

$$A \cap (B_1 \cup B_2 \cup \cdots \cup B_n) = (A \cap B_1) \cup (A \cap B_2) \cup \cdots \cup (A \cap B_n).$$

8. a) Develop a recursive definition for the addition of n real numbers $x_1, x_2, \ldots, x_n$, where $n \geq 2$.

b) For all real numbers x_1, x_2, and x_3, the associative law of addition states that $x_1 + (x_2 + x_3) = (x_1 + x_2) + x_3$. Prove that if $n, r \in \mathbf{Z}^+$, where $n \geq 3$ and $1 \leq r < n$, then

$$(x_1 + x_2 + \cdots + x_r) + (x_{r+1} + \cdots + x_n) = x_1 + x_2 + \cdots + x_r + x_{r+1} + \cdots + x_n.$$

9. a) Develop a recursive definition for the multiplication of n real numbers $x_1, x_2, \ldots, x_n$, where $n \geq 2$.

b) For all real numbers x_1, x_2, and x_3, the associative law of multiplication states that $x_1(x_2x_3) = (x_1x_2)x_3$. Prove that if $n, r \in \mathbf{Z}^+$, where $n \geq 3$ and $1 \leq r < n$, then

$$(x_1x_2 \cdots x_r)(x_{r+1} \cdots x_n) = x_1x_2 \cdots x_rx_{r+1} \cdots x_n.$$

10. For all $x \in \mathbf{R}$,

$$|x| = \sqrt{x^2} = \left\{ \begin{array}{ll} x, & \text{if } x \geq 0 \\ -x, & \text{if } x < 0 \end{array} \right\}, \quad \text{and}$$

$-|x| \leq x \leq |x|$. Consequently, $|x + y|^2 = (x + y)^2 = x^2 + 2xy + y^2 \leq x^2 + 2|x||y| + y^2 = |x|^2 + 2|x||y| + |y|^2 = (|x| + |y|)^2$, and $|x + y|^2 \leq (|x| + |y|)^2 \Rightarrow |x + y| \leq |x| + |y|$, for all $x, y \in \mathbf{R}$.

Prove that if $n \in \mathbf{Z}^+$, $n \geq 2$, and $x_1, x_2, \ldots, x_n \in \mathbf{R}$, then

$$|x_1 + x_2 + \cdots + x_n| \leq |x_1| + |x_2| + \cdots + |x_n|.$$

11. Define the integer sequence $a_0, a_1, a_2, a_3, \ldots$, recursively by

1) $a_0 = 1$, $a_1 = 1$, $a_2 = 1$; and

2) For $n \geq 3$, $a_n = a_{n-1} + a_{n-3}$.

Prove that $a_{n+2} \geq (\sqrt{2})^n$ for all $n \geq 0$.

12. For $n \geq 0$ let F_n denote the nth Fibonacci number. Prove that

$$F_0 + F_1 + F_2 + \cdots + F_n = \sum_{i=0}^{n} F_i = F_{n+2} - 1.$$

13. Prove that for any positive integer n,

$$\sum_{i=1}^{n} \frac{F_{i-1}}{2^i} = 1 - \frac{F_{n+2}}{2^n}.$$

14. As in Example 4.20 let $L_0, L_1, L_2, \ldots$ denote the Lucas numbers, where (1) $L_0 = 2$, $L_1 = 1$; and (2) $L_{n+2} = L_{n+1} + L_n$, for $n \geq 0$. When $n \geq 1$, prove that

$$L_1^2 + L_2^2 + L_3^2 + \cdots + L_n^2 = L_n L_{n+1} - 2.$$

15. If $n \in \mathbf{N}$, prove that $5F_{n+2} = L_{n+4} - L_n$.

16. Give a recursive definition for the set of all

a) positive even integers

b) nonnegative even integers

17. One of the most common uses for the recursive definition of sets is to define the *well-formed formulae* in various mathematical systems. For example, in the study of logic we can define the well-formed formulae as follows:

1) Each primitive statement p, the tautology T_0, and the contradiction F_0 are well-formed formulae; and

2) If p, q are well-formed formulae, then so are

i) $(\neg p)$ **ii)** $(p \vee q)$ **iii)** $(p \wedge q)$
iv) $(p \rightarrow q)$ **v)** $(p \leftrightarrow q)$

Using this recursive definition, we find that for the primitive statements p, q, r, the compound statement $((p \wedge (\neg q)) \rightarrow (r \vee T_0))$ is a well-formed formula. We can derive this well-formed formula as follows:

Steps	**Reasons**
1) p, q, r, T_0	Part (1) of the definition
2) $(\neg q)$	Step (1) and part (2i) of the definition
3) $(p \wedge (\neg q))$	Steps (1) and (2) and part (2iii) of the definition
4) $(r \vee T_0)$	Step (1) and part (2ii) of the definition
5) $((p \wedge (\neg q)) \rightarrow (r \vee T_0))$	Steps (3) and (4) and part (2iv) of the definition

For the primitive statements p, q, r, and s, provide derivations showing that each of the following is a well-formed formula.

a) $((p \vee q) \rightarrow (T_0 \wedge (\neg r)))$

b) $(((\neg p) \leftrightarrow q) \rightarrow (r \wedge (s \vee F_0)))$

18. Consider the permutations of 1, 2, 3, 4. The permutation 1432, for instance, is said to have one *ascent*—namely, 14 (since $1 < 4$). This same permutation also has two *descents*—namely, 43 (since $4 > 3$) and 32 (since $3 > 2$). The permutation 1423, on the other hand, has two ascents, at 14 and 23—and the one descent 42.

a) How many permutations of 1, 2, 3 have k ascents, for $k = 0, 1, 2$?

b) How many permutations of 1, 2, 3, 4 have k ascents, for $k = 0, 1, 2, 3$?

c) If a permutation of 1, 2, 3, 4, 5, 6, 7 has four ascents, how many descents does it have?

d) Suppose a permutation of $1, 2, 3, \ldots, m$ has k ascents, for $0 \leq k \leq m - 1$. How many descents does the permutation have?

e) Consider the permutation $p = 12436587$. This permutation of $1, 2, 3, \ldots, 8$ has four ascents. In how many of the nine locations (at the start, end, or between two numbers) in p can we place 9 so that the result is a permutation of $1, 2, 3, \ldots, 8, 9$ with (i) four ascents; (ii) five ascents?

f) Let $\pi_{m,k}$ denote the number of permutations of $1, 2, 3, \ldots, m$ with k ascents. Note how $\pi_{4,2} = 11 = 2(4) + 3(1) = (4 - 2)\pi_{3,1} + (2 + 1)\pi_{3,2}$. How is $\pi_{m,k}$ related to $\pi_{m-1,k-1}$ and $\pi_{m-1,k}$?

19. a) For $k \in \mathbf{Z}^+$ verify that $k^2 = \binom{k}{2} + \binom{k+1}{2}$.

b) Fix n in $\mathbf{Z}^+$. Since the result in part (a) is true for all $k = 1, 2, 3, \ldots, n$, summing the n equations

$$1^2 = \binom{1}{2} + \binom{2}{2}$$

$$2^2 = \binom{2}{2} + \binom{3}{2}$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$n^2 = \binom{n}{2} + \binom{n+1}{2}$$

we have $\sum_{k=1}^{n} k^2 = \sum_{k=1}^{n} \binom{k}{2} + \sum_{k=1}^{n} \binom{k+1}{2} = \binom{n+1}{3} + \binom{n+2}{3}$. [The last equality follows from Exercise 26 for Section 3.1 because $\sum_{k=1}^{n} \binom{k}{2} = \binom{1}{2} + \binom{2}{2} + \binom{3}{2} + \cdots + \binom{n}{2} = 0 + \binom{2}{0} + \binom{3}{1} + \cdots + \binom{n}{n-2} = \binom{n+1}{n-2} = \binom{n+1}{3}$ and $\sum_{k=1}^{n} \binom{k+1}{2} = \binom{2}{2} + \binom{3}{2} + \binom{4}{2} + \cdots + \binom{n+1}{2} = \binom{2}{0} + \binom{3}{1} + \binom{4}{2} + \cdots + \binom{n+1}{n-1} = \binom{n+2}{n-1} = \binom{n+2}{3}$. Show that

$$\binom{n+1}{3} + \binom{n+2}{3} = \frac{n(n+1)(2n+1)}{6}.$$

c) For $k \in \mathbf{Z}^+$ verify that $k^3 = \binom{k}{3} + 4\binom{k+1}{3} + \binom{k+2}{3}$.

d) Use part (c) and the results from Exercise 26 for Section 3.1 to show that

$$\sum_{k=1}^{n} k^3 = \binom{n+1}{4} + 4\binom{n+2}{4} + \binom{n+3}{4} = \frac{n^2(n+1)^2}{4}$$

e) Find $a, b, c, d \in \mathbf{Z}^+$ so that for any $k \in \mathbf{Z}^+$, $k^4 = a\binom{k}{4} + b\binom{k+1}{4} + c\binom{k+2}{4} + d\binom{k+3}{4}$.

20. a) For $n \geq 2$, if $p_1, p_2, p_3, \ldots, p_n, p_{n+1}$ are statements, prove that

$$[(p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge \cdots \wedge (p_n \rightarrow p_{n+1})]$$
$$\Rightarrow [(p_1 \wedge p_2 \wedge p_3 \wedge \cdots \wedge p_n) \rightarrow p_{n+1}].$$

b) Prove that Theorem 4.2 implies Theorem 4.1.

c) Use Theorem 4.1 to establish the following: If $\emptyset \neq S \subseteq \mathbf{Z}^+$, so that $n \in S$ for some $n \in \mathbf{Z}^+$, then S contains a least element.

d) Show that Theorem 4.1 implies Theorem 4.2.

4.3 The Division Algorithm: Prime Numbers

Although the set $\mathbf{Z}$ is not closed under nonzero division, in many instances one integer (exactly) divides another. For example, 2 divides 6 and 7 divides 21. Here the division is exact and there is no remainder. Thus 2 dividing 6 implies the existence of a quotient—namely, 3—such that $6 = 2 \cdot 3$. We formalize this idea as follows.

Definition 4.1 If $a, b \in \mathbf{Z}$ and $b \neq 0$, we say that *b divides a*, and we write $b|a$, if there is an integer n such that $a = bn$. When this occurs we say that b is a *divisor* of a, or a is a *multiple* of b.

With this definition we are able to speak of division inside of $\mathbf{Z}$ without going to $\mathbf{Q}$. Furthermore, when $ab = 0$ for $a, b \in \mathbf{Z}$, then either $a = 0$ or $b = 0$, and we say that $\mathbf{Z}$ has no *proper divisors of* 0. This property enables us to *cancel* as in $2x = 2y \Rightarrow x = y$, for $x, y \in \mathbf{Z}$, because $2x = 2y \Rightarrow 2(x - y) = 0 \Rightarrow 2 = 0$ or $x - y = 0 \Rightarrow x = y$. (Note that at no time did we mention multiplying both sides of the equation $2x = 2y$ by $\frac{1}{2}$. The number $\frac{1}{2}$ is outside the system $\mathbf{Z}$.)

We now summarize some properties of this division operation. Whenever we divide by an integer a, we assume that $a \neq 0$.

THEOREM 4.3 For all $a, b, c \in \mathbf{Z}$

a) $1|a$ and $a|0$.

b) $[(a|b) \wedge (b|a)] \Rightarrow a = \pm b$.

c) $[(a|b) \wedge (b|c)] \Rightarrow a|c$.

d) $a|b \Rightarrow a|bx$ for all $x \in \mathbf{Z}$.

e) If $x = y + z$, for some $x, y, z \in \mathbf{Z}$, and a divides two of the three integers x, y, and z, then a divides the remaining integer.

f) $[(a|b) \wedge (a|c)] \Rightarrow a|(bx + cy)$, for all $x, y \in \mathbf{Z}$. (The expression $bx + cy$ is called a *linear combination of* b, c.)

g) For $1 \leq i \leq n$, let $c_i \in \mathbf{Z}$. If a divides each c_i, then $a|(c_1x_1 + c_2x_2 + \cdots + c_nx_n)$, where $x_i \in \mathbf{Z}$ for all $1 \leq i \leq n$.

Proof: We prove part (f) and leave the remaining parts for the reader.

If $a|b$ and $a|c$, then $b = am$ and $c = an$, for some $m, n \in \mathbf{Z}$. So $bx + cy = (am)x + (an)y = a(mx + ny)$ (by the Associative Law of Multiplication and the Distributive Law of Multiplication over Addition—since the elements in $\mathbf{Z}$ satisfy both of these laws). Since $bx + cy = a(mx + ny)$, with $mx + ny \in \mathbf{Z}$, it follows that $a|(bx + cy)$.

We find part (g) of the theorem useful when we consider the following question.

EXAMPLE 4.23 Do there exist integers x, y, z (positive, negative, or zero) so that $6x + 9y + 15z = 107$? Suppose that such integers did exist. Then since $3|6$, $3|9$, and $3|15$, it would follow from part (g) of Theorem 4.3 that 3 is a divisor of $6x + 9y + 15z$ and, consequently, 3 is a divisor of 107—but this is not so. Hence there do not exist such integers x, y, z.

Several parts of Theorem 4.3 help us in the following

EXAMPLE 4.24

Let a, $b \in \mathbf{Z}$ so that $2a + 3b$ is a multiple of 17. (For example, we could have $a = 7$ and $b = 1$—and $a = 4$, $b = 3$ also works.) Prove that 17 divides $9a + 5b$.

Proof: We observe that $17|(2a + 3b) \Rightarrow 17|(-4)(2a + 3b)$, by part (d) of Theorem 4.3. Also, since $17|17$, it follows from part (f) of the theorem that $17|(17a + 17b)$. Hence, $17|[(17a + 17b) + (-4)(2a + 3b)]$, by part (e) of the theorem. Consequently, as $[(17a + 17b) + (-4)(2a + 3b)] = [(17 - 8)a + (17 - 12)b] = 9a + 5b$, we have $17|(9a + 5b)$.

Using this binary operation of integer division we find ourselves in the area of mathematics called *number theory*, which examines the properties of integers and other sets of numbers. Once considered an area of strictly pure (abstract) mathematics, number theory is now an essential applicable tool—especially, in dealing with computer and Internet security. But for now, as we continue to examine the set $\mathbf{Z}^+$ further, we notice that for all $n \in \mathbf{Z}^+$ where $n > 1$, the integer n has at least two positive divisors, namely, 1 and n itself. Some integers, such as 2, 3, 5, 7, 11, 13, and 17 have exactly two positive divisors. These integers are called *primes*. All other positive integers (greater than 1 and not prime) are called *composite*. An immediate connection between prime and composite integers is expressed in the following lemma.

LEMMA 4.1

If $n \in \mathbf{Z}^+$ and n is composite, then there is a prime p such that $p|n$.

Proof: If not, let S be the set of all composite integers that have no prime divisor(s). If $S \neq \emptyset$, then by the Well-Ordering Principle, S has a least element m. But if m is composite, then $m = m_1m_2$, where $m_1, m_2 \in \mathbf{Z}^+$ with $1 < m_1 < m$ and $1 < m_2 < m$. Since $m_1 \notin S$, m_1 is prime or divisible by a prime—so, there exists a prime p such that $p|m_1$. Since $m = m_1m_2$, it now follows from part (d) of Theorem 4.3 that $p|m$, and so $S = \emptyset$.

Now why did we call the preceding result a *lemma* instead of a theorem? After all, it had to be proved like all other theorems in the book so far. The reason is that although a lemma is itself a theorem, its major role is to help prove other theorems.

In listing the primes we are inclined to believe that there are infinitely many such numbers. We now verify that this is true.

THEOREM 4.4

(Euclid) There are infinitely many primes.

Proof: If not, let $p_1, p_2, \ldots, p_k$ be the finite list of all primes, and let $B = p_1p_2 \cdots p_k + 1$. Since $B > p_i$ for all $1 \leq i \leq k$, B cannot be a prime. Hence B is composite. So by Lemma 4.1 there is a prime p_j, where $1 \leq j \leq k$ and $p_j|B$. Since $p_j|B$ and $p_j|p_1p_2 \cdots p_k$, by Theorem 4.3(e) it follows that $p_j|1$. This contradiction arises from the assumption that there are only finitely many primes; the result follows.

Yes, this is the same Euclid from the fourth century B.C. whose *Elements*, written on 13 parchment scrolls, included the first organized coverage of the geometry we studied in high school. One finds, however, that these 13 books are also concerned with number theory. In particular, Books VII, VIII, and IX dwell on this topic. The preceding theorem (with proof) is found in Book IX.

We turn now to the major idea of this section. This result enables us to deal with nonzero division in **Z** when that division is not exact.

THEOREM 4.5

The Division Algorithm. If $a, b \in \mathbf{Z}$, with $b > 0$, then there exist unique $q, r \in \mathbf{Z}$ with $a = qb + r$, $0 \leq r < b$.

Proof: If $b|a$ the result follows with $r = 0$, so consider the case where $b \nmid a$ (that is, b does not divide a).

Let $S = \{a - tb | t \in \mathbf{Z}, a - tb > 0\}$. If $a > 0$ and $t = 0$, then $a \in S$ and $S \neq \emptyset$. For $a \leq 0$, let $t = a - 1$. Then $a - tb = a - (a - 1)b = a(1 - b) + b$, with $(1 - b) \leq 0$, because $b \geq 1$. So $a - tb > 0$ and $S \neq \emptyset$. Hence, for any $a \in \mathbf{Z}$, S is a nonempty subset of $\mathbf{Z}^+$. By the Well-Ordering Principle, S has a least element r, where $0 < r = a - qb$, for some $q \in \mathbf{Z}$. If $r = b$, then $a = (q + 1)b$ and $b|a$, contradicting $b \nmid a$. If $r > b$, then $r = b + c$, for some $c \in \mathbf{Z}^+$, and $a - qb = r = b + c \Rightarrow c = a - (q + 1)b \in S$, contradicting r being the least element of S. Hence, $r < b$.

This now establishes a quotient q and remainder r, where $0 \leq r < b$, for the theorem. But are there other q's and r's that also work? If so, let $q_1, q_2, r_1, r_2 \in \mathbf{Z}$ with $a = q_1 b + r_1$, for $0 \leq r_1 < b$, and $a = q_2 b + r_2$, for $0 \leq r_2 < b$. Then $q_1 b + r_1 = q_2 b + r_2 \Rightarrow b|q_1 - q_2| = |r_2 - r_1| < b$, because $0 \leq r_1, r_2 < b$. If $q_1 \neq q_2$, we have the contradiction $b|q_1 - q_2| < b$. Hence $q_1 = q_2$, $r_1 = r_2$, and the quotient and remainder are unique.

As we mentioned in the preceding proof, when $a, b \in \mathbf{Z}$ with $b > 0$, then there exists a unique *quotient* q and a unique *remainder* r where $a = qb + r$, with $0 \leq r < b$. Furthermore, under these circumstances, the integer b is called the *divisor* while a is termed the *dividend.*

EXAMPLE 4.25

a) When $a = 170$ and $b = 11$ in the division algorithm, we find that $170 = 15 \cdot 11 + 5$, where $0 \leq 5 < 11$. So when 170 is divided by 11, the quotient is 15 and the remainder is 5.

b) If the dividend is 98 and the divisor is 7, then we find that $98 = 14 \cdot 7$. So in this case the quotient is 14 and the remainder is 0, and 7 (exactly) divides 98.

c) For the case of $a = -45$ and $b = 8$ we have $-45 = (-6)8 + 3$, where $0 \leq 3 < 8$. Consequently, the quotient is -6 and the remainder is 3 when the dividend is -45 and the divisor is 8.

d) Let $a, b \in \mathbf{Z}^+$.

  1) If $a = qb$ for some $q \in \mathbf{Z}^+$, then $-a = (-q)b$. So, in this case, when $-a$ (< 0) is divided by b (> 0) the quotient is $-q$ (< 0) and the remainder is 0.

  2) If $a = qb + r$ for some $q \in \mathbf{N}$ and $0 < r < b$, then $-a = (-q)b - r = (-q)b - b + b - r = (-q - 1)b + (b - r)$. For this case, when $-a$ (< 0) is divided by b (> 0) the quotient is $-q - 1$ (< 0) and the remainder is $b - r$, where $0 < b - r < b$.

Despite the proof of Theorem 4.5 and the results in Example 4.25, we really do *not* have any systematic way to calculate the quotient q and remainder r when we divide an integer a (the dividend) by the positive integer b (the divisor). The proof of Theorem 4.5 guarantees the existence of such integers q and r, but the proof is *not* constructive. It does not appear to tell us how to actually calculate q and r, and it does not mention anything about the ability to use multiplication tables or perform long division. To remedy this situation we provide the procedure (written in pseudocode) in Fig. 4.10. Our next example illustrates the idea presented in part of this procedure.

```
procedure IntegerDivision (a, b: integers)
begin
  if $a = 0$ then
    begin
      quotient := 0
      remainder := 0
    end
  else
    begin
      r := abs(a) {the absolute value of a}
      q := 0
      while $r \geq b$ do
        begin
          r := r - b
          q := q + 1
        end
      if $a > 0$ then
        begin
          quotient := q
          remainder := r
        end
      else if $r = 0$ then
        begin
          quotient := -q
          remainder := 0
        end
      else
        begin
          quotient := -q - 1
          remainder := b - r
        end
    end
end
```

Figure 4.10

EXAMPLE 4.26

Just as the multiplication of positive integers may be viewed as repeated addition, so too can we view (integer) division as repeated subtraction. We see that subtraction does play a role in the definition of the set S in the proof of Theorem 4.5.

When calculating $4 \cdot 7$, for example, we can think in terms of repeated addition and write

$$2 \cdot 7 = 7 + 7 = 14$$

$$3 \cdot 7 = (2 + 1) \cdot 7 = 2 \cdot 7 + 1 \cdot 7 = (7 + 7) + 7 = 14 + 7 = 21$$

$$4 \cdot 7 = (3 + 1) \cdot 7 = 3 \cdot 7 + 1 \cdot 7 = ((7 + 7) + 7) + 7 = 21 + 7 = 28.$$

If, on the other hand, we wish to divide 37 by 8, then we should think of the quotient q as the number of 8's contained in 37. When each one of these 8's is removed (that is, subtracted) and no other 8 can be removed without giving us a negative result, then the integer that is left (remaining) is the remainder r. So we can calculate q and r by thinking in terms of repeated subtraction as follows:

$$\begin{aligned} 37-8&=29\geq 8,\\ 29-8=(37-8)-8&=37-2\cdot 8=21\geq 8,\\ 21-8=((37-8)-8)-8&=37-3\cdot 8=13\geq 8,\\ 13-8=(((37-8)-8)-8)-8&=37-4\cdot 8=5<8. \end{aligned}$$

The last line shows that four 8's can be subtracted from 37 before we obtain a nonnegative result — namely, 5 — that is smaller than 8. Therefore, in this example we have $q=4$ and $r=5$.

Using the division algorithm, we consider some results on representing integers in bases other than 10.

EXAMPLE 4.27

Write 6137 in the octal system (base 8). Here we seek nonnegative integers $r_0, r_1, r_2, \ldots, r_k$, with $0<r_k<8$, such that $6137=(r_k\cdots r_2r_1r_0)_8$.

With $6137=r_0+r_1\cdot 8+r_2\cdot 8^2+\cdots+r_k\cdot 8^k=r_0+8(r_1+r_2\cdot 8+\cdots+r_k\cdot 8^{k-1})$, r_0 is the remainder obtained in the division algorithm when 6137 is divided by 8.

Consequently, since $6137=1+8\cdot 767$, we have $r_0=1$ and $767=r_1+r_2\cdot 8+\cdots+r_k\cdot 8^{k-1}=r_1+8(r_2+r_3\cdot 8+\cdots+r_k\cdot 8^{k-2})$. This yields $r_1=7$ (the remainder when 767 is divided by 8) and $95=r_2+r_3\cdot 8+\cdots+r_k\cdot 8^{k-2}$. Continuing in this manner, we find $r_2=7$, $r_3=3$, $r_4=1$, and $r_i=0$ for all $i\geq 5$, so

$$6137=1\cdot 8^4+3\cdot 8^3+7\cdot 8^2+7\cdot 8+1=(13771)_8.$$

We can arrange the successive divisions by 8 as follows:

	Remainders
$8\,\lfloor\underline{6137}$	
$8\,\lfloor\underline{767}$	$1(r_0)$
$8\,\lfloor\underline{95}$	$7(r_1)$
$8\,\lfloor\underline{11}$	$7(r_2)$
$8\,\lfloor\underline{1}$	$3(r_3)$
0	$1(r_4)$

EXAMPLE 4.28

In the field of computer science, the binary number system (base 2) is very important. Here the only symbols that one may use are the bits 0 and 1. In Table 4.3 we have listed the binary representations of the (base-10) integers from 0 to 15. Here we have included leading zeros and find that we need four bits because of the leading 1 in the representations for the integers from 8 to 15. With five bits we can continue up to 31 ($=32-1=2^5-1$); six bits are necessary to proceed to 63 ($=64-1=2^6-1$). In general, if $x\in\mathbf{Z}$ and $0\leq x<2^n$, for $n\in\mathbf{Z}^+$, then we can write x in base 2 by using n bits. Leading zeros appear when $0\leq x\leq 2^{n-1}-1$, and for $2^{n-1}\leq x\leq 2^n-1$ the first (most significant) bit is 1.

Information is generally stored in machines in units of eight bits called bytes, so for machines with memory cells of one byte we can store in a single cell any one of the binary

Table 4.3

Base 10	Base 2	Base 10	Base 2
0	0 0 0 0	8	1 0 0 0
1	0 0 0 1	9	1 0 0 1
2	0 0 1 0	10	1 0 1 0
3	0 0 1 1	11	1 0 1 1
4	0 1 0 0	12	1 1 0 0
5	0 1 0 1	13	1 1 0 1
6	0 1 1 0	14	1 1 1 0
7	0 1 1 1	15	1 1 1 1

equivalents of the integers from 0 to $2^8 - 1 = 255$. For a machine with two-byte cells, any one of the integers from 0 to $2^{16} - 1 = 65{,}535$ can be stored in binary form in each cell. A machine with four-byte cells would take us up to $2^{32} - 1 = 4{,}294{,}967{,}295$.

When a human deals with long sequences of 0's and 1's, the job soon becomes very tedious and the chance for error increases with the tedium. Consequently, it is common (especially in the study of machine and assembly languages) to represent such long sequences of bits in another notation. One such notation is the *hexadecimal* (*base*-16) *notation*. Here there are 16 symbols, and because we have only 10 symbols in the standard base-10 system, we introduce the following six additional symbols:

A	(Alfa)	C	(Charlie)	E	(Echo)
B	(Bravo)	D	(Delta)	F	(Foxtrot)

In Table 4.4 the integers from 0 to 15 are given in terms of both the binary and the hexadecimal number systems.

Table 4.4

Base 10	Base 2	Base 16	Base 10	Base 2	Base 16
0	0 0 0 0	0	8	1 0 0 0	8
1	0 0 0 1	1	9	1 0 0 1	9
2	0 0 1 0	2	10	1 0 1 0	A
3	0 0 1 1	3	11	1 0 1 1	B
4	0 1 0 0	4	12	1 1 0 0	C
5	0 1 0 1	5	13	1 1 0 1	D
6	0 1 1 0	6	14	1 1 1 0	E
7	0 1 1 1	7	15	1 1 1 1	F

To convert from base 10 to base 16, we follow a procedure like the one outlined in Example 4.27. Here we are interested in the remainders upon successive divisions by 16. Therefore, if we want to represent the (base-10) integer 13,874,945 in the hexadecimal system, we do the following calculations:

$$\begin{array}{rll}
 & \textbf{Remainders} & \\
16\,\underline{|13{,}874{,}945} & & \\
16\,\underline{|867{,}184} & 1 & (r_0) \\
16\,\underline{|54{,}199} & 0 & (r_1) \\
16\,\underline{|3{,}387} & 7 & (r_2) \\
16\,\underline{|211} & 11\,(=\mathrm{B}) & (r_3) \\
16\,\underline{|13} & 3 & (r_4) \\
0 & 13\,(=\mathrm{D}) & (r_5)
\end{array}$$

Consequently, 13,874,945 = $(\mathrm{D3B701})_{16}$.

There is, however, an easier approach for converting between base 2 and base 16. For example, if we want to convert the binary (one-byte) integer 01001101 to its base-16 counterpart, we break the number into blocks of four bits:

$$\underbrace{0100}_{4}\quad\underbrace{1101}_{\mathrm{D}}$$

We then convert each block of four bits to its base-16 representation (as shown in Table 4.4), and we have $(01001101)_2 = (4\mathrm{D})_{16}$. If we start with the (two-byte) number $(\mathrm{A13F})_{16}$ and want to convert in the other direction, we replace each hexadecimal symbol by its (four-bit) binary equivalent (also as shown in Table 4.4):

$$\overbrace{1010}^{\mathrm{A}}\quad\overbrace{0001}^{1}\quad\overbrace{0011}^{3}\quad\overbrace{1111}^{\mathrm{F}}$$

This results in $(\mathrm{A13F})_{16} = (1010000100111111)_2$.

EXAMPLE 4.29

We need negative integers in order to perform the binary operation of subtraction in terms of addition [that is, $(a - b) = a + (-b)$]. When we are dealing with the binary representation of integers, we can use a popular method that enables us to perform addition, subtraction, multiplication, and (integer) division: the *two's complement method*. The method's popularity rests on its implementation by only two electronic circuits — one to invert and the second to add.

In Table 4.5 the integers from -8 to 7 are represented by the four-bit patterns shown. The nonnegative integers are represented as they were in Tables 4.3 and 4.4. To obtain the results for $-8 \le n \le -1$, first consider the binary representation of $|n|$, the absolute value of n. Then do the following:

1) Replace each 0(1) in the binary representation of $|n|$ by 1(0); this result is called the *one's complement* of (the given representation of) $|n|$.
2) Add 1 (= 0001 in this case) to the result in step (1). This result is called the *two's complement* of n.

For example, to obtain the two's complement (representation) of -6, we proceed as follows.

6

1) Start with the binary representation of 6. ↓ 0110

2) Interchange the 0's and 1's; this result is the one's complement of 0110. ↓ 1001

3) Add 1 to the prior result. ↓ 1001 + 0001 = 1010

We can also obtain the four-bit patterns for the values $-8 \leq n \leq -1$ by using the four-bit patterns for the integers from 0 to 7 and complementing (interchanging 0's and 1's) these patterns as shown by four such pairs of patterns in Table 4.5. Note in Table 4.5 that the four-bit patterns for the nonnegative integers start with 0, whereas 1 is the first bit for the negative integers in the table.

Table 4.5

Two's Complement Notation				
Value Represented	**Four-Bit Pattern**			
7	0	1	1	1
6	0	1	1	0
5	0	1	0	1
4	0	1	0	0
3	0	0	1	1
2	0	0	1	0
1	0	0	0	1
0	0	0	0	0
−1	1	1	1	1
−2	1	1	1	0
−3	1	1	0	1
−4	1	1	0	0
−5	1	0	1	1
−6	1	0	1	0
−7	1	0	0	1
−8	1	0	0	0

EXAMPLE 4.30

How do we perform the subtraction $33 - 15$ in base 2, using the two's complement method with patterns of eight bits (= one byte)?

We want to determine $33 - 15 = 33 + (-15)$. We find that $33 = (00100001)_2$, and $15 = (00001111)_2$. Therefore we represent -15 by

$$11110000 + 00000001 = 11110001.$$

The addition of integers represented in two's complement notation is the same as ordinary binary addition, except that all results must have the same size bit patterns. This means that when two integers are added by the two's complement method, any extra bit that results on the left of the answer (by a final carry) must be discarded. We illustrate this in the following calculations.

$$\begin{array}{r} 33 \\ \underline{-\,15} \end{array} \longrightarrow \begin{array}{r} 00100001 \\ \underline{+\,11110001} \\ 1\underbrace{00010010}_{\text{Answer} = (00010010)_2 = 18} \end{array}$$

This bit is discarded.

This bit indicates that the answer is nonnegative.

To find $15 - 33$ we use $15 = (00001111)_2$ and $33 = (00100001)_2$. Then, to calculate $15 - 33$ as $15 + (-33)$, we represent -33 by $11011110 + 00000001 = 11011111$. This gives us the results

$$\begin{array}{r} 15 \\ \underline{-\,33} \end{array} \longrightarrow \begin{array}{r} 00001111 \\ \underline{+\,11011111} \\ 11101110 \end{array}$$

This bit indicates that the answer is negative.

In order to get the positive form of the answer, we proceed as follows:

	11101110
1) Take the one's complement.	↓ 00010001
2) Add 1 to the prior result.	↓ 00010010

Since $(00010010)_2 = 18$, the answer is -18.

One problem we have avoided in the two preceding calculations involves the size of the integers that we can represent by eight-bit patterns. No matter what size patterns we use, the size of the integers that can be represented is limited. When we exceed this size, an *overflow error* results. For example, if we are working with eight-bit patterns and try to add 117 and 88, we obtain

$$\begin{array}{r} 117 \\ \underline{+\;\;88} \end{array} \longrightarrow \begin{array}{r} 01110101 \\ \underline{+\,01011000} \\ 11001101 \end{array}$$

This bit indicates that the answer is negative.

This result shows how we can detect an overflow error when adding two numbers. Here an overflow error is indicated: The sum of the eight-bit patterns for two positive integers has resulted in the eight-bit pattern for a negative integer. Similarly, when the addition of (the eight-bit patterns of) two negative integers results in the eight-bit pattern of a positive integer, an overflow error is detected.

To see why the procedure in Example 4.30 works in general, let $x, y \in \mathbf{Z}^+$ with $x > y$. Let $2^{n-1} \leq x < 2^n$. Then the binary representation for x is made up of n bits (with the leading bit 1). The binary representation for 2^n consists of $n + 1$ bits: a leading bit 1 followed by n 0's. The binary representation for $2^n - 1$ consists of n 1's.

When we subtract y from $2^n - 1$, we have

$$(2^n - 1) - y = \underbrace{11\ldots1}_{n\text{ 1's}} - y, \text{ the one's complement of } y.$$

Then $(2^n - 1) - y + 1$ gives us the two's complement of $-y$, and

$$x - y = x + [(2^n - 1) - y + 1] - 2^n,$$

where the final term, -2^n, results in the removal of the extra bit that arises on the left of the answer.

We close this section with one final result on composite integers.

EXAMPLE 4.31

If $n \in \mathbf{Z}^+$ and n is composite, then there exists a prime p such that $p|n$ and $p \leq \sqrt{n}$.

Proof: Since n is composite, we can write $n = n_1 n_2$, where $1 < n_1 < n$ and $1 < n_2 < n$. We claim that one of the integers n_1, n_2 must be less than or equal to $\sqrt{n}$. If not, then $n_1 > \sqrt{n}$ and $n_2 > \sqrt{n}$ give us the contradiction $n = n_1 n_2 > (\sqrt{n})(\sqrt{n}) = n$. Without loss of generality, we shall assume that $n_1 \leq \sqrt{n}$. If n_1 is prime, the result follows. If n_1 is not prime, then by Lemma 4.1 there exists a prime $p < n_1$ where $p|n_1$. So $p|n$ and $p \leq \sqrt{n}$.

EXERCISES 4.3

1. Verify the remaining parts of Theorem 4.3.

2. Let $a, b, c, d \in \mathbf{Z}^+$. Prove that (a) $[(a|b) \wedge (c|d)] \Rightarrow ac|bd$; (b) $a|b \Rightarrow ac|bc$; and (c) $ac|bc \Rightarrow a|b$.

3. If p, q are primes, prove that $p|q$ if and only if $p = q$.

4. If $a, b, c \in \mathbf{Z}^+$ and $a|bc$, does it follow that $a|b$ or $a|c$?

5. For all integers a, b, and c, prove that if $a \nmid bc$, then $a \nmid b$ and $a \nmid c$.

6. Let $n \in \mathbf{Z}^+$ where $n \geq 2$. Prove that if $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n \in \mathbf{Z}^+$ and $a_i|b_i$ for all $1 \leq i \leq n$, then $(a_1 a_2 \cdots a_n)|(b_1 b_2 \cdots b_n)$.

7. a) Find three positive integers a, b, c such that $31|(5a + 7b + 11c)$.

b) If $a, b, c \in \mathbf{Z}$ and $31|(5a + 7b + 11c)$, prove that $31|(21a + 17b + 9c)$.

8. A grocery store runs a weekly contest to promote sales. Each customer who purchases more than \$20 worth of groceries receives a game card with 12 numbers on it; if any of these numbers sum to exactly 500, then that customer receives a \$500 shopping spree (at the grocery store). After purchasing \$22.83 worth of groceries at this store, Eleanor receives her game card on which are printed the following 12 numbers: 144, 336, 30, 66, 138, 162, 318, 54, 84, 288, 126, and 456. Has Eleanor won a \$500 shopping spree?

9. Let $a, b \in \mathbf{Z}^+$. If $b|a$ and $b|(a + 2)$, prove that $b = 1$ or $b = 2$.

10. If $n \in \mathbf{Z}^+$, and n is odd, prove that $8|(n^2 - 1)$.

11. If $a, b \in \mathbf{Z}^+$, and both are odd, prove $2|(a^2 + b^2)$ but $4 \nmid (a^2 + b^2)$.

12. Determine the quotient q and remainder r for each of the following, where a is the dividend and b is the divisor.

a) $a = 23, \quad b = 7$ **b)** $a = -115, \quad b = 12$

c) $a = 0, \quad b = 42$ **d)** $a = 434, \quad b = 31$

13. If $n \in \mathbf{N}$, prove that $3|(7^n - 4^n)$.

14. Write each of the following (base-10) integers in base 2, base 4, and base 8.

a) 137 **b)** 6243 **c)** 12,345

15. Write each of the following (base-10) integers in base 2 and base 16.

a) 22 **b)** 527 **c)** 1234 **d)** 6923

16. Convert each of the following hexadecimal numbers to base 2 and base 10.

a) A7 **b)** 4C2 **c)** 1C2B **d)** A2DFE

17. Convert each of the following binary numbers to base 10 and base 16.

a) 11001110 **b)** 00110001

c) 11110000 **d)** 01010111

18. For what base do we find that $251 + 445 = 1026$?

19. Find all $n \in \mathbf{Z}^+$ where n divides $5n + 18$.

20. Write each of the following integers in two's complement representation. Here the results are eight-bit patterns.

a) 15 **b)** -15 **c)** 100

d) -65 **e)** 127 **f)** -128

21. If a machine stores integers by the two's complement method, what are the largest and smallest integers that it can store if it uses bit patterns of (a) 4 bits? (b) 8 bits? (c) 16 bits? (d) 32 bits? (e) 2^n bits, $n \in \mathbf{Z}^+$?

22. In each of the following problems, we are using four-bit patterns for the two's complement representations of the integers from -8 to 7. Solve each problem (if possible), and then convert the results to base 10 to check your answers. Watch for any overflow errors.

a) $\begin{array}{r} 0101 \\ +\,0001 \\ \hline \end{array}$ **b)** $\begin{array}{r} 1101 \\ +\,1110 \\ \hline \end{array}$

c) $\begin{array}{r} 0111 \\ \underline{+\ 1000} \end{array}$ **d)** $\begin{array}{r} 1101 \\ \underline{+\ 1010} \end{array}$

23. If $a, x, y \in \mathbf{Z}$, and $a \neq 0$, prove that $ax = ay \Rightarrow x = y$.

24. Write a computer program (or develop an algorithm) to convert a positive integer in base 10 to base b, where $2 \leq b \leq 9$.

25. The Division Algorithm can be generalized as follows: For $a, b \in \mathbf{Z}$, $b \neq 0$, there exist unique $q, r \in \mathbf{Z}$ with $a = qb + r$, $0 \leq r < |b|$. Using Theorem 4.5, verify this generalized form of the algorithm for $b < 0$.

26. Write a computer program (or develop an algorithm) to convert a positive integer in base 10 to base 16.

27. For $n \in \mathbf{Z}^+$, write a computer program (or develop an algorithm) that lists all positive divisors of n.

28. Define the set $X \subseteq \mathbf{Z}^+$ recursively as follows:

1) $3 \in X$; and

2) If $a, b \in X$, then $a + b \in X$.

Prove that $X = \{3k | k \in \mathbf{Z}^+\}$, the set of all positive integers divisible by 3.

29. Let $n \in \mathbf{Z}^+$ with $n = r_k \cdot 10^k + \cdots + r_2 \cdot 10^2 + r_1 \cdot 10 + r_0$ (the base-10 representation of n). Prove that

a) $2|n$ if and only if $2|r_0$

b) $4|n$ if and only if $4|(r_1 \cdot 10 + r_0)$

c) $8|n$ if and only if $8|(r_2 \cdot 10^2 + r_1 \cdot 10 + r_0)$

State a general theorem suggested by these results.

4.4 The Greatest Common Divisor: The Euclidean Algorithm

Continuing with the division operation developed in Section 4.3, we turn our attention to the divisors of a pair of integers.

Definition 4.2 For $a, b \in \mathbf{Z}$, a positive integer c is said to be a *common divisor of a and b* if $c|a$ and $c|b$.

EXAMPLE 4.32 The common divisors of 42 and 70 are 1, 2, 7, and 14, and 14 is the *greatest* of the common divisors.

Definition 4.3 Let $a, b \in \mathbf{Z}$, where either $a \neq 0$ or $b \neq 0$. Then $c \in \mathbf{Z}^+$ is called a *greatest common divisor* of a, b if

a) $c|a$ and $c|b$ (that is, c is a common divisor of a, b), and

b) for any common divisor d of a and b, we have $d|c$.

The result in Example 4.32 satisfies these conditions. That is, 14 divides both 42 and 70, and any common divisor of 42 and 70 — namely, 1, 2, 7, and 14 — divides 14. However, this example deals with two small integers. What would we do with two integers each having 20 digits? We consider the following questions.

1) Given $a, b \in \mathbf{Z}$, where at least one of a, b is not 0, does a greatest common divisor of a and b always exist? If so, how does one find such an integer?

2) How many greatest common divisors can a pair of integers have?

In dealing with these questions, we concentrate on $a, b \in \mathbf{Z}^+$.

THEOREM 4.6 For all $a, b \in \mathbf{Z}^+$, there exists a unique $c \in \mathbf{Z}^+$ that is *the* greatest common divisor of a, b.

Proof: Given $a, b \in \mathbf{Z}^+$, let $S = \{as + bt | s, t \in \mathbf{Z}, as + bt > 0\}$. Since $S \neq \emptyset$, by the Well-Ordering Principle S has a least element c. We claim that c is a greatest common divisor of a, b.

Since $c \in S$, $c = ax + by$, for some $x, y \in \mathbf{Z}$. Consequently, if $d \in \mathbf{Z}$ and $d|a$ and $d|b$, then by Theorem 4.3(f) $d|(ax + by)$, so $d|c$.

If $c \nmid a$, we can use the division algorithm to write $a = qc + r$, with $q, r \in \mathbf{Z}^+$ and $0 < r < c$. Then $r = a - qc = a - q(ax + by) = (1 - qx)a + (-qy)b$, so $r \in S$, contradicting the choice of c as the least element of S. Consequently, $c|a$, and by a similar argument, $c|b$.

Hence all $a, b \in \mathbf{Z}^+$ have a greatest common divisor. If c_1, c_2 both satisfy the two conditions of Definition 4.3, then with c_1 as a greatest common divisor, and c_2 as a common divisor, it follows that $c_2|c_1$. Reversing roles, we find that $c_1|c_2$, and so we conclude from Theorem 4.3(b) that $c_1 = c_2$ because $c_1, c_2 \in \mathbf{Z}^+$.

We now know that for all $a, b \in \mathbf{Z}^+$, the greatest common divisor of a, b exists — and it is unique. This number will be denoted by $\gcd(a, b)$. Here $\gcd(a, b) = \gcd(b, a)$; and for each $a \in \mathbf{Z}$, if $a \neq 0$, then $\gcd(a, 0) = |a|$. Also when $a, b \in \mathbf{Z}^+$, we have $\gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b) = \gcd(a, b)$. Finally, $\gcd(0, 0)$ is not defined and is of no interest to us.

From Theorem 4.6 we see that not only does $\gcd(a, b)$ exist but that $\gcd(a, b)$ is also the *smallest positive integer* we can write as a *linear combination* of a and b. However, we must realize that if $a, b, c \in \mathbf{Z}^+$ and $c = ax + by$ for some $x, y \in \mathbf{Z}$, then we do *not* necessarily know that c is $\gcd(a, b)$ — unless we somehow also know that c is the smallest positive integer that can be written as such a linear combination of a and b.

Finally, integers a and b are called *relatively prime* when $\gcd(a, b) = 1$ — that is, when there exist $x, y \in \mathbf{Z}$ with $ax + by = 1$.

EXAMPLE 4.33

Since $\gcd(42, 70) = 14$, we can find $x, y \in \mathbf{Z}$ with $42x + 70y = 14$, or $3x + 5y = 1$. By inspection, $x = 2$, $y = -1$ is a solution; $3(2) + 5(-1) = 1$. But for $k \in \mathbf{Z}$, $1 = 3(2 - 5k) + 5(-1 + 3k)$, so $14 = 42(2 - 5k) + 70(-1 + 3k)$, and the solutions for x, y are not unique.

In general, if $\gcd(a, b) = d$, then $\gcd((a/d), (b/d)) = 1$. (Verify this!) If $(a/d)x_0 + (b/d)y_0 = 1$, then $1 = (a/d)(x_0 - (b/d)k) + (b/d)(y_0 + (a/d)k)$, for each $k \in \mathbf{Z}$. So $d = a(x_0 - (b/d)k) + b(y_0 + (a/d)k)$, yielding infinitely many solutions to $ax + by = d$.

The preceding example and the prior observations work well enough when a, b are fairly small. But how does one find $\gcd(a, b)$ for some arbitrary $a, b \in \mathbf{Z}^+$? If $a|b$, then $\gcd(a, b) = a$; and if $b|a$, then $\gcd(a, b) = b$ — otherwise, we turn to the following result, which we owe to Euclid.

THEOREM 4.7

Euclidean Algorithm. Let $a, b \in \mathbf{Z}^+$. Set $r_0 = a$ and $r_1 = b$ and apply the division algorithm n times as follows:

$$\begin{array}{ll}
r_0 = q_1 r_1 + r_2, & 0 < r_2 < r_1 \\
r_1 = q_2 r_2 + r_3, & 0 < r_3 < r_2 \\
r_2 = q_3 r_3 + r_4, & 0 < r_4 < r_3 \\
\cdots\cdots\cdots & \cdots\cdots \\
r_i = q_{i+1} r_{i+1} + r_{i+2}, & 0 < r_{i+2} < r_{i+1} \\
\cdots\cdots\cdots & \cdots\cdots \\
r_{n-2} = q_{n-1} r_{n-1} + r_n, & 0 < r_n < r_{n-1} \\
r_{n-1} = q_n r_n. &
\end{array}$$

Then r_n, the last nonzero remainder, equals $\gcd(a, b)$.

Proof: To verify that $r_n = \gcd(a, b)$, we establish the two conditions of Definition 4.3.

Start with the first division process listed (where $r_0 = a$ and $r_1 = b$). If $c|r_0$ and $c|r_1$, then as $r_0 = q_1r_1 + r_2$, it follows that $c|r_2$. Next $[(c|r_1) \wedge (c|r_2)] \Rightarrow c|r_3$, because $r_1 = q_2r_2 + r_3$. Continuing down through the division processes, we get to where $c|r_{n-2}$ and $c|r_{n-1}$. From the next-to-last equation, we conclude that $c|r_n$, and this verifies condition (b) of Definition 4.3.

To establish condition (a) we go in reverse order. From the last equation, $r_n|r_{n-1}$, and so $r_n|r_{n-2}$, because $r_{n-2} = q_{n-1}r_{n-1} + r_n$. Continuing up through the equations, we get to where $r_n|r_4$ and $r_n|r_3$, so $r_n|r_2$. Then $[(r_n|r_3) \wedge (r_n|r_2)] \Rightarrow r_n|r_1$ (that is, $r_n|b$), and finally $[(r_n|r_2) \wedge (r_n|r_1)] \Rightarrow r_n|r_0$, (that is, $r_n|a$). Hence $r_n = \gcd(a, b)$.

We have now used the word *algorithm* in describing the statements set forth in Theorems 4.5 and 4.7. This term will recur frequently throughout other chapters of this text, so it may be a good idea to consider just what it connotes.

First and foremost, an *algorithm* is a list of *precise* instructions designed to solve a particular *type* of problem — not just one special case. In general, we expect all of our algorithms to receive *input* and provide the needed result(s) as *output*. Also, an algorithm should provide the same result whenever we repeat the value(s) for the input. This happens when the list of instructions is such that each intermediate result that comes about from the execution of each instruction is unique, depending on only the (initial) input and on any results that may have been derived at any preceding instructions. In order to accomplish this any possible vagueness must be eliminated from the algorithm; the instructions must be described in a simple yet unambiguous manner, a manner that can be executed by a machine. Finally, our algorithms cannot go on indefinitely. They must terminate after the execution of a *finite* number of instructions.

In Theorem 4.7 we are confronted with the determination of the greatest common divisor of any two positive integers. Hence this algorithm receives the two positive integers a, b as its input and generates their greatest common divisor as the output.

The use of the word *algorithm* in Theorem 4.5 is based on tradition. As stated, it does not provide the precise instructions we need to determine the output we want. (We mentioned this fact prior to Example 4.26.) To eliminate this shortcoming of Theorem 4.5, however, we set forth the instructions in the pseudocode procedure of Fig. 4.10.

We now apply the Euclidean algorithm in the following five examples.

EXAMPLE 4.34

Find the greatest common divisor of 250 and 111, and express the result as a linear combination of these integers.

$$\begin{aligned} 250 &= 2(111) + 28, && 0 < 28 < 111 \\ 111 &= 3(28) + 27, && 0 < 27 < 28 \\ 28 &= 1(27) + 1, && 0 < 1 < 27 \\ 27 &= 27(1) + 0. \end{aligned}$$

So 1 is the last nonzero remainder. Therefore $\gcd(250, 111) = 1$, and 250 and 111 are relatively prime. Working backward from the third equation, we have $1 = 28 - 1(27) = 28 - 1[111 - 3(28)] = (-1)(111) + 4(28) = (-1)(111) + 4[250 - 2(111)] = 4(250) - 9(111) = 250(4) + 111(-9)$, a linear combination of 250 and 111.

This expression of 1 as a linear combination of 250 and 111 is not unique, for $1 = 250[4 - 111k] + 111[-9 + 250k]$, for any $k \in \mathbf{Z}$.

We also have

$$\gcd(-250, 111) = \gcd(250, -111) = \gcd(-250, -111) = \gcd(250, 111) = 1.$$

Our next example is somewhat more general, as it concerns the greatest common divisor for an infinite number of pairs of integers.

EXAMPLE 4.35

For any $n \in \mathbf{Z}^+$, prove that the integers $8n + 3$ and $5n + 2$ are relatively prime.

When $n = 1$ we find that $\gcd(8n + 3, 5n + 2) = \gcd(11, 7) = 1$.

For $n \geq 2$ we have $8n + 3 > 5n + 2$, and as in the previous example, we may write

$$\begin{aligned} 8n+3 &= 1(5n+2) + (3n+1), && 0 < 3n+1 < 5n+2 \\ 5n+2 &= 1(3n+1) + (2n+1), && 0 < 2n+1 < 3n+1 \\ 3n+1 &= 1(2n+1) + n, && 0 < n < 2n+1 \\ 2n+1 &= 2(n) + 1, && 0 < 1 < n \\ n &= n(1) + 0. \end{aligned}$$

Consequently, the last nonzero remainder is 1, so $\gcd(8n + 3, 5n + 2) = 1$ for all $n \geq 1$. But we could also have arrived at this conclusion if we had noticed that

$$(8n + 3)(-5) + (5n + 2)(8) = -15 + 16 = 1.$$

And since 1 is expressed as a linear combination of $8n + 3$ and $5n + 2$, and no *smaller* positive integer can have this property, it follows that the greatest common divisor of $8n + 3$ and $5n + 2$ is 1, for any positive integer n.

EXAMPLE 4.36

At this point we shall use the Euclidean algorithm to develop a procedure (in pseudocode) that will find $\gcd(a, b)$ for all $a, b \in \mathbf{Z}^+$. The procedure in Fig. 4.11 employs the binary operation **mod,** where for $x, y \in \mathbf{Z}^+$, x **mod** y = the remainder after x is divided by y. For example, 7 **mod** 3 is 1, and 18 **mod** 5 is 3. (We shall deal with "the arithmetic of remainders" in more detail in Chapter 14.)

```
procedure gcd(a, b: positive integers)
begin
  $r := a \bmod b$
  $d := b$
  while $r > 0$ do
    begin
      $c := d$
      $d := r$
      $r := c \bmod d$
    end
end {gcd(a, b) is d, the last nonzero remainder}
```

Figure 4.11

Meanwhile, if we call this procedure for $a = 168$ and $b = 456$, the procedure first assigns r the value 168 **mod** 456 = 168 and d the value 456. Since $r > 0$ the code in the **while** loop is executed (for the first time) and we obtain the following: $c = 456$, $d = 168$,

$r = 456 \textbf{ mod } 168 = 120$. We then find that the code in the **while** loop is executed three more times with the following results:

(2nd pass): $c = 168, d = 120, r = 168 \textbf{ mod } 120 = 48$

(3rd pass): $c = 120, d = 48, r = 120 \textbf{ mod } 48 = 24$

(4th pass): $c = 48, d = 24, r = 48 \textbf{ mod } 24 = 0.$

Since r is now 0, the procedure tells us that $\gcd(a, b) = \gcd(168, 456) = 24$, the final value of d (the last nonzero remainder).

EXAMPLE 4.37

Griffin has two unmarked containers. One container holds 17 ounces and the other holds 55 ounces. Explain how Griffin can use his two containers to measure exactly one ounce.

From the Euclidean algorithm we find that

$$55 = 3(17) + 4, \qquad 0 < 4 < 17$$
$$17 = 4(4) + 1, \qquad 0 < 1 < 4.$$

Therefore $1 = 17 - 4(4) = 17 - 4[55 - 3(17)] = 13(17) - 4(55)$. Consequently, Griffin must fill his smaller (17-ounce) container 13 times and empty the contents (for the first 12 times) into the larger container. (Griffin empties the larger container whenever it is full.) Before he fills the smaller container for the thirteenth time, Griffin has $12(17) - 3(55) = 204 - 165 = 39$ ounces of water in the larger (55-ounce) container. After he fills the smaller container for the thirteenth time, he will empty 16 ($= 55 - 39$) ounces from this container, filling the larger container. Exactly one ounce will be left in the smaller container.

EXAMPLE 4.38

Assisting students in programming classes, Brian finds that on the average he can help a student debug a Java program in six minutes, but it takes 10 minutes to debug a program written in C++. If he works continuously for 104 minutes and doesn't waste any time, how many programs can he debug in each language?

Here we seek integers $x, y \geq 0$, where $6x + 10y = 104$, or $3x + 5y = 52$. As $\gcd(3, 5) = 1$, we can write $1 = 3(2) + 5(-1)$, so $52 = 3(104) + 5(-52) = 3(104 - 5k) + 5(-52 + 3k)$, $k \in \mathbf{Z}$. In order to obtain $0 \leq x = 104 - 5k$ and $0 \leq y = -52 + 3k$, we must have $(52/3) \leq k \leq (104/5)$. So $k = 18, 19, 20$ and there are three possible solutions:

a) $(k = 18)$: $x = 14, \quad y = 2$ **b)** $(k = 19)$: $x = 9, \quad y = 5$

c) $(k = 20)$: $x = 4, \quad y = 8$

The equation in Example 4.38 is an example of a *Diophantine equation*: a linear equation requiring integer solutions. This type of equation was first investigated by the Greek algebraist Diophantus, who lived in the third century A.D.

Having solved one such equation, we seek to discover when a Diophantine equation has a solution. The proof is left to the reader.

THEOREM 4.8

If $a, b, c \in \mathbf{Z}^+$, the Diophantine equation $ax + by = c$ has an integer solution $x = x_0, y = y_0$ if and only if $\gcd(a, b)$ divides c.

We close this section with a concept that is related to the greatest common divisor.

Definition 4.4 For $a, b, c \in \mathbf{Z}^+$, c is called a *common multiple* of a, b if c is a multiple of both a and b. Furthermore, c is the *least common multiple* of a, b if it is the smallest of all positive integers that are common multiples of a, b. We denote c by $\text{lcm}(a, b)$.

If $a, b \in \mathbf{Z}^+$, then the product ab is a common multiple of both a and b. Consequently, the set of all (positive) common multiples of a, b is nonempty. So it follows from the Well-Ordering Principle that the $\text{lcm}(a, b)$ does exist.

EXAMPLE 4.39

a) Since $12 = 3 \cdot 4$ and no other smaller positive integer is a multiple of both 3 and 4, we have $\text{lcm}(3, 4) = 12 = \text{lcm}(4, 3)$. However, $\text{lcm}(6, 15) \neq 90$ — for although 90 is a multiple of both 6 and 15, there is a smaller multiple, namely, 30. And since no other common multiple of 6 and 15 is smaller than 30, it follows that $\text{lcm}(6, 15) = 30$.

b) For all $n \in \mathbf{Z}^+$, we find that $\text{lcm}(1, n) = \text{lcm}(n, 1) = n$.

c) When $a, n \in \mathbf{Z}^+$, we have $\text{lcm}(a, na) = na$. [This statement is a generalization of part (b). The earlier statement follows from this one when $a = 1$.]

d) If $a, m, n \in \mathbf{Z}^+$ with $m \leq n$, then $\text{lcm}(a^m, a^n) = a^n$. [And $\gcd(a^m, a^n) = a^m$.]

THEOREM 4.9 Let $a, b, c \in \mathbf{Z}^+$, with $c = \text{lcm}(a, b)$. If d is a common multiple of a and b, then $c|d$.

Proof: If not, then because of the division algorithm we can write $d = qc + r$, where $0 < r < c$. Since $c = \text{lcm}(a, b)$, it follows that $c = ma$ for some $m \in \mathbf{Z}^+$. Also, $d = na$ for some $n \in \mathbf{Z}^+$, because d is a multiple of a. Consequently, $na = qma + r \Rightarrow (n - qm)a = r > 0$, and r is a multiple of a. In a similar way r is seen to be a multiple of b, so r is a common multiple of a, b. But with $0 < r < c$, we contradict the claim that c is the least common multiple of a, b. Hence $c|d$.

Our last result for this section ties together the concepts of the greatest common divisor and the least common multiple. Furthermore, it provides us with a way to calculate $\text{lcm}(a, b)$ for all $a, b \in \mathbf{Z}^+$. The proof of this result is left to the reader.

THEOREM 4.10 For all $a, b \in \mathbf{Z}^+$, $ab = \text{lcm}(a, b) \cdot \gcd(a, b)$.

EXAMPLE 4.40

By virtue of Theorem 4.10 we have the following:

a) For all $a, b \in \mathbf{Z}^+$, if a, b are relatively prime, then $\text{lcm}(a, b) = ab$.

b) The computations in Example 4.36 establish the fact that $\gcd(168, 456) = 24$. As a result we find that

$$\text{lcm}(168, 456) = \frac{(168)(456)}{24} = 3{,}192.$$

EXERCISES 4.4

1. For each of the following pairs $a, b \in \mathbf{Z}^+$, determine $\gcd(a, b)$ and express it as a linear combination of a, b.

a) 231, 1820 b) 1369, 2597 c) 2689, 4001

2. For $a, b \in \mathbf{Z}^+$ and $s, t \in \mathbf{Z}$, what can we say about $\gcd(a, b)$ if

a) $as + bt = 2$? b) $as + bt = 3$?

c) $as + bt = 4$? d) $as + bt = 6$?

3. For $a, b \in \mathbf{Z}^+$ and $d = \gcd(a, b)$, prove that

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

4. For $a, b, n \in \mathbf{Z}^+$, prove that $\gcd(na, nb) = n \gcd(a, b)$.

5. Let $a, b, c \in \mathbf{Z}^+$ with $c = \gcd(a, b)$. Prove that c^2 divides ab.

6. Let $n \in \mathbf{Z}^+$.

a) Prove that $\gcd(n, n+2) = 1$ or 2.

b) What possible values can $\gcd(n, n+3)$ have? What about $\gcd(n, n+4)$?

c) If $k \in \mathbf{Z}^+$, what can we say about $\gcd(n, n+k)$?

7. For $a, b, c, d \in \mathbf{Z}^+$, prove that if $d = a + bc$, then

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

8. Let $a, b, c \in \mathbf{Z}^+$ with $\gcd(a, b) = 1$. If $a|c$ and $b|c$, prove that $ab|c$. Does the result hold if $\gcd(a, b) \neq 1$?

9. Let $a, b \in \mathbf{Z}$, where at least one of a, b is nonzero.

a) Using quantifiers, restate the definition for $c = \gcd(a, b)$, where $c \in \mathbf{Z}^+$.

b) Use the result in part (a) in order to decide when $c \neq \gcd(a, b)$ for some $c \in \mathbf{Z}^+$.

10. If a, b are relatively prime and $a > b$, prove that $\gcd(a - b, a + b) = 1$ or 2.

11. Let $a, b, c \in \mathbf{Z}^+$ with $\gcd(a, b) = 1$. If $a|bc$, prove that $a|c$.

12. Let $a, b \in \mathbf{Z}^+$ where $a \geq b$. Prove that $\gcd(a, b) = \gcd(a - b, b)$.

13. Prove that for any $n \in \mathbf{Z}^+$, $\gcd(5n + 3, 7n + 4) = 1$.

14. An executive buys \$2490 worth of presents for the children of her employees. For each girl she gets an art kit costing \$33; each boy receives a set of tools costing \$29. How many presents of each type did she buy?

15. After a weekend at the Mohegan Sun Casino, Gary finds that he has won \$1020—in \$20 and \$50 chips. If he has more \$50 chips than \$20 chips, how many chips of each denomination could he possibly have?

16. Let $a, b \in \mathbf{Z}^+$. Prove that there exist $c, d \in \mathbf{Z}^+$ such that $cd = a$ and $\gcd(c, d) = b$ if and only if $b^2|a$.

17. Determine those values of $c \in \mathbf{Z}^+$, $10 < c < 20$, for which the Diophantine equation $84x + 990y = c$ has no solution. Determine the solutions for the remaining values of c.

18. Verify Theorems 4.8 and 4.10.

19. If $a, b \in \mathbf{Z}^+$ with $a = 630$, $\gcd(a, b) = 105$, and $\operatorname{lcm}(a, b) = 242, 550$, what is b?

20. For each pair a, b in Exercise 1, find $\operatorname{lcm}(a, b)$.

21. For each $n \in \mathbf{Z}^+$, what are $\gcd(n, n+1)$ and $\operatorname{lcm}(n, n+1)$?

22. Prove that $\operatorname{lcm}(na, nb) = n \operatorname{lcm}(a, b)$ for all $n, a, b \in \mathbf{Z}^+$.

4.5 The Fundamental Theorem of Arithmetic

In this section we extend Lemma 4.1 and show that for each $n \in \mathbf{Z}^+$, $n > 1$, either n is prime or n can be written as a product of primes, where the representation is unique up to order. This result, known as the *Fundamental Theorem of Arithmetic*, can be found in an equivalent form in Book IX of Euclid's *Elements*.

The following two lemmas will help us accomplish our goal.

LEMMA 4.2 If $a, b \in \mathbf{Z}^+$ and p is prime, then $p|ab \Rightarrow p|a$ or $p|b$.

Proof: If $p|a$, then we are finished. If not, then because p is prime, it follows that $\gcd(p, a) = 1$, and so there exist integers x, y with $px + ay = 1$. Then $b = p(bx) + (ab)y$, where $p|p$ and $p|ab$. So it follows from parts (d) and (e) of Theorem 4.3 that $p|b$.

LEMMA 4.3 Let $a_i \in \mathbf{Z}^+$ for all $1 \leq i \leq n$. If p is prime and $p|a_1a_2 \cdots a_n$, then $p|a_i$ for some $1 \leq i \leq n$.

Proof: We leave the proof of this result to the reader.

Using Lemma 4.2 we now have another opportunity to establish a result by the method of proof by contradiction.

EXAMPLE 4.41

We want to show that $\sqrt{2}$ is irrational.

If not, we can write $\sqrt{2} = a/b$, where $a, b \in \mathbf{Z}^+$ and $\gcd(a, b) = 1$. Then $\sqrt{2} = a/b \Rightarrow 2 = a^2/b^2 \Rightarrow 2b^2 = a^2 \Rightarrow 2|a^2 \Rightarrow 2|a$. (Why?) Also, $2|a \Rightarrow a = 2c$ for some $c \in \mathbf{Z}^+$, so $2b^2 = a^2 = (2c)^2 = 4c^2$ and $b^2 = 2c^2$. But then $2|b^2 \Rightarrow 2|b$. Since 2 divides both a and b, it follows that $\gcd(a, b) \geq 2$—but this contradicts the earlier claim that $\gcd(a, b) = 1$. [*Note:* The preceding proof for the irrationality of $\sqrt{2}$ was known to Aristotle (384–322 B.C.) and is similar to that given in Book X of Euclid's *Elements*.]

Before we turn to the main result for this section, let us point out that the integer 2 in the preceding example is not that special. The reader will be asked to show in the Section Exercises that in fact $\sqrt{p}$ is irrational for every prime p. Now that we have mentioned this fact, it is time to present the Fundamental Theorem of Arithmetic.

THEOREM 4.11

Every integer $n > 1$ can be written as a product of primes uniquely, up to the order of the primes. (Here a single prime is considered a product of one factor.)

Proof: The proof consists of two parts: The first part covers the existence of a prime factorization, and the second part deals with its uniqueness.

If the first part is not true, let $m > 1$ be the smallest integer not expressible as a product of primes. Since m is not a prime, we are able to write $m = m_1m_2$, where $1 < m_1 < m$, $1 < m_2 < m$. But then m_1, m_2 can be written as products of primes, because they are less than m. Consequently, with $m = m_1m_2$ we can obtain a prime factorization of m.

In order to establish the uniqueness of a prime factorization, we shall use the alternative form of the Principle of Mathematical Induction (Theorem 4.2). For the integer 2, we have a unique prime factorization, and assuming uniqueness of representation for 3, 4, 5, $\ldots$, $n-1$, we suppose that $n = p_1^{s_1}p_2^{s_2}\cdots p_k^{s_k} = q_1^{t_1}q_2^{t_2}\cdots q_r^{t_r}$, where each p_i, $1 \leq i \leq k$, and each q_j, $1 \leq j \leq r$, is a prime. Also $p_1 < p_2 < \cdots < p_k$, and $q_1 < q_2 < \cdots < q_r$, and $s_i > 0$ for all $1 \leq i \leq k$, $t_j > 0$ for all $1 \leq j \leq r$.

Since $p_1|n$, we have $p_1|q_1^{t_1}q_2^{t_2}\cdots q_r^{t_r}$. By Lemma 4.3, $p_1|q_j$ for some $1 \leq j \leq r$. Because p_1 and q_j are primes, we have $p_1 = q_j$. In fact $j = 1$, for otherwise $q_1|n \Rightarrow q_1 = p_e$ for some $1 < e \leq k$ and $p_1 < p_e = q_1 < q_j = p_1$. With $p_1 = q_1$, we find that $n_1 = n/p_1 = p_1^{s_1-1}p_2^{s_2}\cdots p_k^{s_k} = q_1^{t_1-1}q_2^{t_2}\cdots q_r^{t_r}$. Since $n_1 < n$, by the induction hypothesis it follows that $k = r$, $p_i = q_i$ for $1 \leq i \leq k$, $s_1 - 1 = t_1 - 1$ (so $s_1 = t_1$), and $s_i = t_i$ for $2 \leq i \leq k$. Hence the prime factorization of n is unique.

This result is now used in the following five examples.

EXAMPLE 4.42

For the integer 980,220 we can determine the prime factorization as follows:

$$\begin{aligned} 980{,}220 &= 2^1(490{,}110) = 2^2(245{,}055) = 2^23^1(81{,}685) = 2^23^15^1(16{,}337)\\ &= 2^23^15^117^1(961) = 2^2\cdot 3\cdot 5\cdot 17\cdot 31^2 \end{aligned}$$

EXAMPLE 4.43

Suppose that $n \in \mathbf{Z}^+$ and that

$$(*)\qquad 10\cdot 9\cdot 8\cdot 7\cdot 6\cdot 5\cdot 4\cdot 3\cdot 2\cdot n = 21\cdot 20\cdot 19\cdot 18\cdot 17\cdot 16\cdot 15\cdot 14.$$

Since 17 is a prime factor of the integer on the right-hand side of Eq. (*) it must also be a factor for the left-hand side (by the uniqueness part of the Fundamental Theorem of

Arithmetic). But 17 does not divide any of the factors $10, 9, 8, \ldots, 3$ or 2, so it follows that $17|n$. (A similar argument shows us that $19|n$).

EXAMPLE 4.44

For $n \in \mathbf{Z}^+$, we want to count the number of positive divisors of n. For example, the number 2 has two positive divisors: 1 and itself. Likewise, 1 and 3 are the only positive divisors of 3. In the case of 4, we find the three positive divisors 1, 2, and 4.

To determine the result for each $n \in \mathbf{Z}^+$, $n > 1$, we use Theorem 4.11 and write $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, where for each $1 \leq i \leq k$, p_i is a prime and $e_i > 0$. If $m|n$, then $m = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$, where $0 \leq f_i \leq e_i$ for all $1 \leq i \leq k$. So by the rule of product, the number of positive divisors of n is

$$(e_1 + 1)(e_2 + 1) \cdots (e_k + 1).$$

For example, since $29{,}338{,}848{,}000 = 2^8 3^5 5^3 7^3 11$, we find that 29,338,848,000 has $(8+1)(5+1)(3+1)(3+1)(1+1) = (9)(6)(4)(4)(2) = 1728$ positive divisors.

Should we want to know how many of these 1728 divisors are multiples of $360 = 2^3 3^2 5$, then we must realize that we want to count the integers of the form $2^{t_1} 3^{t_2} 5^{t_3} 7^{t_4} 11^{t_5}$ where

$$3 \leq t_1 \leq 8, \qquad 2 \leq t_2 \leq 5, \qquad 1 \leq t_3 \leq 3, \qquad 0 \leq t_4 \leq 3, \qquad \text{and} \qquad 0 \leq t_5 \leq 1.$$

Consequently, the number of positive divisors of 29,338,848,000 that are divisible by 360 is

$$[(8-3)+1][(5-2)+1][(3-1)+1][(3-0)+1][(1-0)+1]$$
$$= (6)(4)(3)(4)(2) = 576.$$

To determine how many of the 1728 positive divisors of 29,338,848,000 are perfect squares, we need to consider all divisors of the form $2^{s_1} 3^{s_2} 5^{s_3} 7^{s_4} 11^{s_5}$, where each of s_1, s_2, s_3, s_4, s_5 is an even nonnegative integer. Consequently, here we have

5 choices for s_1 — namely, 0, 2, 4, 6, 8;

3 choices for s_2 — namely, 0, 2, 4;

2 choices for each of s_3, s_4 — namely, 0, 2; and

1 choice for s_5 — namely, 0.

It then follows that the number of positive divisors of 29,338,848,000 that are perfect squares is $(5)(3)(2)(2)(1) = 60$.

For our next example we shall need the multiplicative counterpart of the Sigma-notation (for addition) that we first observed in Section 1.3. Here we use the capital Greek letter Π for the Pi-notation.

We can use the Pi-notation to express the product $x_1 x_2 x_3 x_4 x_5 x_6$, for example, as $\prod_{i=1}^{6} x_i$. In general, one can express the product of the $n - m + 1$ terms $x_m, x_{m+1}, x_{m+2}, \ldots, x_n$, where $m, n \in \mathbf{Z}$ and $m \leq n$, as $\prod_{i=m}^{n} x_i$. As with the Sigma-notation the letter i is called the *index* of the product, and here this index accounts for all $n - m + 1$ integers starting with the *lower limit m* and continuing on up to (and including) the *upper limit n*.

This notation is demonstrated in the following:

1) $\prod_{i=3}^{7} x_i = x_3 x_4 x_5 x_6 x_7 = \prod_{j=3}^{7} x_j$, since there is nothing special about the letter i;

2) $\prod_{i=3}^{6} i = 3 \cdot 4 \cdot 5 \cdot 6 = 6!/2!$;

3) $\prod_{i=m}^{n} i = m(m+1)(m+2)\cdots(n-1)(n) = n!/(m-1)!$, for all $m, n \in \mathbf{Z}^+$ with $m \le n$; and

4) $\prod_{i=7}^{11} x_i = x_7x_8x_9x_{10}x_{11} = \prod_{j=0}^{4} x_{7+j} = \prod_{j=0}^{4} x_{11-j}$.

EXAMPLE 4.45

If $m, n \in \mathbf{Z}^+$, let $m = p_1^{e_1}p_2^{e_2}\cdots p_t^{e_t}$ and $n = p_1^{f_1}p_2^{f_2}\cdots p_t^{f_t}$, with each p_i prime and $0 \le e_i$ and $0 \le f_i$ for all $1 \le i \le t$. Then if $a_i = \min\{e_i, f_i\}$, the minimum (or smaller) of e_i and f_i, and $b_i = \max\{e_i, f_i\}$, the maximum (or larger) of e_i and f_i, for all $1 \le i \le t$, we have

$$\gcd(m, n) = p_1^{a_1}p_2^{a_2}\cdots p_t^{a_t} = \prod_{i=1}^{t} p_i^{a_i} \quad \text{and} \quad \operatorname{lcm}(m, n) = p_1^{b_1}p_2^{b_2}\cdots p_t^{b_t} = \prod_{i=1}^{t} p_i^{b_i}.$$

For example, let $m = 491{,}891{,}400 = 2^3 3^3 5^2 7^2 11^1 13^2$ and let $n = 1{,}138{,}845{,}708 = 2^2 3^2 7^1 11^2 13^3 17^1$. Then with $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, $p_6 = 13$, and $p_7 = 17$, we find $a_1 = 2$, $a_2 = 2$, $a_3 = 0$ (the exponent of 5 in the prime factorization of n must be 0, because 5 does not appear in the prime factorization), $a_4 = 1$, $a_5 = 1$, $a_6 = 2$, and $a_7 = 0$. So

$$\gcd(m, n) = 2^2 3^2 5^0 7^1 11^1 13^2 17^0 = 468{,}468.$$

We also have

$$\operatorname{lcm}(m, n) = 2^3 3^3 5^2 7^2 11^2 13^3 17^1 = 1{,}195{,}787{,}993{,}400.$$

Our final result for this section ties together the Fundamental Theorem of Arithmetic with the fact that any two consecutive integers are relatively prime (as observed in Exercise 21 for Section 4.4).

EXAMPLE 4.46

Here we seek an answer to the following question. Can we find three consecutive positive integers whose product is a perfect square—that is, do there exist $m, n \in \mathbf{Z}^+$ with $m(m+1)(m+2) = n^2$?

Suppose that such positive integers m, n do exist. We recall that $\gcd(m, m+1) = 1 = \gcd(m+1, m+2)$, so for any prime p, if $p|(m+1)$, then $p \nmid m$ and $p \nmid (m+2)$. Furthermore, if $p|(m+1)$, it follows that $p|n^2$. And since n^2 is a perfect square, by the Fundamental Theorem of Arithmetic, we find that the exponents on p in the prime factorizations of both $m+1$ and n^2 must be the same *even* integer. This is true for each prime divisor of $m+1$, so $m+1$ is a perfect square. With n^2 and $m+1$ both being perfect squares, we conclude that the product $m(m+2)$ is also a perfect square. However, the product $m(m+2)$ is such that $m^2 < m^2 + 2m = m(m+2) < m^2 + 2m + 1 = (m+1)^2$. Consequently, we find that $m(m+2)$ is wedged between two *consecutive* perfect squares—and is not equal to either of them. So $m(m+2)$ cannot be a perfect square, and there are no three consecutive positive integers whose product is a perfect square.

EXERCISES 4.5

1. Write each of the following integers as a product of primes $p_1^{n_1}p_2^{n_2}\cdots p_k^{n_k}$, where $0 < n_i$ for all $1 \le i \le k$ and $p_1 < p_2 < \cdots < p_k$.

a) 148,500 **b)** 7,114,800 **c)** 7,882,875

2. Determine the greatest common divisor and the least common multiple for each pair of integers in the preceding exercise.

3. Let $t \in \mathbf{Z}^+$ and $p_1, p_2, p_3, \ldots, p_t$ be distinct primes. If $m \in \mathbf{Z}^+$ has prime factorization $p_1^{e_1}p_2^{e_2}p_3^{e_3}\cdots p_t^{e_t}$, what is the prime factorization of (a) m^2? (b) m^3?

4. Verify Lemma 4.3.

5. Prove that $\sqrt{p}$ is irrational for any prime p.

6. The change machine at Cheryll's laundromat contains n quarters, $2n$ nickels, and $4n$ dimes, where $n \in \mathbf{Z}^+$. Find all values of n so that these coins total k dollars, where $k \in \mathbf{Z}^+$.

7. Find the number of positive divisors for each integer in Exercise 1.

8. a) How many positive divisors are there for

$$n = 2^{14}3^{9}5^{8}7^{10}11^{3}13^{5}37^{10}?$$

b) For the divisors in part (a), how many are

i) divisible by $2^{3}3^{4}5^{7}11^{2}37^{2}$?

ii) divisible by 1,166,400,000?

iii) perfect squares?

iv) perfect squares that are divisible by $2^{2}3^{4}5^{2}11^{2}$?

v) perfect cubes?

vi) perfect cubes that are multiples of $2^{10}3^{9}5^{2}7^{5}11^{2}13^{2}37^{2}$?

vii) perfect squares and perfect cubes?

9. Let $m, n \in \mathbf{Z}^{+}$ with $mn = 2^{4}3^{4}5^{3}7^{1}11^{3}13^{1}$. If $\operatorname{lcm}(m, n) = 2^{2}3^{3}5^{2}7^{1}11^{2}13^{1}$, what is $\gcd(m, n)$?

10. Extend the results in Example 4.45 and find the greatest common divisor and least common multiple for the three integers in Exercise 1.

11. How many positive integers n divide $100137n + 248396544$?

12. Let $a \in \mathbf{Z}^{+}$. Find the smallest value of a for which $2a$ is a perfect square and $3a$ is a perfect cube.

13. a) Let $a \in \mathbf{Z}^{+}$. Prove or disprove: (i) If $10|a^2$, then $10|a$; and (ii) If $4|a^2$, then $4|a$.

b) Generalize the true result(s) in part (a).

14. Let $a, b, c \in \{0, 1, 2, \dots, 9\}$ with at least one of a, b, c nonzero. Prove that the six-digit integer $abcabc$ is divisible by at least three distinct primes.

15. Determine the smallest perfect square that is divisible by 7!

16. For all $n \in \mathbf{Z}^{+}$, prove that n is a perfect square if and only if n has an odd number of positive divisors.

17. Find the smallest positive integer n for which the product $1260 \times n$ is a perfect cube.

18. Two hundred coins numbered 1 to 200 are put in a row across the top of a cafeteria table. Two hundred students are assigned numbers (from 1 to 200) and are asked to turn over certain coins. The student assigned number 1 is supposed to turn over all the coins. The student assigned number 2 is supposed to turn over every other coin, starting with the second coin. In general, the student assigned the number n, for each $1 \le n \le 200$, is supposed to turn over every nth coin, starting with the nth coin.

a) How many times will the 200th coin be turned over?

b) Will any other coin(s) be turned over as many times as the 200th coin?

c) Will any coin be turned over more times than the 200th coin?

19. How many different products can one obtain by multiplying any two (distinct) integers in the set

a) $\{4, 8, 16, 32\}$? **b)** $\{4, 8, 16, 32, 64\}$?

c) $\{4, 8, 9, 16, 27, 32, 64, 81, 243\}$?

d) $\{4, 8, 9, 16, 25, 27, 32, 64, 81, 125, 243, 625, 729, 3125\}$?

e) $\{p^2, p^3, p^4, p^5, p^6, q^2, q^3, q^4, q^5, q^6, r^2, r^3, r^4, r^5\}$, where p, q, and r are distinct primes?

20. Write a computer program (or develop an algorithm) to find the prime factorization of an integer $n > 1$.

21. In triangle ABC the length of side BC is 293. If the length of side AB is a perfect square, the length of side AC is a power of 2, and the length of side AC is twice the length of side AB, determine the perimeter of the triangle.

22. Express each of the following in simplest form.

a) $\displaystyle\prod_{i=1}^{10}(-1)^{i}$

b) $\displaystyle\prod_{i=1}^{2n+1}(-1)^{i}$, where $n \in \mathbf{Z}^{+}$

c) $\displaystyle\prod_{i-4}^{8}\frac{(i+1)(i+2)}{(i-1)(i)}$

d) $\displaystyle\prod_{i-n}^{2n}\frac{i}{2n-i+1}$, where $n \in \mathbf{Z}^{+}$

23. a) Let $n = 88{,}200$. In how many ways can one factor n as ab where $1 < a < n$, $1 < b < n$, and $\gcd(a, b) = 1$. (*Note*: Here order is not relevant. So, for example, $a = 8$, $b = 11{,}025$, and $a = 11{,}025$, $b = 8$ result in the same unordered factorization.)

b) Answer part (a) for $n = 970{,}200$.

c) Generalize the results in parts (a) and (b).

24. Use the Pi-notation to write each of the following.

a) $(1^2+1)(2^2+2)(3^2+3)(4^2+4)(5^2+5)$

b) $(1+x)(1+x^2)(1+x^3)(1+x^4)(1+x^5)$

c) $(1+x)(1+x^3)(1+x^5)(1+x^7)(1+x^9)(1+x^{11})$

25. Prove that if $n \in \mathbf{Z}^{+}$ and $n \ge 2$, then

$$\prod_{i-2}^{n}\left(1-\frac{1}{i^2}\right)=\frac{n+1}{2n}.$$

26. When does a positive integer n have exactly

a) two positive divisors? **b)** three positive divisors?

c) four positive divisors? **d)** five positive divisors?

27. Let $n \in \mathbf{Z}^{+}$. We say that n is a *perfect* integer if $2n$ equals the sum of all the positive divisors of n. For example, since $2(6) = 12 = 1 + 2 + 3 + 6$, it follows that 6 is a perfect integer.

a) Verify that 28 and 496 are perfect integers.

b) If $m \in \mathbf{Z}^{+}$ and $2^m - 1$ is prime, prove that $2^{m-1}(2^m - 1)$ is a perfect integer. [You may find the result from part (a) of Exercise 2 for Section 4.1 useful here.]

4.6 Summary and Historical Review

According to the Prussian mathematician Leopold Kronecker (1823–1891), "God made the integers, all the rest is the work of man . . . . All results of the profoundest mathematical investigation must ultimately be expressible in the simple form of properties of the integers." In the spirit of this quotation, we find in this chapter how the handiwork of the Almighty has been further developed by men and women over the last 24 centuries.

Starting in the fourth century B.C. we find in Euclid's *Elements* not only the geometry of our high school experience but also the fundamental ideas of number theory. Propositions 1 and 2 of Euclid's Book VII include an example of an algorithm to determine the greatest common divisor of two positive integers by using an efficient technique to solve, in a *finite* number of steps, a specific type of problem.

The term *algorithm*, like its predecessor *algorism*, was unknown to Euclid. In fact, this term did not enter the vocabulary of most people until the late 1950s when the computer revolution began to make its impact on society. The word comes from the name of the famous Islamic mathematician, astronomer, and textbook writer Abu Ja'far Mohammed ibn Mûsâ al-Khowârizmî (c. 780–850). The last part of his name, al-Khowârizmî, which is translated as "a man from the town of Khowârizm," gave rise to the term *algorism*. The word *algebra* comes from al-jabr, which is contained in the title of al-Khowârizmî's textbook *Kitab al-jabr w'al muquabala*. Translated into Latin during the thirteenth century, this book had a profound impact on the mathematics developed during the European Renaissance.

Euclid (c. 400 B.C.)

Al-Khowârizmî (c. 780–850)

As mentioned in Section 4.4, our use of the word *algorithm* connotes a precise step-by-step method for solving a problem in a finite number of steps. The first person credited with developing the concept of a computer algorithm was Augusta Ada Byron (1815–1852), the Countess of Lovelace. The only child of the famous poet Lord Byron and Annabella Millbanke, Augusta Ada was raised by a mother who encouraged her intellectual talents. Trained in mathematics by the likes of Augustus DeMorgan (1806–1871), she continued her studies by assisting the gifted English mathematician Charles Babbage (1792–1871) in the development of his design for an early computing machine — the "Analytical Engine."

The most complete accounts of this machine are found in her writings, wherein one finds a great deal of literary talent along with the essence of the modern computer algorithm. Further details on the work of Charles Babbage and Augusta Ada Byron Lovelace can be found in Chapter 2 of the work by S. Augarten [1].

Augusta Ada Byron, Countess of Lovelace (1815–1852)

In the century following Euclid, we find some number theory in the work of Eratosthenes. However, it was not until five centuries later that the first major new accomplishments in the field were made by Diophantus of Alexandria. In his work *Arithmetica*, his integer solutions of linear (and higher-order) equations stood as a mathematical beacon in number theory until the French mathematician Pierre de Fermat (1601–1665) came on the scene.

The problem we stated in Theorem 4.8 was investigated by Diophantus and further analyzed during the seventh century by Hindu mathematicians, but it was not actually solved completely until the 1860s, by Henry John Stephen Smith (1826–1883).

For more on some of these mathematicians and others who have worked in the theory of numbers, consult L. Dickson [4]. Chapter 5 in I. Niven, H. S. Zuckerman, and H. L. Montgomery [10] deals with the solutions of Diophantine equations and their applications.

In the work *Formulario Matematico*, published in 1889, Giuseppe Peano (1858–1932) formulated the set of nonnegative integers on the basis of three undefined terms: zero, number, and successor. His formulation is as follows:

a) Zero is a number.

b) For each number n, its successor is a number.

c) No number has zero as its successor.

d) If two numbers m, n have the same successor, then $m = n$.

e) If T is a set of numbers where $0 \in T$, and where the successor of n is in T whenever n is in T, then T is the set of all numbers.

In these postulates the notion of order (successor) and the technique called mathematical induction are seen to be intimately related to the idea of number (that is, nonnegative integer). Peano attributed the formulation to Richard Dedekind (1831–1916), who was the first to develop these ideas; nonetheless, these postulates are generally known as "Peano's postulates."

The first European to apply the Principle of Mathematical Induction in proofs was the Venetian scientist Francisco Maurocylus (1491–1575). His book, *Arithmeticorum Libri Duo* (published in 1575), contains a proof, by mathematical induction, that the sum of the first n positive odd integers is n^2. In the next century, Pierre de Fermat made further improvements on the technique in his work involving "the method of infinite descent." Blaise Pascal (c. 1653), in proving such combinatorial results as $C(n, k)/C(n, k+1) = (k+1)/(n-k)$, $0 \leq k \leq n-1$, used induction and referred to the technique as the work of Maurocylus. The actual term *mathematical induction* was not used, however, until the nineteenth century when it appeared in the work of Augustus DeMorgan (1806–1871). In 1838 he described the process with great care and gave it the name *mathematical induction*. (An interesting survey on this topic is found in the article by W. H. Bussey [2].)

The text by B. K. Youse [13] illustrates many varied applications of the Principle of Mathematical Induction in algebra, geometry, and trigonometry. For more on the relevance of this method of proof to the problems of programming and the development of algorithms, the text by M. Wand [12] (especially Chapter 2) provides ample background and examples.

More on the theory of numbers can be found in the texts by G. H. Hardy and E. M. Wright [5], W. J. LeVeque [7, 8], and I. Niven, H. S. Zuckerman, and H. L. Montgomery [10]. At a level comparable to that of this chapter, Chapter 3 of V. H. Larney [6] provides an enjoyable introduction to this material. The text by K. H. Rosen [11] integrates applications in cryptography and computer science in its development of the subject. The journal article by M. J. Collison [3] examines the history of the Fundamental Theorem of Arithmetic. The articles in [9] recount some interesting developments in number theory.

REFERENCES

1. Augarten, Stan. *BIT by BIT, An Illustrated History of Computers*. New York: Ticknor & Fields, 1984.
2. Bussey, W. H. "Origins of Mathematical Induction." *American Mathematical Monthly* 24 (1917): pp. 199–207.
3. Collison, Mary Joan. "The Unique Factorization Theorem: From Euclid to Gauss." *Mathematics Magazine* 53 (1980): pp. 96–100.
4. Dickson, L. *History of the Theory of Numbers*. Washington, D.C.: Carnegie Institution of Washington, 1919. Reprinted by Chelsea, in New York, in 1950.
5. Hardy, Godfrey Harold, and Wright, Edward Maitland. *An Introduction to the Theory of Numbers*, 5th ed. Oxford: Oxford University Press, 1979.
6. Larney, Violet Hachmeister. *Abstract Algebra: A First Course*. Boston: Prindle, Weber & Schmidt, 1975.
7. LeVeque, William J. *Elementary Theory of Numbers*. Reading, Mass.: Addison-Wesley, 1962.
8. LeVeque, William J. *Topics in Number Theory*, Vols. I and II. Reading, Mass.: Addison-Wesley, 1956.
9. LeVeque, William J., ed. *Studies in Number Theory*. MAA Studies in Mathematics, Vol. 6. Englewood Cliffs, N.J.: Prentice-Hall, 1969. Published by the Mathematical Association of America.
10. Niven, Ivan, Zuckerman, Herbert S., and Montgomery, Hugh L. *An Introduction to the Theory of Numbers*, 5th ed. New York: Wiley, 1991.
11. Rosen, Kenneth H. *Elementary Number Theory*, 4th ed. Reading, Mass.: Addison-Wesley, 2000.
12. Wand, Mitchell. *Induction, Recursion, and Programming*. New York: Elsevier North Holland, 1980.
13. Youse, Bevan K. *Mathematical Induction*. Englewood Cliffs, N.J.: Prentice-Hall, 1964.

SUPPLEMENTARY EXERCISES

1. Let a, d be fixed integers. Determine a summation formula for $a + (a + d) + (a + 2d) + \cdots + (a + (n - 1)d)$, for $n \in \mathbf{Z}^+$. Verify your result by mathematical induction.

2. In the following pseudocode program segment the variables n and *sum* are integer variables. Following the execution of this program segment, which value of n is printed?

```
n := 3
sum := 0
while sum < 10,000 do
  begin
    n := n + 7
    sum := sum + n
  end
print n
```

3. Consider the following five equations.

1) $1 = 1$

2) $1 - 4 = -(1 + 2)$

3) $1 - 4 + 9 = 1 + 2 + 3$

4) $1 - 4 + 9 - 16 = -(1 + 2 + 3 + 4)$

5) $1 - 4 + 9 - 16 + 25 = 1 + 2 + 3 + 4 + 5$

Conjecture the general formula suggested by these five equations, and prove your conjecture.

4. For $n \in \mathbf{Z}^+$, prove each of the following by mathematical induction:

a) $5|(n^5 - n)$ **b)** $6|(n^3 + 5n)$

5. For all $n \in \mathbf{Z}^+$, let $S(n)$ be the open statement: $n^2 + n + 41$ is prime.

a) Verify that $S(n)$ is true for all $1 \leq n \leq 9$.

b) Does the truth of $S(k)$ imply that of $S(k + 1)$ for all $k \in \mathbf{Z}^+$?

6. For $n \in \mathbf{Z}^+$ define the sum s_n by the formula

$$s_n = \frac{1}{2!} + \frac{2}{3!} + \frac{3}{4!} + \cdots + \frac{(n-1)}{n!} + \frac{n}{(n+1)!}.$$

a) Verify that $s_1 = \frac{1}{2}$, $s_2 = \frac{5}{6}$, and $s_3 = \frac{23}{24}$.

b) Compute s_4, s_5, and s_6.

c) On the basis of your results in parts (a) and (b), conjecture a formula for the sum of the terms in s_n.

d) Verify your conjecture in part (c) for all $n \in \mathbf{Z}^+$ by the Principle of Mathematical Induction.

7. For all $n \in \mathbf{Z}$, $n \geq 0$, prove that

a) $2^{2n+1} + 1$ is divisible by 3.

b) $n^3 + (n + 1)^3 + (n + 2)^3$ is divisible by 9.

8. Let $n \in \mathbf{Z}^+$ where n is odd and n is not divisible by 5. Prove that there is a power of n whose units digit is 1.

9. Find the digits x, y, z where $(xyz)_9 = (zyx)_6$.

10. If $n \in \mathbf{Z}^+$, how many possible values are there for $\gcd(n, n + 3000)$?

11. If $n \in \mathbf{Z}^+$ and $n \geq 2$, prove that $2^n < \binom{2n}{n} < 4^n$.

12. If $n \in \mathbf{Z}^+$, prove that 57 divides $7^{n+2} + 8^{2n+1}$.

13. For all $n \in \mathbf{Z}^+$, show that if $n \geq 64$, then n can be written as a sum of 5's and/or 17's.

14. Determine all $a, b \in \mathbf{Z}$ such that $\frac{a}{7} + \frac{b}{12} = \frac{1}{84}$.

15. Given $r \in \mathbf{Z}^+$, write $r = r_0 + r_1 \cdot 10 + r_2 \cdot 10^2 + \cdots + r_n \cdot 10^n$, where $0 \leq r_i \leq 9$ for $0 \leq i \leq n - 1$, and $0 < r_n \leq 9$.

a) Prove that $9|r$ if and only if $9|(r_n + r_{n-1} + \cdots + r_2 + r_1 + r_0)$.

b) Prove that $3|r$ if and only if $3|(r_n + r_{n-1} + \cdots + r_2 + r_1 + r_0)$.

c) If $t = 137486\underline{x}225$, where x is a single digit, determine the value(s) of x such that $3|t$. Which values of x make t divisible by 9?

16. Frances spends \$6.20 on candy for prizes in a contest. If a 10-ounce box of this candy costs \$.50 and a 3-ounce box costs \$.20, how many boxes of each size did she purchase?

17. a) How many positive integers can we express as a product of nine primes (repetitions allowed and order not relevant) where the primes may be chosen from $\{2, 3, 5, 7, 11\}$?

b) How many of the positive integers in part (a) have at least one occurrence of each of the five primes?

18. Find the product of all (positive) divisors of (a) 1000; (b) 5000; (c) 7000; (d) 9000; (e) $p^m q^n$, where p, q are distinct primes and $m, n \in \mathbf{Z}^+$; and (f) $p^m q^n r^k$, where p, q, r are distinct primes and $m, n, k \in \mathbf{Z}^+$.

19. a) Ten students enter a locker room that contains 10 lockers. The first student opens all the lockers. The second student changes the status (from closed to open, or vice versa) of every other locker, starting with the second locker. The third student then changes the status of every third locker, starting at the third locker. In general, for $1 < k \leq 10$, the kth student changes the status of every kth locker, starting with the kth locker. After the tenth student has gone through the lockers, which lockers are left open?

b) Answer part (a) if 10 is replaced by $n \in \mathbf{Z}^+$, $n \geq 2$.

20. Let $A = \{a_1, a_2, a_3, a_4, a_5\} \subseteq \mathbf{Z}^+$. Prove that A contains a nonempty subset S where the sum of the elements in S is a multiple of 5. (Here it is possible to have a sum consisting of only one summand.)

21. Consider the set $\{1, 2, 3\}$. Here we may write $\{1, 2, 3\} = \{1, 2\} \cup \{3\}$, where $1 + 2 = 3$. For the set $\{1, 2, 3, 4\}$ we find that $\{1, 2, 3, 4\} = \{1, 4\} \cup \{2, 3\}$, where $1 + 4 = 2 + 3$.

However, things change when we examine the set $\{1, 2, 3, 4, 5\}$. In this case, if $C \subseteq \{1, 2, 3, 4, 5\}$ and we let s_C denote the sum of the elements in C, then we find that there is no way to write $\{1, 2, 3, 4, 5\} = A \cup B$, with $A \cap B = \emptyset$ and $s_A = s_B$.

a) For which $n \in \mathbf{Z}^+$, $n \geq 3$, can we write $\{1, 2, 3, \ldots, n\} = A \cup B$, with $A \cap B = \emptyset$ and $s_A = s_B$? (As above, s_A and s_B denote the sums of the elements in A and B, respectively.)

b) Let $n \in \mathbf{Z}^+$ with $n \geq 3$. If we can write $\{1, 2, 3, \ldots, n\} = A \cup B$ with $A \cap B = \emptyset$ and $s_A = s_B$, describe how such sets A and B can be determined.

22. Determine those integers n for which $\frac{5n-4}{6}$ and $\frac{7n+1}{4}$ are also integers.

23. Let $a, b \in \mathbf{Z}^+$.

a) Prove that if $a^2 | b^2$ then $a | b$.

b) Is it true that if $a^2 | b^3$ then $a | b$?

24. Let n be a fixed positive integer that satisfies the property: For all $a, b \in \mathbf{Z}^+$, if $n | ab$ then $n | a$ or $n | b$. Prove that $n = 1$ or n is prime.

25. Suppose that $a, b, k \in \mathbf{Z}^+$ and that k is not a power of 2.

a) Prove that if $a^k + b^k \neq 2$, then $a^k + b^k$ is composite.

b) If $n \in \mathbf{Z}^+$ and n is not a power of 2, prove that if $2^n + 1$ is prime, then n is prime.

For the next three exercises, recall that H_n, F_n, and L_n denote the nth harmonic, Fibonacci, and Lucas numbers, respectively.

26. Prove that for all $n \in \mathbf{N}$, $H_{2^n} \leq 1 + n$.

27. Prove that $F_n \leq (5/3)^n$ for all $n \in \mathbf{N}$.

28. For $n \in \mathbf{N}$, prove that

$$L_0 + L_1 + L_2 + \cdots + L_n = \sum_{i=0}^{n} L_i = L_{n+2} - 1.$$

29. a) For the five-digit integers (from 10000 to 99999) how many are palindromes and what is their sum?

b) Write a computer program to check the answer for the sum in part (a).

30. Let a, b be odd with $a > b$. Prove that $\gcd(a, b) = \gcd\left(\frac{a-b}{2}, b\right)$.

31. Let $n \in \mathbf{Z}^+$ with u the units digit of n. Prove that $7 | n$ if and only if $7 | (\frac{n-u}{10} - 2u)$.

32. Let $m, n \in \mathbf{Z}^+$ with $19m + 90 + 8n = 1998$. Determine m, n so that (a) n is minimal; (b) m is minimal.

33. Catrina selects three integers from $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ and then forms the six possible three-digit integers (leading zero allowed) they determine. For instance, for the selection 1, 3, and 7, she would form the integers 137, 173, 317, 371, 713, and 731. Prove that no matter which three integers she initially selects, it is not possible for all six of the resulting three-digit integers to be prime.

34. Consider the three-row and four-column table shown in Fig. 4.12. Show that it is possible to place eight of the nine integers 2, 3, 4, 7, 10, 11, 12, 13, 15 in the remaining eight cells of the table so that the average of the integers in each row is the same integer and the average of the integers in each column is the same integer. Specify which of the nine integers given cannot be used and show how the other eight integers are placed in the table.

		14	
	5		9
1			

Figure 4.12

35. Allen writes the consecutive integers $1, 2, 3, \ldots, n$ on a blackboard. Then Barbara erases one of these integers. If the average of the remaining integers is $35\frac{7}{17}$, what is n and what integer was erased?

36. Leslie selects a random integer between 1 and 100 (inclusive). Find the probability her selection is divisible by (a) 2 or 3; (b) 2, 3, or 5.

37. Let $m = p_1^{e_1} p_2^{e_2} p_3^{e_3} p_4^{e_4}$ and $n = p_1^{f_1} p_2^{f_2} p_3^{f_3} p_5^{f_5}$, where p_1, p_2, p_3, p_4, p_5 are distinct primes, and e_1, e_2, e_3, e_4, f_1, f_2, f_3, $f_5 \in \mathbf{Z}^+$. How many common divisors are there for m, n?